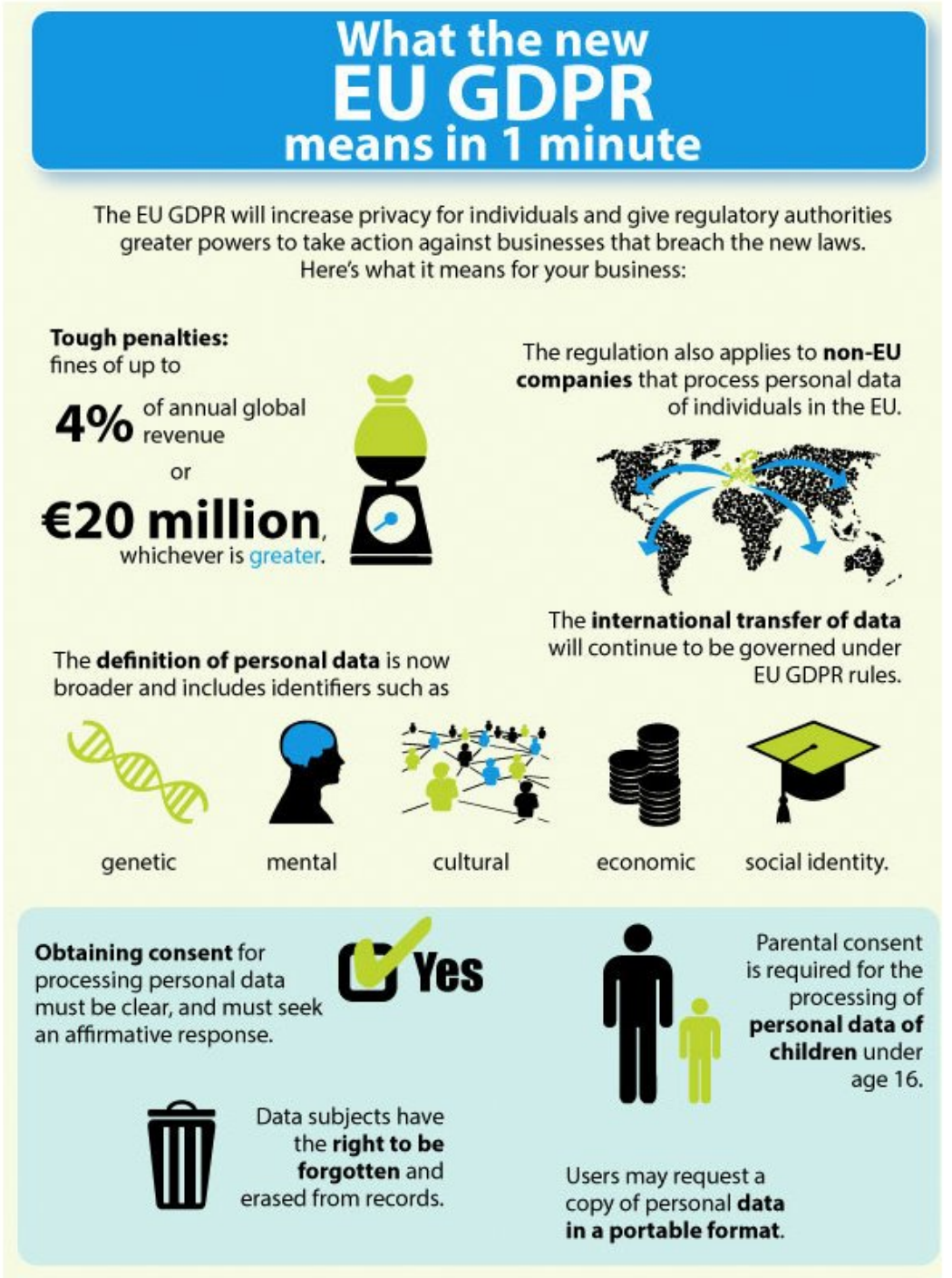
Data Privacy Laws in Europe, Asia and the U.S.: Where Are We and Where Are We Headed?

FDCC

What is GDPR?

- The current benchmark for data protection
- "Protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data"
- One unique body of law for all EU/EEA member states ("federal law")
- Mainly "evolution" from prior EU data protection laws, but a few substantial changes
- Strong emphasis on data protection / privacy management requirements
- Focus on fines and stricter enforcement



Largest Single GDPR Fines

Country Assessing Fine	Amount of Fine	Fine Description
France	€50 million	Google fined for infringements of transparency principle and lack of valid consent
Germany	€35.3 million	H&M fined for comprehensively recording and storing private life circumstances of some employees
Italy	€27.8 million	TIM fined for contacting non-customers without proper consent
Austria	€18 million	Austrian Post fined for selling personal information of 3 million individuals
Sweden	€7 million	Google fined for improper handling of requests to have names removed under “right to be forgotten”

Nations with the Highest Amount of Fines (as of Oct 6, 2020)

Country	Amount of Fines Levied	Number of Fines Levied
France	€51,350,000	6
Italy	€57,371,000	30
Germany	€61,636,633	27
Austria	€18,070,100	8
Sweden	€7,085,430	6
Spain	€3,803,910	134
The Netherlands	€3,490,000	6

Infringements / Fines

- A company may be fined for failing to comply with collection, processing, and storage protocols
  - A company can be fined up to 4% of annual global turnover or €20 million (whichever is greater)
  - Insurance carriers have begun to offer comprehensive insurance coverage packages in response to these hefty fines
  - Packages are tailored to each business as GDPR necessitates coverage for variety of violations
- Claims of individuals for compensation (Art. 82), including joint liability and non-material damages
- Right to file a complaint with authorities
- Lawsuits of consumer protection organizations / competitors
- Investigations by supervisory authorities, i.e. information requests, investigations, prohibitions

Why do Organizations Fail GDPR Compliance?

- Between implementation and January 2020, 160,000 data breach notifications were reported across the European Economic Area
- The most common reasons for compliance breaches and fines are:
  - Insufficient technical and organizational measures to ensure information security
    - Compliance officers are not sure if the regulated date is stored in a secure location
  - Insufficient legal basis for data processing
    - Entities collect more customer data than the law permits
    - Entities do not track how the regulated data is shared
  - Non-compliance with general data processing principles
    - Entities do not categorize the personal data they collect
    - Entities do not have a data retention program in place
  - Insufficient fulfilment of data subjects' rights

Noteworthy Decision – *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*

- While the first two years of GDPR litigation were quiet, courts have begun ramping up decisions and fines on tech companies
  - On July 16 2020, the Court of Justice for the European Union (CJEU), the EU's highest court, issued a decision *in Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* invalidating the Privacy Shield and prohibiting further transfers under the Privacy Shield
    - GDPR prohibits transfers of personal data to the United States unless the company transferring the data has provided legally-appropriate safeguards
      - Prior to the decision, the EU-U.S. Privacy Shield framework (the Privacy Shield) was used by over 5,000 companies as that safeguard
      - The CJEU's decision is based on concerns about the impact of U.S. government surveillance programs on the privacy of EU residents' personal data

Impact of *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*

- Effects of decision
  - Businesses that directly rely on the Privacy Shield need to find an alternative mechanism for personal data transfers from the EU
  - Businesses using third-party vendors to manage data transfers that rely on the Privacy Shield need to understand what alternative mechanism the vendor will put in place to safeguard the transfers
  - Businesses that receive personal data in the U.S. through SCCs can expect increased scrutiny from transferring entities in the EU
  - Swiss-US Privacy Shield has also been ruled no longer adequate
  - EU-US Privacy Shield no longer adequate for Israel-US data transfers

Cross-Border Data Transfers

- Art. 45 Transfers on the basis of an adequacy decision
  - EU-US Privacy Shield was ruled adequate until July 16, 2020
- Art. 46 Transfers subject to appropriate safeguards
  - Binding corporate rules (BCRs) covered by Art. 47
  - Standard contractual clauses (SCCs)/Model clauses
  - Approved code of conduct with binding and enforceable commitments
  - Approved certification mechanism with binding and enforceable commitments
- Art. 49 Derogations for specific situations
  - Explicit consent by data subject
  - Performance of a contract between data subject and controller
  - Performance of a contract in the interest of a data subject
  - Important reasons of public interest
  - Establishment, exercise or defense of legal claims
  - Protection of vital interests of data subject
  - Made from a register which is intended to provide information to the public

European Union and Japan Adequacy Decision

- Japan's data protection legislation and practice constitutes an "adequate framework" based on an analysis of the Japanese Act on the Protection of Personal Information ("APPI") already in place
- Japanese business operators must be mindful of the following requirements when handling EU personal data:
  - Data is only processed for the purpose for which they were legally transferred from the EU, unless EU citizens give their consent for processing for a different purpose.
  - Data is processed to the extent necessary for this purpose.
  - Data is kept no longer than necessary for this purpose.
  - Data is kept accurate and up to date.
  - Data is never further transferred to individuals or entities abroad that do not guarantee an adequate level of protection, unless consent of EU individuals is obtained for such transfer.
  - The processing should be done under appropriate security measures, protected against unauthorized or unlawful processing and against accidental loss, destruction or damage.
  - Additional safeguards apply to sensitive data (data revealing health conditions, sexual orientation, political opinions, etc.).

Information Security (Art. 32)

- Controller and Processor shall implement appropriate technical and organizational security measures
  - Pseudonymization and encryption of personal data
  - Ensure ongoing confidentiality, integrity, availability and resilience
  - Able to restore availability and access to personal data in a timely manner
  - Regular testing, assessing, and evaluating the effectiveness
- Risk taken into consideration when determining appropriate level of security
- To demonstrate compliance: adherence to an approved code of conduct (Art. 40) or approved certification (Art. 42)
  - No approved certification yet
- Processors and sub-processors must process only upon instruction from the controllers or processors, unless required by Union or Member State law

ISO Framework for GDPR Compliance

- The Privacy Information Management System, defined by ISO 27701, provides a framework for integrating privacy into organizational practices
- ISO 27701 uses the lexicon of GDPR
- ISO 27701 broadens the existing ISO 27001:2013 by providing:
  - A top-down management view on information security and privacy
  - Guidance on the implementation of a set of wide-reaching security and privacy controls
  - An integrated management system of both information security and privacy
- ISO 27701 ensures privacy is included within wider organizational risk management practices and counters the notion that it must be treated as a stand-alone exercise

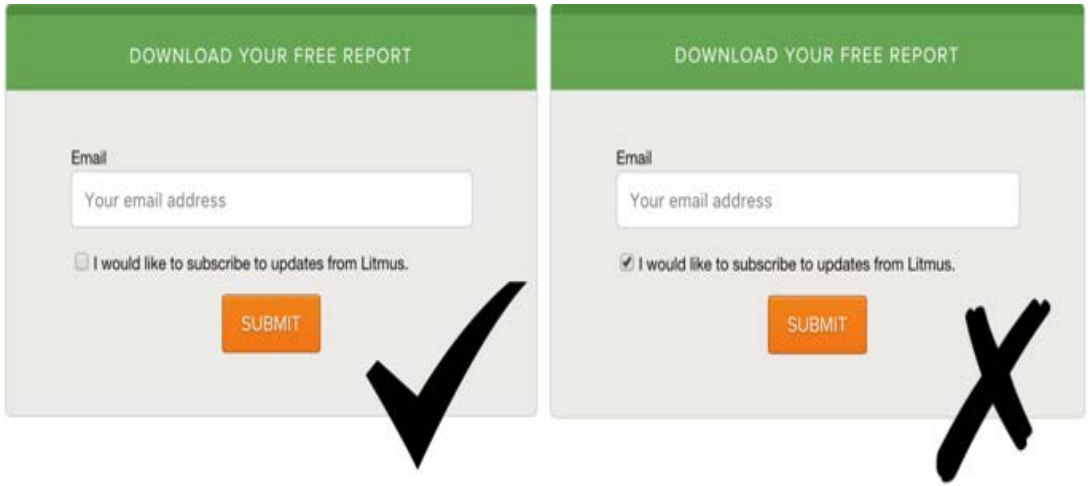
Data Breach (Art. 33, 34)

- In the event of a data breach, a company has 72 hours after becoming aware of breach to notify the supervising authority
- Failure to report a breach within the timeframe will require an explanation to the supervising authority / otherwise may result in a fine
- First of all, an assessment is required if there is any risk (e.g. no encryption)
- Notification of a breach must include the following:
  - A description of the nature of the personal data breach
  - Communication of the name and contact details of the data protection officer where more information can be obtained
  - A description of the consequences of the data breach
  - A description of the measures taken/proposed be the controller to address the breach
- Notification of all affected data subjects in case of “high risk”

Lawfulness requirement / Consent

- For every processing activity where a company processes or uses any personal data of an individual ("data subject") in the EU, the company must ensure it has a lawful reasons, e.g. consent, contract, legitimate interests, etc.
  - Personal data includes any information relating to an identified or identifiable natural person (i.e. name, ID number, location data, etc.)
- "Consent" in practice is a difficult concept
  - Requires an affirmative "opt-in" action; default consent is not sufficient
  - Consent requires extensive information
  - Consent must be voluntary (employees??)
  - Consent may not be "bundled" (marketing)
  - Consent is revocable

"Cookie consent" requirements currently under review



Accountability Principle, Art. 5, 24

GDPR requires a controller / processor to have privacy management scheme:

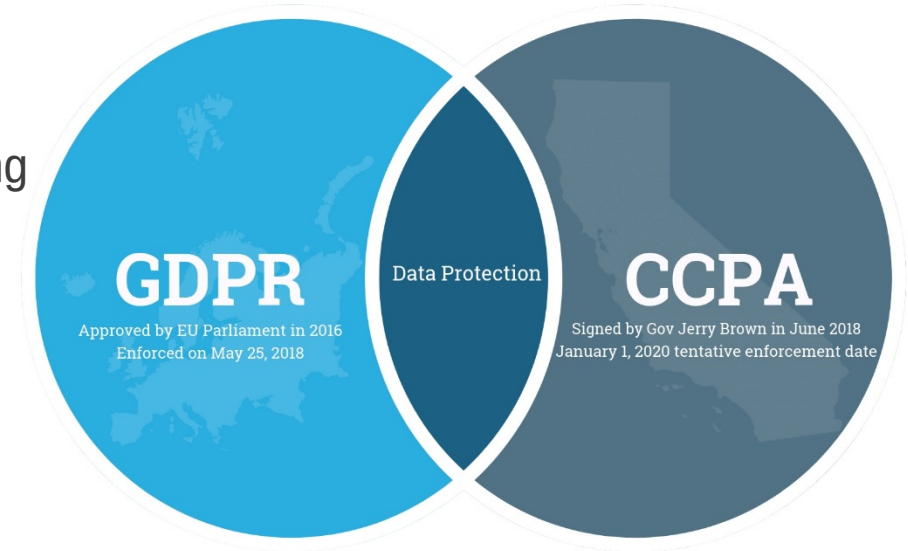
- Processing register of all processing activities Art. 30
- Company data protection officer, Art. 37 - 39
- Introduction of adequate internal procedures
  - Risk assessment (Art. 24, 25, 32, etc.)
  - Data Protection Impact Assessment (Art. 35, 36)
  - Privacy by design (Art. 25)
  - Data Breach Notification (Art. 33, 34)
  - Data Subject Rights handling (Art. 12-22)
- Policies and guidelines required (Art. 5, 24)
- Proof / documentation of compliance with procedures, rules

Data Subjects Rights (Art. 12 - 22)

- Transparency Principle: Detailed information obligations for direct collection (Art. 13) and collection from others (Art. 14), i.e. “privacy notices” / “privacy policies” on websites, etc.
- Right to access, including a right to receive a copy of all personal data (Art. 15)
- Right to rectification (Art. 16)
- Right to erasure (“right to be forgotten”), but not if data is rightfully used and archived (Art. 17), and right to restriction of processing, Art. 18
- Right to data portability, Art. 20 (cf. Art. 29 WP 242)
- Right to object, in particular to direct marketing and profiling, Art. 21
- Handling of these requests needs to follow general requirements, usually within one month (Art. 12)

California Consumer Privacy Act (CCPA)

- Passed by the California State Legislature and signed into law by Jerry Brown (then Governor of CA) on June 28, 2018
- New law went into effect January 1, 2020
- Enforcement began in July 2020
- CCPA grants a right of privacy for the collection and sale of person information
- Consumers have the right to ask business for the types/categories of personal information being collected
- Requires business to disclose the purpose for collecting/selling the information



CCPA – Disclosure of Categories

- A consumer has the right to request that a business that collects a consumer's personal information disclose the categories and specific pieces of personal information collected
- These requests may include:
  - Categories of information collected about that consumer
  - Categories of sources of information
  - The purpose for collection/selling
  - Categories of third parties with whom business share personal information
  - Specific information a business maintains of that specific consumer

CCPA – Right to Request Deletion

- A business that collects personal information must acknowledge the consumer's right to request deletion
- Upon request, businesses must delete any personal information and direct their service providers also to delete that information
- Exceptions where a company is NOT required to delete information include when the business needs the personal information to:
  - Complete a transaction to provide a good/service requested by the consumer within the context of the ongoing relationship between customer/business
  - Engage in public/peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the business's deletion of the information is likely to render impossible or impair the achievement of such research
  - Comply with a legal obligation
  - Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business

CCPA – Selling Personal Information

- Companies must disclose certain facts prior to selling consumers personal information, including categories of personal information that the business:
  - Collected about the consumer
  - Sold and to whom it was sold
  - Disclosed for business purposes
- Businesses must comply with consumer requests not to sell their personal information ("opt out")
- A company cannot discriminate against consumers because they chose to opt out of having their information sold, but they may offer financial incentives for the collection/sale/deletion of personal information

CCPA – Civil Remedies

- (1) Recovery of damages in an amount not less that one hundred dollars ($100) and not greater than seven hundred fifty dollars ($750) per consumer per incident or actual damages, whichever is greater
- (2) Injunctive or declaratory relief
- (3) Any other relief the court deems proper

CCPA – Practical Effects

- Many businesses around the world fall under the scope of CCPA and must become compliant
- The California DOJ estimates between 15,000 and 400,000 business are affected by the CCPA
  - 50% of those affected business are considered ”small businesses,” despite CCPA’s authors attempting to limit small business from its scope
  - Prior to CCPA going to affect 95% of business were not prepared
- Although likely front-loaded, initial compliance costs are approximately $55 billion
- The first 6 months of 2020 has produced more than 50 consumer class actions alleging CCPA violations
  - Specifically, multiple consumer class actions have been brought against Zoom Video Communications Inc. for improper collection of consumer information, among other allegations

States Following California's Lead – New York

- New York passed the Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") on October 23, 2019
  - This law was an expansion of existing data breach law
- The Act broadens the definition of private information to include:
  - Credit and debit card numbers
  - Biometric information
  - Username and email addresses with a password for accessing an online account
- Expands the definition of breach to include not just unauthorized "acquisition" of private information, but also unauthorized "access" to private information
- Expands the territorial scope of the breach notification requirement to any person that owns or licenses private information of a NY resident
- Grants Attorney General power to seek fines and injunctions against continued violators

States Following California's Lead – Nevada

- Inspired by CCPA, the Nevada State Legislature passed its new privacy law, Senate Bill 220 Online Privacy Law, which became effective on October 1, 2019
  - Consumers now have the right to additional information on how their information is collected and how it is distributed/shared
  - Businesses must provide notice of a designated email, toll-free number, or website address that allows consumers the right to opt-out of the "sale" of their personal information.
  - Provides notice requirement exemptions for financial institutions subject to the GLBA, healthcare providers subject to HIPAA, certain motor vehicle manufacturers, and third-party service providers supporting the business of an operator.
- There is no private right of action established under SB 220
  - The Nevada Attorney General will have the exclusive enforcement authority for violations of SB 220 through the institution of appropriate legal action
  - Organizations that violate the privacy and security requirements of the newly revised law will be subject to:
    - 1) a temporary or permanent injunction; or
    - 2) a civil penalty of up to $5,000 for each violation. These consequences are in addition to any other penalties that are provided by the law.

States Following California's Lead – Maine

- The Maine State Legislature passed the Maine Act to Protect the Privacy of Online Consumer Information, which became fully effective in July 2020
  - The law is applicable only to broadband providers operating within Maine when providing services to individuals physically located in Maine
- Prohibits broadband Internet access service providers from using, selling, distributing or permitting access to customer personal information for purposes other than providing services, unless the customer expressly consents to that use, disclosure, sale, or access
- Customers may revoke consent at any time ("opt out") and providers are prohibited from refusing to serve a customer who does not consent to the use, sale, disclosure, or sharing of their customer personal information
- Providers are allowed to use information to:
  - Provide the service from which the customer's personal information is derived or for the services necessary to the provision of such service
  - Advertise or market the provider's communications-related services to the customer
  - Comply with a lawful court order
  - Collect payment for Internet service
  - Protect users from fraud, and to
  - Provide location information to assist in the delivery of emergency services.

States Following California's Lead – Maryland

- HR Bill 1154, the Personal Information Protection Act (PIPA), which amends existing data protection laws, was passed on October 1, 2019
- Expands the required actions a business must take after becoming aware of a data security breach
  - Businesses that own, license, or maintain personal information of Maryland residents must conduct a reasonable, prompt and good faith investigation if they realize a data security breach occurred
  - The owner or licensee of personal information cannot use information related to the breach of the security of a system other than to provide notification, protect or secure personal information, or provide notification

Washington, DC

- Enacted on March 26, 2020 “Security Breach Protection Amendment Act of 2020.”

- Acting as an amendment of Section 28 of Chapter 38 of the District of Columbia Code, the Act: (1) expands the definition of “personal information,” (2) amends breach notification requirements, (3) adds new security requirements; and (4) expands the Act’s enforcement.

California Privacy Rights and Enforcement Act ("CPREA")

- CPREA, colloquially referred to as CCPA 2.0, is an initiative which progresses to expand the scope of the notice, access, and deletion rights, as well as add new privacy rights to the existing CCPA
- CPREA would:
  - Allow California residents to request that businesses correct inaccurate personal information ("PI") and the right to opt out of the use of "sensitive PI" for marketing
  - Require businesses to maintain the accuracy and security of the PI they collect, as well as disclose their political activities and their automated profiling practices involving PI
  - Subject businesses to a new administrative enforcement regime
  - mandate disclosures regarding the use of PI for political purposes
  - Require disclosures of the "logic" behind automated profiling practices that may have a significant adverse impact on consumers in certain contexts
  - Expand definition of "sensitive personal information" and require opt-in consent for the collection of PI from consumers younger than 16 years old
  - Require a business to direct "all third parties" and contractors who have accessed a consumer's PI from or through the business to delete the consumer's PI, not just service providers
  - Establish a new California Privacy Protection Agency to administer and enforce the new law

FEDERAL PRIVACY LEGISLATION

- Consumer Online Privacy Act (COPRA) (Democratic)
- Consumer Data Privacy Act (CDPA) (Republican)
- Consumer Data Privacy and Security Act (CDPSA) (Republican)

FEDERAL PRIVACY LEGISLATION DATA TREATMENT

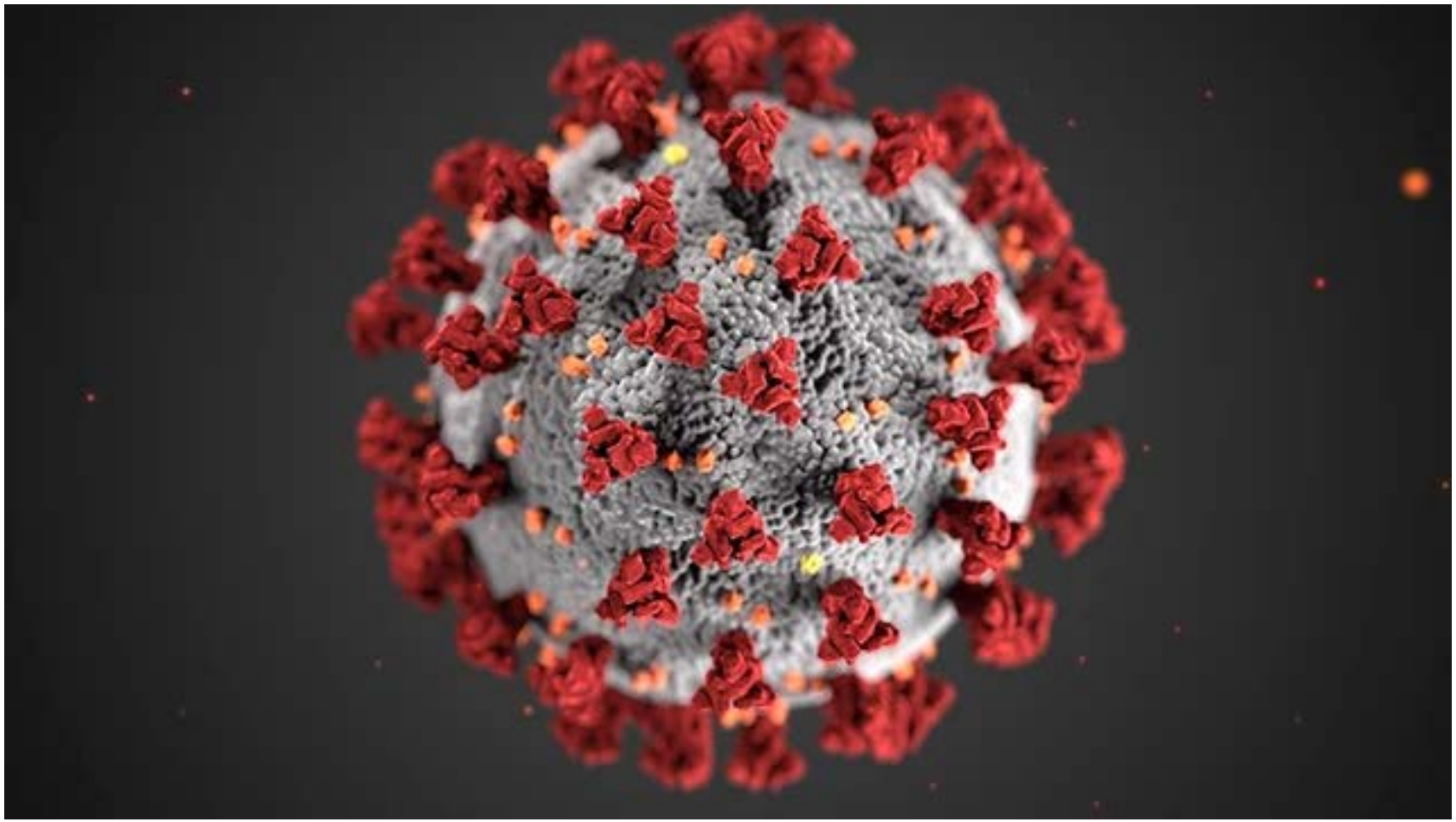
- All three statutes divide data into two categories:
  - Data that "is linked or reasonably linkable to a specific individual"
    - "Personal data" under CDPSA and CDPA
    - "Covered data" under COPRA
      - Also includes derived data
  - "Sensitive data"
    - includes geo-location data, data related to sexual orientation, and financial data.
    - COPRA's "sensitive covered data" includes metadata from the data subject's communications, email addresses, account credentials, and "information revealing online activities over time and across third-party website or online services."

FEDERAL LEGISLATIVE PROPOSALS COMMONALITIES

- Privacy policies
- Right to deletion provision
- Data minimization

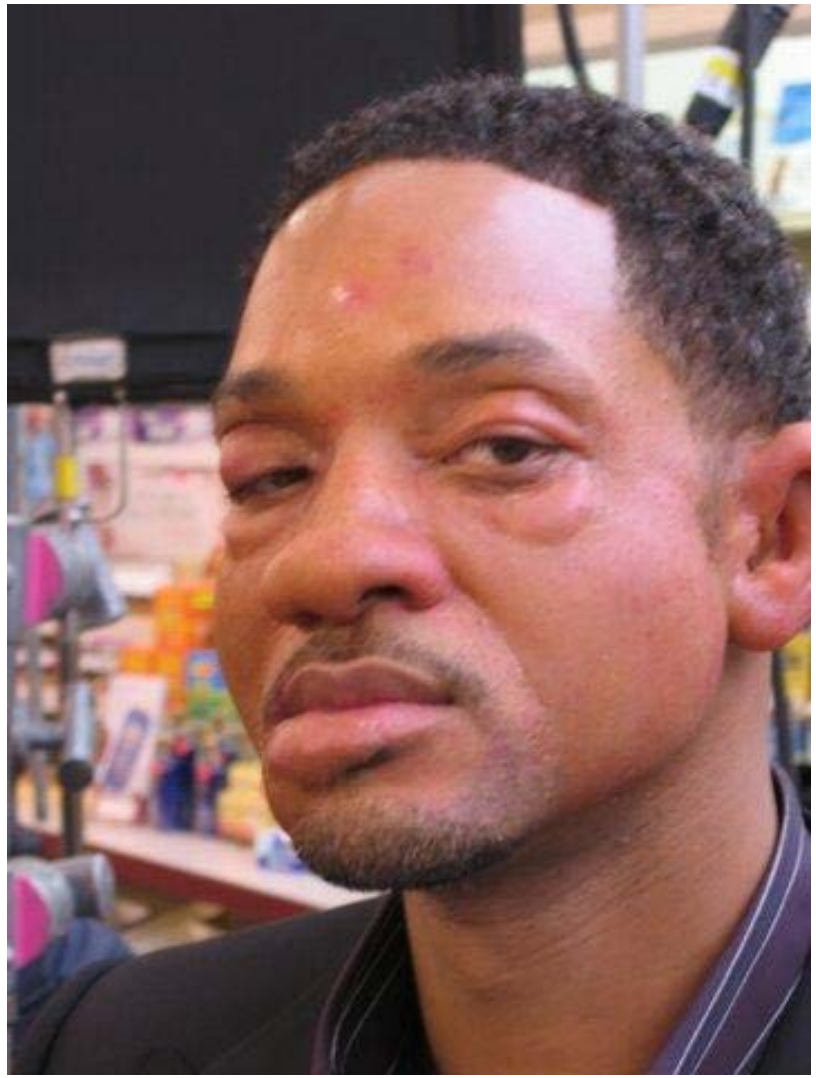
FEDERAL PROPOSAL DIFFERENCES

- State law preemption
- Private right of action



MARCH 2020

October 2020



Data Privacy during COVID-19

- The COVID-19 pandemic has raised a tangle of privacy issues around access to mobility and proximity data, health information, and other forms of personal information that may or may not be useful for public health
- Many governments are taking unprecedented measures to track, trace and contain the spread of the novel coronavirus (COVID-19), by turning to digital technologies and advanced analytics to collect, process and share data for effective front-line responses.
  - With this contact tracing, entities have information regarding a consumer's past geolocation and health information
  - Without robust data privacy laws, entities could utilize this geolocation and health data for improper and unrelated uses

ADVANCED PERSISTENT THREATS (APTs)

- Foreign governments are exploiting the pandemic to launch cyberattacks against American businesses
  - Russians
  - Chinese
- They act through organizations known as APTs
- During the pandemic, APTs have employed
  - Online scams and phishing
  - Disruptive malware (Ransomware and DDOS)
  - Malicious/copycat domains
  - Data-Harvesting Malware
    - “Free COVID-19 testing”
    - “COVID-19 prevention measures”
  - Misinformation about the pandemic

Q & A

- **Marisa A. Trasatti**, Partner, Wilson Elser Moskowtiz Edelman & Dicker LLP

Marisa.Trasatti@wilsonelser.com

- Sarah Cushard, Senior Security Specialist, GreyCastle Security

cushard@greycastlesecurity.com

- Sean C. Griffin, Commercial Litigation Attorney, Dykema

SGriffin@dykema.com