HARMONIZING FINANCIAL PRIVACY AND SECURITY LAWS

October 24, 2024

McDermott Will & Emery

PRIVILEGED / FOR EDUCATIONAL PURPOSES / NOT TO BE USED AS LEGAL ADVICE

SPEAKERS

ELLIOT GOLDING

Partner

Washington, DC

egolding@mwe.com

KEITH VOORHEIS

Assistant General Counsel & Chief Privacy Officer

Volkswagen Financial Services

MARK SAUCHELLI

Lead Counsel, Data, Digital & Marketing

Mass Mutual

DOUGLAS SMITH

Head of Wealth Management | Cyber and Privacy Legal

Morgan Stanley

INTRODUCTION

- Financial regulation is a complex patchwork.
- There are both federal laws and state laws with varying applicability/requirements.
- Businesses need to harmonize these rules to support business data needs while mitigating risk.

WHY DO WE CARE?

- **Active enforcement** with **investigations, fines**.
- Regulator investigation can be triggered by simple **review of public website**.
- Investigation would create **months of intensive work**.

GENERAL PRIVACY LAWS

- **State comprehensive privacy laws.**
  - CCPA, CPA, TDPSA, and more.
- **FTC Section 5 Authority (and equivalent state UDAP laws).**
  - Broad authority to regulate unfair and deceptive practices, including privacy practices.
- **State data breach notification laws.**

State	GLBA Data Exemptions?*
California	Data
Colorado	Entity
Connecticut	Entity
Oregon	Data
Texas	Entity
Utah	Entity
Virginia	Entity
Montana	Entity

*FCRA data is also generally exempt.

FINANCIAL PRIVACY LAWS

Gramm-Leach-Bliley Act (GLBA) and Implementing Regulations
(Enforcement through FTC and CFPB)

Fair Credit Reporting Act

State Financial Privacy Laws

State Insurance Privacy Laws

Requirements/Applicability

- Applies to Nonpublic Information (NPI).
- Initial and annual privacy disclosures.
- Limits permissible uses and disclosures.
- **FCRA only**: requires certain disclosures and consents for background checks and otherwise restricts use of credit reports.

CYBER LAWS AND STANDARDS

General state cyber laws
(e.g., NY Shield Act, forthcoming CCPA cyber regs)

Financial-specific state cyber laws
(e.g., NYDFS)

Insurance Data Security Model Law

Payment Card Industry Data Security Standard
(PCI DSS)

FTC Safeguards Rule

Requirements/Applicability

- MFA, audit, access controls, written policies.
- Risk assessments, testing, monitoring, and specific training.
- Incident response planning and training (e.g., IRP, tabletop).

ACTIVITY-SPECIFIC LAWS

- **Marketing** (CAN-SPAM Act and TCPA).
- **AI**
  - California draft regulations on automated decision-making technology (ADMT) (in rulemaking stage).
  - Utah AI Policy Act (in effect).
  - Colorado Artificial Intelligence Act (effective Feb. 2026).
- **Tracking Technologies**
  - State wiretapping laws (often CA).
  - Unfair and deceptive practices claims (e.g., NY guidance).
  - VPPA.
- **Other** (E.g., FDCA, FERPA, etc.).

BRINGING IT ALL TOGETHER

Law	Applicability	Notice Requirements	Permissible Use and Disclosures	Consent	Consumer Rights	Contracting Requirements
GLBA	Financial institutions processing NPI in connection with providing a financial product or service for personal, family or household use	Before establishing customer relationship and annual	Necessary to process transactions Legal, safety, security, and similar reasons Business transaction Complying with laws inc. FCRA	Opt-out of sharing with non-affiliates for marketing (unless joint marketing)	No	Yes (prohibiting disclosures or uses beyond the purposes specified in the contract)
CalFIPA ***& other state financial privacy laws***	Financial institutions processing NPI in CA in connection with providing a financial product or service for personal, family or household use	Before establishing customer relationship and annual	Necessary to process transactions Legal, safety, security, and similar reasons Business transaction Complying with laws inc. FCRA	CalFIPA: Opt-in to sharing with non-affiliates for marketing (unless joint marketing); Opt-out of sharing with affiliates for marketing & nonaffiliates for joint marketing OTHER: generally opt out	No	Yes (prohibiting disclosures or uses beyond the purposes specified in the contract)

BRINGING IT ALL TOGETHER CNTD.

Law	Applicability	Notice Requirements	Permissible Use and Disclosures	Consent	Consumer Rights	Contracting Requirements
State insurance privacy laws	Insurance institutions, agents, and support organizations processing NPI in connection with an insurance transaction	At the time of delivery of a policy or point of collection + annually	Necessary to process transactions Legal, safety, security, and similar reasons Business transaction Complying with laws inc. FCRA	MOST: Opt-out of sharing with non-affiliates for marketing purposes OUTLIERS: some require opt-in consent.	Yes (access, correct, delete)	Yes (prohibiting disclosures or uses beyond the purposes specified in the contract)
State privacy laws	Non-exempt businesses processing non-exempt personal data in the relevant state	Before or at the point of collection	Legal, safety, security, and similar reasons Internal business purposes De-identified data	Opt-out of sales of data/targeted advertising (incl. marketing)	Yes (access, correct, delete, opt-out, limit SPI processing, appeal)	Yes (prohibiting disclosures or uses beyond the purposes specified in the contract)
FCRA	Prohibits consumer reporting agencies from disclosing consumer reports outside of purposes initially permitted, such as: with consent, in connection with a credit transaction involving the consumer, employment purposes (subject to certain additional requirements), underwriting insurance, etc.					

CREATING AN ACTION PLAN

ELEMENTS OF COMPLIANCE PROGRAM

- **Workstream #1:** Info gathering and scoping/harmonization.
- **Workstream #2:** Create data inventories/maps (if applicable).
- **Workstream #3:** Update external-facing privacy policy(ies).
- **Workstream #4:** Create and/or update consent and data subject rights ("DSR") procedures.
- **Workstream #5:** Create/update contracting program.
- **Workstream #6:** Update governance, internal documentation, training.
- **Workstream #7:** Update data security plans, breach readiness.

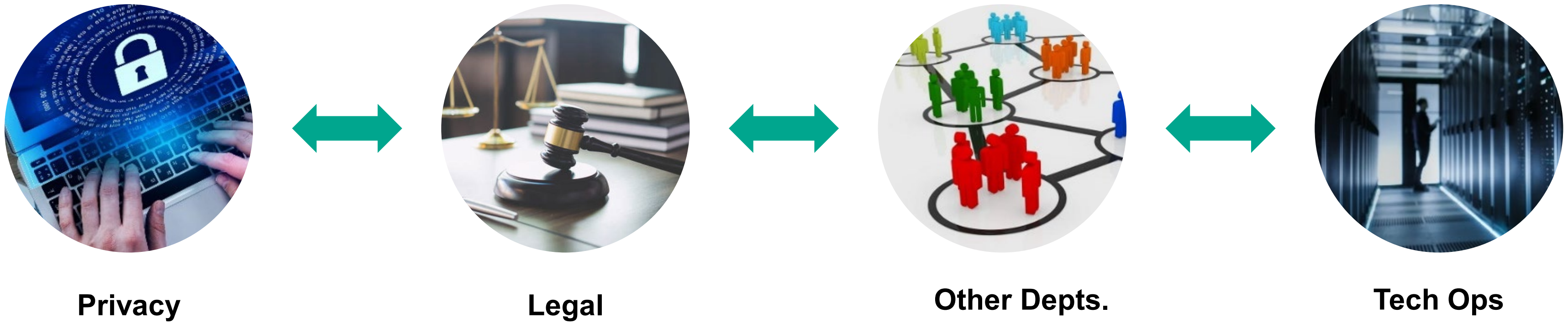
WORKSTREAM #1:
INFO GATHERING, SCOPING & HARMONIZATION

Info Gathering & Scoping

- Identify which laws/state apply + exceptions.
- Identify practices subject to the respective laws.
- Identify appropriate stakeholders.
- Identify external resources (e.g., counsel, vendors).

Harmonization

- Identify existing privacy compliance measures.
- Conduct gap analysis against current practices.
- Make risk-based decisions to incorporate new processing activities.



Privacy

Legal

Other Depts.

Tech Ops

WORKSTREAM #2: CREATE DATA INVENTORIES/MAPS

Complete a “data inventory” or “data mapping” exercise, including tracking technologies. Consider technology solutions

Work backwards from goal (e.g., system inventory, checking security, identifying third party sharing, etc.)

Establish process for periodic updates

WORKSTREAM #3: UPDATE PRIVACY POLICY(IES)

Specific requirements vary across laws (e.g., separate financial notice/model form)

Evaluate “material change issues”

Establish process to ensure compliance with representations and conduct periodic updates (annual and new/changing practices). Make sure to “future proof” where possible (e.g., AI disclosures)

WORKSTREAM #4:
REVIEW/UPDATE DSR PROCEDURES

- Know/Access
- Correct
- Delete
- Opt-out/opt-in selling, sharing, targeted advertising, and affiliate/ nonaffiliate sharing
- SPI processing (opt-in vs. opt-out)
- Opt out of profiling/automated decision-making
- Appeal
- Opt-in to financial incentive

Each general state privacy law includes a right to **non-discrimination.**

TRACKING TECH & ONLINE ADVERTISING

- **Tracking technology** is a script or code on a website or mobile app used to gather information about users when they interact with websites/mobile apps.
  - **Cookies** are files placed on a user’s device to customize a user’s browsing experience but can also be used to track a user's activities.
  - **A web beacon or tracking pixel** is a tiny graphic image (usually 1 pixel) placed on a webpage that allows the website owner or a third party to collect information regarding the use of the webpage that contains the web beacon.
  - **Session replay scripts** record a user’s activities (e.g., mouse movements, clicks, and typing) when using a webpage or app.
  - **Fingerprinting** uses a browser’s and/or device’s unique configurations and settings to track user activity.

ADTECH-RELATED RIGHTS

- **Sale** (all states): disclosing/making PI available to a third party for any “consideration,” including non-monetary consideration.
- **Sharing** (CA only): disclosing/making available PI to a third party for cross-contextual behavioral advertising.
- **Targeted advertising** (other states): displaying ads based on inferences from PI collected over time and across unaffiliated websites/applications.
- **All general state privacy laws give right to opt out**.
  - California Attorney General July 2021 Guidance: Selling occurs even when third party collects that data directly from your website (i.e., not necessary to affirmatively disclose to the third party).
  - Enforcement cases seem to indicate that collection by a third-party cookie provider, absent a service provider commitment by such provider, may be a “sale” to such provider.

CREATING OPPORTUNITIES

- **Key considerations**
  - What data is being used? First-party / third-party / both?
  - Is data being made available to third parties, or kept in-house?
- **Examples**
  - **Publisher:** Creating segments with first-party data and allowing third parties to target ads within various company apps and websites.
  - **Data Mart:** Creating segments and making them available for activation (without disclosing the underlying first-party data).
    - Using first-party data only or enhancing with third-party data.
  - **Market Research:** Providing insights to third parties using first-party data.
  - **Other Data Monetization:** Enhancing third-party data for a fee; Verifying linkages between online and offline data (identity graph).

HANDLING DIGITAL ADVERTISING: OPERATIONAL CONSIDERATIONS

- **Cookie Management**
  - Identifying and categorizing cookies.
  - Confirming legal obligations/compliance approach.
  - Selecting third-party vendor.

- **Cookie Banner**
  - Whether to have cookie banner.
  - Functionality of banner.
  - Banner text.
  - Buttons for banner.
  - Geofencing.

HANDLING DIGITAL ADVERTISING: OPERATIONAL CONSIDERATIONS (CONT.)

- **Preference Center:**
  - Whether to have preference center.
  - Preference center options (e.g., opt-in vs. opt-out, granular choice vs. all-or-nothing choice).
  - Preference center copy.
  - Preference center placement on websites.
  - Geofencing.
  - Global Privacy Controls functionality.

- **Data subject requests:**
  - Which requests to honor.
  - How to receive requests.
  - How to process requests internally.
  - Template communications.
  - Recordkeeping.

HANDLING DIGITAL ADVERTISING: OPERATIONAL CONSIDERATIONS (CONT.)

- **Privacy notices:**
  - Determining in-scope laws.
  - One privacy notice vs. multiple (product-specific, entity-specific, etc.).
  - Privacy notice text.
  - Presentation/delivery.
  - Material change review.

- **Other marketing:**
  - Identifying marketing channels (e.g., text messaging, email).
  - Opt-in vs. opt-out.
  - Consent language.
  - Consent placement/delivery.
  - Recordkeeping.

WORKSTREAM #5: CREATE/UPDATE VENDOR/DATA RECIPIENT CONTRACTING PROGRAM

- Specific terms required.
- Potential challenges depending on the type of vendor (e.g., adtech).
- Update contracts with service providers/vendors with terms designed to protect personal information you share with them.

WORKSTREAM #6: UPDATE GOVERNANCE, DOCUMENTATION & TRAINING

Internal policies

Update and/or develop internal policies to support compliance (*e.g.*, internal privacy policies, data retention policy, record keeping)

Training

Develop & implement training materials

High-risk processing

Determine whether the business engages in any "high-risk processing" (*e.g.*, processing SPI, profiling)

WORKSTREAM #7: UPDATE DATA SECURITY PLANS, BREACH READINESS

Breach notices

Privacy laws have security and breach notification requirements, are tied to breach notification laws

Security policies

Review and update security policies to meet "reasonableness" standard and stricter requirements under financial laws

Update plans

Update incident response plan and conduct tabletop

TAKEAWAYS

1. More lead time is needed than you may think
2. A lot of options to implement – no “one size fits all”
3. Exemptions are construed narrowly in most cases
4. Devil is in the details
5. Test before launching

THANK YOU / QUESTIONS?

This material is for general information purposes only and should not be construed as legal advice or any other advice on any specific facts or circumstances. No one should act or refrain from acting based upon any information herein without seeking professional legal advice. McDermott Will & Emery* (McDermott) makes no warranties, representations, or claims of any kind concerning the content herein. McDermott and the contributing presenters or authors expressly disclaim all liability to any person in respect of the consequences of anything done or not done in reliance upon the use of contents included herein.
*For a complete list of McDermott entities visit mwe.com/legalnotices.