Data Privacy and Security for Franchisors

Michael R. Cohen
Tedrick Housh
Gaylen Knack
Emily Holpert

July 28, 2021

Lathrop GPM

Roadmap for Our Time Together

- The Importance of Data to the Franchisor
- Recent Data Legislation & Regulatory Developments
- Practical Tips and Takeaways

A franchisor must balance the costs and benefits of managing personal data, including the risk of a data breach.

Supporting Franchisees without Owning their Failures

Franchisors must protect the brand but try to avoid liability for acts of franchisees.

- Include a general description of privacy and security requirements for franchisees in franchise disclosure document.
- Template privacy policies, procedures, and related documents for franchisee to customize and use in its data privacy and security program
- Provide information on cyber insurance and training resources
- Update Franchise Agreements when appropriate and necessary
- Update Operations Manual to suggest administrative, technical, and physical safeguards such as strong passwords, encryption, and training.
- Consider security audits

Who Owns the Data, the Franchisor or Franchisee? Reading the Signs.

- What does the Franchise Agreement and other contracts say?
- Is the franchisor empowered to access or download data from franchisee computer systems?
- Is the franchisee allowed to use customer data as necessary to engage in direct customer transactions?
- How is the loyalty program structured? Who collects the data? Who uses it? Where is it stored?
- To whom do consumers direct requests to delete, correct or see their data? How do they know?
- What happens to the data upon termination?
- What happens to data in a merger or sale?

Recent Case Example: Franchisor Enforcement of Data Rights

On April 1, 2021, federal District Court granted a Preliminary Injunction. It found Franchisee:

- Operated a competing business out of the same NC location.
- Downloaded Franchisor's client relationship (CRM) database before leaving the franchise.
- Emailed customers, while still a franchisee, to say it was moving to competing software.
- Transferred to the new database the billing information, membership, business records, attendance and other Franchisor data.

Core Progression Franchise LLC v. O'Hare, No. 21-CV-0643-WJM-NYW, 2021 WL 1222768 (D. Colo. Apr. 1, 2021).

On June 23, 2021, Court issued sanctions for violation of the PI, requiring Franchisee to:

- Cease use of a new digital application created after termination of the franchise.
- Return to Franchisor all copies of the data taken from Franchisor's CRM.

Core Progression Franchise LLC v. O'Hare, No. 21-CV-0643-WJM-NYW, 2021 WL 2566890 (D. Colo. June 23, 2021).

Case is now on appeal.

With Personal Data Comes Great Responsibility

The United States and over 100 countries now have some form of data privacy and protection law and the risks for non-compliance include fines, claims for compensation, government enforcement actions, statutory damages, and reputational harm.

We will first look at recent developments in data protection law, first in the US and then the world.

EMPLOYMENT AND ECONOMIC DEVELOPMENT

Lathrop GPM

A Legal Guide To PRIVACY AND DATA SECURITY

2021

A Collaborative Effort

Minnesota Department of Employment and Economic Development

Lathrop GPM

Patchwork of State & Federal Privacy Laws in USA

- No comprehensive federal privacy law
- No federal breach notification statute
- Typically, resident state of the data subject governs
- Federal consumer and criminal statutes can apply
- Each state has its own requirements for breach notification
- California- first and most active in data privacy
- Massachusetts- gold standard for data security
- More states are enacting or amending their data privacy laws

California Consumer Privacy Act (CCPA)

- Effective January 1, 2020
- New consumer rights to access, deletion, and porting of personal data
- Specific disclosure requirements
- Penalties with statutory damages
- **Private right of action for data breaches**

California Privacy Rights Act (CPRA)

- Effective January 1, 2023
- Extends CCPA B2B and HR exemptions to January 1, 2023.
- Doubles CCPA threshold of consumers and households from 50,000 to 100,000
- Adds sensitive information as category
- Adds new right to correct inaccurate data; expands others
- New enforcement authority dedicated to privacy-California Privacy Protection Agency

Application of the CCPA to Franchisors & Franchisees

A franchisor or franchisee must independently comply with the CCPA if it is

- a **business** as defined in the CCPA; or
- an "entity that **controls or is controlled** by a business" and "**shares common branding** with the business."

"Control" means not only ownership rights, but "the power to exercise a **controlling influence over the management**."

"Common branding" means a "**shared name, servicemark, or trademark.**" Most, if not all, franchises are based on common branding.

Result: If either franchisor or franchisee is a CCPA "business," and one is controlled by the other and they share common branding, both are likely subject to the CCPA.

Strategy: To limit or reduce risk under the CCPA, a franchisor may attempt to limit "control" over franchisees without diminishing the brand.

“Control” over Franchisees is Definitely a Gray Area

In *Hall v. Marriott International, Inc.,* No. 319CV01715JLSAHG, 2021 WL 1906464, at *11 (FN 10 & 11) (S.D. Cal. May 12, 2021), the court recently ordered the franchisor to produce resort fee data of its franchisees, commenting:

> “Typical franchise agreements, for example, include an audit provision that gives the franchisor the right to access the franchisee's books and see all the information used to calculate the franchisor's portion of that revenue.”

> “Plaintiff noted at the hearing that Defendant handles the website where consumers can book rooms in both Defendant's hotels and franchise hotels. Thus, access to the data from online bookings likely should be readily available without needing to request it from the franchisees.”

> “At the hearing, Defendant contended that the franchised hotels are completely separate entities from Marriott-managed hotels, and that Defendant does not have control over the franchise hotels and could not request the resort fee data from them. However, as explained at the hearing, the Court was able to find Marriott franchise agreements through a simple online search, which contain nearly identical audit provisions.”

California AG on Application of the CCPA to Franchises

Comment / Question to the California AG about the new CCPA regulations:

- Does CCPA apply to the franchisee for collecting data on behalf of the franchisor?

The California Attorney General's response:

- The regulation provides general guidance for CCPA compliance.
- Further analysis is necessary before proposing a regulation that provides guidance specific to the franchisor/franchisee relationship and the statutory definition of "business" in CCPA.

In other words, wait and see.

Two Recently Passed State Data Protection Laws

Colorado Privacy Act

•Effective July 1, 2023
•**Unlike CCPA there are no revenue thresholds**
•Excludes job applicants and employees
•Right of access, correction, deletion, portability, and **includes universal opt-out**
•Enforcement by AG-no private right of action
•Penalties governed by Colorado Consumer Protection Act

Virginia Consumer Data Protection Act

•Effective January 1, 2023
•Similar to CCPA and CPRA
•Requires **GDPR-like data protection assessments**
•Like GDPR includes “controller” and “processor” terminology
•No private right of action – enforcement limited to AG

and a new Uniform Law.

Federal Law by Sector

Financial

- GLBA Gramm-Leach-Bliley Act
- FCRA Fair Credit Reporting Act
- FACTA Fair Accurate Credit Transactions Act

Healthcare

- HIPAA

Health Insurance Portability & Accountability Act

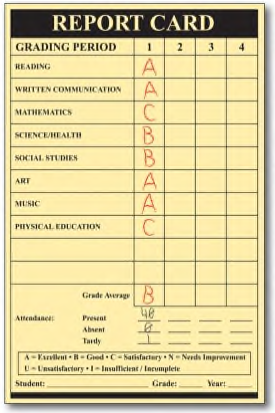
Federal Law by Type of Information

COPPA
Childrens Online Privacy & Protection Act

TCPA
Telephone Consumer Protection Act

CAN-SPAM
Commercial and Marketing Spam

FERPA
Federal Education Rights & Privacy
Protection Act



Federal Law Changes Coming?

- Federal Privacy Law

- Expanded or Diminished Role of the FTC

Payment Card Industry – PCI DSS

- Franchisees that collect credit card payments will be required to comply with what is known as the Payment Card Industry Data Security Standard ("PCI DSS").
- PCI DSS contains a set of security requirements that uses current technology and physical security best practices to protect cardholder data. All organizations that process, store, or transmit credit card information must be PCI DSS compliant.
- Franchisors may be at risk of violations if franchisees fail to adhere to PCI DSS or maintain poor security controls in their storefronts and businesses.

FTC Enforcement Orders for Data Security

Upon entering a consent order, the FTC will typically require companies to put in place a comprehensive, process-based data security program with specifics such as:

- Annual employee training
- Access controls
- Monitoring systems for data security incidents
- Patch management systems
- Encryption
- Outside assessors to audit and document the security program
- Annual presentation of written information security plan to Board
- Senior manager certification of program under oath

UN Conference on Trade and Development: Data Regulation Map

66%
COUNTRIES WITH
LEGISLATION

10%
COUNTRIES WITH
DRAFT LEGISLATION

19%
COUNTRIES WITH
NO LEGISLATION

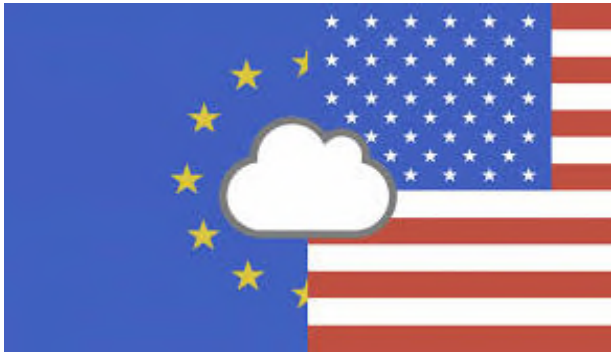
5%
COUNTRIES WITH
NO DATA

https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Key Global Privacy and Data Security Laws

- GDPR (EU's General Data Protection Regulation)
- BDSG (Germany's Bundesdatenschutzgesetz)
- CPPA (Canada's Consumer Privacy Protection Act)
- DSL (China's Data Security Law)
- Brazil, India, Australia, Japan, Chile


WHAT IS GDPR AND WHY SHOULD YOU CARE
AS AN AMERICAN ?



KEY DATA PROTECTION QUESTIONS

What steps can a franchisor take to be better prepared for a data breach?

What should a franchisor do upon discovering the unauthorized access to or use of personal information?

Building a Data Privacy and Security Framework

- Map and prioritize your data by importance and sensitivity
- Vet and manage vendors for data privacy and security
- Have an Information Security Policy
- Have an Incident Response Plan
- Set up vendors in advance
- Practice with Table Top Exercises
- Regularly inform and update C-Suite and Board on efforts
- Maintain an inventory of contracts for data notification
- Evaluate your cyberinsurance

Ransomware & Cyberinsurance

- Ransomware as a Service is rampant.
- Maintain effective backups of your data, so you need not pay a ransom.
- Cyber insurance is now more expensive with tougher underwriting.
- Many franchisee policies or one blanket master policy?
- What is excluded from coverage? Language matters.

Five Takeaways for Franchisors

1. Make sure your Privacy Policy is accurate and your franchisees understand their data obligations.
2. Know who owns or controls the customer data in your framework.
3. Maintain and practice your Incident Response Plan with your Incident Response Team.
4. Regularly discuss data privacy and security issues and progress with your C-Suite and Board.
5. Keep recent backups and use anti-phishing exercises and other training to avoid ransomware and malware.

For Kansas CLE Attendees

ATTENDEE VERIFICATION CODE:

LathopGPM2021

Thank you!

Michael R. Cohen
612.632.3345
michael.cohen@lathropgpm.com

Gaylen Knack
612.632.3217
gaylen.knack@lathropgpm.com

Tedrick Housh
816.460.5642
tedrick.housh@lathropgpm.com

Emily Holpert
312.920.3321
emily.holpert@lathropgpm.com