Data Security and Privacy

Updates on the Regulatory and Legislative Landscape

Michele L. Cohen | Mid-Atlantic CIO Forum | November 16, 2023

MILES & STOCKBRIDGE

A (very) High Level View of the Data Security and Privacy Landscape

Security and Exchange Commission Cybersecurity Rules Update

State of Federal Privacy Laws - The American Data Privacy Protection Act

State of the States – Status of State Privacy Laws

Cross Borders – EU-U.S. Data Privacy Framework/U.K.-U.S. Data Bridge

MILES & STOCKBRIDGE

SEC Cybersecurity Final Rule

New disclosure requirements tied to (i) cybersecurity risk management and governance; and (ii) obligations surrounding the timing and scope of material cybersecurity incidents disclosures.

Provide investors with sufficient information regarding material risk and the steps companies are taking to mitigate such risk.

Continues SEC's pattern of more aggressive practice in recent years in addressing cybersecurity incidents and related disclosures/disclosure controls.

SEC Cybersecurity Final Rule

Key Dates:

July 26, 2023: SEC adopts final rules requiring public companies disclose material cybersecurity incidents and cybersecurity risk management, strategy, and governance.

September 5, 2023: Rules Effective Date.

December 15, 2023: Annual disclosure obligations in Regulation S-K Item 106 and comparable items in Form 20-F.

December 18, 2023: Current disclosure obligations of Item 1.05 for most companies

December 15 and 18, 2024: Disclosures become subject to additional formatting requirements (i.e., formatting these disclosures in Inline XBRL to allow for automated searchability and analysis).

SEC Cybersecurity Final Rule

Rules Summary:

1. Public companies must provide enhanced and standardized disclosures regarding "cybersecurity risk management, strategy, governance, and incidents."

2. Companies must disclose material cyber breaches within four business days.

    Limited exceptions

    Must disclose even if investigation isn't complete

SEC Cybersecurity Final Rule

Form 10K Disclosures

- Cyber Risk Management Strategy - Reg. S-K Item 106(b)
  - Disclosures regarding processes for assessing, identifying and managing material risk – *A reasonable investor must be able to understand*
  - Disclose whether there are processes and how adopted; whether company engages third parties to assist; whether company has processes to manage these third parties
  - Disclose whether there are *material* risks to the company from cybersecurity threats (including past incidents)

SEC Cybersecurity Final Rule

Form 10K Disclosures

- Cyber Risk Management Strategy - Reg. S-K Item 106(b)
  - Disclosures regarding Board and Management Role
  - Board: Describe oversight role; are there committees or subcommittees having oversight; how is the board or relevant committee is informed about such risks.
  - Management: Describe management's role in assessing and managing material risks from cybersecurity threats, and its role in implementing policies, procedures, and strategies.

SEC Cybersecurity Final Rule

Form 8K Disclosures

- Cyber Risk Management Strategy - Form 8K Item 105
  - Current Reporting: Must disclose a "*cybersecurity incident*" within *4 business days* of determination that the incident is material
    - Limited exclusion based on DOJ determination
    - Must file initial disclosure and may later supplement
  - Disclosure: Must include material aspects of the nature, scope, and timing of the incident; and the material impact or reasonably likely material impact on the company, including its financial condition and results of operations.
    - Do not need to disclose technical information about a planned response, cybersecurity systems, related networks and devices, or vulnerabilities, to the extent disclosure would interfere with the response or remediation of the incident

SEC Cybersecurity Final Rule

MILES & STOCKBRIDGE

Definitions:

- Materiality: An incident is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision. The materiality determination "must be made without unreasonable delay after discovery of an incident."
- Cybersecurity Incident: An unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a company's information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing therein.

o Information Systems: Electronic information resources, owned or used by the company, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the company's information to maintain or support the company's operations

SEC Cybersecurity Final Rule

In addition:

- Note XBRL Tagging requirements for the Form 8K and 10K disclosures
- Limited Safe Harbor: Failure to file a Form 8-K on a timely basis will not result in a loss of Form S-3 eligibility. In addition, the rules provide a limited safe harbor from securities fraud liability
- Enforcement: SEC was already becoming more aggressive in addressing cybersecurity incidents and related disclosures/disclosure controls
  - Investigations included demands for potentially privileged information, including: (1) inputs and substance of materiality determinations; (2) "worksheets" or outputs of materiality determinations; and information and work product from investigations conducted following an incident, even when such investigations occur at the direction of counsel.
  - Anticipate this will continue, especially following a publicly reported incident believed to impact a range of entities.
  - Consult with counsel when conducting materiality determinations, to confirm processes are in place to protect privilege where appropriate, taking into account anticipated requests from both the SEC and company auditors.

SEC Cybersecurity Final Rule

Important Exclusion! The final rule rolled back disclosure requirement regarding director cybersecurity expertise.

Draft rule (proposed Item 407(j) of Regulation S-K) included required disclosure of whether any member of the registrant's board of directors has cybersecurity expertise (*expertise not being expressly defined*).

SEC concluded that such disclosure *may not be material for all companies*, that "effective cybersecurity processes are designed and administered largely at the *management level*, and that directors with *broad-based skills in risk management and strategy often effectively oversee management's efforts* without specific subject matter expertise, as they do with other sophisticated technical matters."

Recommendations:

1. Review with counsel, as there continues to be continued scrutiny of company cyber awareness and preparedness at the SEC and investor level.

2. Consider adding or retaining such questions if cybersecurity expertise is a qualification that is material to your risk management and strategy or governance.

Federal Privacy Laws/The American Data Privacy Protection Act

Still **no comprehensive Federal Privacy Law** on the books!

Patchwork of Federal laws that touch on privacy. These include:

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm–Leach–Bliley Act (GLBA)

Limited applicability: These apply solely and exclusively with respect to data subject to the requirements of such regulations.

Federal Privacy Laws/The American Data Privacy Protection Act

MILES & STOCKBRIDGE

July 20, 2022 – Bipartisan group of Senators and Congressmen introduced the **American Data Privacy and Protection Act (ADPPA)**

A comprehensive privacy law applicable to all states (and *superseding current state privacy laws*)

More closely ***tracks GDPR-style state privacy laws****:*

Consumer Rights: Consumers have rights over their data, including the right to access, correct, delete, or transfer data.

Covered Entity Obligations: Business must provide consumers with an opt-out prior to transferring data to a third party or targeting them with digital advertising.

Transparency: Businesses must share the types of data collected, the purposes for the data, and retention periods.

GDPR focus creates conflict with the California CPPA and CPRA, especially concerning consumer control and consent. But, like CPRA, ADPPA has a private right of action:

Consumers have a two-year window to sue certain businesses for noncompliance.

Consumers must: 1. give notice of intent to sue, 2. provide a 45 day cure period, 3. inform the FTC OR state attorney general (and allow the governmental entity 60 days in which to intervene).

The American Data Privacy Protection Act

MILES & STOCKBRIDGE

What does ADPP Cover?

- Activities related to the collection, processing, and transfer of "covered data" (i.e., any information that identifies or links an individual or their device, with *special emphasis placed on the protection of "sensitive covered data"*).
  - *Sensitive covered data* includes: race, religion, ethnicity, union membership, internal browsing history, overtime work information

The American Data Privacy Protection Act

MILES & STOCKBRIDGE

Who is covered?

- U.S. Residents
- Business Entities and their Processors/Service Providers
- Special Category for Large Data Holders
  - Large Data Holder must: have annual revenue exceeding $250 million, process more than 5 million individuals' data, and process more than 200,000 individuals' sensitive data
  - Meant to capture search engines and social media platforms.

The American Data Privacy Protection Act

Status: Bill faces significant pushback from legislators from states having privacy laws, in particular, California.

- No indication that this legislation will move forward in the near term.

State of the State: Status of State Privacy Laws

How it started:

California: The California Consumer Privacy Act in January 2020, as amended by the California Privacy Rights Act in November 2020

Next Up:

Virginia and Colorado: Enacted laws in 2021

Utah and Connecticut: Enacted laws in 2022

No End in Sight!

8 more states in 2023: Iowa, Indiana, Tennessee, Montana, Florida, Oregon, Texas, Delaware

State of the State: Status of State Privacy Laws

MILES & STOCKBRIDGE

Some General Concepts

1. Consumer Protection Focus. Many states have exemptions for business/employee contact information, other employment information, information covered by other federal or state laws.

   These distinctions are too voluminous to address in this presentation.

2. Target is Primarily "For-Profit" Businesses.

   Colorado, Delaware and Oregon also cover non-profits.

3. Transparency and Disclosure are Favored. Businesses must advise consumers regarding their collection practices. Privacy policies must be prominently displayed, and consumers must have clear notice of how they may contact the business.

   States may require multiple methods of communication, considering where/how consumers interact with the company.

4. State Controls Enforcement. Most state laws have only regulatory enforcement (with statutory penalties).

   California has a limited private right of action tied to data breach.

   Note that the ADPPA would also provide for a limited private right of action.

State Laws - Definitions

CONSUMER RIGHTS

Right to access — The right for a consumer to access from a business/data controller the information or categories of information collected about a consumer, the information or categories of information shared with third parties, or the specific third parties or categories of third parties to which the information was shared; or, some combination of similar information.

Right to correct — The right for a consumer to request that incorrect or outdated personal information be corrected but not deleted.

Right to delete — The right for a consumer to request deletion of personal information about the consumer under certain conditions.

Right to opt out of certain processing — The right for a consumer to restrict a business's ability to process personal information about the consumer.

State Laws - Definitions

Right to portability — The right for a consumer to request personal information about the consumer be disclosed in a common file format.

Right to opt-out — The right for a consumer to opt out of the sale of personal information about the consumer to third parties.

Right to opt in — The right for a consumer to opt in before a business can process their sensitive data.

Right against automated decision making — A prohibition against a business making decisions about a consumer based solely on an automated process without human input.

Private right of action — The right for a consumer to seek civil damages from a business for violations of a statute.

State Laws - Definitions

BUSINESS OBLIGATIONS

Opt-in default — A restriction placed on a business to treat consumers under a certain age with an opt-in default for the sale/sharing of their personal information.

Notice/transparency — An obligation placed on a business to provide notice to consumers about certain data practices, privacy operations, and/or privacy programs.

Risk assessments — An obligation placed on a business to conduct formal risk assessments of privacy and/or security projects or procedures.

Prohibition on discrimination (exercising rights) — A prohibition against a business treating a consumer who exercises a consumer right differently than a consumer who does not exercise a right.

Purpose/processing limitation — An EU General Data Protection Regulation–style restrictive structure that prohibits the collection/processing of personal information except for a specific purpose

State Law Summary

	CA	CO	CT	DE	IN	IA	MT	OR	TN	TX	UT	VA
Name	CA Consumer Privacy Act of 2018 amended by California Privacy Rights Act of 2020 (CCPA as amended)	CO Privacy Act of 2021 (CPA)	CT Data Privacy Act of 2022	DE Personal Data Privacy Act	IN Consumer Data Protection Act of 2023	IA Consumer Data Protection Act of 2023	MT Consumer Data Privacy Act of 2023	OR Consumer Privacy Act	TN Information Protection Act of 2023	TX Data Privacy and Security Act	UT Consumer Privacy Act of 2022	VA Consumer Data Protection Act of 2021
Effective Date	1.1.20 (CCPA) 1.1.23 (CPRA)	7.1.23	7.1.23	1.1.25	1.1.26	1.1.25	10.1.24	7.1.24	7.1.25	7.1.24	12.31.23	1.1.23
Access	X	X	X	X	X	X	X	X	X	X	X	X
Correct		X	X	X	X		X	X	X	X		X
Delete	X	X	X	X	X	X	X	X	X	X	X	X
Opt Out/ Processing		*	**	**	**		**	**	**	**	**	**
Portability	X	X	X	X	X	X	X	X	X	X	X	X
Opt Out/Selling	X	X	X	X	X	X	X	X	X	X	X	X
Opt In/ Sensitive Data		X	X	X	X		X	X	X	X		X
Automated Decision-Making	CPRA	***	***	X	***	***	***	***	***	***		***
Key: ***Applies to Sensitive Data** ****Applies to Data collected for profiling or targeted advertising** *****Opt-Out may apply**												

State Law Summary

	CA	CO	CT	DE	IN	IA	MT	OR	TN	TX	UT	VA
Name	CA Consumer Privacy Act of 2018 amended by California Privacy Rights Act of 2020 (CCPA as amended)	CO Privacy Act of 2021 (CPA)	CT Data Privacy Act of 2022	DE Personal Data Privacy Act	IN Consumer Data Protection Act of 2023	IA Consumer Data Protection Act of 2023	MT Consumer Data Privacy Act of 2023	OR Consumer Privacy Act	TN Information Protection Act of 2023	TX Data Privacy and Security Act	UT Consumer Privacy Act of 2022	VA Consumer Data Protection Act of 2021
Effective Date	1.1.20 (CCPA) 1.1.23 (CPRA)	7.1.23	7.1.23	1.1.25	1.1.26	1.1.25	10.1.24	7.1.24	7.1.25	7.1.24	12.31.23	1.1.23
Business Obligations												
Opt In Default (age)	16	16	13*	13*	13*	13*	13*	13*	13*	13*	13	13*
Notice/ Transparency	X	X	X	X	X	X	X	X	X	X	X	X
Risk Assessments	CPRA	X	X	X	X		X	X	X	X		X
No Discrimination (exercising rights)	CPRA	X	X	X	X	X	X	X	X	X	X	X
Limitations on Purpose/ Processing	X	X	X	X	X	X	X	X	X	X		X

State Law Compliance

How does a company manage compliance with this myriad of state laws (and Federal laws and GDPR/International laws)??

There is no easy answer!

Some considerations:

1. Where are you located?
2. Do you operate nationally? Internationally?
3. Are you a non-profit? For-profit? Subject to any Federal Laws?
4. Do you collect data for third party sales or sharing as a part of your business?

California Developments

California Privacy Protection Agency: August 28, 2023 - Released draft regulations tied to cybersecurity audits and risk assessments.

Will require businesses to perform annual cybersecurity audits and regularly submit risk assessments to the CPPA regarding their processing of personal information.

a. Require annual independent audits to assess, document and summarize the components of cybersecurity programs, focusing on any gaps or weaknesses.
b. Provide examples of "negative impacts" on consumers security and safeguards businesses use to protect personal information that must be assessed in the context of the cybersecurity program.
c. Address privacy-related risks posed by artificial intelligence and automated decision-making technologies.
d. Risk assessments would be conducted and submitted whenever a business's personal information processing presents a significant risk to consumers' privacy or security.

Remains subject to the formal rulemaking process and revisions are expected

California Developments

1. **The Delete Act**: Signed October 2023. January 2026 Implementation Date

   Allows CA residents to get data brokers to delete their personal information with a single request, rather than the multiple asks.

   Enforced through the California Privacy Protection Agency.

2. **CPRA Amendments: Signed October 2023**

   Immigration data is now deemed sensitive personal data.
   Reproductive heath data as personal data.

EU-U.S. Data Privacy Framework/ U.K.-U.S. Data Bridge

MILES & STOCKBRIDGE

A Brief History:

U.K.-U.S.-EU triangle is one of the most important pieces in the global-transfers puzzle, with trans-Atlantic data flows estimated to underpin more than $1 trillion in trade and investment annually.

The General Data Protection Regulation (GDPR) and U.K. GDPR, respectively govern data transfers to the third countries when coming from the EU and U.K.

> Transfer is permitted only where the third country in which the recipient company is located can ensure an adequate level of protection to safeguard personal data, also known as "adequacy."

The U.S. is not adequate under the GDPR or U.K. GDPR because it does not have any comprehensive personal data privacy laws at the federal level.

Two prior frameworks designed to create a trans-Atlantic data transfer framework, the U.S.-EU Safe Harbor and EU-U.S. Privacy Shield, were invalidated by the Court of Justice of the European Union (CJEU).

EU-U.S. Data Privacy Framework/ U.K.-U.S. Data Bridge

MILES & STOCKBRIDGE

Remaining options, following elimination of Safe Harbor and Privacy Shield are cumbersome and complex!

1. Companies must first complete a transfer-impact assessment to evaluate whether protections for individuals under the GDPR would be undermined by the laws and practices of the third country; and then implement a transfer mechanism, such as standard contractual clauses or binding corporate rules as for overarching company compliance.

The SCCs are standardized and generally not subject to modification

BCRs must receive approval from each country from which the company will receive data.

2. Compliance requires a comprehensive assessment of U.S. surveillance laws and practices, which most U.S. businesses do not have the bandwidth for.

EU-U.S. Data Privacy Framework/ U.K.-U.S. Data Bridge

MILES & STOCKBRIDGE

The EU-U.S. Data Privacy Framework ("DPF"): Announced July 10, 2023. The European Commission will recognize U.S. businesses participating in the DPF as "adequate" for purposes of EU-U.S data transfers.

The DPF sets out the requirements tied to the use and treatment of personal data received from the EU and the access and recourse mechanisms that participants must provide to EU.

The U.K.-U.S. Data Bridge: Announced September 21, 2023.

Provides conforming guidance as to U.K.-U.S. transfers.

Data Bridge is not available independently and can only be used once a company certifies into DPF and then opts into the U.K.

Compliance with the DPF and Data Bridge frameworks allows U.S. companies to bypass other compliance methods.

EU-U.S. Data Privacy Framework/ U.K.-U.S. Data Bridge

MILES & STOCKBRIDGE

Who is eligible?

Companies subject to the jurisdiction of the Federal Trade Commission or the U.S. Department of Transportation may self-certify for the DPF and, if desired, also participate in the Data Bridge.

Impact on Companies Operating Under Existing Mechanisms?

May continue to use SCCs and BCRs

EU-U.S. Data Privacy Framework/ U.K.-U.S. Data Bridge

MILES & STOCKBRIDGE

Self-Certification Process:

Compliance - Companies must commit to comply with a detailed set of privacy obligations. These include:

Developing a Privacy Policy conforming with DPF requirements to protect data subjects' rights under GDPR

Identifying an independent recourse mechanism and publicly commit to compliance with DPF Principles.

Agreeing to delete personal data when it is no longer necessary for the purpose for which it was collected, and to ensure "downstream" continuity of protection when personal data is shared with third parties.

Timing:

Companies currently certified under Privacy Shield could immediately benefit under the DPF by issuing updated privacy policies no later than October 10, 2023.

EU-U.S. Data Privacy Framework/ U.K.-U.S. Data Bridge

MILES & STOCKBRIDGE

How to Self-Certify:

Online process – U.S. Department of Commerce launched the Data Privacy Framework program website, where U.S.-based organizations can submit for self-certification and find information on participating companies. May transfer data under DPF once DOC confirms certification is complete.

https://www.dataprivacyframework.gov/s/

EU-U.S. Data Privacy Framework/ U.K.-U.S. Data Bridge

MILES & STOCKBRIDGE

Post-Certification Requirements:

1. Organizations must annually recertify their compliance with DPF Principles.

2. Companies must handle complaints, access requests and other issues.

    Must provide readily available recourse mechanisms to investigate unresolved complaints, including a free system of alternative dispute resolution by an independent third party.

    Must implement dispute resolution process prior to self-certification.

3. Companies looking to withdraw from Privacy Shield and not certify under DPF must complete a formal process.

EU-U.S. Data Privacy Framework/ U.K.-U.S. Data Bridge

MILES & STOCKBRIDGE

What's Next?

Prepare for new legal challenges. Schrems III is expected

Modifications/Supplements:

1. Data transfer mechanisms tailored to specific sectors currently excluded from the scope of the DPF (such as financial services and health industries).
2. Additional adequacy arrangements with other countries.
3. U.S. State-level collaboration, especially with California.
4. Eventual cooperation in connection with the ADPPA or other federal law.

Firm Overview

Miles & Stockbridge P.C. is a leading law firm with offices in the mid-Atlantic region, including offices in Baltimore and Washington, D.C. Its lawyers help global, national, local and emerging business clients preserve and create value by helping them solve their most challenging problems.

Miles & Stockbridge P.C.

www.mslaw.com
Twitter: @mstockbridgelaw

The opinions expressed and any legal positions asserted in this presentation are those of the author and do not necessarily reflect the opinions or positions of Miles & Stockbridge P.C. or its other lawyers. No part of this presentation may be reproduced or transmitted in any way without the written permission of the author. Images are subject to copyright. All rights reserved.