PROGRAM MATERIALS
Program #2989
July 17, 2019

Data Protection Laws: Following GDPR Enactment, U.S. States Take Action

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

Data Protection Laws: Following GDPR Enactment, U.S. States Take Action

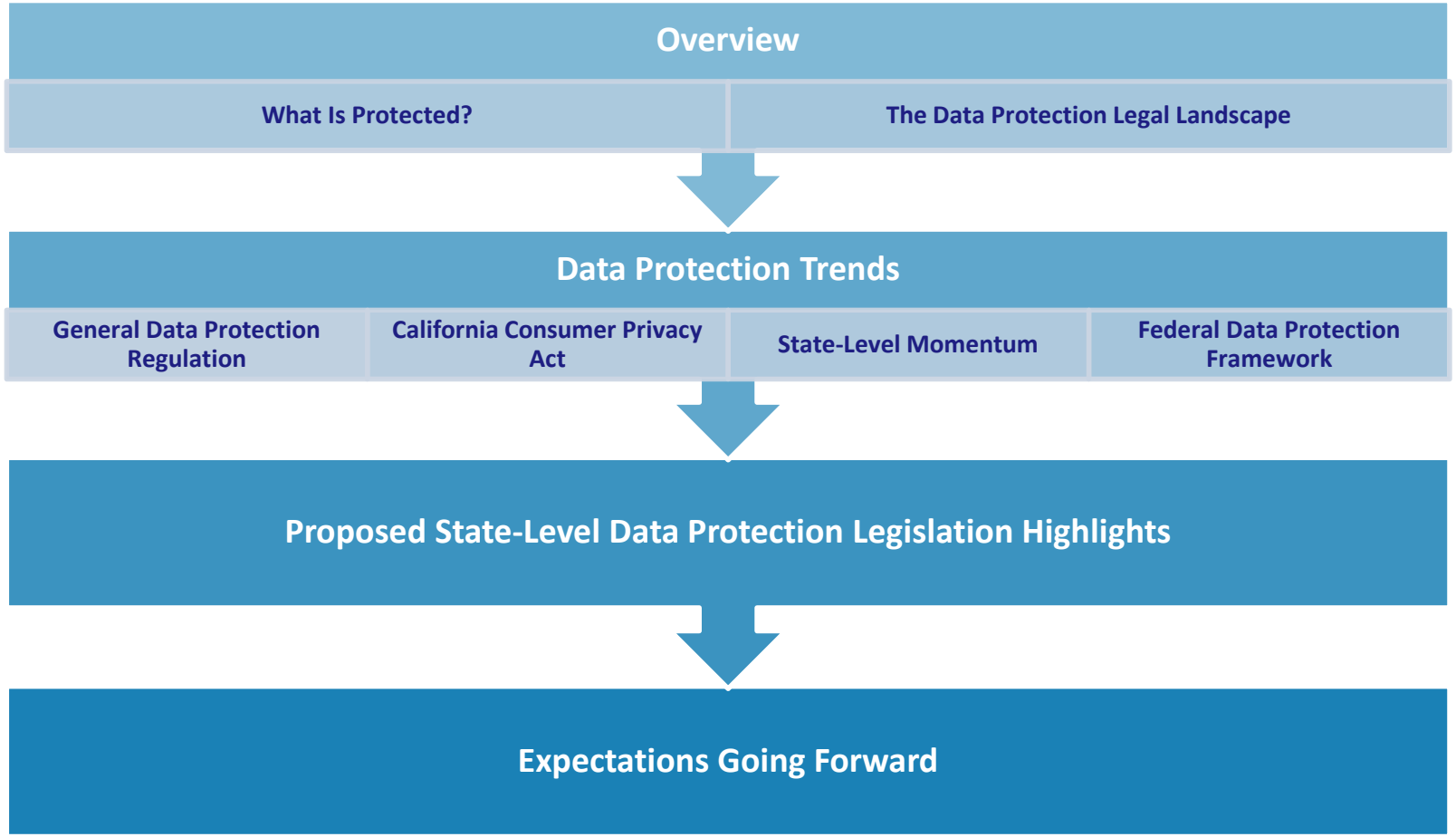
SEDGWICK M. JEANITE, ESQ.
COUNSEL

TANIA S. SORIS, ESQ., CIPP/US
ASSOCIATE

WHITE AND WILLIAMS LLP – NEW YORK
JULY 17, 2019

White and Williams LLP

INTRODUCTION



OVERVIEW

WHAT IS PROTECTED?

PERSONAL DATA (GDPR) – means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. *GDPR, Art. 4(1)* .

SENSITIVE PERSONAL DATA (GDPR) - means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. *GDPR, Art. 9*

CCPA : "Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. *1798.140 (o)*

HIPPA: "Protected health information" means individually identifiable health information that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. *45 CFR § 160.103*

GLBA: "Nonpublic personal information" means personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution.

The Legal Landscape

Cybersecurity Laws

- New York DFS Cybersecurity Requirements for Financial Services
- Massachusetts Data Breach Notification Law
- California Internet of Things Law
- Ohio Data Protection Act
- Nebraska Data Privacy and Security Law

Biometric Laws

- Health Insurance Portability and Accountability Act
- Illinois Biometric Information Privacy Law
- The Texas Capture or Use of Biometric Identifier Act
- Washington Biometric Information Law

Privacy Laws

- Gramm-Leach Bliley Act
- Federal Trade Commission Act
- California Consumer Privacy Act
- Children's Online Privacy Protection Act
- Controlling the Assault of Non-Solicited Pornography and Marketing Act

Enacted Laws

Although the California Consumer Privacy Act (the "CCPA"), discussed later, garners most of the attention at the moment, certain states enacted legislation prior to the CCPA which addressed cybersecurity, biometric and privacy concerns. Such legislations include the following:

- **New York.** Department of Financial Services Regulation 23 NYCRR 500. The regulation outlines the requirements for developing and implementing an effective cybersecurity program. The law is focused primarily on financial institutions like chartered banks, licensed lenders, private bankers, mortgage companies, insurance companies and foreign banks licensed to operate in New York. (Enacted March 1, 2017; Effective February 15, 2018)

- **South Carolina.** Insurance Data Security Act. The Act establishes stringent standards for both data security programs, and an entity's response to a "cybersecurity event" through an organized and methodical investigation and notification to the state's Department of Insurance. The Act requires insurers to submit to the Department of Insurance annual certification of compliance . The Act has a ratcheted implementation of portions of the legislation on insurers and brokers operating or otherwise licensed to do business in the state. It does not create a private cause of action. (Enacted May 3, 2018; Effective January 1, 2019)

- **Illinois.** Biometric Information Privacy Act. This law imposes requirements on companies that collect "biometric information" of Illinois employees including fingerprints, retina or iris scans, voiceprints, scan of hand or face geometry. It includes a private right of action granting Illinois employees the right to sue a private employer who breaches the law. Pursuant to an Illinois Supreme Court's recent holding, individuals can file suit for a mere violation of the law's requirements, even if the individuals do not suffer any actual harm. Local and state governmental employers are specifically exempted from the Act. (Passed in 2008)

DATA PROTECTION TRENDS

GENERAL DATA PROTECTION REGULATION

General Data Protection Regulation

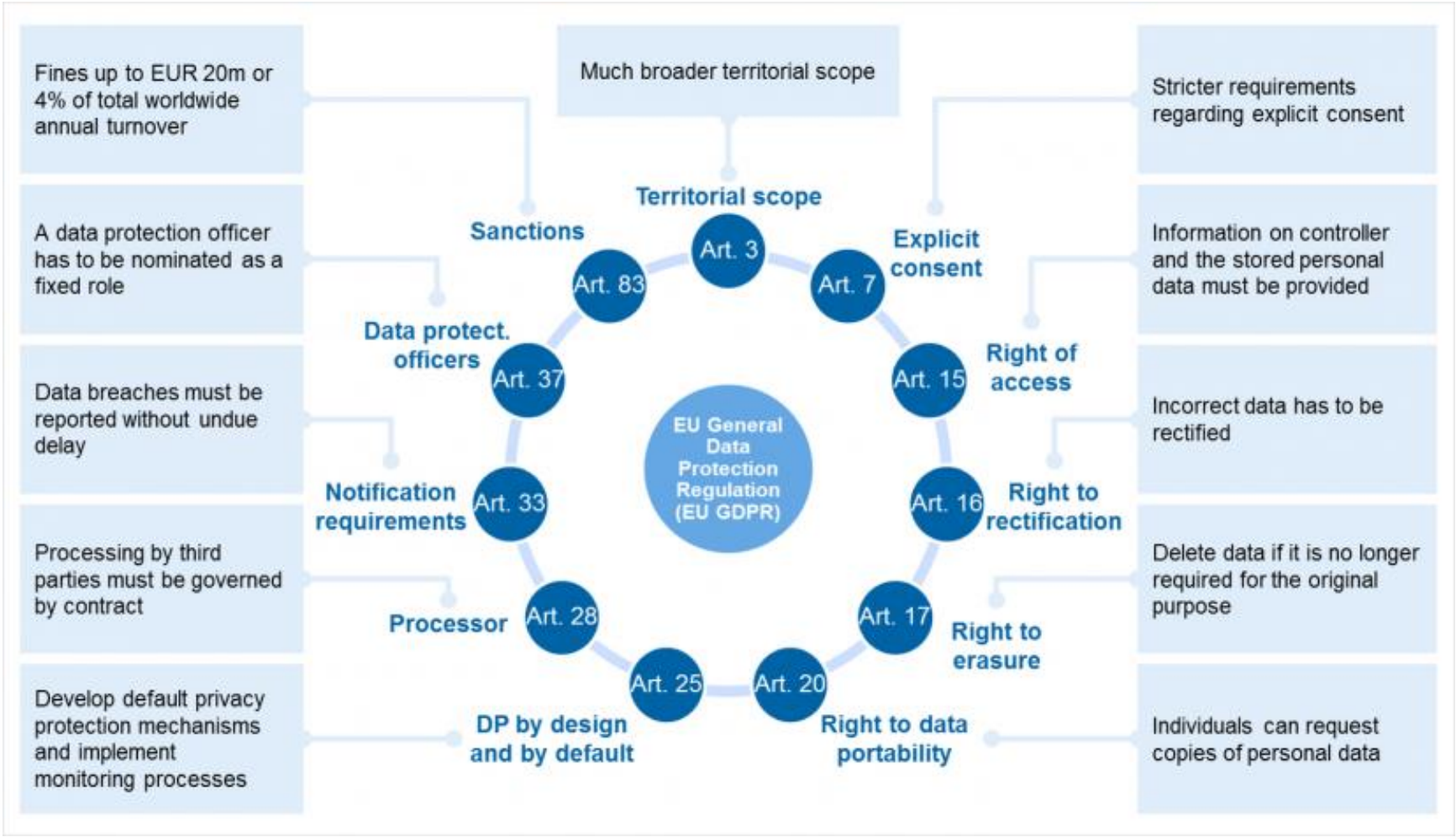
- The General Data Protection Regulation (the "GDPR") was agreed upon by the European Parliament and Council in April 2016, replacing the Data Protection Directive 95/46/EC in the Spring 2018 as the primary law regulating how companies protect EU citizens' "personal data".

- With its extra-jurisdictional reach, it is perhaps the most significant change in the EU's data protection regime in the last 20 years, and its effect has been and will be widespread.

A GDPR PRIMER

GDPR

- Affects companies that process personal data when:
  - **offering goods and services** to data subjects in the EU, regardless of whether payment is a requirement, ***or***
  - **monitoring data subjects'** behavior, such as interacting with websites and other online services, when it takes place in the EU.



Source: Banking Hub, https://www.bankinghub.eu/banking/finance-risk/gdpr-deep-dive-implement-right-forgotten

White and Williams LLP

HOW CAN US COMPANIES COMPLY WITH THE GDPR?

STANDARD CONTRACTUAL CLAUSES

- The European Commission can decide that standard contractual clauses offer sufficient safeguards on data protection for the data to be transferred internationally. It has so far issued two sets of standard contractual clauses for data transfers from data controllers in the EU to data controllers established outside the EU or European Economic Area (EEA). It has also issued one set of contractual clauses for data transfers from controllers in the EU to processors established outside the EU or EEA.

BINDING CORPORATE RULES

- Binding corporate rules (BCR) are data protection policies adhered to by companies established in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises. Such rules must include all general data protection principles and enforceable rights to ensure appropriate safeguards for data transfers. They must be legally binding and enforced by every concerned member of the group.

EU-U.S. PRIVACY SHIELD

- The EU-U.S. Privacy Shield Framework was designed by the U.S. Department of Commerce and the European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce.

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

U.S. States Take Action - California

- Since May 2018, several U.S. States have proposed their own data protection laws, some of which have consumer rights and requirements that mirror the rights and requirements found in the GDPR.

- The most notable legislation is the California Consumer Privacy Act of 2018 (CCPA) signed into law in June 2018. Much has already been written on the California legislation and we will touch on a few of its points.

- The CCPA is broad and applies to businesses that collect, or determine the purposes and means of processing, the personal information of a California consumer.

The CCPA - Who is Covered?

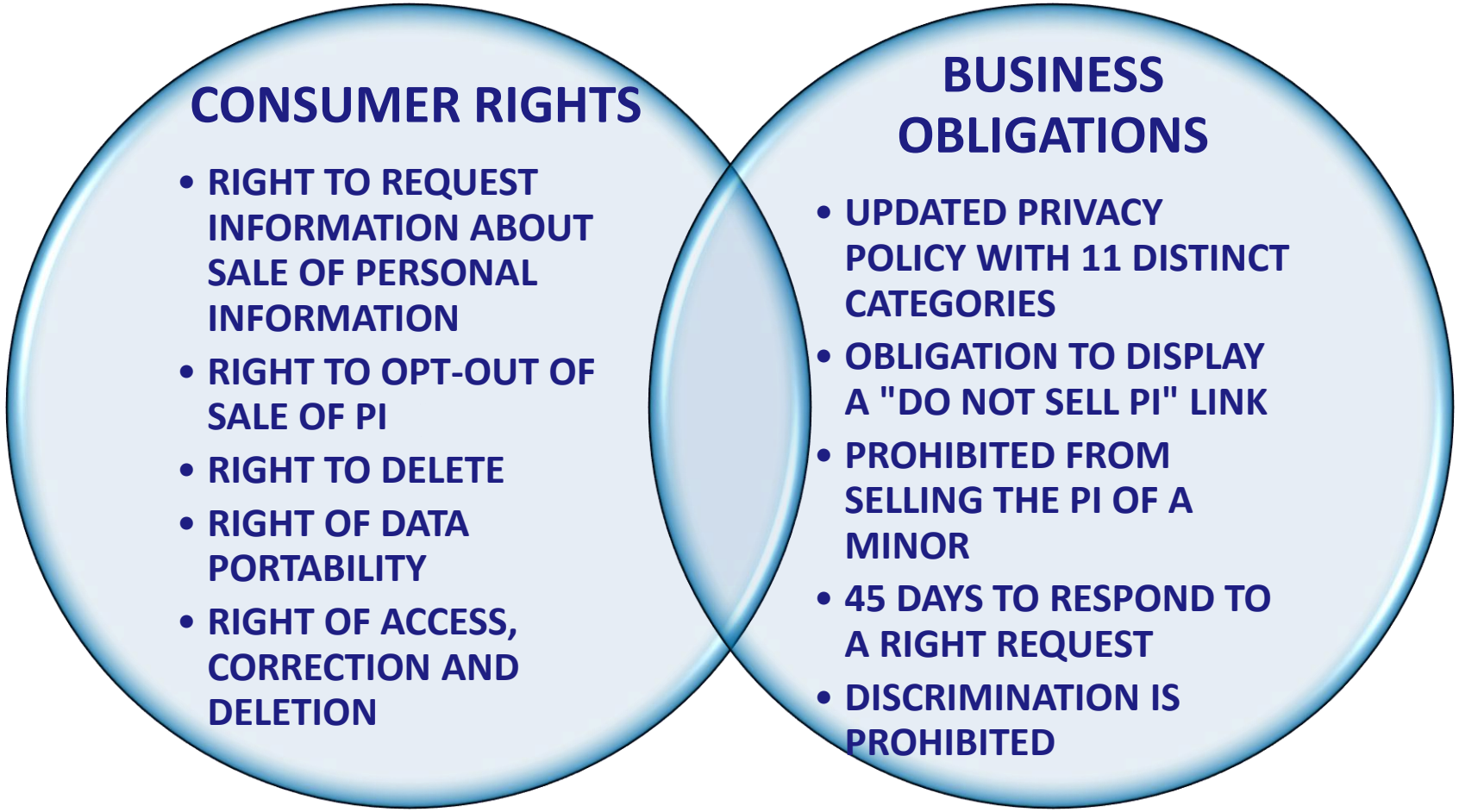
1. A BUSINESS THAT: IS ORGANIZED OR OPERATED FOR THE PROFIT OR FINANCIAL BENEFIT OF ITS SHAREHOLDERS OR OTHER OWNERS;

2. COLLECTS THE PERSONAL INFORMATION OF CALIFORNIA-BASED CONSUMERS; AND

3. SATISFIES ONE OR MORE OF THE FOLLOWING THRESHOLDS:

- ANNUAL GROSS REVENUES IN EXCESS OF $25,000,000; OR
- ANNUALLY BUYS, RECEIVES FOR THE BUSINESS'S COMMERCIAL PURPOSES, SELLS, OR SHARES FOR COMMERCIAL PURPOSES, ALONE OR IN COMBINATION, THE PERSONAL INFORMATION OF 100,000 OR MORE CONSUMERS, HOUSEHOLDS, OR DEVICES; OR
- DERIVES AT LEAST ONE HALF OF ITS ANNUAL REVENUES FROM SELLING CONSUMERS' PERSONAL INFORMATION; OR
- ANY ENTITY THAT: (I) CONTROLS OR IS CONTROLLED BY A BUSINESS UNDER ITEM (1); AND (II) SHARES A NAME, SERVICE MARK, OR TRADEMARK WITH THE BUSINESS.

The CCPA - Main Provisions



Similarities and Differences between the GDPR and CCPA

- **Scope of Covered Entities**
  - GDPR – Entities located within the EU, but also entities outside of the EU if they offer goods/services to, or monitor the behavior of EU subjects
  - CCPA – Only entities doing business in California with annual gross of over $25M in revenue

- **Right to Access**
  - Both the GDPR and the CCPA allow individuals to obtain information regarding whether their personal data is being processed

- **Right to Deletion**
  - GDPR – Grants consumers this right with respect to all data concerning the individual
  - CCPA – Grants consumers this right but only with respect to data collected from the consumer

- **Right to Opt-Out**
  - GDPR – Does not provide consumers with this right
  - CCPA – Provides consumers with such right

STATE-LEVEL MOMENTUM

A PROLIFERATION OF CCPA-LIKE PROPOSED LAWS

White and Williams LLP

NEVADA ACT RELATING TO INTERNET PRIVACY (Effective 10/01/2019)

Applies to businesses that:

(a) Own or operate an Internet website or online service for commercial purposes;

(b) Collect and maintain covered information from consumers who reside in this State and use or visit the Internet website or online service; and

(c) Purposefully direct their activities toward Nevada, consummate some transactions with Nevada or residents there, or purposefully avails itself of the privilege of conducting activities in Nevada, or otherwise engage in any activity that constitutes sufficient nexus with Nevada to satisfy the requirements of the US Constitution.

State Laws Enacted Concurrently with the CCPA

- Although the CCPA is receiving all of the attention at the moment, we note that certain states enacted certain related legislation prior to the CCPA. While those legislations were important, they did not impact the U.S. landscape as the CCPA clearly has to date. Those legislations include the following:
- **Vermont.**
  - Vermont Act 171 of 2018 - Data Broker Regulation. The regulation applies to data brokers, which are businesses that collect personal information about consumers and sell that information to other businesses. The information is generally collected from public and non-public sources such as court records, property records, voter registration information and web browsing activities. The law contains annual disclosure requirements, opt-out options, prohibitions on the acquisition and use of brokered personal information among other requirements. (Enacted May 22, 2018)

State Laws Enacted Concurrently with the CCPA

- **Colorado.**
  - The Colorado Protections for Consumer Data Privacy Act was signed into law on May 29, 2018. The new privacy law provisions are part of the Colorado Consumer Protection Act and involve three major changes:

    - New updates to the law requires entities, both commercial and governmental, that collect personal identifying information to dispose of it when they no longer need it, and to ensure that it is rendered unreadable upon disposal. Businesses and agencies must have a written policy explaining how they will depose of the personal information they collect and must follow through on those procedures.

    - Entities are required to notify consumers when their personal information may have been compromised. The notification must occur within 30 days of the entity determining a breach has occurred that may lead to misuse of your information. In addition, the notice must provide certain information that could help you to protect yourself against identity theft. If more than 500 Coloradans are impacted by a compromise, the entity must notify the Attorney General's Office of Colorado.

    - Entities that collect your personal identifying information must take reasonable steps to protect it from being compromised. The Act does not create a private right of action.

Presenter to read NY Code

This code is required for all attorneys wishing to receive CLE credit in the state of NY

Please notate it carefully

The presenter will only be able to read the code twice and will not be able to repeat it or email it to you.

Thank you!

State Laws Enacted Concurrently with the CCPA

- **Maine.**
  - On June 6, 2019, the Governor of Maine signed into law the Act to Protect the Privacy of Online Consumer Information (LD 946). The Act imposes data privacy requirements on internet service providers and requires ISPs to obtain customer consent before "using, disclosing, selling or permitting access" to their data with a third party. In addition, an ISP is prohibited from refusing to serve a customer based on their refusal to consent to the data usage terms. Finally, ISPs will also be required to take "reasonable measures" to protect customer personal information from "unauthorized use, disclosure, sale or access".
  - The law is applicable to all ISPs that service customers physically based and billed for within the State. The Maine law will take effect July 1, 2020.
  - Based on its text, the Act does not specifically create a private right of action.

PRIVATE RIGHT OF ACTION

ENACTED LEGISLATION

CALIFORNIA CONSUMER PRIVACY ACT
- PRIVATE RIGHT OF ACTION
- ENFORCEMENT BY AG

ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT
- PRIVATE RIGHT OF ACTION

PROPOSED LEGISLATION

MARYLAND PROPOSED ONLINE CONSUMER PROTECTION ACT
- PRIVATE RIGHT OF ACTION
- ENFORCEMENT BY AG

MASSACHUSETTS PROPOSED CONSUMER DATA PRIVACY ACT
- PRIVATE RIGHT OF ACTION

NEW YORK PROPOSED RIGHT TO KNOW ACT & THE NEW YORK PRIVACY ACT
- PRIVATE RIGHT OF ACTION
- ENFORCEMENT BY AG

PENNSYLVANIA PROPOSED PROTECTION OF DIGITAL PRIVACY ACT
- PRIVATE RIGHT OF ACTION

LOUISIANA PROPOSED INTERNET AND SOCIAL MEDIA DATA PRIVACY & PROTECTION ACT
- PRIVATE RIGHT OF ACTION

WASHINGTON PROPOSED CONSUMER DATA TRANSPARENCY ACT
- PRIVATE RIGHT OF ACTION

FEDERAL DATA PROTECTION FRAMEWORK

Federal Privacy Legislation

Over the past 100 years, the U.S. federal government has enacted several laws in an effort to protect consumers and their personal information. For example we have the following laws enacted by the federal government:

- Federal Trade Commission Act of 1914
- Fair Credit Reporting Act of 1970
- Family Educational Rights and Privacy Act of 1974
- Right to Financial Privacy Act of 1978
- Health Insurance Portability and Accountability Act of 1996
- Children's Online Privacy Protection Act of 1998
- Gramm-Leach-Bliley Act of 1999 (Financial Services Modernization Act)
- Fair and Accurate Credit Transactions Act of 2003

Proposed Federal Legislation

- To date, the U.S. has not enacted any legislation that compares to the broad privacy protections afforded in the GDPR. Several members of Congress have recently proposed federal privacy laws for consideration including the following:

  - Information Transparency and Personal Data Control Act (Dem. Rep. DelBene (WA) – 2018). The proposed legislation would give people control over their most sensitive information while ensuring the government can enforce these rules. It would do so by:
    - Ensuring all users are presented with a company's privacy policy in "plain English."
    - Requiring companies to allow users to "opt in" before companies can use a consumers' most sensitive private information in ways the public might not expect.
    - Require companies to declare if and with whom private and behavioral data will be shared, and the purpose of sharing such information.
    - Giving the FTC privacy targeted rule making authority and empower state attorney generals to also pursue violations of this legislation, including granting the FTC the ability to fine bad actors on their first offense.
    - Require companies to obtain privacy audits by a neutral third party and submit the results to the FTC biannually.

Proposed Federal Legislation (cont.)

Consumer Data Protection Act (Dem. Sen. Wyden – Nov. 2018). The proposed legislation would protect Americans' privacy, allow consumers to control the sale and sharing of their data, provide the FTC with the authority to be an effective cop on the beat, and expects to spur a new market for privacy-protecting services.

- The proposed bill would empower the FTC to do the following:

  (1) Establish minimum privacy and cybersecurity standards.

  (2) Issue steep fines (up to 4% of annual revenue), on the first offense for companies and 10-20 year criminal penalties for senior executives.

  (3) Create a national Do Not Track system that lets consumers stop third-party companies from tracking them on the web by sharing data, selling data, or targeting advertisements based on their personal information. It permits companies to charge consumers who want to use their products and services, but don't want their information monetized.

  (4) Give consumers a way to review what personal information a company has about them, learn with whom it has been shared or sold, and to challenge inaccuracies in that information.

  (5) Hire 175 more staff members to police the largely unregulated market for private data.

  (6) Require companies to assess the algorithms that process consumer data to examine their impact on accuracy, fairness, bias, discrimination, privacy, and security.

Proposed Federal Legislation (cont.)

Data Care Act (Dem. Sen. Schatz (Hawaii) – 2018)

- Senator Schatz, the top Democrat on the Senate Communications, Technology, Innovation, and the Internet Subcommittee, led a group of 15 senators in introducing the Data Care Act. The Act would require websites, apps, and other online providers to take responsible steps to safeguard personal information and stop the misuse of users' data.

➢ The Data Care Act establishes reasonable duties that will require providers to protect user data and will prohibit providers from using user data to their detriment. Some of the requirements of the proposed Act include:

- ➢ Duty of Care – Entities must reasonably secure individual identifying data and promptly inform users of data breaches that involve sensitive information;
- ➢ Duty of Loyalty – Entities may not use individual identifying data in ways that harm users;
- ➢ Duty of Confidentiality – Entities must ensure that the duties of care and loyalty extend to third parties when disclosing, selling, or sharing individual identifying data;
- ➢ Federal and State Enforcement – A violation of the duties will be treated as a violation of an FTC rule with fine authority. States may also bring civil enforcement actions, but the FTC can intervene.
- ➢ Rulemaking Authority – FTC is granted rulemaking authority to implement the Act.

Federal Inactivity Leads to State Action

- In light of the current stalemate in Congress, with a divided government, what can U.S. citizens reasonably expect from their Congressional leaders in the area of data privacy. At this time – Nothing.

- Several State Legislatures felt they had no choice but to take matters into their own hands to protect their residents. This enactment of state level privacy laws will lead to a patchwork of state laws which companies and their legal counsel will have to navigate.

PROPOSED STATE-LEVEL LEGISLATION HIGHLIGHTS

Highlights of the Proposed Legislation

- **Maryland.** Senate Bill 613
  - Maryland's proposed law contains similar rights for Maryland consumers as provided by the CCPA. The proposed law would also impose similar, though more limited, disclosure obligations on businesses as those found in the CCPA.
  - However, the ***right to opt out*** may be more expansive under the proposed law because it applies to any disclosure of personal information to third parties, rather than just data sales. In addition, the proposed law contains a ***complete prohibition on the "knowing" disclosure of children's personal information*** (under the age of 18) without exception.
  - Notably, the proposed law ***does not include a private right of action*** for consumers.

Highlights of the Proposed Legislation

- **Hawaii.** Senate Bill 418
  - Hawaii's proposed law would also provide similar rights to Hawaii consumers as the CCPA. The bill imposes limited disclosure obligations on businesses than those found in the CCPA. However, the proposed law could potentially have even broader impact than the CCPA because it likely applies to any business entity, ***regardless of size***, that collects identifying information about an individual who interacts with a business within the state of Hawaii.
  - Notably, the proposed law ***does not include a private right of action*** for consumers and does not identify the penalties that may be imposed by the Hawaii Office of Consumer Protection.

Highlights of the Proposed Legislation

- **Massachusetts.** Bill SD 341
  - Massachusetts's proposed law would provide similar rights to Massachusetts consumers and impose similar, though more limited, disclosure obligations on businesses as those found in the CCPA.
  - The bill would require companies to inform consumers that they have a right to request a copy of their personal information, the deletion of their personal information, and to opt out of third party disclosure. The ***right to opt out may be more expansive*** than the CCPA because it applies to any disclosure of personal information to third parties, rather than just data sales.
  - The proposed law ***provides a private right of action*** for consumers who have suffered any violation of the proposed law. It would allow consumers to recover statutory damages up to $750 per incident or actual damages, whichever is greater.

Highlights of the Proposed Legislation

- **New Jersey.** Senate Bill S2834
  - The New Jersey privacy law includes some of the core features of the CCPA, such as the right to opt out of the sale of personal information. However, it modifies the right to access from the one contained in the CCPA to focus on disclosures of personal identifiable information to third parties.
  - The law requires website owners (called "operators") to disclose the personally identifiable information it collects, all third parties to which it may disclose the personal identifiable information. An email address or toll free telephone number to request information must be provided to consumers.
  - An operator that discloses personal identifiable information to a third party must make available upon request the personal identifiable information disclosed and the contact information for the third parties. The response to a consumer request shall occur within 30 days.
  - It also requires operators to give consumers the ability to opt-out of the sale of personal information. An operator is prohibited from discriminating against or penalizing a customer if the customer chooses to opt out.

Highlights of the Proposed Legislation

- **New York.** Senate Bill No. S00224

➢ New York's proposed law focuses on the transparency of the disclosure of personal information without granting the other significant consumer rights (including the right to deletion) found in the CCPA.

➢ A business is required to make available to the customer the categories of personal information disclosed to third parties and the names and contact information of all the third parties that received the customer's personal information from the business. This proposed law is drafted broader than the CCPA because it ***applies to any person or entity that does business in New York***.

➢ The New York proposed law ***provides a private right of action*** and permits a "customer" of a business, the New York attorney general, a district attorney, a city attorney, or a city prosecutor to bring a civil action to recover "penalties" for violations of the bill.

Highlights of the Proposed Legislation

- **Washington.** Senate Bill 5376
  - Unlike other legislations which have followed the CCPA, Washington's proposed law ***incorporates several concepts from the GDPR*** into the general framework of the CCPA.
  - The proposed law applies to entities that conduct business in Washington or produce products or services that are intentionally targeted to Washington residents and that meet one of two thresholds like those contained in the CCPA. The proposed law requires a business to make available a privacy notice disclosing the categories of personal data collected, the purposes for which personal data are used, and information relating to the sharing and sale of personal data.
  - The rights provided to consumers closely reflect the rights made available under the GDPR: the right to knowledge and access to personal data, the right to the correction of personal data, the right to the deletion of personal data, the right to restrict or object to the processing of personal data and the prohibition against certain decisions based solely on profiling from facial recognition.
  - The law would provide the Washington attorney general the ability to use its enforcement authority under Washington's consumer protection act for violations of the law, as well as to seek injunction or civil penalty.
  - However, ***it would not grant any private right of action*** to consumers.

Highlights of the Proposed Legislation

- **Mississippi.** HB 2153.
  - At the time, the proposed bill appeared to be the closest in structure to the CCPA.
  - The proposed bill so closely mirrored the CCPA that it copied the duplicate statements of access rights and similar sections regarding notice requirements.
  - Certain categories of data that constitute personal information are slightly different (for example, probabilistic identifiers are missing).
  - In addition, the private right of action under the proposed bill was not limited to data covered by the breach notification law, which was a separate category of more sensitive data. It provided that any unauthorized access of any personal information could give rise to a lawsuit.

Highlights of the Proposed Legislation

- **New Mexico.** SB176

  - This legislation was introduced on January 19, 2019 by State Senator Michael Padilla (a Democrat). The law provides for a civil penalty for an intentional violation by a person, business, or service provider for up to $10,000 for each violation.

  - Right of Access and Right to Delete – Businesses must provide the information gathered to consumers in a format of their choosing (mail or electronic) as part of the right of access. Businesses also must delete personal information upon request unless it meets one of the six specified exemptions.

  - Right to Opt Out of the Sale of Personal Information – The proposed law would provide a consumer the right to opt out of the sale of their personal information at any time. A third party that is sold personal information may not resell it without providing the consumer with explicit notice and the opportunity to opt out of the sale.

  - Private Cause of Action – The bill permits victims of data breaches where the business did not implement and maintain reasonable security procedures and practices to bring a civil action seeking statutory damages of up to $750 per incident.

  - The New Mexico privacy bill also specifies various disclosures about privacy practices that businesses must make in order to increase their transparency.

Highlights of the Proposed Legislation

- **Nevada.** SB 220. The proposed law amends the state's existing law by requiring operators to accept and honor consumers' requests to opt-out of having their covered information sold to third parties. Notable differences between the Nevada law and CCPA include:

  - Nevada defines its triggering term ("covered information") more narrowly than the CCPA's triggering term ("personal information").

  - Nevada does not provide consumers with access and deletion rights.

  - Nevada limits its definition of "sale" to exchanges for monetary consideration and expressly excludes several types of sharing, including disclosures that are consistent with the consumer's reasonable expectations.

  - Nevada does not require a "Do Not Sell My Personal Information" link on the homepage of the operator's website.

  - Nevada's exemption for businesses subject to laws such as the Gramm-Leach Bliley Act or HIPAA is broader than similar exemptions found within the CCPA.

Status of the Legislations - Pending

- **New York.** Senate Bill S2224
  - Currently in the Senate

- **New Jersey.** Senate Bill S2834
  - It was introduced last July into the Senate and referred to the Senate Commerce Committee.
  - The House version was introduced in January and just received a favorable recommendation from the Assembly's Science, Innovation and Technology Committee. It has been referred to the Assembly Appropriations Committee.

Status of the Legislations - Defeated

- **Mississippi.** HB 2153
  - The bill was the closest in structure to the CCPA. The Mississippi bill did not succeed in the state legislature.
  - Although unsuccessful, the bill still signifies how state legislators across the U.S. are considering consumer privacy.

- **Washington.** Senate Bill 5376
  - Legislation appeared to be making progress with the Washington State Senate voting 46-1 to approve the Washington Privacy Act on March 6, 2019
  - However, the bill was not successful in the Washington State House by the April 17, 2019 legislative deadline
  - Democratic State Senator Reuven Carlyle and fellow sponsors of the bill remain committed to pushing the bill forward again in the 2020 legislative session.

Status of the Legislations – Remain in Consideration

- **Maryland.** Senate Bill 613
- **Massachusetts.** Bill SD 341
- **New Mexico.** SB176

EXPECTATIONS GOING FORWARD

Expectations Going Forward

- We anticipate several more states will adopt privacy legislations to protect their consumers and residents – Maine's ISP Privacy Law (June 2019)

- Additional states that have indicated their interest in adopting their own privacy laws include:
  - Connecticut – SB 1108
  - Rhode Island – S0234
  - New York. S. 5642 – The New York Privacy Act
  - Texas – Texas Consumer Privacy Act; Texas Privacy Protection Act

- Until Congress adopts a federal privacy law that provides all of its citizens with protection for their personal information, consumers and business will be left with navigating a patchwork of state laws.

QUESTIONS

- Thank you for participating in this program.

- Feel free to e-mail us with questions regarding any topic discussed during this presentation. We can be reached at jeanites@whiteandwilliams.com and sorist@whiteandwilliams.com.