



The Changing Cybersecurity Threat Landscape: Understanding the Legal Perspective

Jordan L. Fischer, Esq.,
CIPP/US, CIPP/E, CIPM



Agenda

Data Security & Privacy Overview

Global Data Security & Privacy

CCPA & CPRA

Virginia Consumer Data Privacy Act

Cybersecurity Trends

Creating a Cross-Regulatory Program

Questions

About Beckage

- Law firm focused on technology and data security and privacy.
- Clients are global brands and publicly traded companies.
- Beckage team includes lawyers who are also technologists, tech business owners, Certified Information Privacy Professionals by the International Association of Privacy Professionals (IAPP), former federal regulators (AUSA, DOJ), Chief Information Security Officer (CISO), and former public-company executive.
- **Regulatory Compliance** – Policy drafting, contract review, training and tabletop exercises.
- **Incident Response** – Help mitigate legal risk in breach response and identify and coordinate legal notifications and reporting obligations.
- **Litigation** – Represent clients in federal and state technology, data breach and privacy litigations and putative class actions, and during audits and investigations.
- **Risk Management** – Work with clients to evaluate IT network and enterprise from a legal and risk management perspective.
- **Software & Tech IP** – Engage with clients to develop a strategic use of patents, trademarks, copyrights, and trade secrets to protect your most valuable assets. With particular focus on tech IP, Beckage provides counsel on IP needs.
- Beckage is a NYS Certified Women-Owned Business Enterprise (WBE).

Certifications & Recognitions





ABOUT THE PRESENTERS

Jordan L. Fischer, Esq., CIPP/US, CIPP/E, CIPM

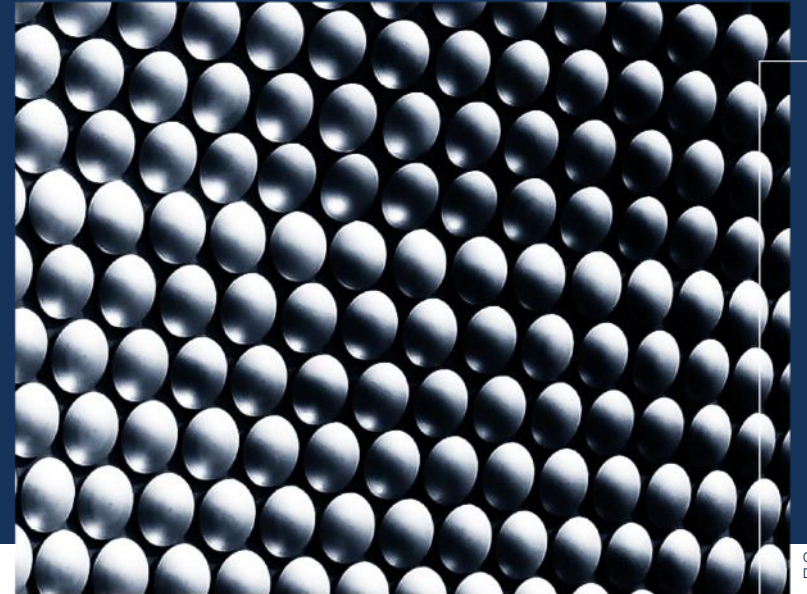
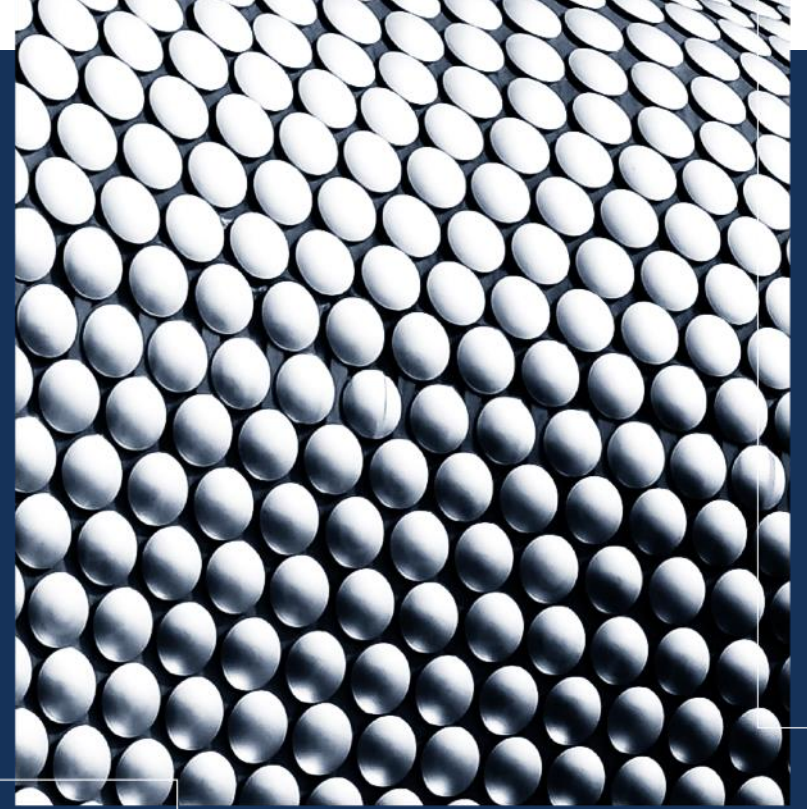
Email: jfischer@beckage.com

Cell: (267) 536-9376

- A Certified Information Privacy Professional for Europe (CIPP/E) and a Certified Information Privacy Professional for the United States (CIPP/US), as well as a Certified Information Privacy Manager (CIPM), as certified by the International Association of Privacy Professionals (IAPP).
- Beckage Global Data Privacy Practice Group Leader
- Counsels clients on the diverse global data protection laws, including the EU's General Data Protection Regulation and Asia Data Privacy Regulations
- Develops international cyber and privacy compliance programs
- Recognized as a Pennsylvania Super Lawyers Rising Star in Technology Law in 2019 and 2020
- Cited in national media including *The New York Times*, *NPR*, and *NBC News*
- Former Clerk on the Court of Justice for the European Union
- Current Associate Professor of Law at Drexel University and Cybersecurity Lecture at UC Berkeley

01.

Data Security & Privacy Overview



Legal Landscape – Data Privacy



International

European Union's GDPR; and the "GDPR Effect"



Federal

Focused on industry/data collected

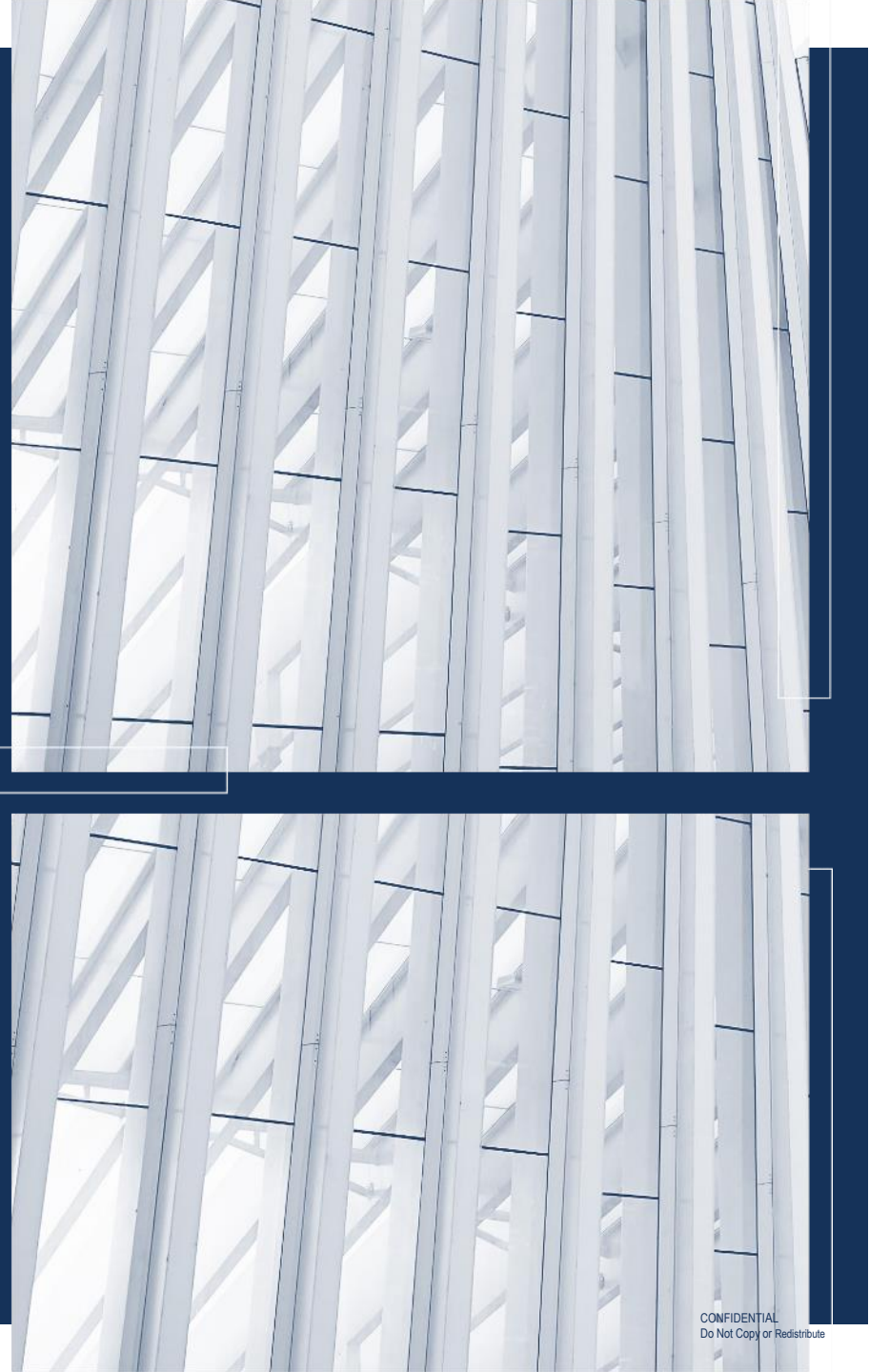


State

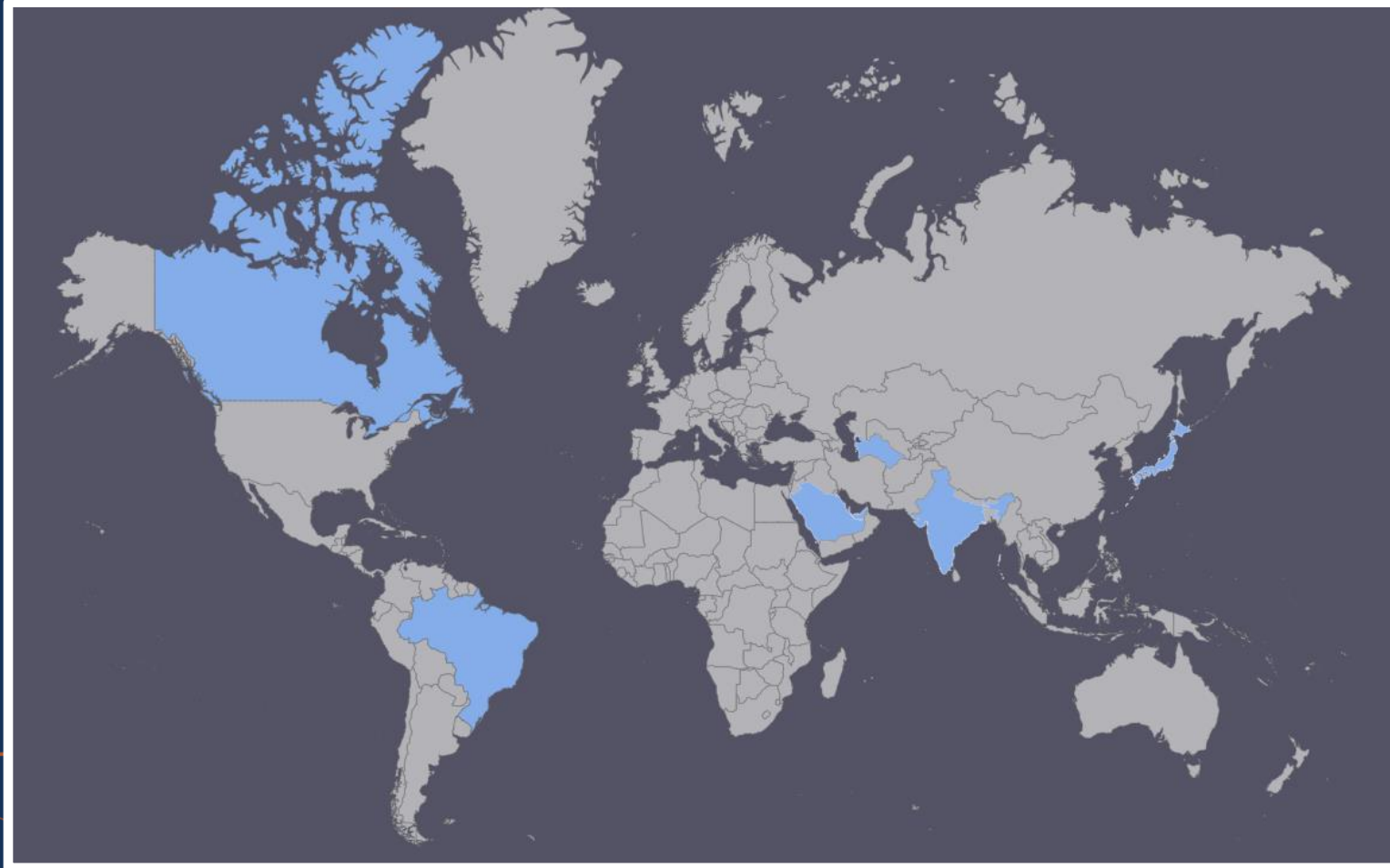
Patchwork of laws CCPA / CPRA and other emerging state privacy laws

02.

Global Data Security & Privacy Landscape



The "GDPR Effect"



...and the list keeps growing!

Legal Landscape – Privacy – International

Cross-Border Data Transfers after *Schrems II*

- The invalidation of the EU-US Privacy Shield
- “Supplemental Measures” under the Standard Contractual Clauses

Future of Cross-Border Data Transfers

- Updates to the Standard Contractual Clauses (SCCs)
- On-going negotiations between EU and US

Member State Trends



CNIL Cookie Guidance

Key Recommendations:

- Cookie walls are not banned per se, but evaluated on a case-by-case basis;
- Website providers must clearly inform users about the purposes behind the use of cookies;
- Consent must be clear affirmative action;
- Refusal of online trackers must be easy and not subject to complex procedures;
- Users must be able to withdraw their consent to the use of cookies at any time; and
- Exempt trackers include those used for authentication of users or which preserve the content of an online shopping cart.

Employee Data

- Employee surveillance & monitoring is a top concern.
 - Transparency
 - Consent
 - Legitimate Business Interest
- Risk → inherent imbalance of power between employer and employee

Tech

BBC

H&M fined for breaking GDPR over employee surveillance

🕒 5 October 2020



European Data Protection Board

Norwegian DPA issues fine to Cyberbook AS

🕒 Thursday, 11 February, 2021

GDPR Breaches & Enforcement

The New York Times

*After a Data Breach, British Airways
Faces a Record Fine*

Forbes

Oct 30, 2020, 06:44am EDT | 816 views

**Marriott Hit With £18.4 Million
GDPR Fine Over Massive 2018 Data
Breach**

Source: AFP/Getty

Cybersecurity

**European Institutions Were Targeted in a
Cyber-Attack Last Week**

By [Alberto Nardelli](#) and [Natalia Drozdak](#)

April 6, 2021, 9:51 AM EDT

Privacy Litigation: GDPR

Historically, the EU is not a litigious region.
But that is changing...

- Regulatory Fines:
 - 4% of Global Revenue, or
 - 20 million euros, *whichever is higher*
- Private Lawsuits
 - Private Right of Action
 - Class action lawsuits are becoming more common
 - B2B Litigation

TECH

Twitter Fined for Breaking EU Privacy Law in First for U.S. Tech Firm

\$546,000 fine for late notification of a data breach took nearly two years to decide

British Airways faces \$230 million fine. It would be a record under Europe's tough data privacy law

By Charles Riley, CNN Business
Updated 11:00 AM EDT, Mon July 8, 2019

03.

US Legal Privacy & Security Overview



Legal Landscape – United States Data Privacy

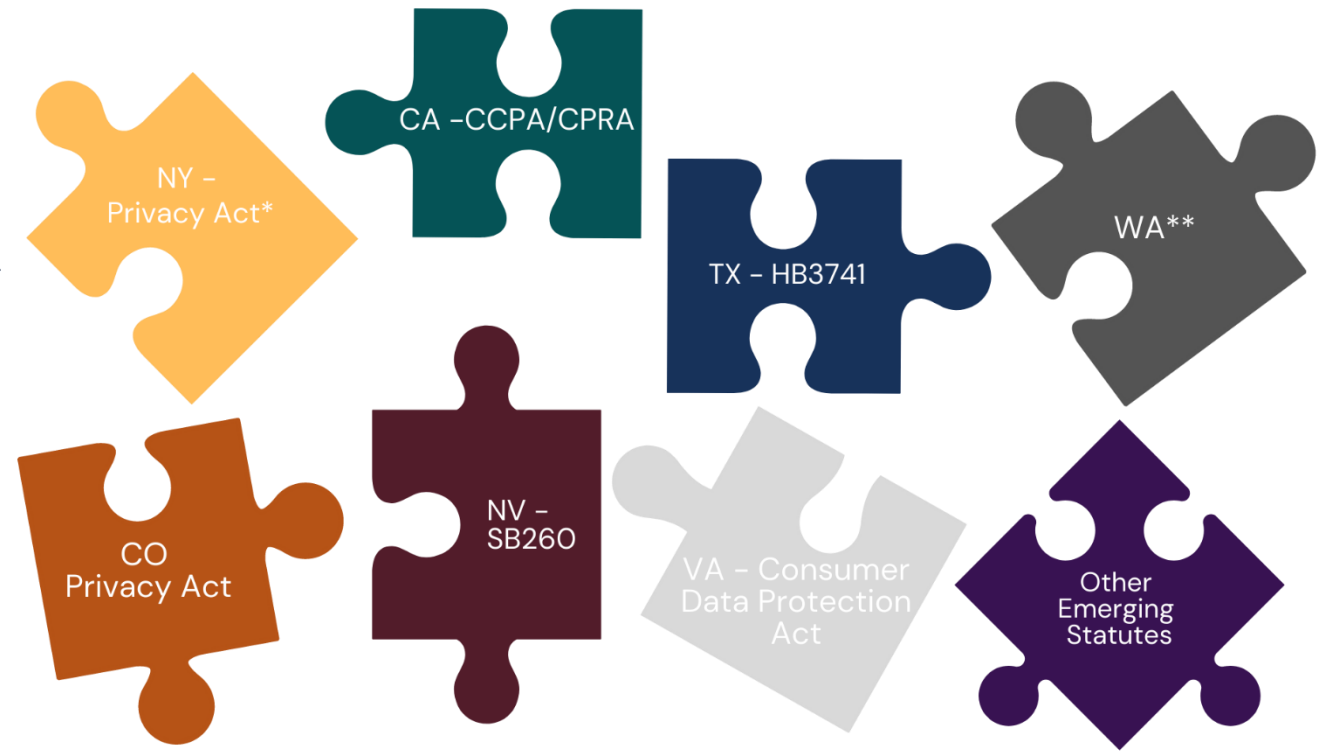
United States has not yet adopted a federal privacy scheme.

How the United States Addresses Privacy



Legal Landscape – United States Data Privacy

Where there is no federal privacy scheme, the States are creating their own privacy laws. It is a patchwork of laws:



* No action taken before Senate adjournment 2021

** Privacy bill has failed three times

Legal Landscape – Emerging Laws

Service Provider Inclusion & Limitations:

Identifying who is a Service Provider, and liability provisions around that relationship.

Exceptions for De-Identified/Aggregated Information:

Some states have made de-identified/aggregated data an exception to the definition of PI if certain steps and standards are followed in de-identifying or aggregating (much like HIPAA).

Employee Data:

Split in whether emerging State laws consider employee data PI.

Fiduciary Duty:

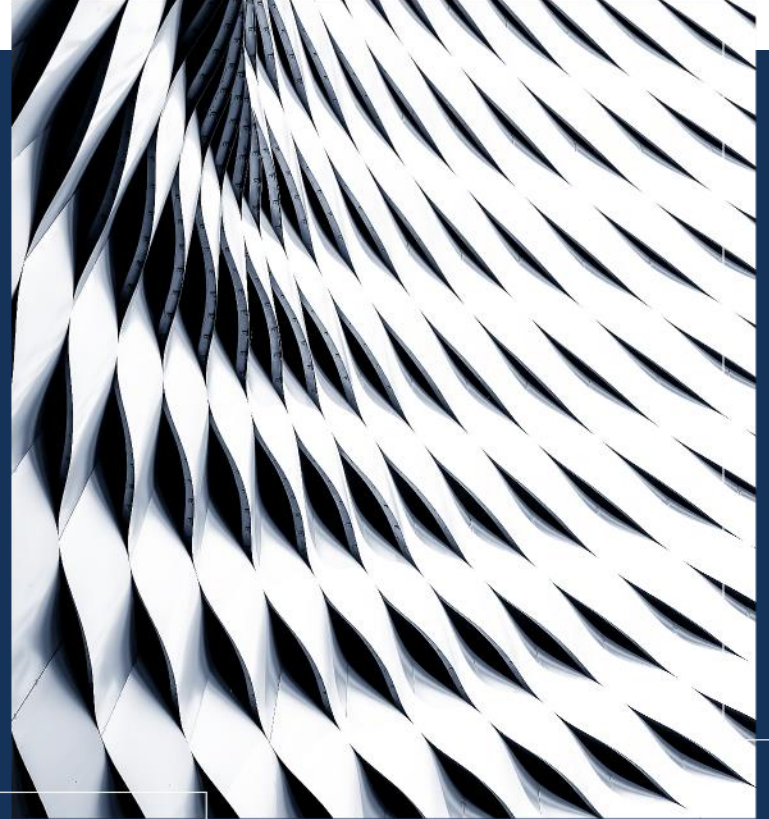
New York attempted to propose a fiduciary duty for businesses regarding their collection, processing and storage of PI. Pennsylvania found a duty in *Dittman v. UPMC*.

Facial Recognition:

States and cities are increasingly regulating the use of facial recognition as is the FTC (see current law, Illinois BIPA).

04.

CPPA & CPRA Overview



Overview of the CCPA

The CCPA applies to the collection of private information related to a “consumer.”

Consumer: A “natural person who is a California resident.”

- Includes every person who is:
 - In California for a purpose other than a temporary or transitory
 - Lives in California, but is outside the state for a temporary or transitory purpose

Businesses Subject to the CCPA

The CCPA Applies to California Businesses that:

Have a gross
revenues exceeding
\$25 million

Buys, receives, sells,
or shares personal
information of more
than 100,000
consumers,
households, or devices

Derives 50% or
more of its annual
revenues from
selling consumers'
personal information

CCPA Definition of Personal Information

Person Information: “[I]nformation 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.”

Includes

Biometric
Information

Internet
Network
Activity

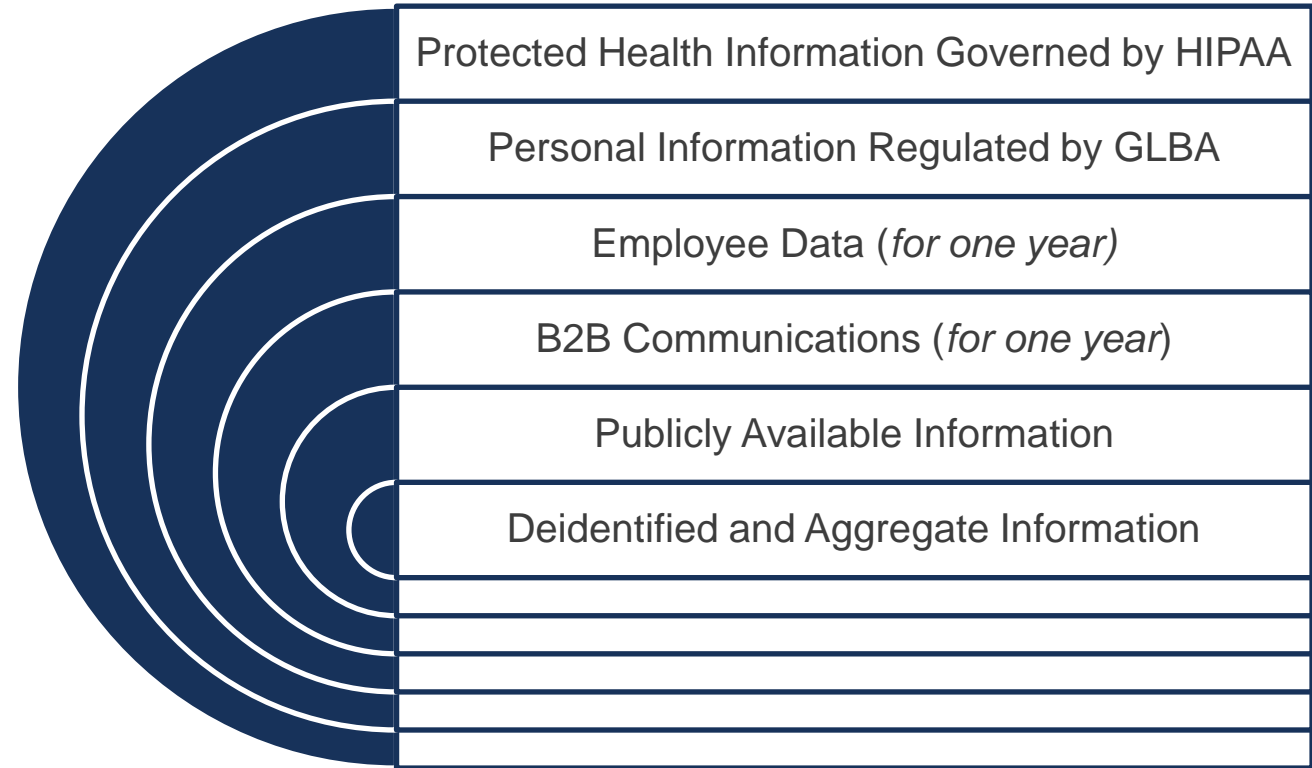
Geolocation
Data

Education
Information

Passport
Numbers


Exempted Data

Information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device.



Deidentified Data

Information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business:



Has implemented technical safeguards that prohibit re-identification of the consumer to whom the information may pertain.
Has implemented business processes that specifically prohibit re-identification of the information.
Has implemented business processes to prevent inadvertent release of deidentified information.
Makes no attempt to re-identify the information.

Collecting vs. Selling Personal Information

Collection: Buying, renting, gathering, obtaining, receiving or even accessing personal information, by any means, whether actively or passively, including by observing a consumer's behavior.

Sale: Selling, renting, releasing, disclosing, disseminating, making available, transferring, or communicating personal information orally, in writing, or by electronic or other means for monetary or other valuable consideration.

- Exclusions for consumer consent; conveying a consumer's opt-out instructions to a third party; or data transfers in the course of mergers, acquisitions, bankruptcies and the like, and for a business purpose.

Website Requirements

Privacy Notice that includes:

- Description of consumer information;
- List of categories of personal information collected in preceding 12 months;
- List of categories of personal information sold in the preceding 12 months;
- List of categories of personal information disclosed in the preceding 12 months;

Review & Update Privacy Notice at least once every 12 months.

A clear and conspicuous link titled “**Do Not Sell My Personal Information**,” to a webpage that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer’s personal information.

Rights Under the CCPA

Right to request that a business disclose the categories of personal information it has collected about a consumer.

Right to request that a business disclose to the consumer the categories of personal information that the business has sold/disclosed and the identity of the third parties to whom such personal information was sold/disclosed.

Right to opt-out of a business's sale of personal information about the consumer.

Right to equal service and price, so that a business is prohibited from discriminating against a consumer because of that consumer's exercise of her rights under the CCPA.

Right to deletion of any personal information about the consumer which the business has collected.

Exemptions to the Right to Deletion

Complete the transaction

Detect and protect against security threats

Debug and repair errors

Exercise free speech

Comply with California Communications Privacy Act

Scientific, historical, or statistical research

Internal purposes “reasonably” aligned with consumer expectations

Comply with legal obligation

Otherwise lawful manner

Verifiable Consumer Request

1. Consumer
Request
Received

2.
Verification
of Request

3. Confirm
Receipt of
Request

Entire Timeline: 45 DAYS

4. Review
of Data

5. Review of
Service
Providers /
Third Parties

6.
Responding
to Request

Verifiable Consumer Request

“Verifiable consumer request”:

- A request made by the consumer that a business can reasonably verify.
- Consumers may submit requests through mail, email, internet web page, internet web portals, and toll-free phone numbers.

Consumers can request:

- The categories and specific pieces of personal information collected about them,
- The categories of sources from which the information was collected,
- The business purpose for collecting or selling the information, and
- The categories of third parties with which the information is shared.

CCPA Violations

There was no “Do Not Sell My Personal Information” link on the business's website.



The business maintained a non-compliant opt-out process.



The business had defective methods for consumers to submit data subject access requests, provided untimely responses to requests, or charged fees for processing the requests.



Frequently Alleged CCPA Violations



The Notice to Consumers was lacking or inaccurate, lacked the required notice of sale of personal information and notice regarding the minor's personal information.



The Privacy Policy failed to provide the required request methods for exercising rights, charging fees for the CCPA, and lacked a toll-free number.



The business failed to obtain the proper verification information when processing data subject requests or required the creation of a customer account to verify identification.

CCPA Violations Examples

A business that manufactures and sells cars failed to notify consumers of the use of personal information when collecting personal information from consumers seeking to test drive vehicles at a dealership location, in addition to other omissions in its privacy policy. After being notified of alleged noncompliance, the business implemented a notice at collection for personal information received in connection with test drives and updated its privacy policy to include required information.

A grocery chain required consumers to provide personal information in exchange for participation in its company loyalty programs. The company did not provide a Notice of Financial Incentive to participating consumers. After being notified of alleged noncompliance, the company amended its privacy policy to include a Notice of Financial Incentive.

A social media app was not timely responding to CCPA requests, and users publicly complained that they were not receiving notice that their CCPA requests had been received or effectuated. The business explained its response processes and submitted detailed plans showing that it updated its CCPA consumer response procedures to include timely receipt confirmations and responses to future requests.

A social media app was not timely responding to CCPA requests, and users publicly complained that they were not receiving notice that their CCPA requests had been received or effectuated. The business explained its response processes and submitted detailed plans showing that it updated its CCPA consumer response procedures to include timely receipt confirmations and responses to future requests.

Source: CA AG Enforcement Update
July 19, 2021

California Privacy Rights Act

The CPRA was adopted via the November 2020 ballot initiative and goes into effect January 1, 2023.

Key Provisions:

Establish the California Privacy Protection Agency (“CPPA”)

Defines “sensitive personal information” stricter than personal information

Creates new obligations for companies and organizations processing sensitive personal information. It would also allow consumers to limit the use and disclosure of their sensitive personal information.

Additional Consumer Rights

Expanded Moratorium for Employee Data until January 1, 2023

Expanded Breach Liability

CPRA: Additional Consumer Rights

Additional Consumer Rights

Right to correct

Right to know length of data retention

Right to opt-out of geolocation utilization

Right to limit business from collecting more data than necessary

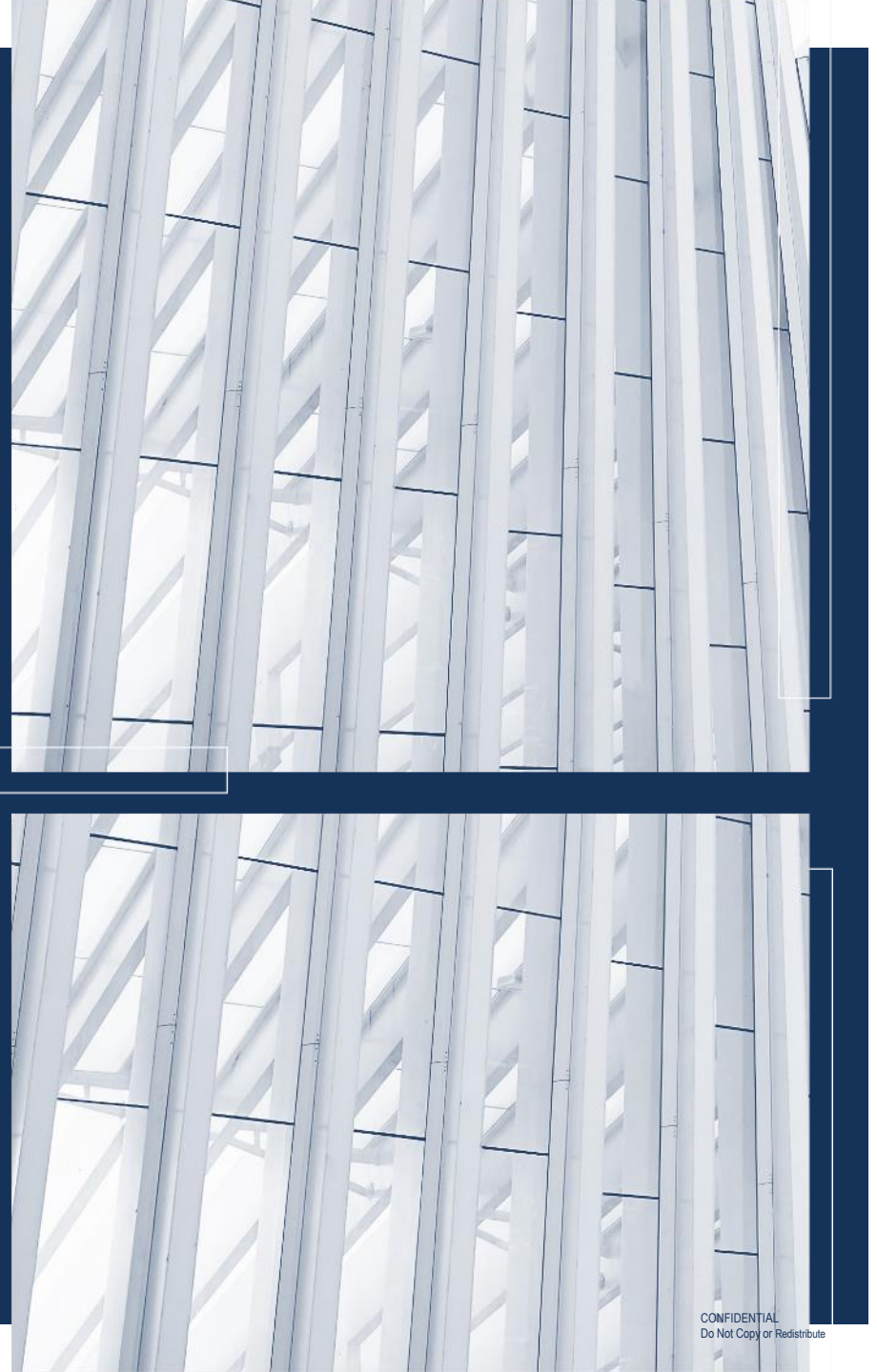
Right to restrict how sensitive personal information is used

Right to know what personal information is sold or shared and to whom


Right to prevent retaliation for exercising privacy rights

05.

Virginia Consumer Data Privacy Act



Virginia's VCDPA



The Virginia Consumer Data Protection Act was signed into law on March 2, 2021, and goes into effect on January 1, 2023.

Adopts GDPR definitions of “Personal Data”, “Controllers,” and “Processors”

Similar data rights

Scope of VCDPA

The VCDPA applies to organizations that :

Conduct business in the
commonwealth of Virginia

OR

Produce products or
services that are targeted
to Virginia residents

AND, during a calendar year:

Control or process
personal data of at least
100,000 Virginia residents

OR

Derive over 50% of gross
revenue from the sale of
personal data and control
or process personal data of
at least 25,000 Virginia
residents

Virginia's VCDPA: Key Definitions

"**Consumer**" is defined as "a natural person who is a resident of the Commonwealth acting only in an individual or household context."

- Expressly excludes employees

"**Personal Information**" is defined as any information that is linked or reasonably linkable to an identified or identifiable natural person.

- "Personal data" does not include de-identified data or publicly available information.

"**Publicly available information**" means information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

"**Sensitive data**" means a category of personal data that includes:

1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;
2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;
3. The personal data collected from a known child; or
4. Precise geolocation data.

Virginia's VCDPA: Exempted Entities

- A body, authority, board, bureau, commission, district, or Virginian agency or any Virginian political subdivision.
- Any financial institution or data subject to the Gramm-Leach-Bliley Act.
- A covered entity or business subject to the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act.
- A nonprofit organization.
- An institution of higher education.

VCDPA: Consumer Data Rights



Right to access.

Right to correct.

Right to delete.

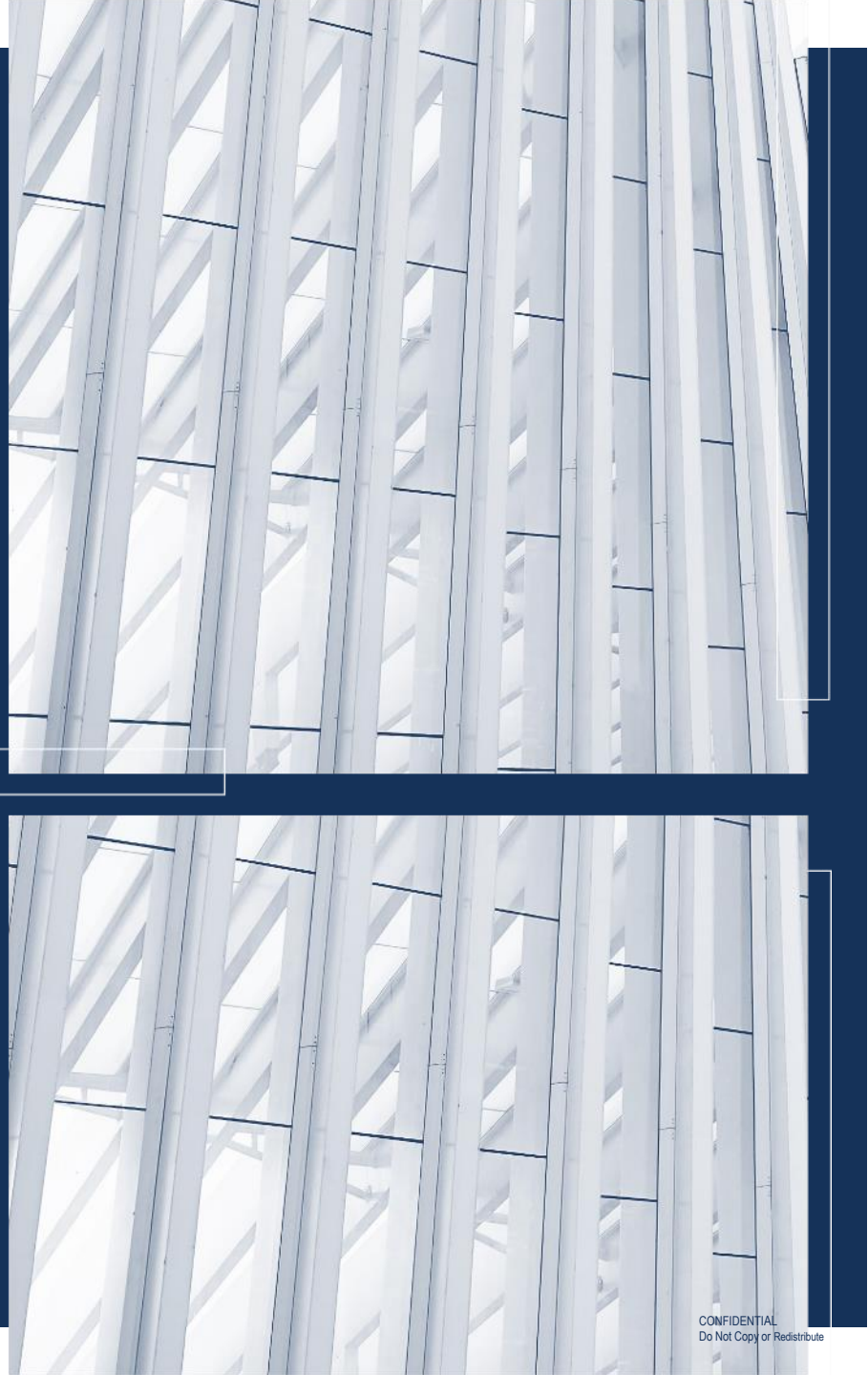
Right to data portability.

Right to opt out.

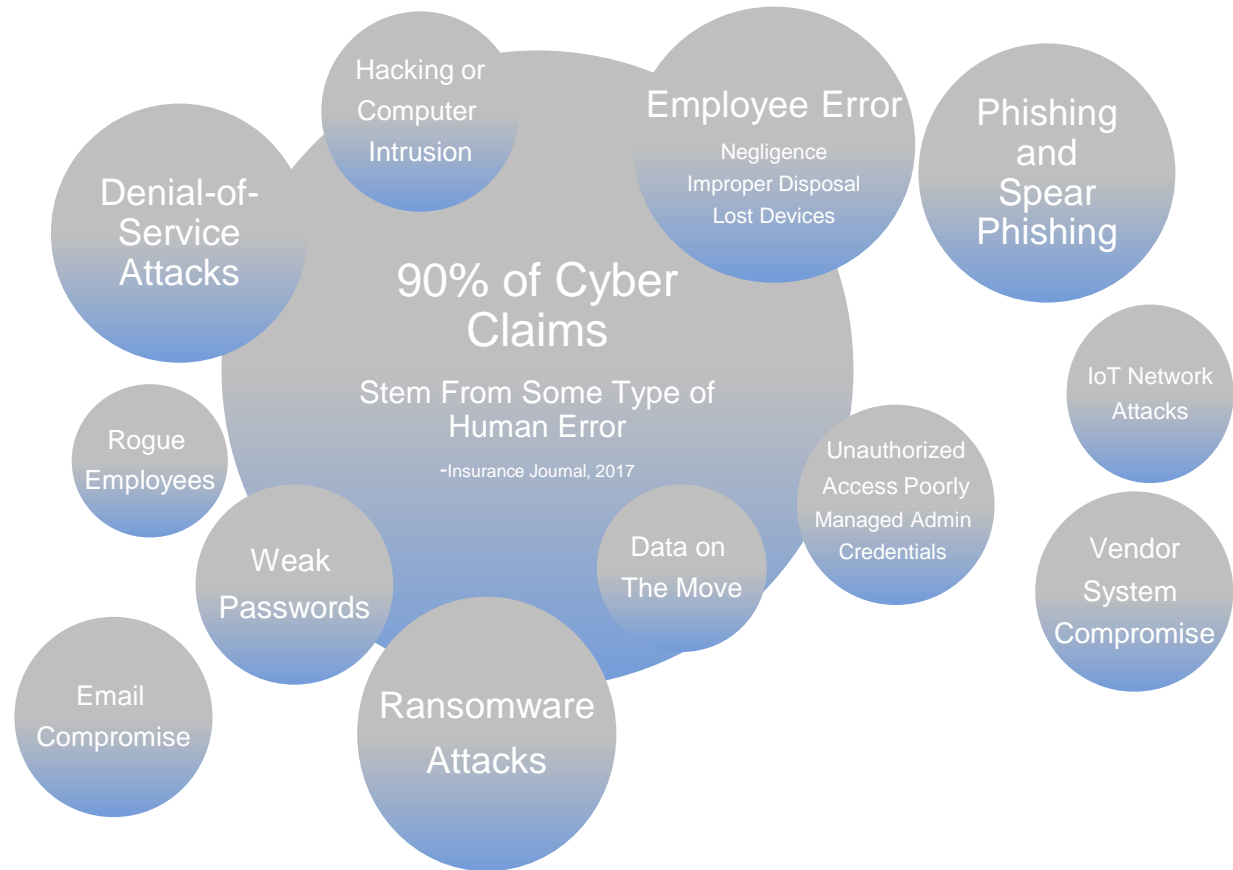
Right to appeal.

06.

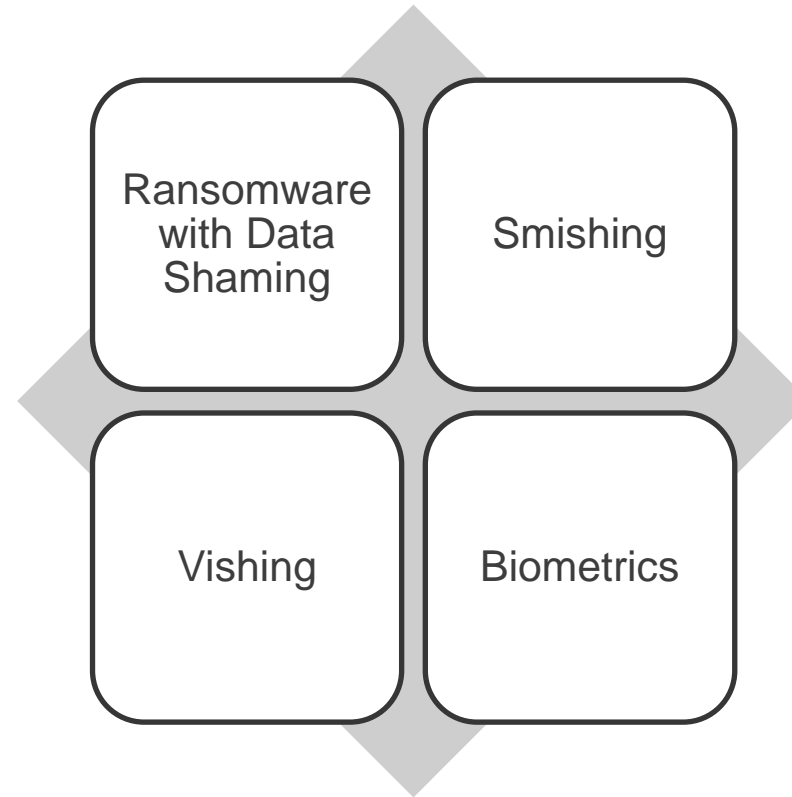
Cybersecurity



Cyber Threat Landscape



IR Trends



*Reminder to review cybersecurity and tech E&O terms.

What Is In The News?



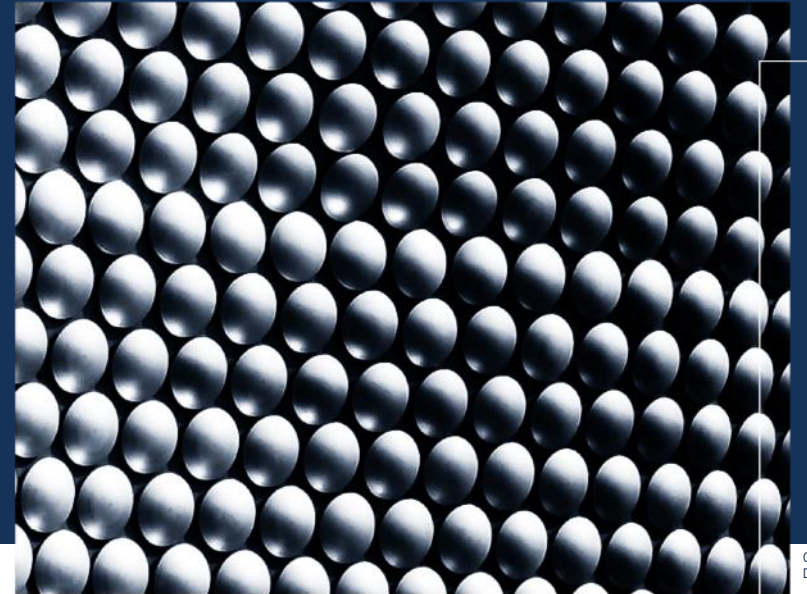
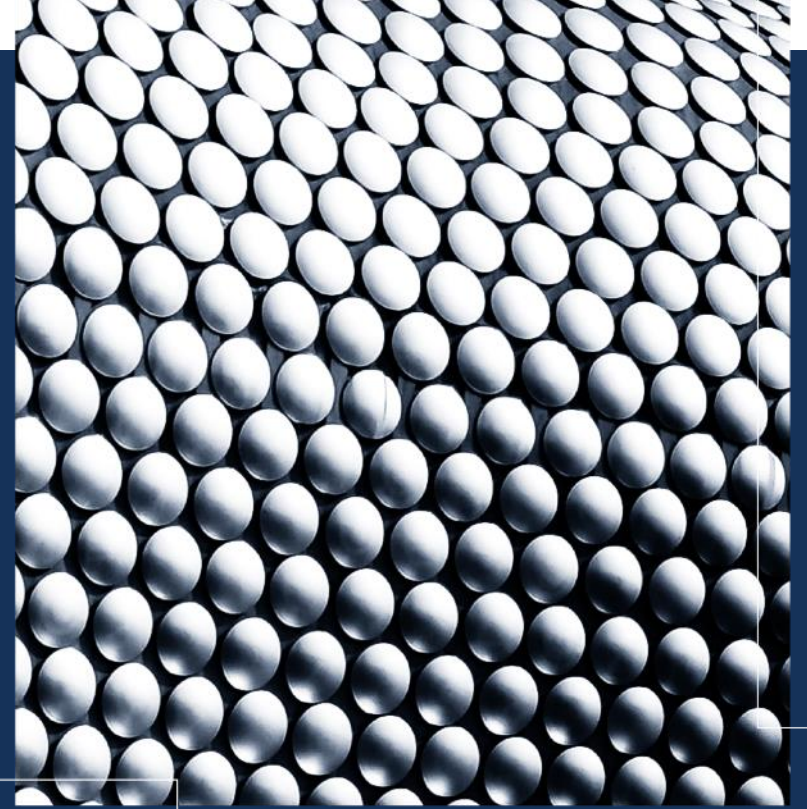
Third Parties: SolarWinds, BlackBaud

More than just PII/PHI/PCI: Florida Infrastructure Attacks, Colonial Pipeline

Ransomware OFAC Guidance

07.

Creating a Cross-Regulatory Program



Assessment of Security & Privacy Needs

Data Mapping

Identify:

- Data flows
- Systems
- Third Parties

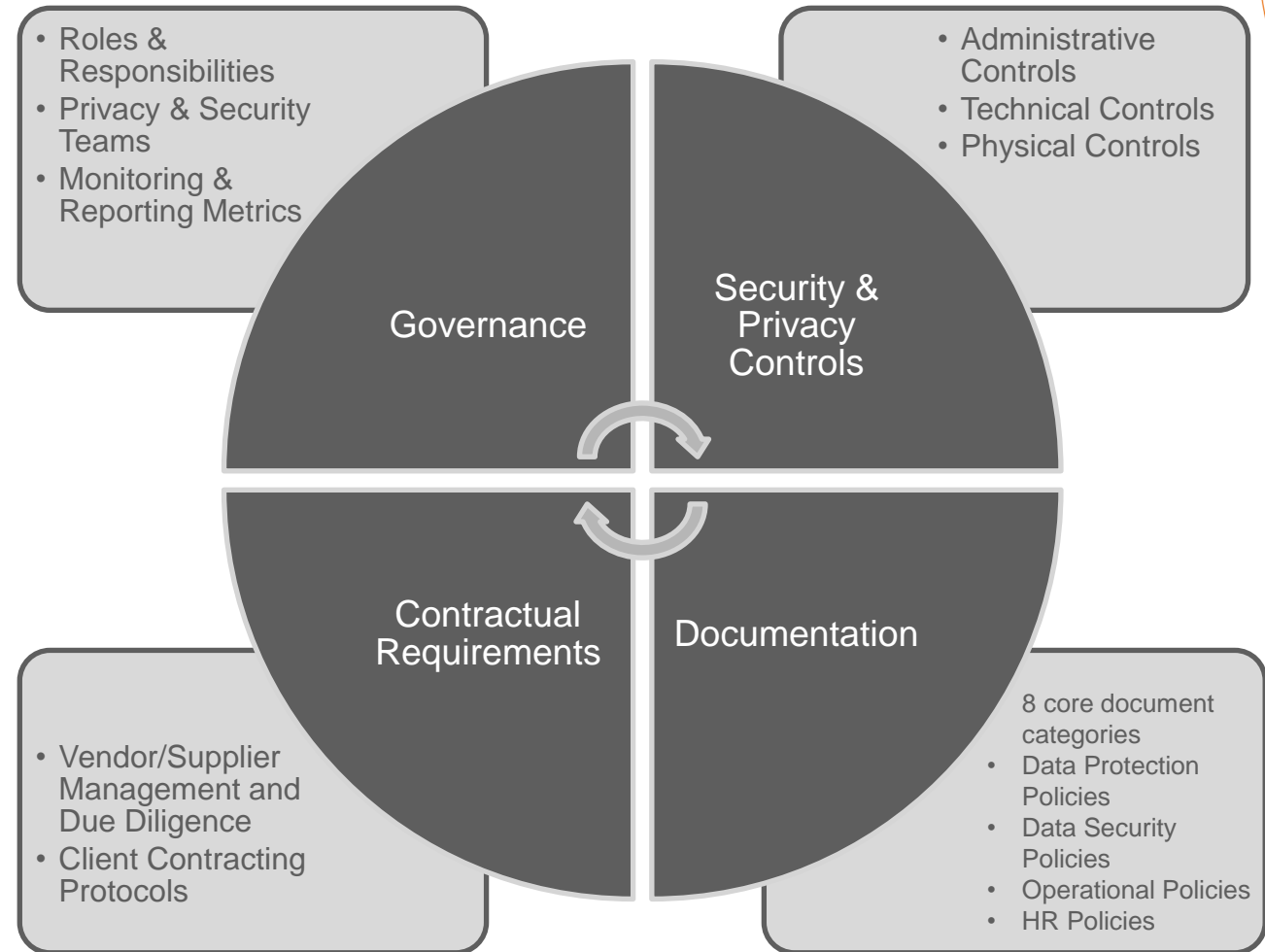
Regulatory Applicability

Assess whether regulations apply to the organization and its operations

Implementation Plan

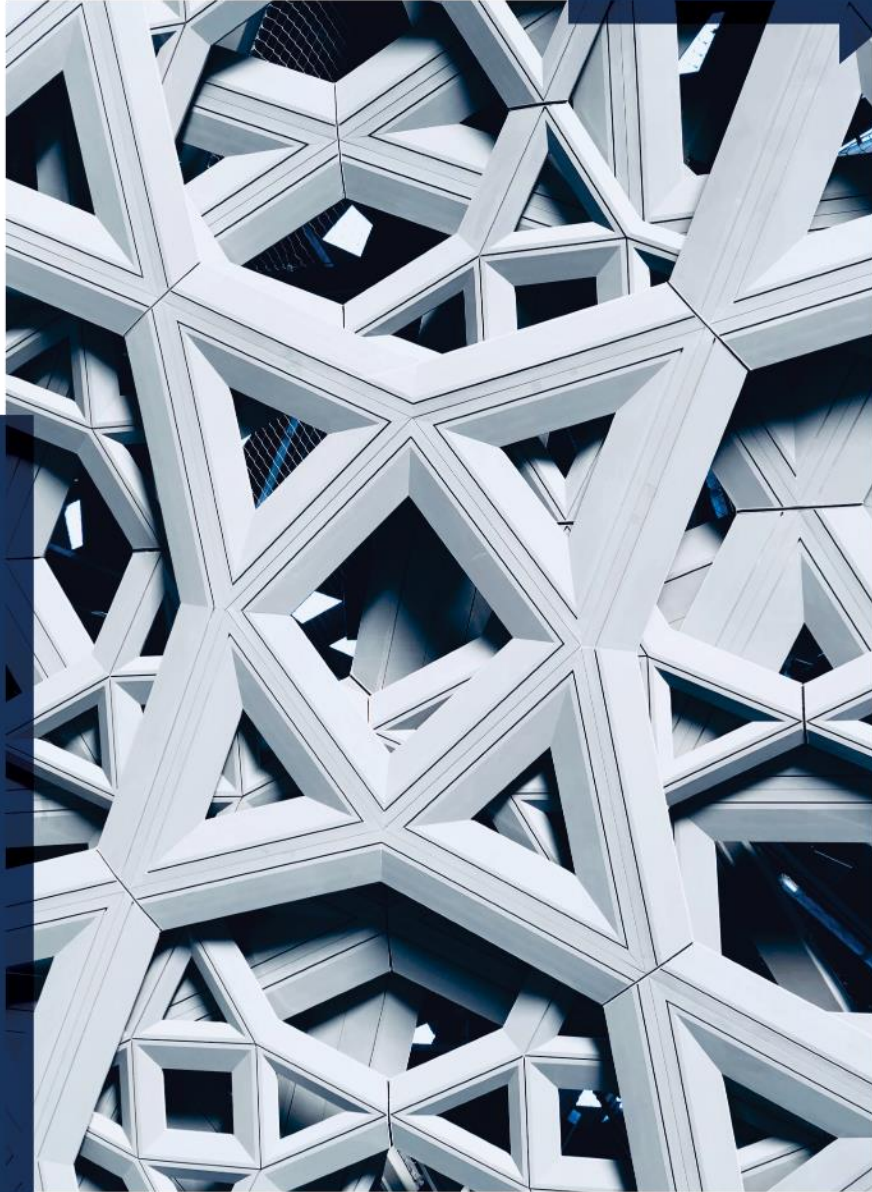
Develop a plan to address regulatory and industry needs for security and privacy

Creating a Global Security & Privacy Program



Questions?





We are lawyers, so we have a legal disclaimer

- Thank you.
- The foregoing is for information and advertising purposes only. The information is not legal advice for any specific matter and does not create an attorney-client relationship. The recipient of this publication cannot rely on its contents.
- If legal advice is required for any specific matter, please consult with qualified legal counsel. We would be happy to assist you.
- For additional questions contact an attorney at Beckage or visit Beckage.com.
- Follow us on LinkedIn or sign up for our newsletter/blogs Beckage.com/blog.