PRIVACY ASSOCIATES INTERNATIONAL LLC

Privacy Update

13th Annual Information Technology Law Seminar
September 10, 2020

Keith A. Cheresko & Robert L. Rothman, Principals,
Privacy Associates International LLC

Purpose of Presentation

- Quickly comment on a couple important international developments
- Discuss in some depth two very significant privacy developments: one at a US state level and one at an international level.
  - The state development relates to California because its jurisdictional provisions affect many, many Michigan businesses
  - The international development relates to the export of European personal information from the EU to the US. The fall-out has extremely significant consequences for Michigan companies doing business in Europe.
- Discuss at a very high level some specific Michigan privacy laws of which you may or may not be aware
- As time permits mention new privacy “frameworks” efforts

PAI

Quick Comment - International

International- Brazil

Brazil General Data Protection Law (Lei Geral de Proteção de Dados Pessoais - Law No. 13,709/2018, as amended) (LGPD)

- Law gives numerous rights to data subjects, imposes numerous burdens on entities dealing with Brazilian personal information and addresses cross border transfers: largely modeled after the European GDPR
- Brazilian President issued a Provisional Measure temporarily delaying the applicability of the LGPD to May 3, 2021
- Provisional Measure required approval by both houses to become permanent - failed in Senate
- No time for further modification, the LGPD will become valid once the President signs the bill, with retroactive applicability date of August 14, 2020
- The LGPD's sanctions provisions, however, will continue to apply from August 1, 2021. The President also has issued a decree creating the new Brazilian National Data Protection Authority that will be responsible for regulating, supervising and applying sanction for violations of data protection

PAI

International- India

India's Personal Data Protection Bill

- Indian government introduced its Personal Data Protection Bill in Parliament on Dec. 11, 2019, after more than two years of fierce debate. With the composition of Parliament it is anticipated the Bill will pass
- Many ways similar to GDPR
- Provides rights to "data principals"
- Government can force firms to share non-personal with it
- Data localization of sensitive personal data
- Creates a new Data Protection Authority
- Provides for penalties and has extraterritorial application

PAI

International- EU

UK

- Brexit means the EU must find the UK to have adequate privacy laws or data transfers to the Continent will be subject to the same onerous rules in effect for the US
- At present UK still following GDPR, which should mean the EU should find the UK to have adequate privacy laws
- However, questions exist about adequacy due to UK national security program and cooperation with US intelligence agencies
- More about this issue later when we discuss *Schrems II*

Switzerland

- As of September 8 the Swiss Federal Data Protection and Information Commissioner (FDPIC) issued a policy statement that it no longer considers the Swiss-US Privacy Shield adequate for transfers of personal data from Switzerland to the US, similar to the EU position.
- The FDPIC does not have authority to invalidate the Shield Framework…….in practice companies may no longer rely on the Shield as a valid transfer mechanism

More about data movement between EU and US to come – but first

PAI

Domestic

California

Why Start with California?

- California has traditionally served as the model for privacy legislation in other states and even at the federal level
- Since there are many businesses in Michigan that operate nationally some will certainly fall within California's privacy law
- When the California law *does* apply, there are numerous and sometime onerous obligations that must be complied with

California

California Consumer Privacy Protection Act (CCPA)

- Enacted in 2018
- Effective January 1, 2020
- California Attorney General's Regulations effective August 14, 2020
- As we are going through this delightful law and accompanying Attorney General Regulations note that the words in the CCPA may not mean what you would expect them to mean

CCPA

- You would think the California Consumer Privacy Protection Act would apply to California entities and California Consumers
- At first glance, the main provision of the law is to simply give consumers control over whether their personal information can be sold to third parties
- However, because of definitions and other details the law is far broader and more significant

California *Consumer* Privacy Protection Act

- A “consumer” is *any* natural person who is a California *resident* – however identified, including by any unique identifier
- A “resident” is an individual who is in California for other than a temporary or transitory purpose, and every individual who is domiciled in California who is outside California for a temporary or transitory purpose.
- Includes employees, applicants, business contacts, etc.

PAI

Are Just Customers California "Consumers"?

- Some limited exceptions set to expire January 2021: applicants, employees, customers, vendors, and individuals associated with commercial customers who are residents of California are not consumers for all the requirements of the CCPA
- Legislation with Governor to extend exemption until 2022 will go into effect *only if* new privacy initiative fails

The Act relates in part to "*sale*" of Consumer Personal Information - don't let that fool you either!

I was taught that a "sale" is the transfer of something from one party to another in exchange for consideration – RIGHT?

UCC meet California's definition of sale for CCPA purposes

What is a “Sale” for CCPA?

- “Sell, “selling” “sale” or “sold” means “selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means” for “monetary or other valuable consideration.”
- A very limited number of “business purpose” transfers we will discuss later are not subject to the same restrictions as other sales

What Information is Covered by CCPA?

Covered information is “Personal Information” defined as anything that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular *consumer or household*

There is a whole litany of information considered PI

Can you be more specific?

Real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

Also included:

- Characteristics of protected classifications under California or federal law
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies
- Biometric information
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Etc., etc., etc. . . .

PAI

Is Your Client a "Business"?

The law is applicable to "businesses." Your client is considered a *business* if *all* of the following are true. The client:

- Is organized or operated for the profit or *financial benefit of your shareholders or other owners*
- Collects consumers' PI, or someone collects PI it on its behalf
- Alone, or jointly with others, determines the purposes and means of processing consumers' PI
- Is doing business in California . . . And

Is it Doing *Business* in California?

- Entities are doing business in CA unless "every aspect of the commercial conduct takes place wholly outside of California"
- Examples:
  - Non-CA business collected PI while the *consumer* was outside of California,
  - No part of the *sale* of the consumer's PI occurred in California
  - No PI collected while the consumer was in California is sold (e.g. a California resident visits a single-source restaurant located outside of California)
  - If California resident makes a restaurant reservation while still in California, that business is included

Does it Meet a Coverage Threshold?

If your client is a business and doing business in California, it must also meet o*ne* of the following thresholds to fall under the law:

- Annual gross revenues in excess of $25 Million;
- Annually buys, receives for its commercial purposes, sells, or shares for commercial purposes PI relating to 50,000 or more consumers, households, or devices; or
- Derives 50% or more of its annual revenue from selling consumer PI
- If it does, it is likely captured under the law

Congratulations, Your Client is Covered

If your client is a business, doing business in California and meets o*ne* of the specified thresholds it is likely captured under the law.

Now what?

Okay, I get it.

- ✓ A Consumer is a California Resident, and
- ✓ A Resident is someone who lives in California, and
- ✓ Personal Information is nearly everything about the individual, and
- ✓ A Sale is virtually any transfer of PI

What now?

Okay, CCPA Applies What Is Required?

It was mentioned that when the California law *does* apply, there are numerous and sometime onerous obligations that must be complied with by the client.

What Types of Obligations?

- Granting Privacy rights e.g. Access, Deletion, Opt out, and more
- Providing mandated privacy disclosures and content
- Explicit “opt out” button/link on websites for consumers to preclude “sales” of their PI
- Security measures for protection of PI
- Employee CCPA training
- Contracting requirements for service providers and third parties regarding data use
- If you don’t get it right, there will be consequences

Right to Access

Right to receive information about, and Copies of, PI

- If asked by a consumer, a business must disclose the categories of PI that the business, within the year preceding the request, has:
  - collected
  - "sold" to a third party
  - disclosed for a business purpose
  - the categories of third parties to whom the Business sold and/or disclosed PI for a business purpose
- Plus requires that a business also disclose:
  - the business or commercial purpose for which PI was collected and/or sold
  - the categories of sources from which PI was collected and
  - the "specific pieces" of PI a business collected about an individual

Right to Delete PI

- CCPA provides consumers with a right to request a business delete any PI that it has collected about the consumer and the business must direct service providers to delete a consumer's PI in response to a verified "deletion" request
- There are exceptions to the obligation to delete such as:
  - completing a transaction,
  - detecting security incidents,
  - debugging to repair intended functionalities
  - where PI is used "to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business,"
  - where a business "otherwise use[s] the consumer's [PI] internally in a lawful manner that is compatible with the context in which the consumer provided the information."

Right to Opt Out

- The right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information.
- A business that sells consumers' personal information to third parties must provide notice to consumers that they have the right to opt out of the sale of their personal information.
- A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information, has not received consent to sell the minor consumer's personal information is prohibited, from selling the consumer's personal information.

What is Not “Selling” and “Business Purposes”?

- “Selling” excludes PI used for a specifically defined “business purpose”, as long as it is reasonably necessary and proportionate to achieve the operational purpose for which the PI was collected or processed or for another compatible operational purpose
- CCPA lists seven specific “business purposes” :
  - counting ad impressions
  - detecting security incidents
  - debugging and repairing functionality
  - short-term “transient use” that isn’t used for profiling
  - performing services on a business’s behalf, such as fulfilling orders or processing payment (classic “data processor” activities)
  - undertaking internal research for technological development
  - undertaking activities to verify or maintain the quality or safety of the business’s service or device

PAI

Right to Be Free from Discrimination

- Prohibits businesses from charging different prices or rates to consumers, providing different services, or denying goods or services to consumers who exercise their CCPA rights
- Exceptions are permitted for example, where the difference in prices or services is reasonably related to the value to the business provided by the consumer's data
- The Act also allows businesses to offer financial incentives in connection with the collection, sale, or deletion of PI
- Consumers must opt-in to such programs, and a business must include a description of the program on its "Do Not Sell My Personal Information" page

PAI

Is Private Enforcement Available?

- Yes, a natural person with California residency has a right of action if their unencrypted or un-redacted PI has been exposed due to a business's failure to maintain appropriate security safeguards (breach)
- The PI definition for breach is narrower and limited to a person's name (at least first initial and last name) and either their social security number, driver's license or state identification number, bank or credit card information, or medical or health insurance information
- A breach involving data that is encrypted or redacted is not subject to the CCPA's private right of action

What if there are no actual damages?

- Pecuniary damages not required; statutory damages between $100 and $750, injunctive or declaratory relief, or “any other relief the court deems proper” is available
- Actual damages are only recoverable if they exceed the statutory damages
- Actions can be aggregated into a class action
- Private enforcement subject to a written notice of the intended action and 30 days cure period. May only proceed if the company fails to fix the problem within the time allotted.
- California AG may stop or superintend a private action.

PAI

What about the Attorney General?

- A business failing to cure within 30 days after notice may be subject to civil penalties exclusively assessed and recovered in a civil action brought by the Attorney General
- Intentional violators liable for a civil penalty of up to $7,500 for each violation
- Other normal remedies are available to the Attorney General

Had enough? Ballot initiative pending that could add more

If enacted, the California Privacy Rights Act (CPRA) would revise the CCPA (even though the CCPA has been in effect for only nine months and AG enforcement just began in August) Among other things the CPRA:

- Modifies definitions
- Creates a new Privacy Protection Agency
- Adds new data rights for consumers
- Clarifies and adds new obligations for service providers, contractors, and third parties

PAI

Domestic

Nevada

Nevada Security and Privacy of Personal Information Law (Chapter 603A100-NRS et. seq.)

- Applies to online businesses, services, and operators of Internet websites operated for commercial purposes
- Collecting and maintaining covered information from consumers who reside in Nevada and use or visit the internet website or online service; and
- Engage in any activity that satisfies the nexus requirements of the United States Constitution

Nevada

Unlike California, Nevada knows what a dictionary is and apparently used it in defining the terms of its law

- "Sale" is the exchange of covered information for monetary consideration by the operator to a person for the person to license or sell the covered information to additional persons
- "Consumer" is a person who seeks or acquires, by purchase or lease, any good, service, money or credit for personal, family or household purposes from" an operator's Internet website or online service.
- "Covered Information" is first and last name, a home or other physical address, email address, telephone number, SSN, identifier that allows a specific person to be contacted & more

Nevada

Nevada does not:

- Require a “Do Not Sell My Personal Information” button or link on websites
- Require that consumers opt-in to the sale of their personal information
- Include the right of access, portability, deletion, or non-discrimination.
- Establish a private right of action against an operator.

Nevada does require entities to provide consumers with an email address, a toll-free telephone number, or an Internet website to submit verified opt-out requests

Nevada

Enforcement

The Nevada Attorney General may institute a legal proceeding against the operator.

If the court finds a violation, it has the authority to impose a civil penalty of up to $5,000 per violation or issue an injunction.

Now for a change of pace.
What about entities in the US moving PI from EU Data Subjects to the US and Privacy Shield?

Schrems II

- EU persons whose rights and freedoms are violated have the right to an effective remedy before a tribunal (Art 47 of the European Convention on Human Rights)
- Data protection and privacy rights of EU persons are established in the EU Charter, the Council of Europe's Convention on Human Rights, and the Treaty on the Functioning of the EU

Schrems II

- Section 702 of the US Foreign Intelligence Surveillance Act and Executive Order 12,333 allows the US to target any non-U.S. person abroad to collect "foreign intelligence information," defined broadly to encompass information related to the "foreign affairs" of the United States
  - The government's targets need not have any connection to terrorism investigations or criminal activity, and can include academics, journalists and human rights workers
  - No notice required
  - In 2018 the US targeted more than 164,000 individuals and groups , including Europeans, under Section 702, resulting in the mass collection of hundreds of millions of communications

Schrems II

- This basic conflict forms the basis for a recent development that has significance for:
  - The perceived human rights of Europeans
  - The perceived ability of the US to do what it believes is necessary for its national defense
  - The ability of tens of thousands of companies to engage in trade between the US and Europe where the transfer of personal information is required.

A Little More Background

- In the 1990s, the EU and the US reached an agreement known as “Safe Harbor,” which allowed companies doing business in Europe to more easily transfer data to the United States
- U.S. businesses which subscribed to certain privacy principles, could ensure an “adequate” level of protection for Europeans’ data thus complying with EU law allowing transfer of personal information to the US
- In 2013, Edward Snowden’s revelations about the scope of NSA surveillance radically undermined that theory

Background

- in 2015, the European Court of Justice (CJEU) invalidated the Safe Harbor agreement.
  - The court indicated serious concerns about the nature of U.S. government surveillance
  - Pointed out lack of meaningful remedies by EU persons because of American standing requirements
  - After describing the record on NSA surveillance, the court explained that, given EU privacy protections, governments may interfere with personal data "only in so far as is strictly necessary"
  - Finally, the court emphasized that E.U. law requires "effective judicial protection" and access to legal remedies for privacy violations.

PAI

Background

- After the CJEU ruling, the US and the EU quickly negotiated a new data-transfer agreement called “Privacy Shield”
- In the meantime, companies seeking to send EU personal information had to rely on other legal bases to transfer personal information to the US, primarily Standard Contractual Clauses

Court of Justice European Union

- Without getting into procedural aspects, in the context of another case by Max Schrems against Facebook, the CJEU was asked to determine whether the Privacy Shield provided adequate protection for the transfer of EU Data Subject data to the US
- In July, 2020 the CJEU decided the Privacy Shield did not provide an *essentially equivalent* level of data protection to that of the EU, and
- Did not provide equivalent judicial redress for EU Data Subjects to that of the EU in cases of US government surveillance

PAI

Privacy Shield

CJEU specifically determined:

- There was a lack of clear statutory limits on US governmental access to EU data subject information transferred to the US (FISA 702 and EO 12,333)
- EU data subjects lacked an effective means for enforcing their individual rights against the US government
- Ombudsperson provided for in the Privacy Shield was not sufficiently independent and lacked the ability to direct intelligence agencies
- The FISA process lacked judicial review or oversight of individual targets, who generally did not even know they were being surveilled

PAI

SCC

- The CJEU also opined that Standard Contractual Clauses (SCC) *may* provide for essentially equivalent safeguards, rights and remedies depending on the laws of the destination country
- SCCs are agreements between European data exporters and non-European data importers
- Government is not party to the SCC agreements
- There is an obligation to evaluate the legal system of the importer's country with regard to data access by public authorities
- If the SCCs do not provide adequate protection in the importer's country, parties may try to remedy by implementing supplementary measures

SCC Obligations

- Data exporter
  - Evaluate and verify whether destination country laws ensure adequate protection under the law
- Data Importer
  - Certify it can comply with SCC under its country's applicable law
  - Promptly report noncompliance
  - Promptly report law changes that are likely to have a substantial negative effect
- Supervisory Authority (SA)
  - must suspend or prohibit transfers if the SCCs cannot be complied with under importer's country law and cannot be mitigated by supplemental measures

PAI

What Now?

- Not sure how US companies can certify they can comply with SCC's: not much individual US companies can do about US government surveillance of EU persons or standing of EU persons in US courts
- New Standard Contractual Clauses being drafted by EU, may help
- Look to derogations under the GDPR, like consent, to provide the basis for transfers
- Prayer
- Alcohol

At Last – Michigan!

Existing Michigan Privacy/Data Security Measures

Michigan has a number of laws on the books designed to protect the privacy of Michiganders

The laws cover topics ranging from children, medical information, financial information, snail mail, credit protection, computer access, social media, social security number protection, data disposal, video/reading materials and data security breach requirements.

Existing Measures

- The Michigan Consumer Protection Act (MCL 445.901 et seq.)
- Protection of Pupil Privacy (MCL 380.1136 et seq.)
- Fraudulent Access to Computers, Computer Systems, and Computer Networks (MCL 752.791 et seq.)
- Preservation of Personal Privacy (MCL 445.1711 et seq.)
- Facsimile Machines (MCL 445.1771 et seq.)
- Unsolicited Commercial E-Mail Protection Act (MCL 445.2501 et seq.)
- Children's Protection Registry Act (MCL 752.1061 et seq.)

PAI

Existing Measures

Social Security Number Privacy Act (MCL 445.81 et seq.)

Identity Theft Protection Act (MCL 445.61 et seq.)

Medical Records Access Act (MCL 333.26261 et seq.)

Security Freeze Act (MCL 445.2511 et seq.)

Mail and Mail Depository Protection Act (MCL 445.31 et seq.)

Michigan Insurance Code (MCL 500.550* et seq.)
*effective Jan 20,2021

What about Michigan?

- In June the Michigan legislature adopted Enrolled Senate Joint Resolution G to be put to a vote of the people
- The resolution if approved amends Section 11 of Article I of the Michigan Constitution requiring the government to obtain a search warrant in order to access a person's electronic data or electronic communication

What about Michigan?

- It provides:

  The person, houses, papers, possessions, electronic data, and electronic communications of every person shall be secure from unreasonable searches and seizures. No warrant to search any place or to seize any person or things or to access electronic data or electronic communications shall issue without describing them, nor without probable cause, supported by oath or affirmation. The provisions of this section shall not be construed to bar from evidence in any criminal proceeding any narcotic drug, firearm, bomb, explosive or any other dangerous weapon, seized by a peace officer outside the curtilage of any dwelling house in this state.

The Future?

The Michigan House proposed legislation that if adopted, would protect current and prospective employees from being required to inhale, ingest, inject or implant a device as a condition of employment. No, you cannot be required to be microchipped like your pet for your employer. The fate of the bill is uncertain. It does indicate the reach of technology and the need for vigilance in protecting our personal privacy as we go forward. (The Microchip Protection Act)

Contact Information

Keith A. Cheresko

Privacy Associates International LLC

kcheresko@privassoc.com

www.privassoc.com

(248) 535-2819

Robert L. Rothman

Privacy Associates International LLC

rrothman@privassoc.com

www.privassoc.com

(248) 880-3942

Supplemental Information

Brazil
Supplemental Information

Centre for Information Policy Leadership paper: *Effective Implementation and Regulation Under the New Brazilian Data Protection Law*

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-idp_white_paper_on_top_priorities_for_public_and_private_organizations_to_effectively_implement_the_lgpd__1_september_2020_.pdf

CIPL/CEDIS-IDP Joint Project on Effective Implementation & Regulation under New Brazilian Data Protection Law (LGPD)

https://www.informationpolicycentre.com/brazilian-data-protection-implementation-and-effective-regulation.html#:~:text=Project%20Description,P%C3%BAblico%20(CEDIS%2DIDP)

Switzerland
Supplemental Information

FDPIC considers CH-US Privacy Shield does not provide adequate level of data protection

https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-80318.html

Policy paper on the transfer of personal data to the USA and other countries lacking an adequate level of data protection within the meaning of Art. 6 Para. 1 Swiss Federal Act on Data Protection

https://www.newsd.admin.ch/newsd/message/attachments/62791.pdf

California Materials

- California Consumer Privacy Act

  http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

- Attorney General Regulation and supporting materials-

  https://oag.ca.gov/privacy/ccpa/regs