FOLEY

FOLEY & LARDNER LLP

2022

CLE Weeks

December 5-16, 2022

FOLEY

FOLEY & LARDNER LLP

2022 CLE WEEKS

Deadlines Fast Approaching For Compliance with New U.S. Consumer Privacy Laws and Latest Cybersecurity Legal Developments

December 14, 2022

Speakers

Jennifer L. Urban
Partner | Milwaukee

T: 414.297.5864
E: jurban@foley.com

Samuel D. Goldstick
Associate | Chicago

T: 312.832.4915
E: sgoldstick@foley.com

Agenda

FOLEY

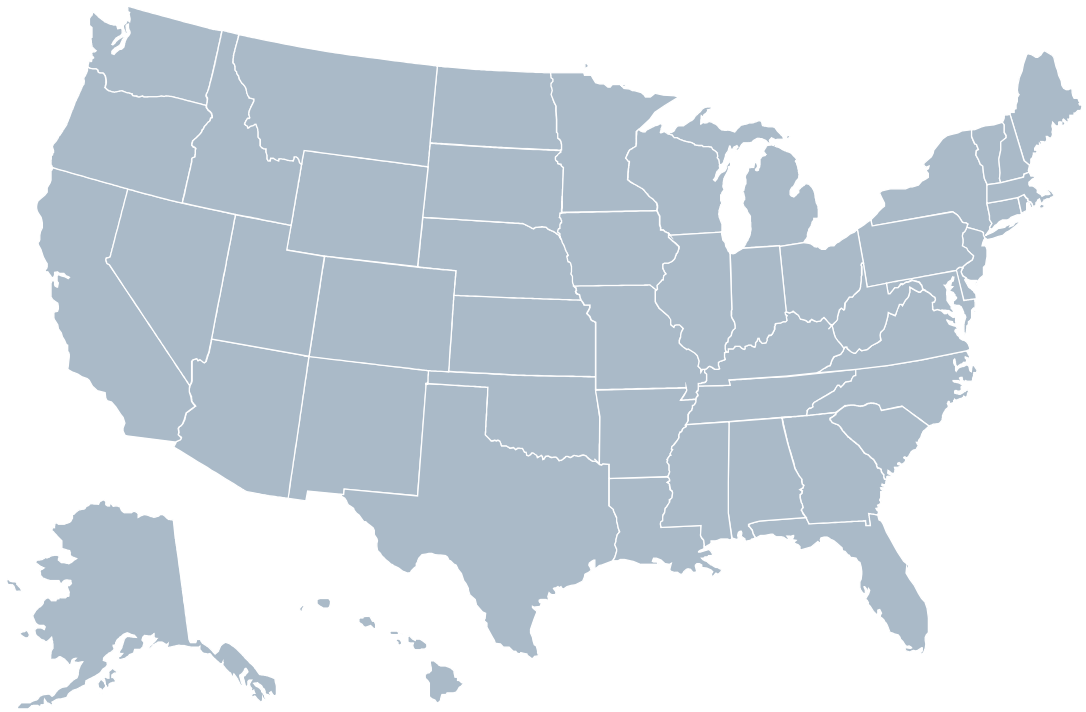
FOLEY & LARDNER LLP

Cyber Threat Landscape Overview

Cost Overview

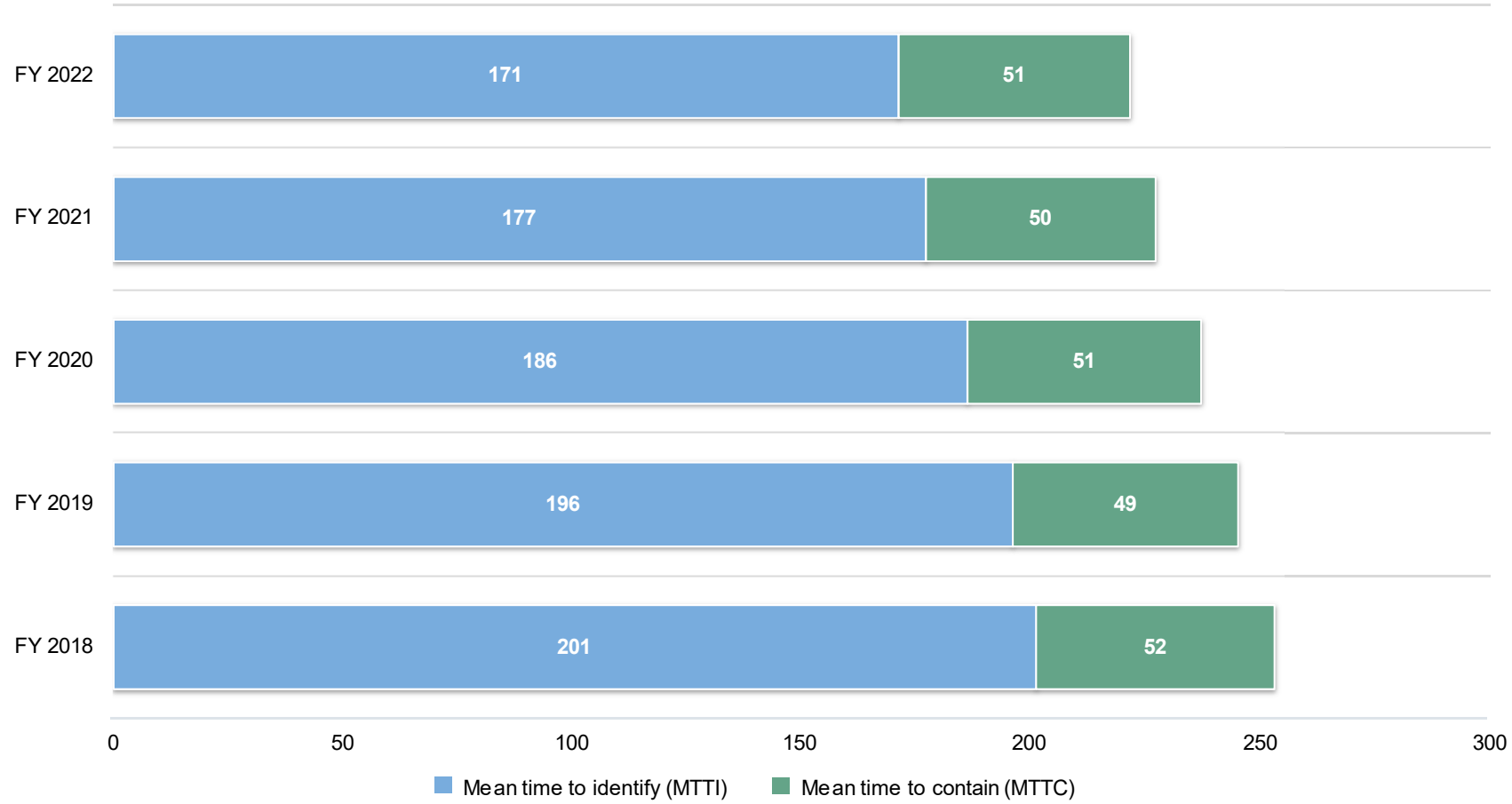
- Average cost of a U.S. breach: **$9.44 million**
  - Global average is $4.35 million

- Cost of a breach can include detection and escalation, notification, ex-post response, and lost business costs



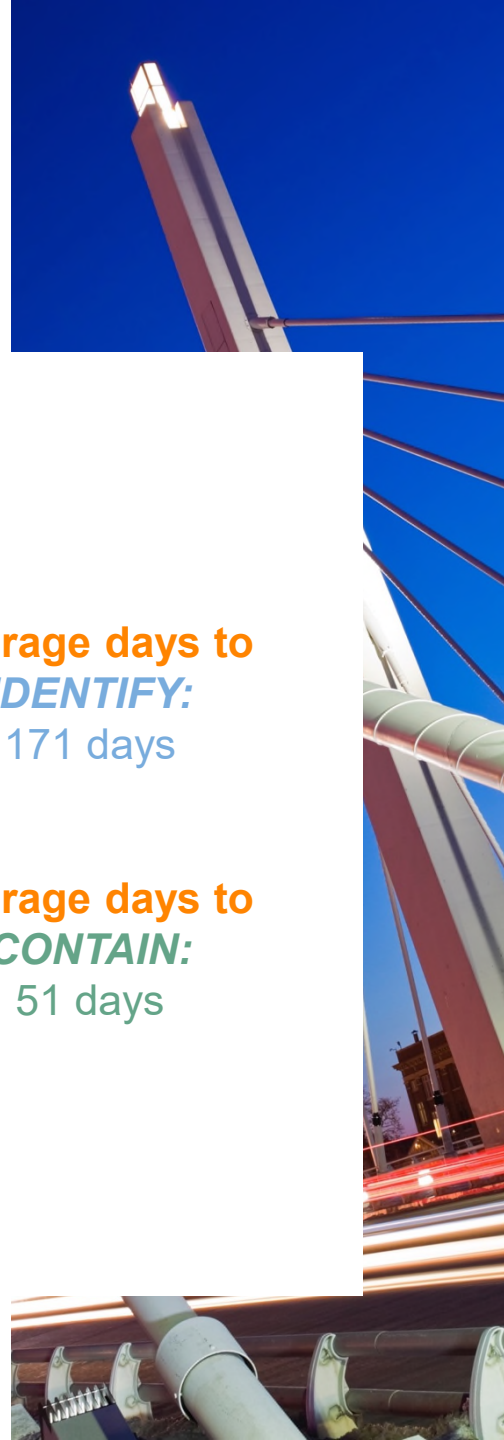
Source: Ponemon Institute© Research Report (sponsored by IBM Security), *2022 Cost of a Data Breach: United States* (July 2022)

Days to Identify and Contain a Data Breach



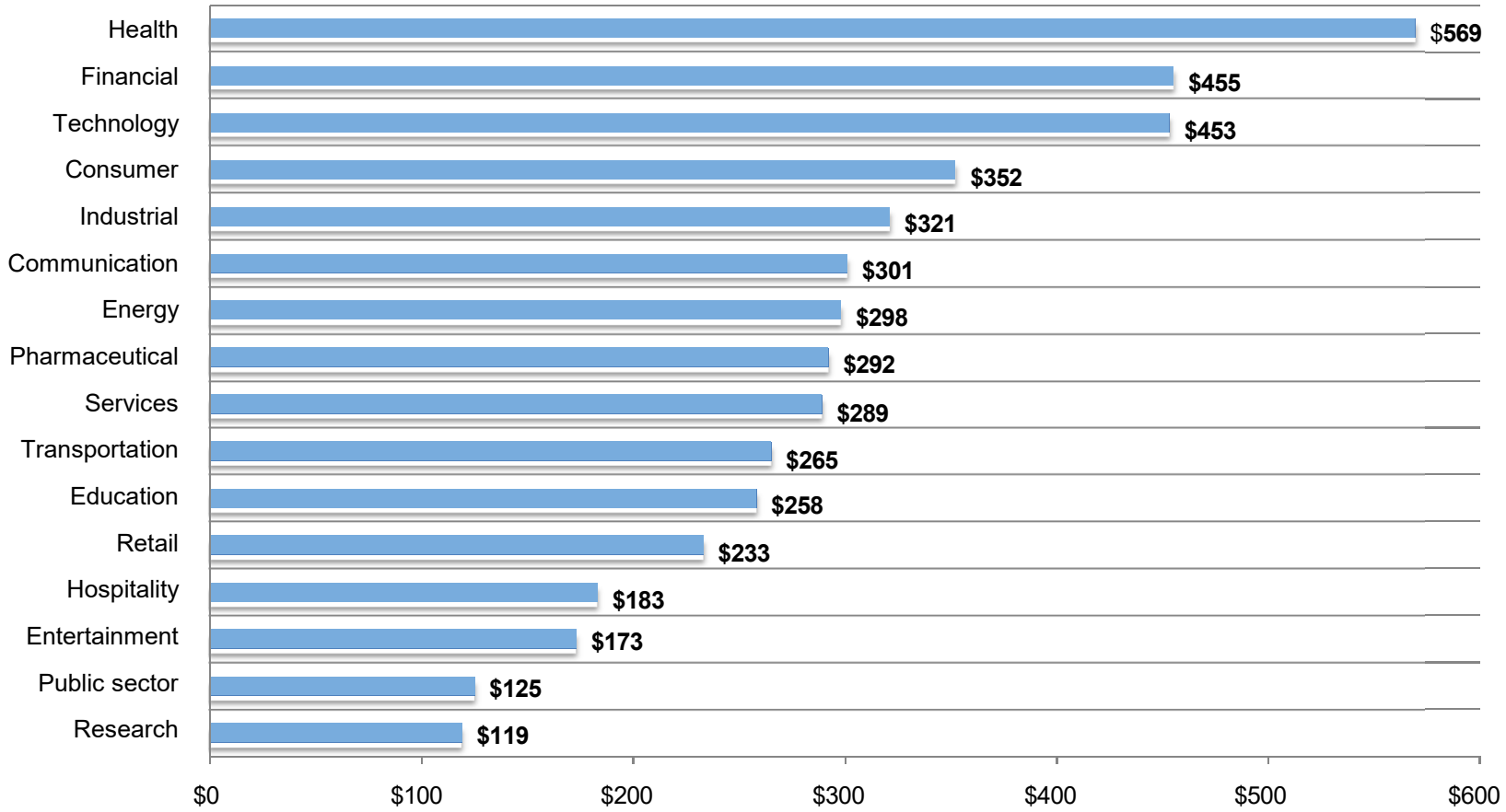
Average days to *IDENTIFY:*
171 days

Average days to *CONTAIN:*
51 days

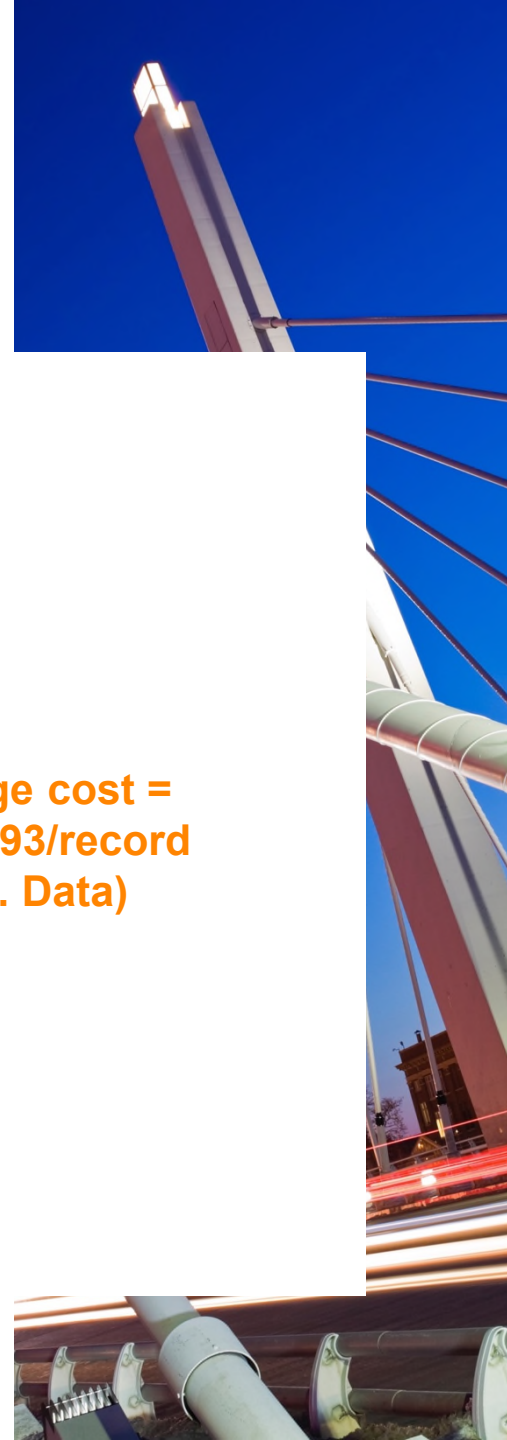


Source: Ponemon Institute© Research Report (sponsored by IBM Security), *2022 Cost of a Data Breach: United States* (July 2022)

Cost Varies By Industry

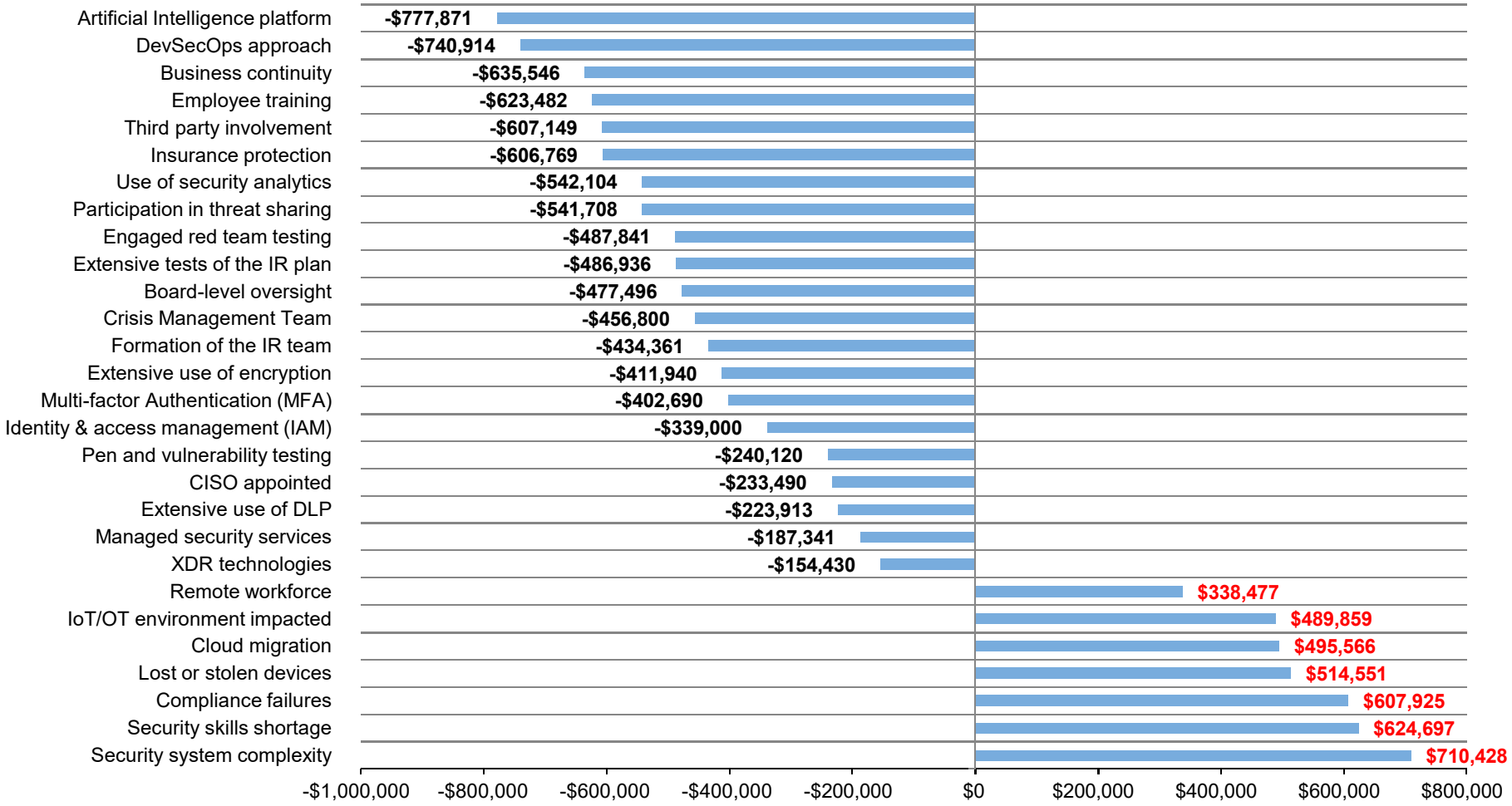


Average cost = USD $293/record (U.S. Data)



Source: Ponemon Institute© Research Report (sponsored by IBM Security), *2022 Cost of a Data Breach: United States* (July 2022)

Factors that May Increase or Decrease the Cost of a Data Breach



Source: Ponemon Institute© Research Report (sponsored by IBM Security),
***2022 Cost of a Data Breach: United States* (July 2022)**

Source of Potential Liability/Costs for Inadequate Security Measures

- FTC and Other Applicable Industry-Specific Agency Enforcement
- State Attorney General/Other Consumer Protection Agencies Enforcement
- International Data Supervisory Authorities
- Class Action and Other Lawsuits
- Contractual Liability
- Data Breach Remediation and Related Costs
- Reputational Costs
- Loss of Competitive Advantage/Profits

State of Cybersecurity From an In-House Perspective

84% of Chief Legal Officers now have at least some cybersecurity-related responsibilities

(up from 76% in 2020)

22% of companies now have a dedicated cybersecurity lawyer

(up from 12% in 2018)

63% of companies now have mandatory annual trainings on cybersecurity for all employees

(up from 43% in 2020)

55% of companies surveyed practice strong cross-functional collaboration by and among their respective IT/cyber and legal departments and other relevant business units to reduce cyber risk

Source: ACC Foundation, *2022 State of Cybersecurity Report, An In-House Perspective* (in collaboration with Ernst & Young, LLP) (Nov. 1, 2022)

FOLEY

FOLEY & LARDNER LLP

Ransomware-specific Considerations

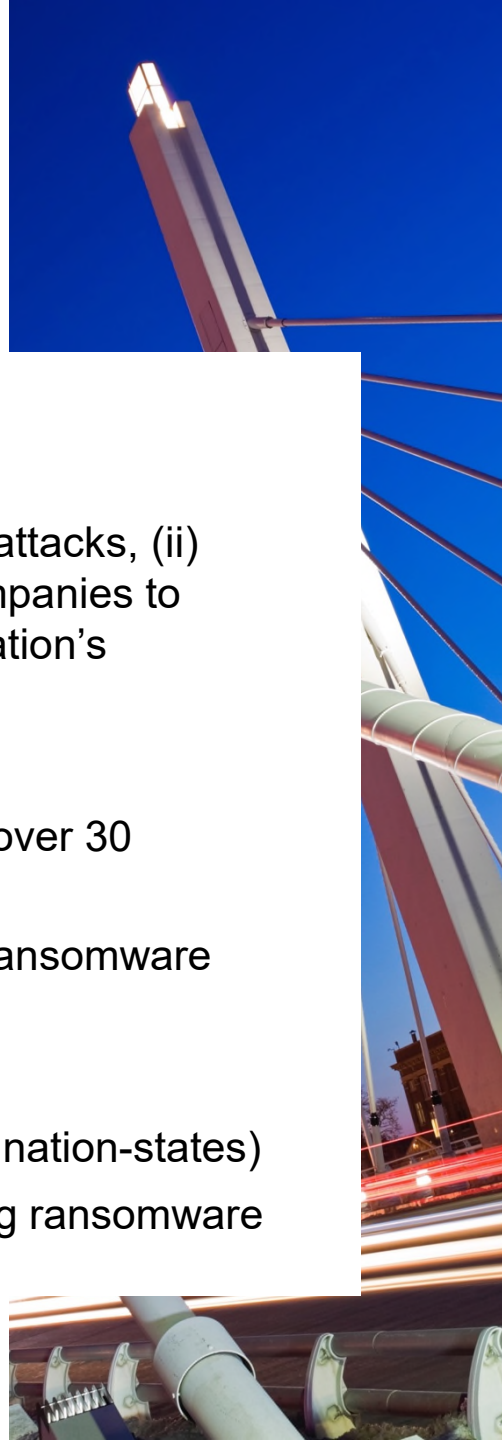
Rise of Ransomware

Ransomware By the Numbers

- In 2022, ransomware attacks increased 13% in the past 12 months[1]
- 236 million ransomware attacks occurred globally in the first half of 2022[2]
- Globally, ransomware attacks ($4.54 million) cost more than the average data breach ($4.35 million)[3]

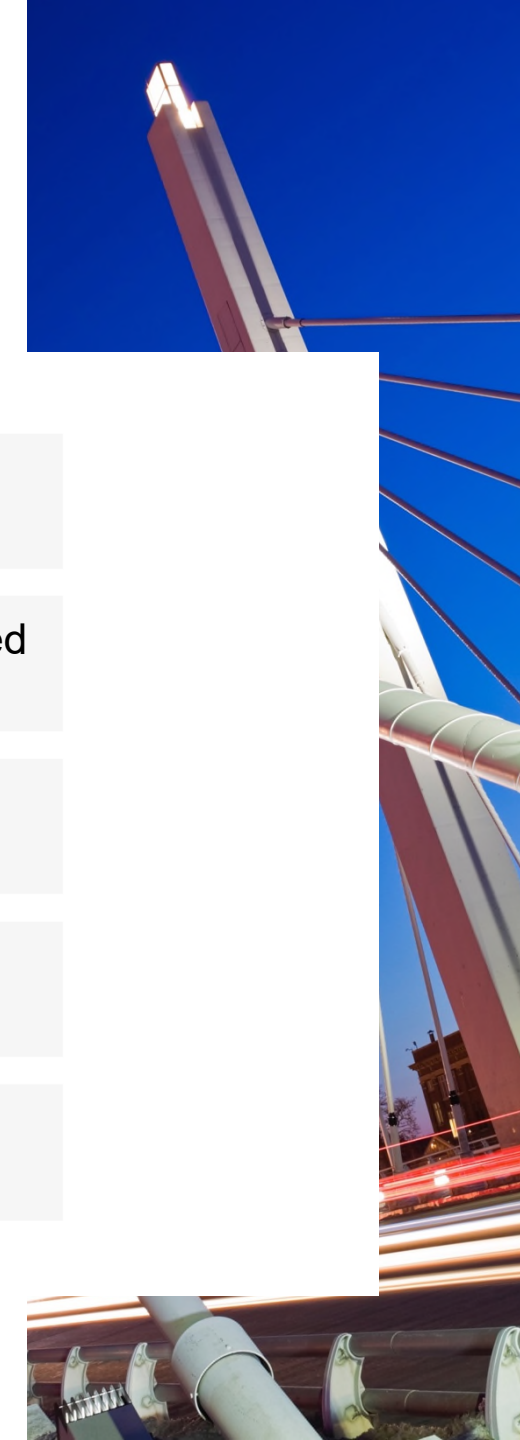
Sources:
[1] 2022 Verizon Data Breach Investigations Report
[2] 2022 SonicWall Cyber Threat Report, Mid-Year Update
[3] Ponemon Institute© Research Report (sponsored by IBM Security), *2022 Cost of a Data Breach: United States* (July 2022)

Steps Taken By the White House to Help Combat Ransomware



- **June 2, 2021**
  - Published an open letter to the private sector (i) warning of the significant threat of ransomware attacks, (ii) recommending steps that businesses of all sizes should take immediately, and (iii) imploring companies to implement cybersecurity best practices as set out in Executive Order 14028 on Improving the Nation's Cybersecurity
- **October 13-14, 2021**
  - Facilitated the 1st annual International Counter Ransomware Initiative (CRI) virtual summit with over 30 countries and the EU, with the goal of accelerating cooperation to counter ransomware
  - Issued a Fact Sheet updating the public on the U.S. government's efforts to address the global ransomware threat
- **October 31-November 1, 2022**
  - Hosted the 2nd annual International CRI summit meeting in-person (attended by 36 CRI partner nation-states)
  - Post-summit, the CRI partners issued a joint statement reaffirming their commitment to disrupting ransomware attacks and protecting their citizens from cybercriminals

Practical Tips to Prepare for and Respond to a Ransomware Attack



1. Conduct a tabletop exercise to test your incident response plan specific to ransomware
2. Review your cyber insurance policy to determine coverage and the process for claims related to ransomware (*e.g.*, panel requirements, ransom payment process and negotiator, etc.)
3. Preserve logs and other forensic data
4. Notify your cyber insurance carrier
5. Engage a forensic firm under attorney-client privilege

Primer on Attorney-Client Privilege for Investigations to Explain Why Attorneys Are Involved

Outside counsel should directly engage forensic experts (*e.g.*, forensic investigators and ransomware negotiators) for advising and defending the client in anticipation of litigation

Incident response efforts should be bifurcated to ensure that non-privileged remediation work is separate from investigative work in anticipation of litigation and for advising on breach notification obligations

Separate engagement letters and written statements of work are needed that specifically reflect the engagement with each applicable forensic expert rather than relying on a master agreement with a retainer only

Any written report prepared by a forensic expert related to such an engagement should only be ***shared by counsel with a limited group of people on a "need-to-know basis"***

Preserve the data and analysis of the forensic expert

Practical Tips to Prepare for and Respond to a Ransomware Attack *(cont'd.)*

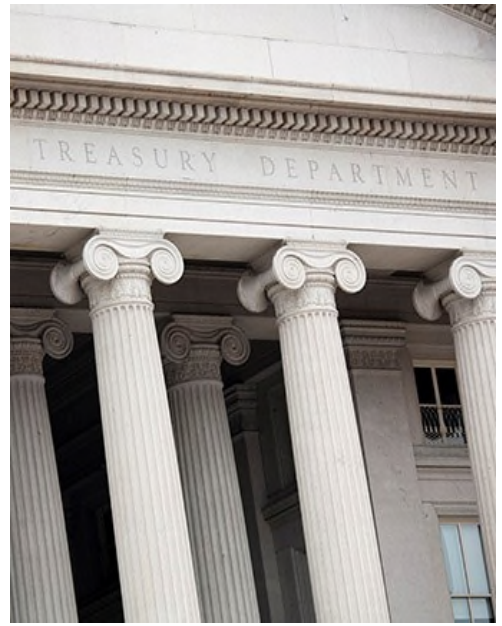
6	Be prepared for pressure to issue customer communications before the extent of the attack has been determined
7	Assess ability and a timeline to recover business operations while continuing the forensic investigation to determine whether regulated data was accessed or exfiltrated
8	Ensure backups are safe to restore before doing so
9	Be aware that ransomware has evolved to exfiltrate data in addition to locking down systems and stifling business operations
10	Conduct dark web and ongoing threat monitoring services

Practical Tips to Prepare for and Respond to a Ransomware Attack *(cont'd.)*

11	Involve appropriate law enforcement
12	Analyze contractual and regulatory notification obligations
13	Prepare Board communications, if applicable
14	Determine if any audit or financial statement disclosures are required
15	Ensure mitigation measures are implemented and conduct a "lessons learned" analysis

U.S. Economic Sanctions

- **Parties subject to U.S. jurisdiction are generally prohibited from engaging in transactions — including ransomware payments — with sanctioned countries or parties**
  - Any U.S. citizen or Legal Permanent Resident
  - Any entity incorporated in the United States
  - Any foreign person on U.S. soil
  - Any activity involving a U.S. territory (including the Cloud)
  - Any activity involving the U.S. financial system
- **Comprehensive and government-based sanctions**
  - Cuba, Iran, Ukraine, North Korea, Syria, other Rogue States
- **List-based sanctions**
  - Parties appearing on sanctions lists administered by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC)
  - Any party at least 50% owned by one or more sanctioned parties, even if they don't appear on actual sanctioned lists



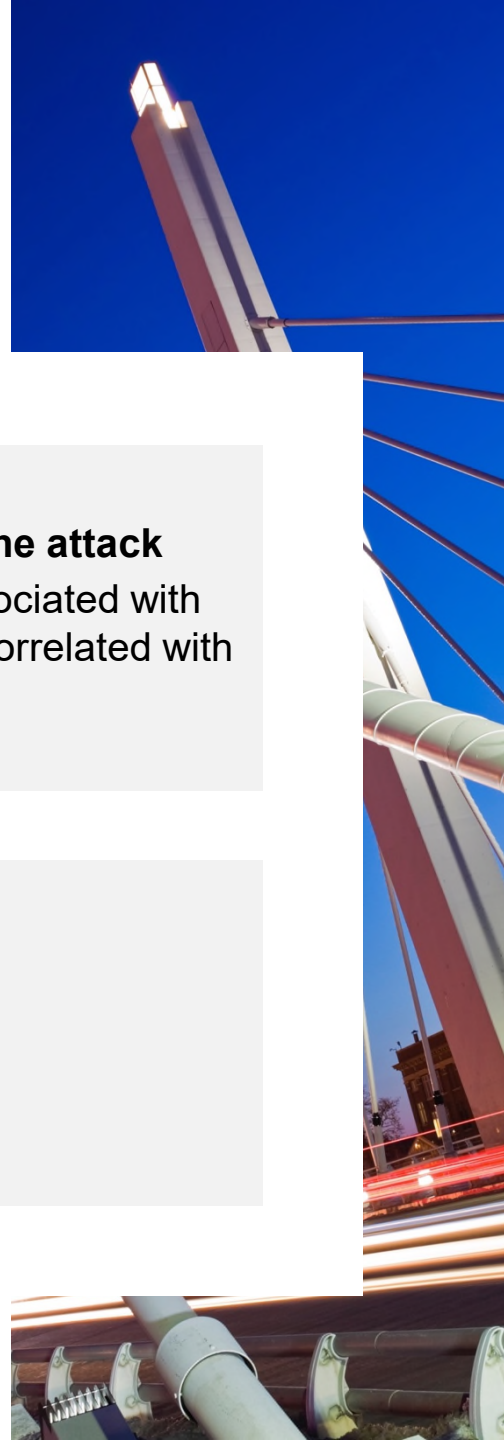
Penalties Can Be Severe

- **Civil penalties**
  - OFAC can hold parties liable for civil penalties if they “knew or should have known” that a ransom payment would violate U.S. economic sanctions
  - Penalties can be up to approximately $307,000 or twice the value of the ransom payment, whichever is higher (per violation)

- **Criminal penalties**
  - DOJ can seek fines up to $1 million per violation, plus up to 20 years incarceration for natural persons

- **Officer and Director liability matters**

Survival Strategies



Gather information about the threat actor

Screening the threat actor's name, address, location, crypto currency wallet, etc., can help identify risks

Gather information about the attack

Some attack vectors are associated with particular groups or can be correlated with them

Cooperate with law enforcement

This can sometimes provide insight into the threat actor as well as reduce the likelihood of civil or criminal enforcement

When in doubt, get help

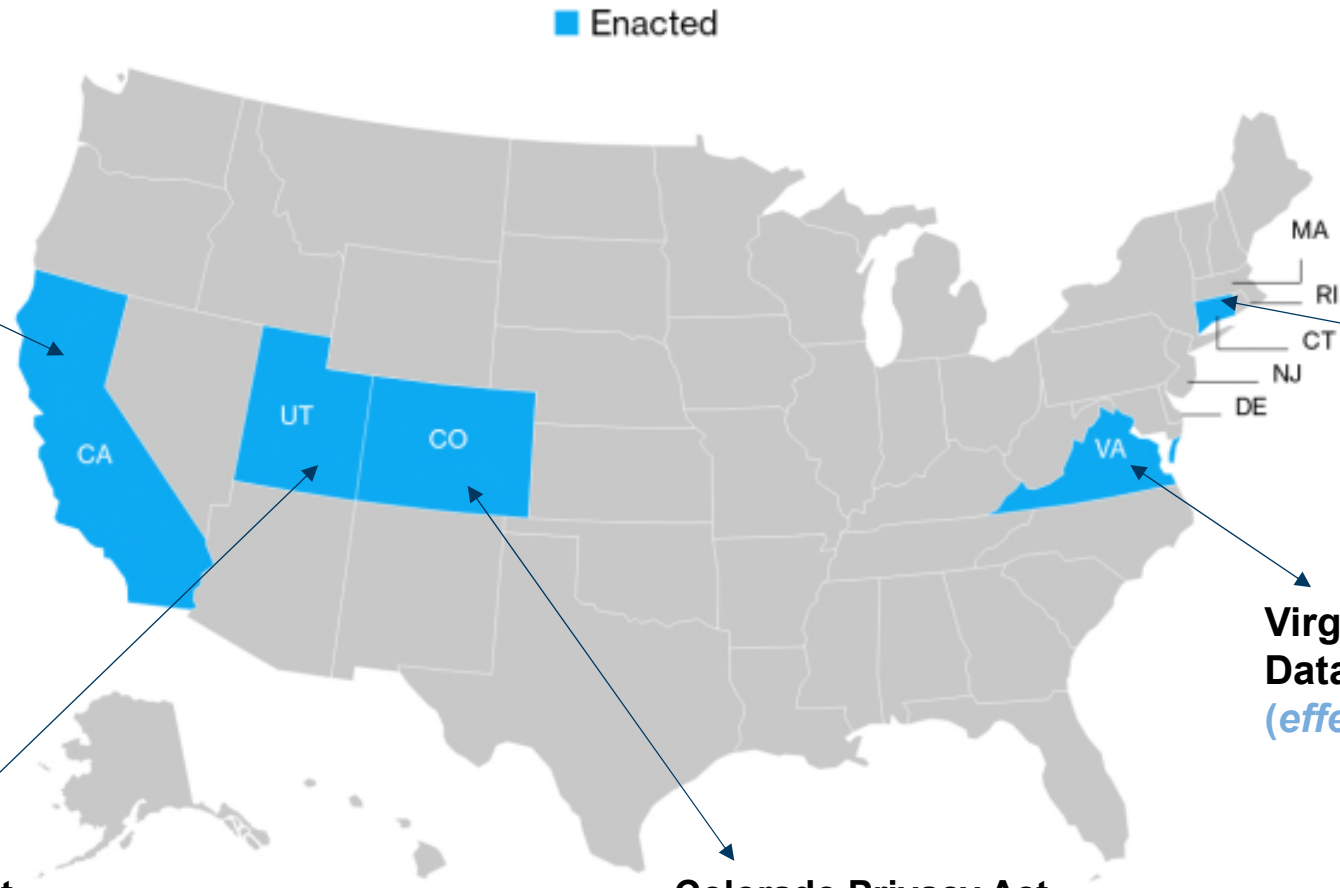
FOLEY

FOLEY & LARDNER LLP

Overview of Comprehensive Data Privacy Laws

Where Are We in the United States?

States With Comprehensive Consumer Privacy Laws



California Consumer Privacy Act
(*currently in effect*)

California Privacy Rights Act
(*effective 1/1/2023*)

Connecticut Data Privacy Act
(*effective 7/1/2023*)

Virginia Consumer Data Protection Act
(*effective 1/1/2023*)

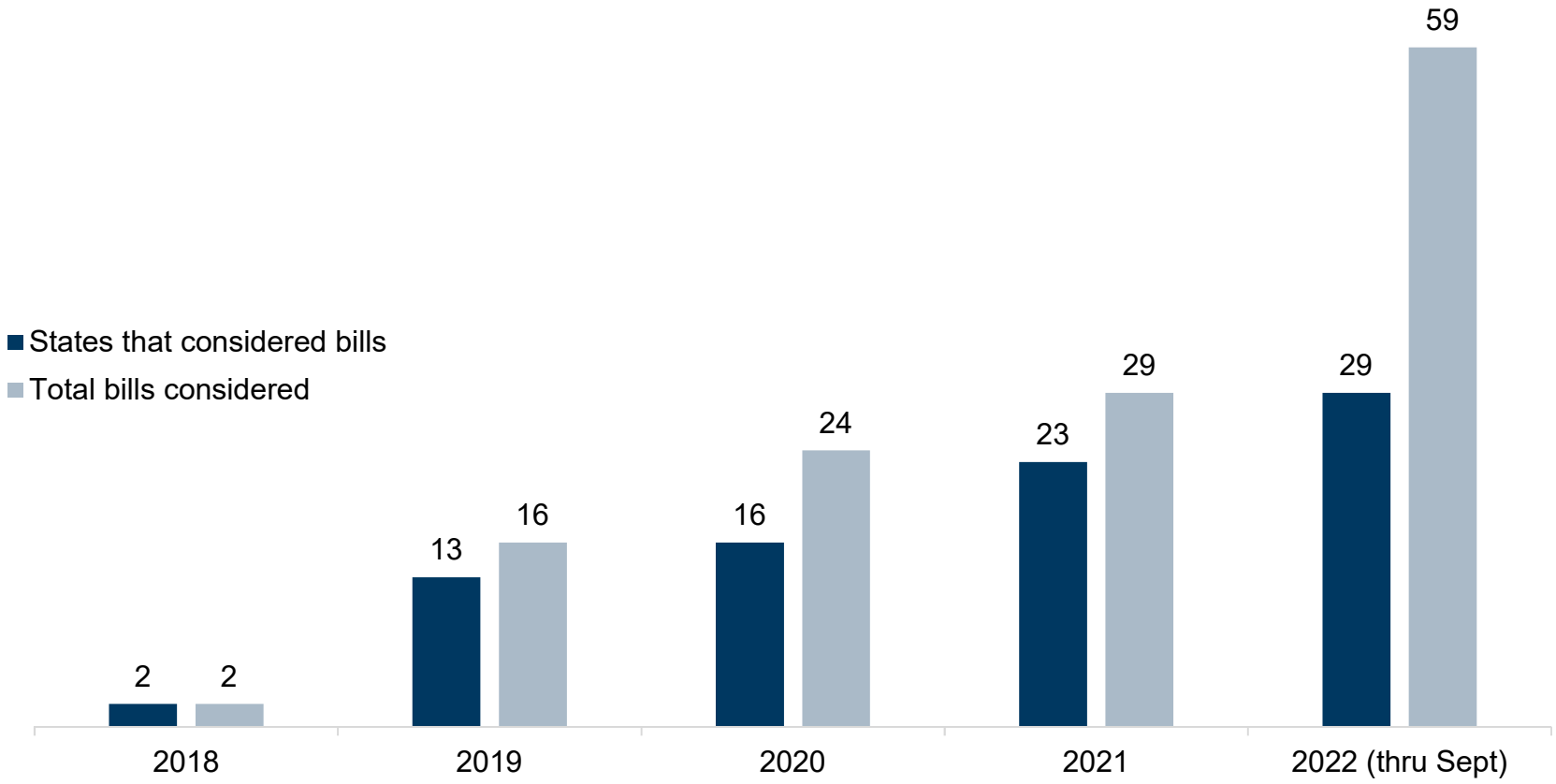
Utah Consumer Privacy Act
(*effective 12/31/2023*)

Colorado Privacy Act
(*effective 7/1/2023*)

California Privacy Rights Act Status

- Takes effect January 1, 2023, but the CPRA's rulemaking process is ongoing.
- On November 3, 2022, the California Privacy Protection Agency (CPPA) approved modifications to the draft regulations and opened a 15-day public consultation that ran through November 21, 2022.
- If no further modifications are required after the public comment period, the CPPA will draft the final rules filing and vote to send the finalized package to the California Office of Administrative Law.
- While the January 2023 target for the final rules remains plausible, there is a proposed regulation to delay the July 1, 2023 CPRA enforcement deadline to allow businesses to implement changes and ensure compliance.

More States Will Enact Comprehensive Consumer Privacy Laws



Source: International Association of Privacy Professionals (IAPP),
***The Growth of State Privacy Legislation* (Sept. 2022)**

Where Are We Around the World?

By the Numbers (as of December 2021)

137

jurisdictions around the world have enacted omnibus data privacy laws

103

of those laws are in jurisdictions outside the European Economic Area

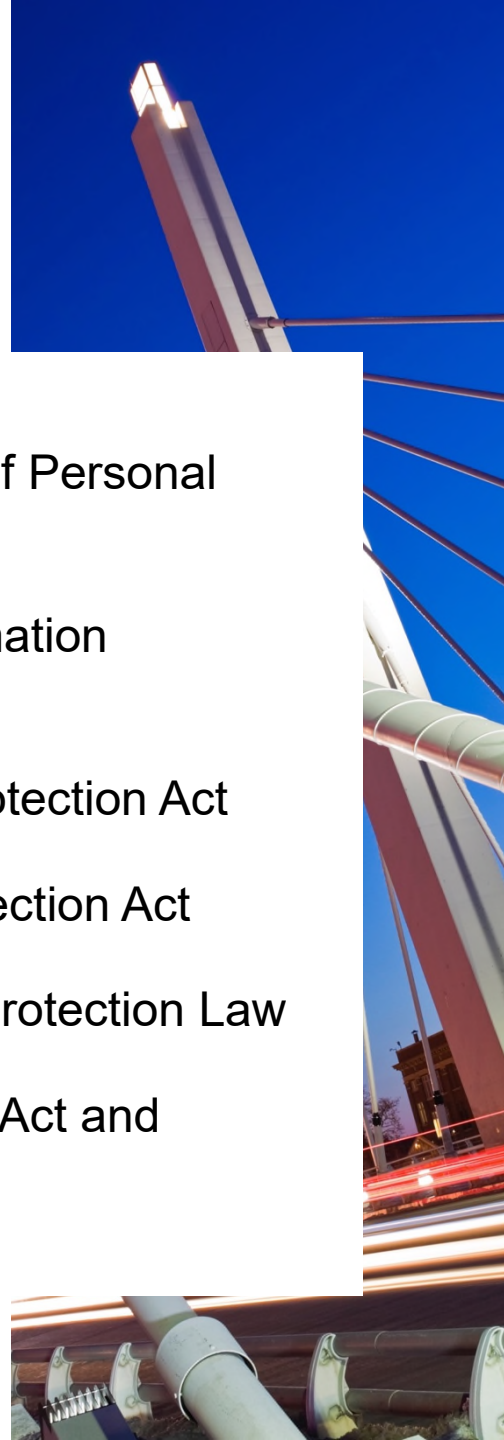
62

of those laws were enacted in the past 10 years and *half of those* within the past five years

By 2023, 65% of the world's population will have its personal data covered under modern privacy regulations, according to Gartner.

Where Are We Around the World? *(cont'd.)*

Examples



EU: EU General Data Protection Regulation (GDPR)

United Kingdom: UK GDPR

Canada: Personal Information Protection and Electronic Documents Act

South Africa: Protection of Personal Information Act

Brazil: General Data Protection Law

Australia: Privacy Act

Japan: Act on the Protection of Personal Information

South Korea: Personal Information Protection Act

Singapore: Personal Data Protection Act

Thailand: Personal Data Protection Act

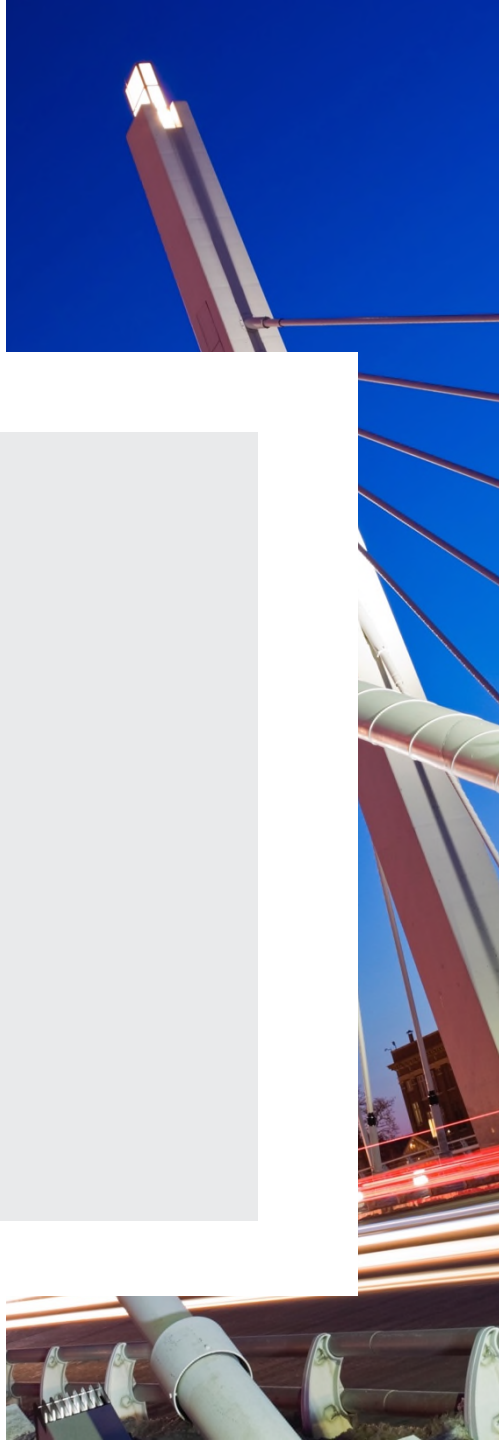
China: Personal Information Protection Law

India: Information Technology Act and Related Directives

Common Principles Across Existing Data Privacy Laws

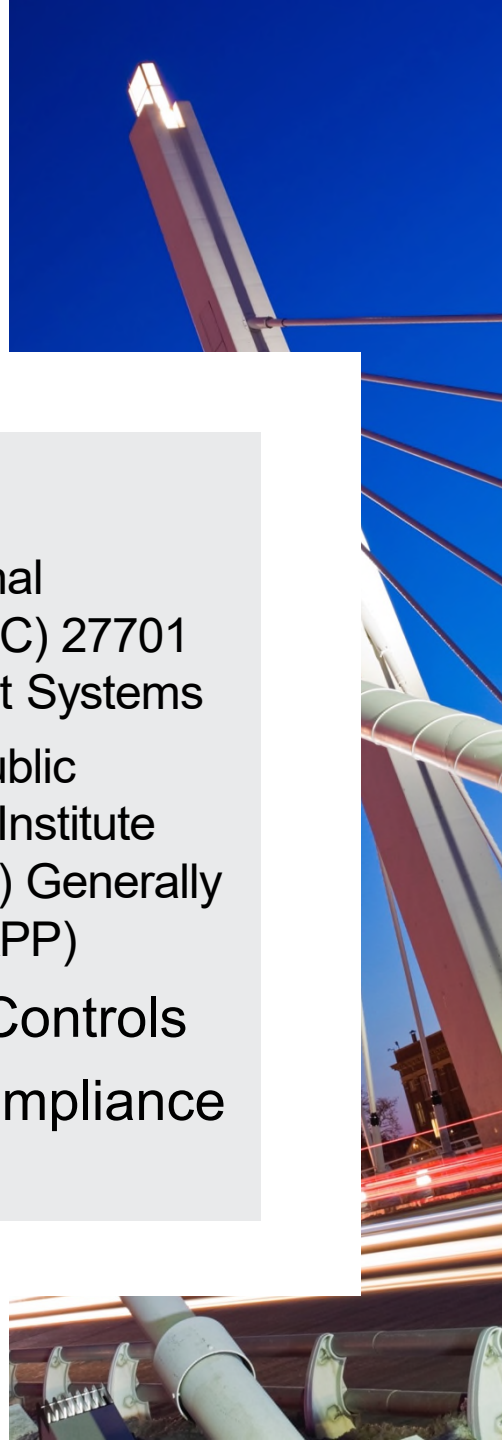
- Scope/Applicability/Exemptions
- Individual Rights — *e.g.*, access, deletion, rectification, restriction, portability, opt-out
- Notice/Transparency Requirements
- Legal Basis for Processing
- Processing Principles — *e.g.*, purpose limitation and data minimization

- Vendor Requirements
- Data Breach Notification
- Security Requirements
- Recordkeeping
- Risk/Impact Assessments
- International Data Transfer Restrictions

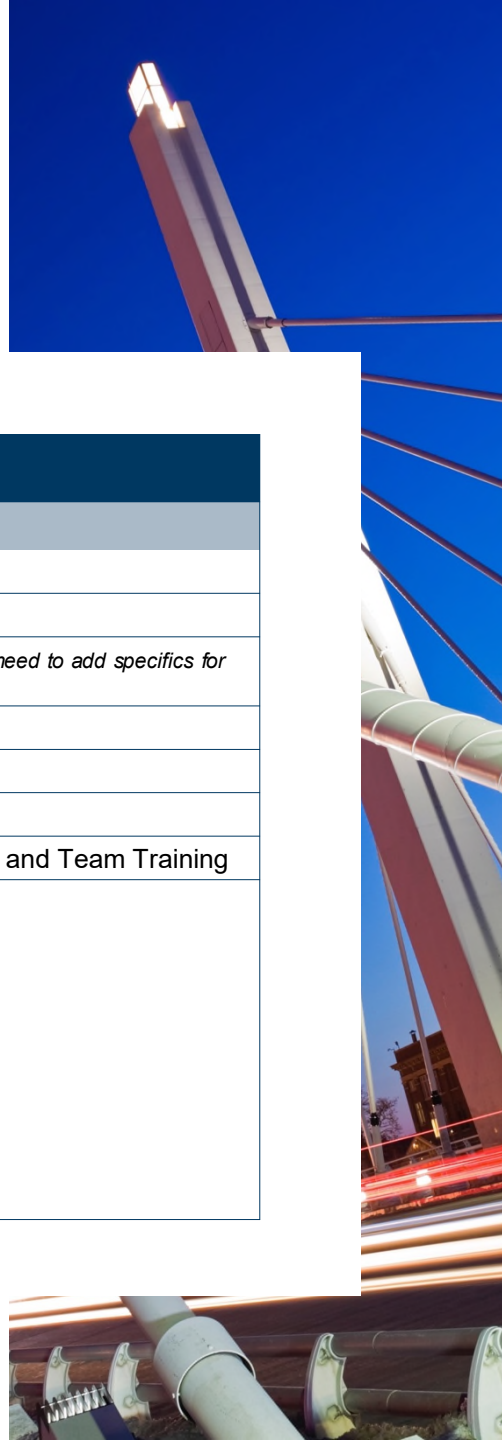


Tips for Developing a Privacy Compliance Program

- Data Mapping
- Performing a Risk Assessment
- Determining Legal and Program Requirements
- Implementing a Privacy Compliance Framework
  - The National Institute of Standards and Technology (NIST) Privacy Framework
  - International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27701 Privacy Information Management Systems
  - American Institute of Certified Public Accountants (AICPA)/Canadian Institute of Chartered Accountants (CICA) Generally Accepted Privacy Principles (GAPP)
- Developing Policies/Internal Controls
- Managing Vendor Privacy Compliance



Foley's Approach to Implementing Privacy Programs: Model Phases and Deliverables



Key Project Components	
PHASE 1	***PHASE 2***
Kickoff and Strategy Meeting(s) with Client Project Team	Incident Response Plan
Data Mapping *(review what has been completed to date)*	Cyber Insurance Coverage and Panel Requirements Review
Online Privacy Notice + Notice at Collection + Cookie Policy ***(multiple policy versions may apply depending on final strategy set for privacy program)***	Employee/IT Information Security Policies *(two separate policies; IT may need to add specifics for particular systems)*
Employee/Applicant Privacy Policies + Notices at Collection ***(two separate sets of policies + notices; may be combined into a single policy + notice based on data use practices)***	Acceptable Use of Assets Policy
B2B Privacy Policy + Notice of Collection ***(separate policy + notice depending on business operations)***	Personal Device/Bring Your Own Device (BYOD) Policy
Data Processing/Vendor Agreements ***(two separate agreements for Controller to Processor and Processor to Controller)***	Social Media Policy
Data Sharing Agreement ***(one agreement for Controller to Controller)***	Meetings with Project Team, Revisions to Key Project Components, and Team Training
Personal Information Protection Policy *(internal document for personnel describing what they can and cannot do with personal information — includes forms for requests/responses)*	
Data Subject Request Playbook *(includes data subject access request procedures and applicable form responses)*	
Document Retention Policy *(optional)*	
Data Privacy Impact Assessment *(only as necessary)*	
Terms of Use	
Meetings with Project Team, Revisions to Key Project Components, and Team Training	

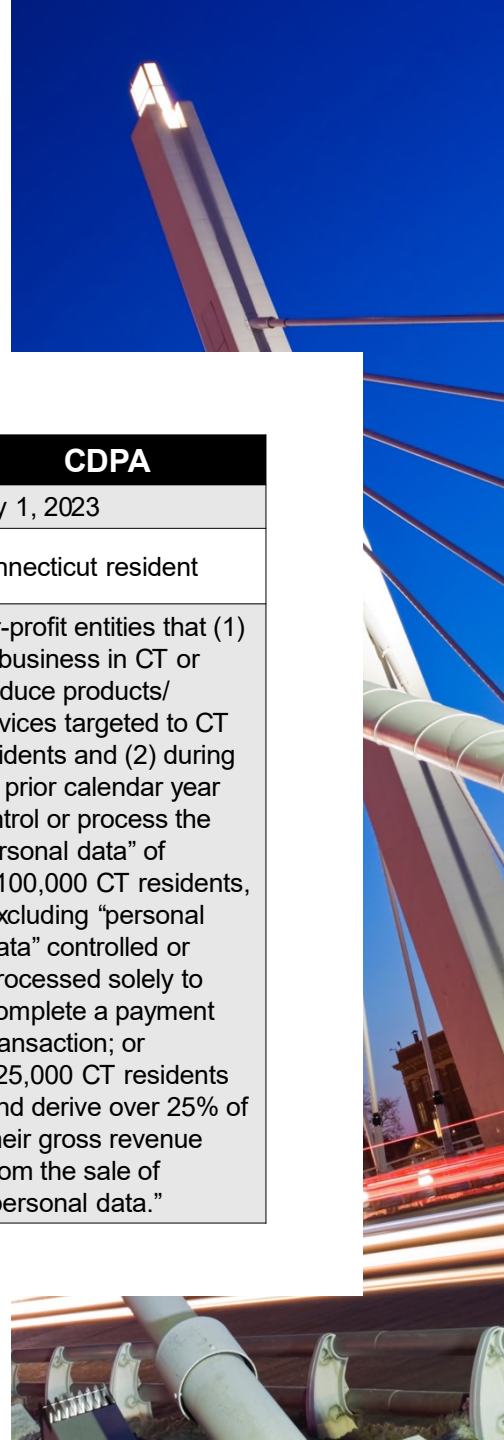
FOLEY

FOLEY & LARDNER LLP

Comparison of Data Privacy Laws in Europe and the United States

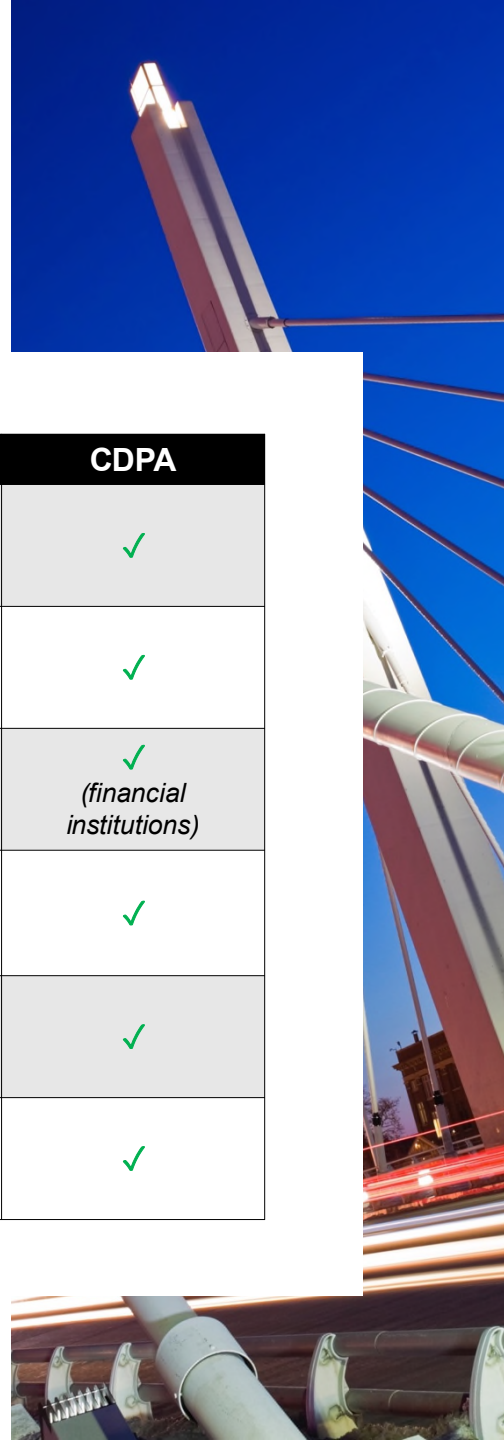
European and U.S. Privacy Laws
The Basics

	GDPR	CCPA	CPRA	VCDPA	CPA	UCPA	CDPA
Effective	May 25, 2018	January 1, 2020	January 1, 2023	January 1, 2023	July 1, 2023	December 31, 2023	July 1, 2023
Protected individuals	Person in the EU	California resident	California resident	Virginia resident	Colorado resident	Utah resident	Connecticut resident
Regulated entities	Entities that are: - Established in the EU and process "personal data" as part of its EU establishment's activities; or - Established outside the EU and offer goods or services to, or monitor the behavior of, individuals in the EU.	For-profit entities that do business in CA and: - Have annual gross revenues in excess of $25 million; or - Annually buys, receives, sells, or shares "personal information" of ≥50,000 CA residents, households, or devices; or - Derives 50% or more of its annual revenues from selling CA residents' "personal information."	For-profit entities that do business in CA and: - Had annual gross revenues in excess of $25 million in the preceding calendar year; or - Annually buys, sells, or shares "personal information" of ≥100,000 CA residents or households; or - Derives 50% or more of annual revenue from selling or sharing CA residents' "personal information."	For-profit entities that conduct business in VA or produce or deliver products/ services that are targeted to VA residents and control or process the "personal data" of: - ≥100,000 VA residents during a calendar year; or - ≥25,000 VA residents and derive more than 50% of gross revenue from the sale of "personal data."	Entities that conduct business in CO or produce or deliver commercial products/ services that are intentionally targeted to CO residents and control or process the personal data of: - ≥100,000 CO residents during a calendar year; or - ≥25,000 CO residents and derives revenue or receives a discount on the price of goods/services from the sale of "personal data."	For-profit entities that (1) do business in UT or produce a product/ service targeted to UT residents, (2) have annual revenue of $25 million or more, and (3) control or process the "personal data" of: - ≥100,000 UT residents during a calendar year; or - ≥25,000 UT residents and derive over 50% of their gross revenue from the sale of "personal data."	For-profit entities that (1) do business in CT or produce products/ services targeted to CT residents and (2) during the prior calendar year control or process the "personal data" of - ≥100,000 CT residents, excluding "personal data" controlled or processed solely to complete a payment transaction; or - ≥25,000 CT residents and derive over 25% of their gross revenue from the sale of "personal data."



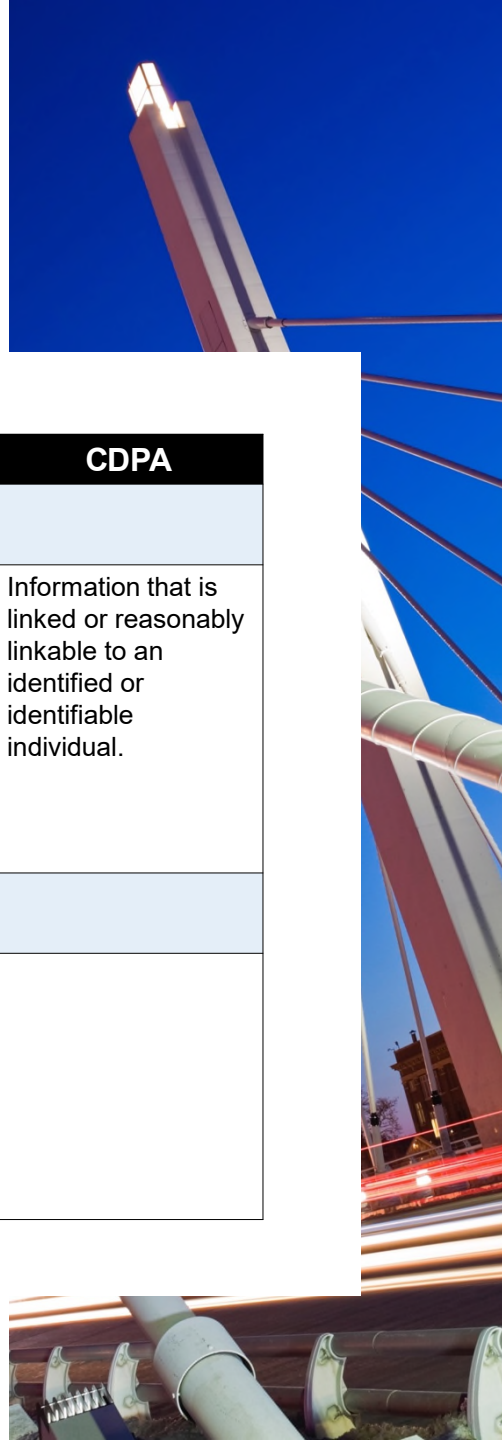
European and U.S. Privacy Laws
Key Exempted Entities

	GDPR	CCPA	CPRA	VCDPA	CPA	UCPA	CDPA
Public sector	X	✓	✓	✓	X	✓	✓
Non-profits	X	✓	✓	✓	X	✓	✓
GLBA	X	X	X	✓ *(financial institutions)*	✓ *(financial institutions and affiliates)*	✓ *(financial institutions and affiliates)*	✓ *(financial institutions)*
HIPAA CEs/Bas	X	✓	✓	✓	✓	✓	✓
Higher education institutions	X	X	X	✓	X	✓	✓
National securities association	X	X	X	X	✓	X	✓



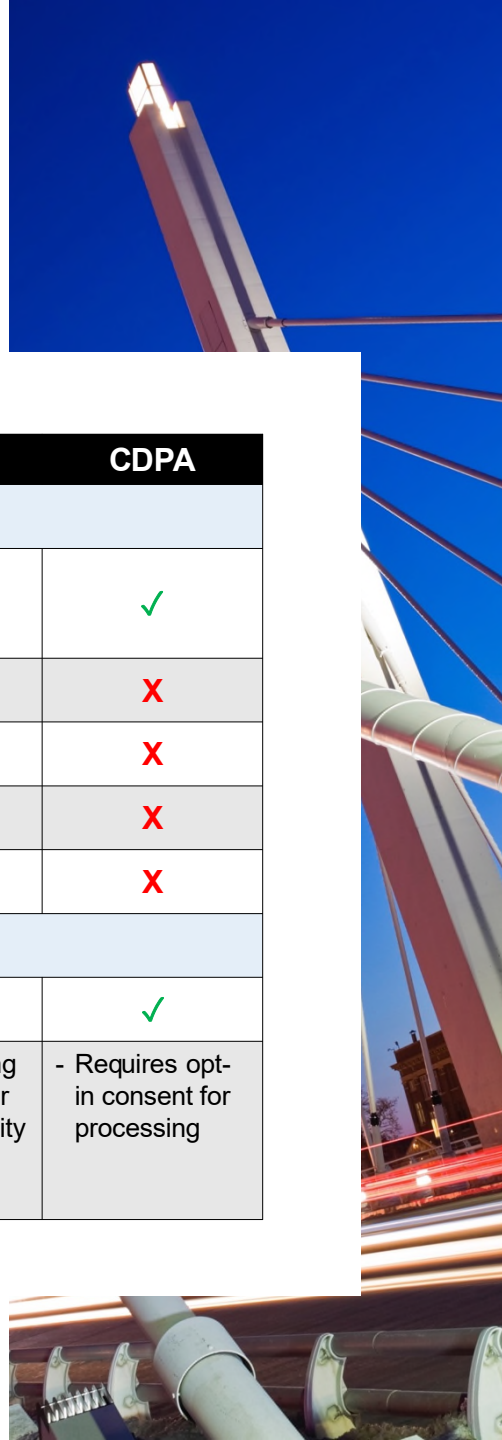
European and U.S. Privacy Laws

Protected Data and Exempted Data (Overview)



GDPR	CCPA	CPRA	VCDPA	CPA	UPCA	CDPA
Personal Data or Information Defined:						
Personal data means any information relating to an identified or identifiable natural person ("data subject").	Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.	Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.	Information that is linked or reasonably linkable to an identified or identifiable individual.	Information that is linked or reasonably linkable to an identified or identifiable individual.	Information that is linked or reasonably linkable to an identified or identifiable individual.	Information that is linked or reasonably linkable to an identified or identifiable individual.
Exempted Data:						
Certain states exempt various types of data as well, including but not limited to: - FERPA-regulated data; - FCRA-regulated data; - COPPA-regulated data; - HIPAA deidentified data; and - Personal data collected, processed, sold, or disclosed pursuant to the GLBA and Driver's Privacy Protection Act of 1994.						

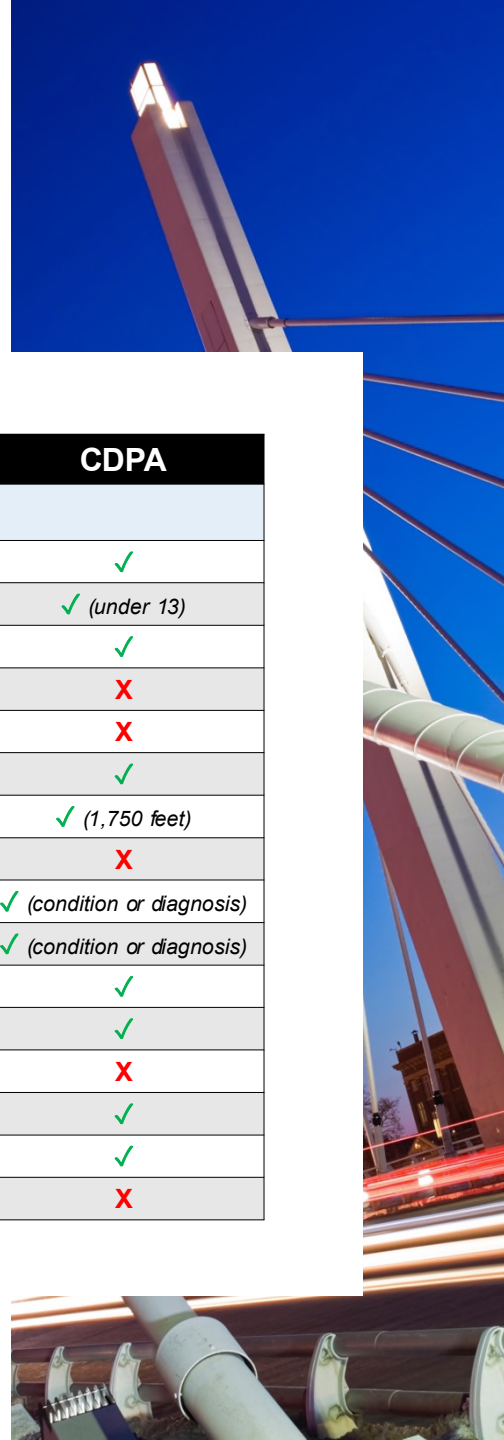
European and U.S. Privacy Laws
Protected Data



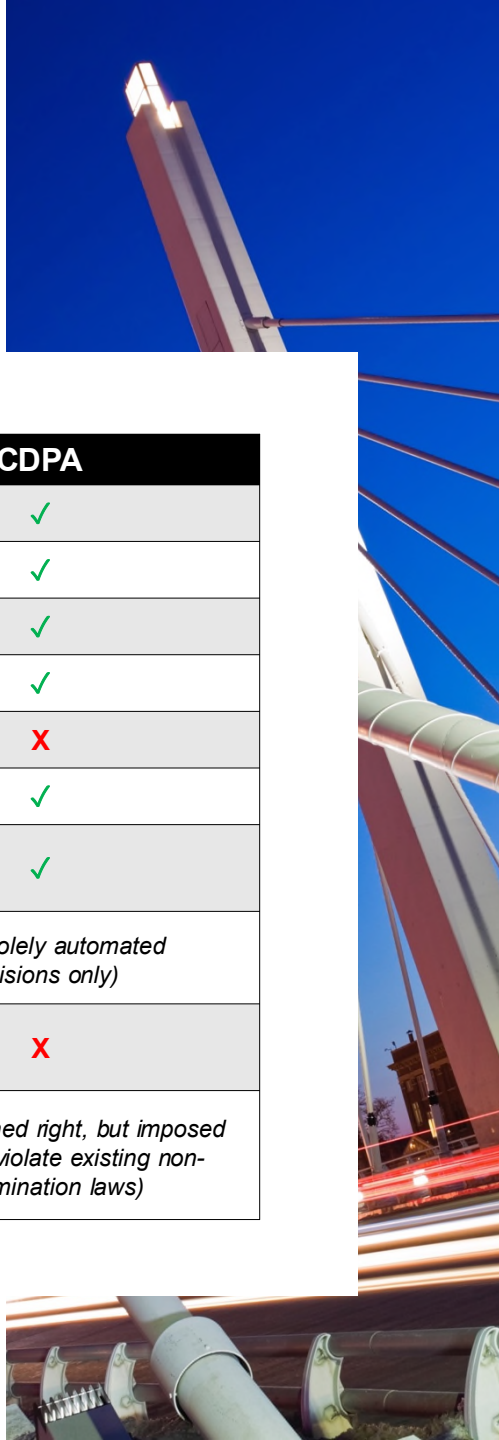
	GDPR	CCPA	CPRA	VCDPA	CPA	UPCA	CDPA
Protected data generally:							
Broad definition of "personal data" or "personal information"	✓	✓	✓	✓	✓	✓	✓
Includes publicly available data	✓	X	X	X	X	X	X
Includes de-identified data	X	X	X	X	X	X	X
Includes B2B data	✓	X	✓	X	X	X	X
Includes employment data	✓	X	✓	X	X	X	X
Sensitive data generally:							
Defined category	✓	X	✓	✓	✓	✓	✓
Heightened protections	- Processing prohibited unless a GDPR Article 9 condition is met	N/A	- Purpose limitations for collection and use - Consumers have a right to limit use and disclosure	- Requires opt-in consent for processing	- Requires opt-in consent for processing	- Requires first presenting the consumer with clear notice and an opportunity to opt-out of the processing	- Requires opt-in consent for processing

European and U.S. Privacy Laws
Sensitive Data

	GDPR	CCPA	CPRA	VCDPA	CPA	UCPA	CDPA
Sensitive data includes:							
Biometric data	✓	N/A	✓	✓	✓	✓	✓
Children's data	X	N/A	X *(under 16)*	✓ *(under 13)*	✓ *(under 13)*	X *(under 13)*	✓ *(under 13)*
Citizenship status	X	N/A	X	✓	✓	✓	✓
Electronic communications	X	N/A	✓ *(content of)*	X	X	X	X
Financial account information	X	N/A	✓ *(credentials or access to)*	X	X	X	X
Genetic data	✓	N/A	✓	✓	✓	✓	✓
Precise/specific geolocation data	X	N/A	✓ *(1,850 feet)*	✓ *(1,750 feet)*	X	✓ *(1,750 feet)*	✓ *(1,750 feet)*
Government ID	X	N/A	✓	X	X	X	X
Mental health	✓	N/A	✓	✓ *(diagnosis)*	✓ *(condition or diagnosis)*	✓ *(medical history, condition, treatment, or diagnosis)*	✓ *(condition or diagnosis)*
Physical health	✓	N/A	✓	✓ *(diagnosis)*	✓ *(condition or diagnosis)*	✓ *(medical history, condition, treatment, or diagnosis)*	✓ *(condition or diagnosis)*
Race/ethnicity	✓	N/A	✓	✓	✓	✓	✓
Religious beliefs	✓	N/A	✓	✓	✓	✓	✓
Philosophical beliefs	✓	N/A	✓	X	X	X	X
Sex life	✓	N/A	✓	X	✓	X	✓
Sexual orientation	✓	N/A	✓	✓	✓	✓	✓
Union membership	✓	N/A	✓	X	X	X	X



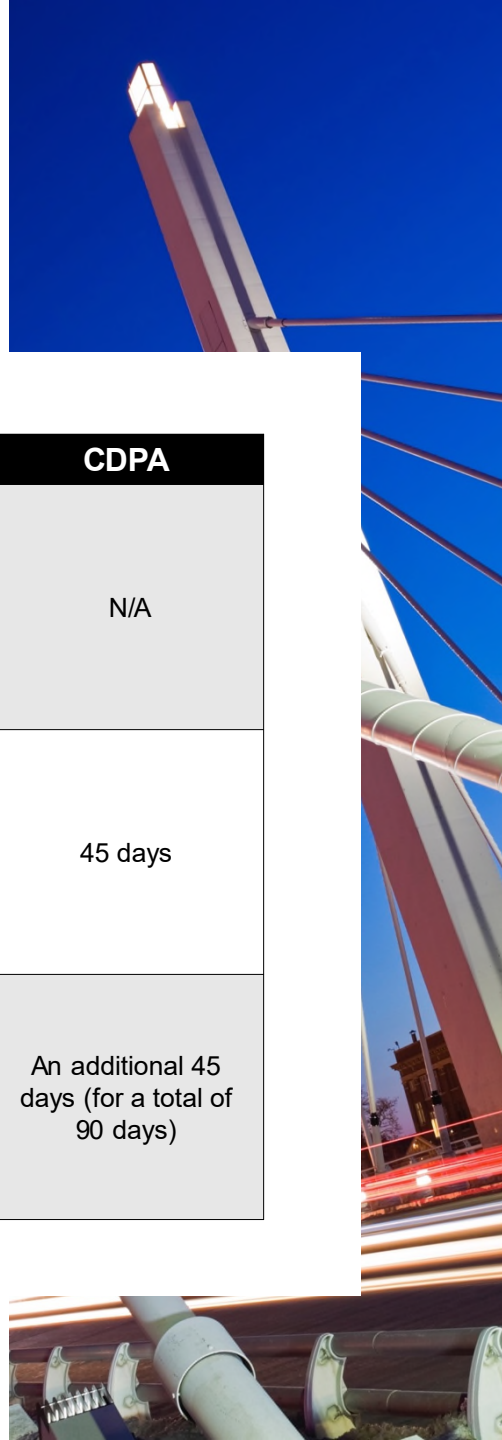
European and U.S. Privacy Laws
Consumer Rights



	GDPR	CCPA	CPRA	VCDPA	CPA	UCPA	CDPA
Right to know/access	✓	✓	✓	✓	✓	✓	✓
Right to data portability	✓	✓	✓	✓	✓	✓	✓
Right to delete	✓	✓	✓	✓	✓	✓	✓
Right to rectify/correct	✓	X	✓	✓	✓	X	✓
Right to limit use of data	✓	X	✓ *(sensitive PI only)*	X	X	X	X
Right to opt-out of sale	✓ *(implied)*	✓	✓	✓	✓	✓	✓
Right to opt-out of "sharing" or processing for "targeted advertising"	✓ *(implied)*	X	✓	✓	✓	✓	✓
Right to opt-out of profiling	✓	✓	✓	✓	✓	X	✓ *(for solely automated decisions only)*
Right to opt-out of or object to automated decision making	✓	X	✓	X	X	X	X
Right to non-discrimination	✓ *(implied)*	✓	✓	✓	✓ *(not a defined right, but imposed duty to not violate existing non-discrimination laws)*	✓	✓ *(not a defined right, but imposed duty to not violate existing non-discrimination laws)*

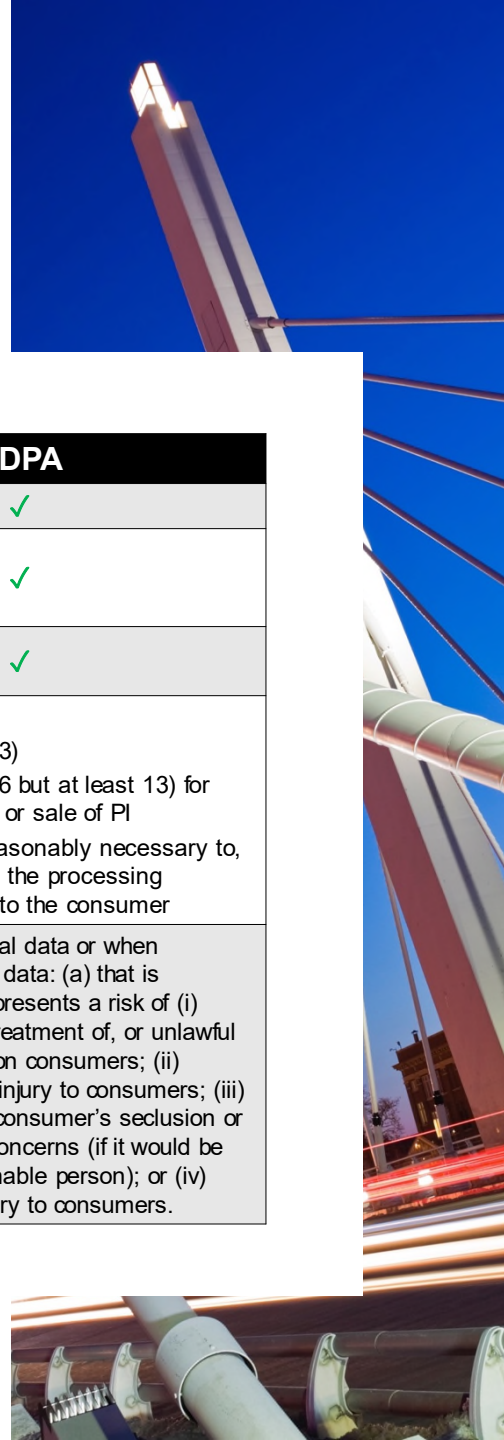
European and U.S. Privacy Laws
Requirements for Consumer Right Requests

	GDPR	CCPA	CPRA	VCDPA	CPA	UCPA	CDPA
Required acknowledgement period	N/A	10 days	10 days	N/A	N/A	N/A	N/A
Statutory response period	One calendar month	45 days	45 days	45 days	45 days	45 days	45 days
Prolonged response period when permitted	Maximum of three calendar months	An additional 45 days (for a total of 90 days)	An additional 45 days (for a total of 90 days)	An additional 45 days (for a total of 90 days)	An additional 45 days (for a total of 90 days)	An additional 45 days (for a total of 90 days)	An additional 45 days (for a total of 90 days)



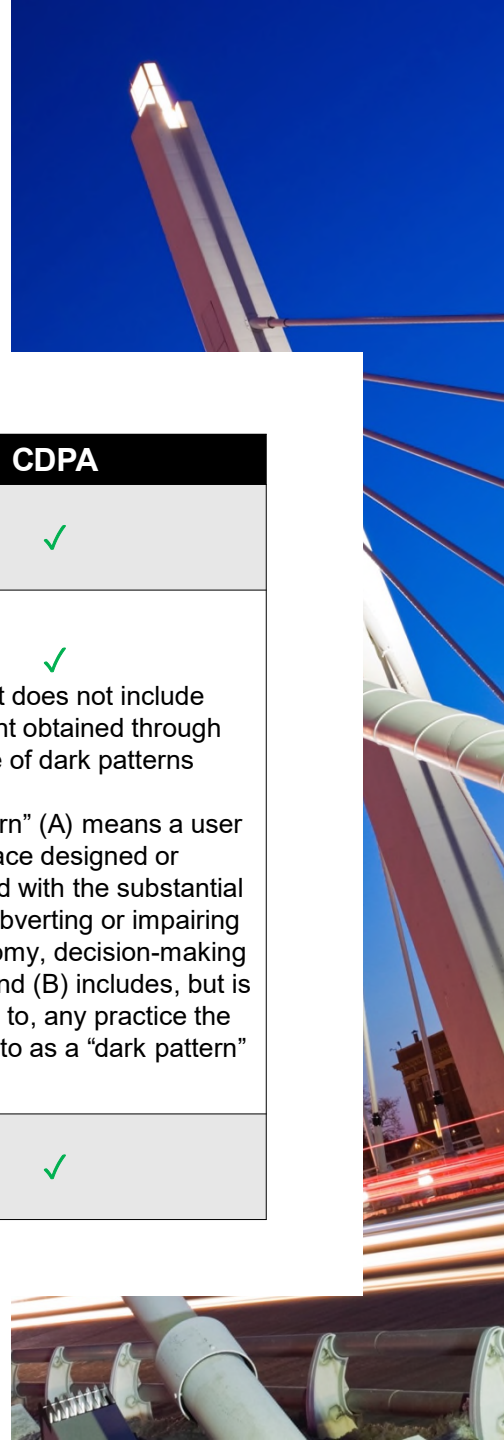
European and U.S. Privacy Laws
Business Obligations

	GDPR	CCPA	CPRA	VCDPA	CPA	UCPA	CDPA
Be transparent	✓	✓	✓	✓	✓	✓	✓
Specify purpose for collection/ processing	✓	✓	✓	✓	✓	✓	✓
Minimize data collection	✓	X	✓	✓	✓	X	✓
Obtain opt-in consent for processing	When consent is the lawful basis for processing	For minors, those who have previously opted-out, and upon entry into a financial incentive program	For minors at least 13 years of age and upon entry into a financial incentive program	For sensitive data	For sensitive data	For minors (under 13)	For sensitive data For minors (under 13) For minors (under 16 but at least 13) for targeted advertising or sale of PI For purposes not reasonably necessary to, nor compatible with, the processing purposes disclosed to the consumer
Conduct risk assessments/ Data Protection Assessments (DPA)	When processing is likely to result in a high risk to the rights and freedoms of natural persons	X	When processing presents significant risk to consumers' privacy or security	When selling personal data or when processing personal data: (a) that is sensitive; (b) for targeted advertising/profiling; or (c) that presents a heightened risk of harm to consumers	When selling personal data or when processing personal data: (a) that is sensitive or (b) that presents a risk of (i) unfair or deceptive treatment of, or unlawful or disparate impact on consumers; (ii) financial or physical injury to consumers; (iii) an intrusion upon a consumer's seclusion or their private affairs/concerns (if it would be offensive to a reasonable person); or (iv) other substantial injury to consumers.	X	When selling personal data or when processing personal data: (a) that is sensitive or (b) that presents a risk of (i) unfair or deceptive treatment of, or unlawful or disparate impact on consumers; (ii) financial or physical injury to consumers; (iii) an intrusion upon a consumer's seclusion or their private affairs/concerns (if it would be offensive to a reasonable person); or (iv) other substantial injury to consumers.



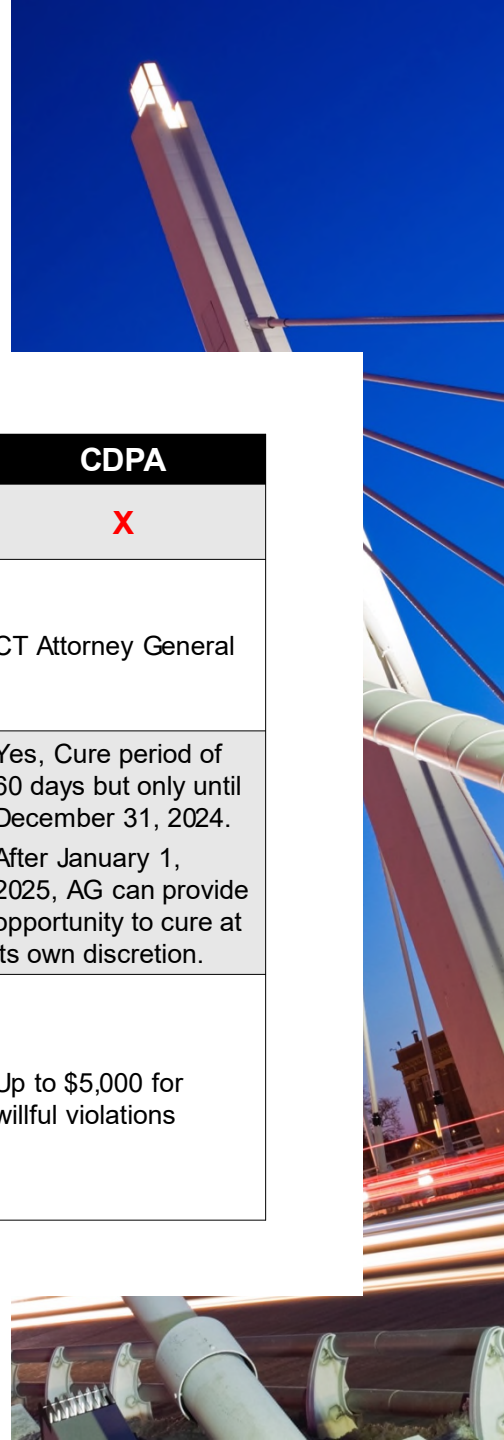
European and U.S. Privacy Laws
Business Obligations *(cont'd.)*

	GDPR	CCPA	CPRA	VCDPA	CPA	UCPA	CDPA
Implement data security practices	✓	✓	✓	✓	✓	✓	✓
Avoid dark patterns to obtain consumer consent	Not specifically mentioned, but implied in various EU jurisdictions	X	✓ Any agreement obtained through the use of dark patterns shall not constitute consumer consent "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation	X	✓ Consent does not include agreement obtained through the use of dark patterns "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice	X	✓ Consent does not include agreement obtained through the use of dark patterns "Dark pattern" (A) means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and (B) includes, but is not limited to, any practice the FTC refers to as a "dark pattern"
Data processing/ vendor agreement	✓	✓	✓	✓	✓	✓	✓



European and U.S. Privacy Laws
Enforcement

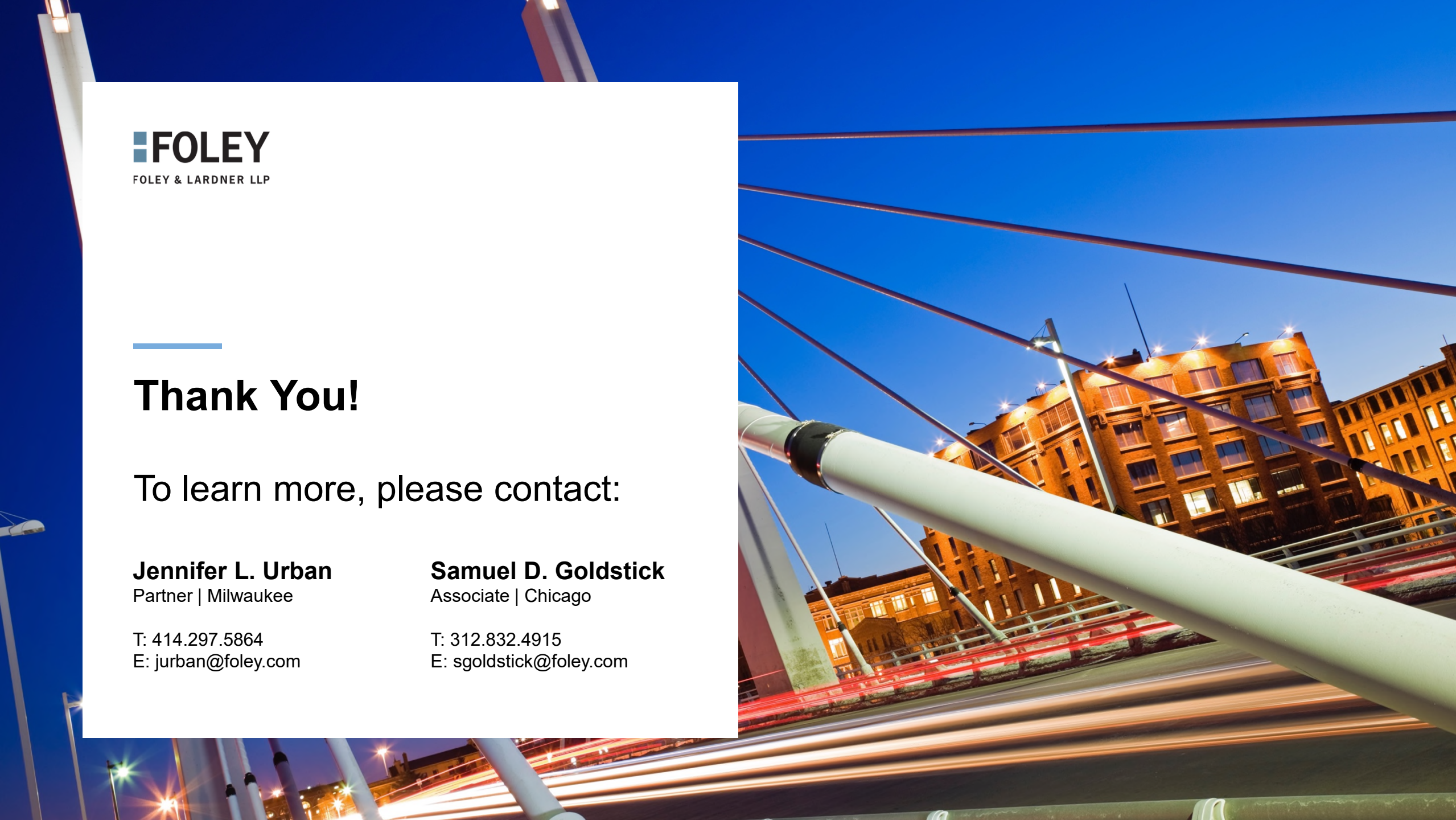
	GDPR	CCPA	CPRA	VCDPA	CPA	UCPA	CDPA
Private right of action	✓	Only for security breaches	Only for security breaches	X	X	X	X
Regulatory authority	EU Supervisory Authorities	CA Attorney General	CA Attorney General and CA Privacy Protection Agency (CPPA)	VA Attorney General	CO Attorney General and District Attorneys	UT Attorney General and UT Consumer Privacy Division (to be established)	CT Attorney General
Opportunity to cure violations	X	Yes, for actions brought by consumers and the AG. Cure period of 30 days.	Yes, but in the context of administrative actions, only at the CPPA's discretion. Cure period of 30 days for consumer actions only.	Yes, cure period of 30 days.	Yes, but only until Jan. 1, 2025. Cure period of 60 days.	Yes, cure period of 30 days.	Yes, Cure period of 60 days but only until December 31, 2024. After January 1, 2025, AG can provide opportunity to cure at its own discretion.
Fines for violations	Up to €20 million or 4% of total worldwide revenue	- Consumers: Actual damages or up to $750 per consumer per incident - AG: up to $2,500/$7,500 per unintentional/ intentional violation	- Consumers: Actual damages or up to $750 per consumer per incident - AG/CPPA: Up to $2,500/$7,500 per unintentional/intentional violation (or each violation involving the personal information of minor consumers)	Up to $7,500 per violation	Up to $20,000 per violation (CPA violations constitute deceptive trade practices under Colorado law)	Actual damages to affected consumers and up to $7,500 per violation	Up to $5,000 for willful violations



FOLEY

FOLEY & LARDNER LLP

Questions?



FOLEY

FOLEY & LARDNER LLP

Thank You!

To learn more, please contact:

Jennifer L. Urban
Partner | Milwaukee

T: 414.297.5864
E: jurban@foley.com

Samuel D. Goldstick
Associate | Chicago

T: 312.832.4915
E: sgoldstick@foley.com

About Foley

Foley & Lardner LLP is a preeminent law firm that stands at the nexus of the energy, health care and life sciences, innovative technology, and manufacturing sectors. We look beyond the law to focus on the constantly evolving demands facing our clients and act as trusted business advisors to deliver creative, practical, and effective solutions. Our 1,100 lawyers across 25 offices worldwide partner on the full range of engagements from corporate counsel to IP work and litigation support, providing our clients with a one-team solution to all their needs. For nearly two centuries, Foley has maintained its commitment to the highest level of innovative legal services and to the stewardship of our people, firm, clients, and the communities we serve.

FOLEY

FOLEY & LARDNER LLP

FOLEY.COM