International Franchise Association
55th Annual Legal Symposium
May 7-9, 2023

Navigating Privacy Regulation and Franchise System Implications in 2023 and Beyond

Allaire Monticollo
Venable LLP
Washington, DC

Mara Zusman
Hilton
McLean, Virginia

Tara Sugiyama Potashnik
Venable LLP
Washington, DC

NAVIGATING PRIVACY REGULATION AND FRANCHISE SYSTEM IMPLICATIONS IN 2023 AND BEYOND[1]

> While many U.S. fora continue to consider whether a consumer privacy legal framework grounded in the notion of control remains the ideal governance structure, what has emerged with the successes of the data economy are the numerous positive outcomes associated with treating data as unattached from property rights[2]

I. Introduction

A sea change in the treatment of personal data occurred in 2018, when the European General Data Protection Regulation ("GDPR") went into effect.[3] For the first time, companies were obligated to be transparent about how they process personal data; were required to grant certain rights to individuals, including the right to access a copy of personal data and the right to request the deletion of personal data; and were ordered to report data breaches within a 72-hour window. Moreover, the GDPR applied not just to companies within the European Economic Area ("EEA"); it also applied to companies outside the EEA that offered goods or services to residents of the EEA.

Since 2018, privacy legislation has proliferated around the globe. From Brazil to Nigeria to China, numerous jurisdictions have enacted different privacy laws. It is the volume of, and variation among, those laws, that has made privacy the complex – and exciting – field it is today.

---

[1] The authors wish to acknowledge Noah Joshua Phillips, Cravath, Swaine & Moore LLP (and Former Commissioner of the Federal Trade Commission) for his contribution as a speaker on this panel and Leslie Pujo, Plave Koch PLC for her contributions to this paper.

[2] THOMAS M. BOYD & TARA SUGIYAMA POTASHNIK, NAT'L BUS. COAL. ON E-COM. & PRIVACY, DATA OWNERSHIP: THE SUITABILITY OF A CONSUMER PROPERTY RIGHT IN A 21ST CENTURY ECONOMY 11 (Sept. 29, 2020), https://www.venable.com/-/media/files/publications/2020/09/data-ownership-paper-final.pdf?la=en&rev=e3522472145456 89b6bb54c821d7ebb&hash=BCAEE50FB4CD8EAE653DF8BB6871C16AFD9E5F27 .

[3] *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L. 119), 1-88 [hereinafter "GDPR"]. A discussion of the requirements of the GDPR and its effect on franchising is beyond the scope of this paper. For more information on the GDPR, *see* Helen Goff Foster, Dawn Newton, & John Pratt, *Collect if You Dare: Practical Strategies to Help Franchise Parties Cope with GDPR and Other International Privacy Laws and the Evolving US Privacy and Data Security Landscape*, AM. BAR ASS'N (Oct. 16, 2019).

As countries and some U.S. states pass privacy and data security legislation, and as consumer awareness of privacy increases, it is critical that those in the franchise space understand the field of data privacy and data security and help ensure they have appropriate processes and policies in place both to meet regulatory requirements and minimize reputational risk.

This paper introduces the field of privacy and data security, explains laws that are applicable to franchisors and franchisees operating in the United States,[4] highlights the importance of privacy programs, and explores several issues that franchisors and franchisees that collect personal data should consider.

II. What is Data Privacy?

Privacy law in the United States covers an array of matters ranging from the Fourth Amendment's protection of a "reasonable expectation of privacy" to torts for invasion of privacy, public disclosure of private facts, appropriation, defamation, infliction of emotional distress, and placing a person in a false light.[5] Although those are all interesting and important areas of law, the focus of this paper is on the growing field of "data" or "information" privacy law.[6] Data privacy law in the United States originated with concerns about eavesdropping in the Colonial period and has developed over time to respond to new technology and methods of gathering (and using) information – from the telegram to the Internet.[7]

---

[4] As set forth in more detail in Part III of this paper, franchisors and franchisees may need to comply with data privacy and security laws of both the countries in which they operate, as well as the countries of the customers they serve. For more information about international privacy laws, *see* Foster et al., *supra* note 3.

[5] *See, e.g.*, Erwin Chemerinsky, *Rediscovering Brandeis's Right to Privacy*, 45 BRANDEIS L.J. 643, 645 (2007); Sahara Williams, *CCPA Tipping the Scales: Balancing Individual Privacy with Corporate Innovation for a Comprehensive Federal Data Protection Law*, 53 IND. L. REV. 217, 220 (2020) (citing DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 32-33 (Wolters Kluwer 6th ed. 2018).

[6]This paper uses the terms, "Data Privacy" and "Data Security" to cover all laws and regulations referring either to "personal data" or "personal information."

[7] *See, e.g.*, Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY 1-36 (2006). Just as technology has evolved over time, so, too, have the concerns about the nature of both the personal information to be protected, as well as the potential misuses. For example, Justice Brandeis's argument for a new right to privacy in 1890 stemmed from his concern about newspapers publishing scurrilous gossip, while 21st Century data privacy and security laws have been enacted in response to concerns about harvesting and selling troves of consumers' personal information, tracking consumer behavior, identity theft, and the right to be forgotten. *Id*.

Today, most businesses collect, use, and/or store personal information of employees and customers, and therefore must be familiar with the changing landscape in data privacy law.[8] Before exploring the data privacy framework applicable to U.S. franchise systems in more detail, it is important to understand the difference between "data privacy" (the focus of this paper) and the related topic of "data security," as well as to identify working definitions for several key terms in data privacy and security law. For example:

- "Data Privacy" means the right to control the collection, use, and dissemination of personal information[9] (or what you must, can, and cannot do with personal data).
- "Data Security" means how personal information is protected from unauthorized access or use and how to respond to any unauthorized access or use.[10]
- "Personal Data" (or "Personal Information") means generally any information that identifies, relates to, or is/could reasonably be linked to an identified or identifiable natural person.[11] Personal data often includes data elements, such as name, date of birth, email address, social security number, and driver's license number, but other data elements – such as IP address, records of products purchased, and geolocation data – also can be considered personal data as defined by privacy laws.

---

[8] *See, e.g.*, Bloomberg Law, *Top Legal Challenges Facing General Counsel in 2023* (Feb. 6, 2023),https://pro.bloomberglaw.com/brief/top-legal-challenges-facing-general-counsel-in-2023/) (listing privacy as one of the top legal challenges facing general counsel in 2023); Oliver Sullivan, *The Top Legal Trends for 2023*, LAW. MONTHLY (Jan. 31, 2023), https://www.lawyer-monthly.com/2023/01/the-top-legal-trends-for-2023/ (including privacy among the top legal trends for 2023).

[9] *See* STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., IL 11207 DATA PROTECTION AND PRIVACY LAW: AN INTRODUCTION (updated Oct. 12, 2022), https://crsreports.congress.gov/product/pdf/IF/IF11207.

[10] *See id*.

[11] *See e.g.,* Cal. Civ. Code § 1798.140(v)(1) (2023) (defining "personal information" as 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") [hereinafter CCPA]; Va. Code Ann. § 59.1-575 (2023) [hereinafter VCDPA]; Colo. Rev. Stat. § 6-1-13-3(17) (2023) [hereinafter CPA]; Utah Code §13-6-1-101(24) (2023) [hereinafter UCPA]; and Conn. Gen. Stat. § 42-515(18) (2023) [hereinafter CTDPA].

- "Controller" means the natural or legal person that determines that determines the purpose and means of processing personal data.[12]
- "Process" or "processing" means "any operation or set of operations performed, whether by manual or automated means on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data."[13]
- "Processor" means "a natural or legal entity that processes personal data on behalf of a controller."[14]

III. The Law(s) Applicable to Franchise Systems Operating in the United States

Franchisors and franchisees operating in the United States are required to comply with applicable U.S. federal and state laws, but they also may have to comply with privacy laws promulgated by countries around the world. Many countries' privacy laws are extraterritorial, meaning that they extend outside that country's borders. GDPR, for example, applies not only to companies that operate within the EEA, but also to companies that are located outside the EEA but target residents of the EEA, such as by making a website available in French. While this paper focuses on the privacy legal framework in the United States, franchisors and franchisees should also recognize that they may need to do a fact-specific analysis to determine whether they also must comply with other countries' privacy laws.

Presently, the United States does not have a generally applicable, comprehensive federal data privacy law, but rather a patchwork of issue-specific, industry-specific, and state-specific laws on the federal and state level.[15] As a result, franchise systems may

---

[12] VCDPA. §59.1-571.

[13] *Id*.

[14] *Id.*

[15] For example, federal laws protect, among other things, the online privacy of children under age 13 (Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6505), health information (Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.)); consumer credit information (Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x;); financial information (Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809); and video privacy (Video Privacy Protection Act, 18 U.S.C. § 2710). In addition, the FTC has promulgated data security rules, and all 50 states have enacted data breach laws. For examples of data security laws and regulations, *see* FTC Safeguards Rule, 16 C.F.R. § 314 (2022); Nat'l Conf. of State Legislatures, *2022 Security Breach Legislation* (last updated Sept. 29, 2022), https://www.ncsl.org/technology-and-communication/2022-security-breach-legislation.

be subject to various privacy laws, including those laws that (1) are applicable to their industry; (2) have been promulgated in the state(s) where their outlets are located; and (3) apply in the countries and states where they seek customers.

This scenario creates a challenging compliance landscape. Franchise systems may have to evaluate whether to: (1) adopt a customer-specific approach to compliance; or (2) comply with the most restrictive privacy law. For example, in the United States, companies may send marketing emails to customers as long as the email contains a link to allow the recipient to unsubscribe from further emails. But GDPR prohibits companies from sending marketing emails to residents of the EEA unless and until the company obtains consent from the recipient of the marketing emails. So if a franchise is located in the United States but targets customers in both the United States and France, the franchise will need to decide whether it is going to treat customers from the United States and France differently for marketing purposes or whether the franchise is going to obtain consent from all customers before sending them marketing emails. Such variations exist among the laws of various countries, and now, as U.S. states increasingly pass privacy legislation, such variations also exist among U.S. states' laws.

A. State Privacy Landscape[16]

In the absence of federal privacy legislation, states have entered the privacy fray by passing their own comprehensive laws. The laws impact franchise systems in many ways, including those that use common point-of-sale systems, reservation systems, loyalty programs, mobile apps, websites/social media, and Internet of Things tools.

(1) Summary of Existing Comprehensive State Privacy Laws and Regulations

In 2018, California became the first U.S. state to enact comprehensive privacy legislation with the California Consumer Privacy Act of 2018 ("CCPA").[17] The CCPA originated as a ballot initiative, and after the ballot initiative obtained enough signatures to go before California voters, members of the California legislature introduced the CCPA in its place. The legislation progressed quickly, was signed into law on September 23, 2018, and became effective on January 1, 2020. After that date, entities that do business

[16] Please note that this paper does not address requirements under Iowa S.F. 262, a new privacy law that was approved by the Iowa legislature and signed into law by Governor Kim Reynolds (R) in the Spring of 2023. S.F. 262, 90th Gen. Assemb., Reg. Sess. (Iowa 2023). The Iowa privacy law will take effect on January 1, 2025. *Id*.

[17] Before 2018, states had not addressed privacy in a comprehensive sense. States addressed privacy in a piecemeal manner, focusing on more limited privacy requirements such as privacy policies. After 2018, and with the passage of the CCPA, states started to more holistically address requirements surrounding businesses' collection, use, and transfer of data about individuals in online and offline spheres.

in California and meet particular data processing[18] or revenue thresholds must: (a) make certain disclosures regarding their personal information collection and processing activities; (b) grant consumers certain rights related to personal information about them; and (c) maintain contracts with their business partners that, among other matters, contain specific terms.[19]

After the CCPA became law, several other states joined California by passing their own versions of comprehensive privacy legislation, and California's CCPA was amended by a new ballot initiative, the California Privacy Rights Act of 2020 ("CPRA"). By the end of 2023, five comprehensive state privacy laws will be in effect: the CPRA, which materially amends the CCPA (collectively, "CCPA")[20], the Virginia Consumer Data Protection Act ("VCDPA")[21], the Colorado Privacy Act ("CPA")[22], the Utah Consumer Privacy Act ("UCPA")[23], and the Connecticut Act Concerning Personal Data Privacy and Online Monitoring ("CTDPA").[24] The timeline below specifies the effective dates of each state's privacy laws.[25]

[18] "Processing" is typically defined to mean any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

[19] CCPA §§ 1798.100 –.199.

[20] *Id.*

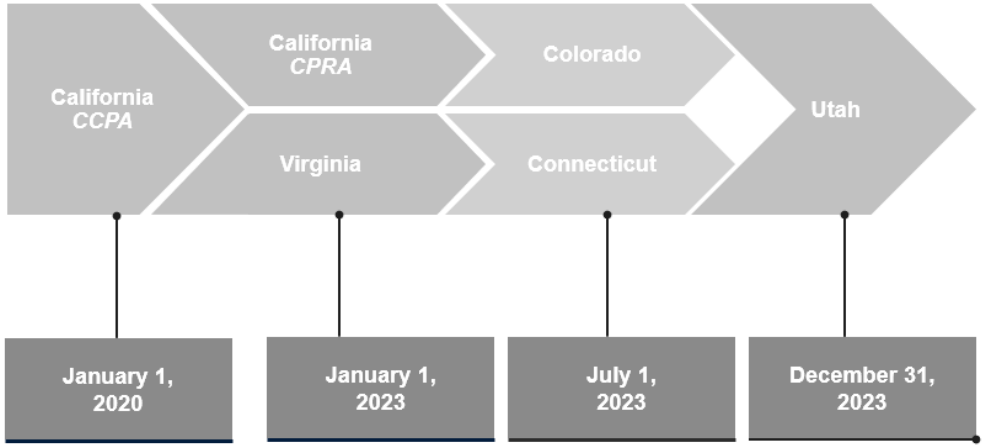
[21] VCDPA. §§ 59.1-575–585.

[22] CPA §§ 6-1-1301–1313; 6-1-104–110.

[23] UCPA §§ 13-61-101–404.

[24] CTDPA §§ 1-12. Several privacy bills are pending in the states. *See, e.g.,* S.B. 947, 32nd Leg., (Haw. 2023); S.B 15, 2023 Gen. Assemb., Reg. Sess. (Ky. 2023); H.B. 807, 445th Sess., (Md. 2023); S.B. 5, 123rd Gen. Assemb., (Ind. 2023); S.B. 384, 68th Leg. Reg. Sess., (Mont. 2023); H.B. 1038, 59th Leg., (Okla. 2023); S.B. 619, 82nd Leg. Assemb., (Or. 2023); H.B. 4, 88th Leg. Reg. Sess., (Tex. 2023).

[25] In addition, the Nevada legislature has enacted a more limited state privacy law that requires regulated entities to make certain public disclosures and provides Nevada residents with a limited right to opt out of sales of covered information. *See* Nev. Rev. Stat. §§ 603A.300–.360 (2023).



The CCPA, VCDPA, CPA, CTDPA, and UCPA (collectively, "comprehensive state privacy laws" or "comprehensive laws") are broadly similar in three respects. First, these comprehensive state privacy laws all apply to information that is linked or reasonably linkable to an individual or household.[26] Second, all of these comprehensive state privacy laws provide consumers of the respective state with certain rights, which, depending on the state, may include rights to access, delete, correct, and opt out of certain activities or transfers of personal information or personal data. Third, all of these comprehensive state privacy laws prescribe notice requirements for businesses that collect and/or process personal information, which generally require businesses to publish a privacy policy that discloses the following: (a) the categories of personal information or personal data that is collected or processed; (b) the purposes for collection or processing such information; and (c) how consumers may exercise their rights, in addition to other information.[27] Though these laws are broadly similar in structure, they vary in a number of key respects, which are summarized in the table below.

Requirement	CCPA	VCDPA	CPA	UCPA	CTDPA
Consumer Right to Know and Access	✓	✓	✓	✓	✓
Consumer Right of Portability	✓	✓	✓	✓	✓
Consumer Right of Deletion	✓	✓	✓	✓	✓
Consumer Right to Opt Out of the Sale of Personal Data	✓	✓	✓	✓	✓

[26] *See, e.g.*, CCPA § 1798.140(v)(1).

[27] The privacy notice requirements under these comprehensive state privacy laws require more robust and detailed disclosures than the requirements that existed before the comprehensive laws were enacted. In addition, the older requirements applied to operators of commercial websites or online products or services that collected certain information; notice requirements under these comprehensive laws apply more broadly.

Requirement	CCPA	VCDPA	CPA	UCPA	CTDPA
Consumer Right to Opt Out of the Sharing of Personal Information for Cross-Context Behavioral Advertising	✓				
Right to Opt Out of Processing Personal Data for Targeted Advertising[28]		✓	✓	✓	✓
Right to Correct Inaccurate Personal Data	✓	✓	✓		✓
Right to Opt Out of Profiling that Produces Legal or Similarly Significant Effects Concerning a Consumer		✓	✓		✓
Rights to Limit Use of or Opt Out of Sensitive Data Processing	✓			✓	
Opt-In Consent for Sensitive Data Processing Required		✓	✓		✓
Individual Rights Request Appeal Process Required		✓	✓		✓
Impact Assessment Requirements	✓	✓	✓		✓
Service Provider/Processor Contractual Provisions	✓	✓	✓	✓	✓
Privacy Policy Requirements	✓	✓	✓	✓	✓
Application to Personnel (Employee) and Business Data	✓				

In addition, as described in more detail below, processes are currently underway in California and Colorado to stand up regulations to implement the CCPA and the CPA, respectively. In California, a brand new state agency called the California Privacy Protection Agency ("CPPA") is tasked with issuing regulations to implement the CCPA and with enforcing the law alongside the California Attorney General. In Colorado, the Colorado Attorney General is tasked with issuing regulations to implement the CPA and with enforcing the law itself.

[28] Under the CCPA, consumers have the right to opt out of "sharing" (*i.e.,* disclosures) of personal data for cross-context behavioral advertising, defined as "targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts." The other states mentioned above provide the right to opt out of the processing of personal data for targeted advertising.

(2) Comparison of Existing Comprehensive state privacy laws and Regulations

The following is a brief summary of how these comprehensive state privacy laws address certain key matters.

Thresholds for Applicability. These comprehensive state privacy laws generally apply to any business that collects and/or processes the personal information of 100,000 consumers or households of the respective state.[29] However, the CCPA has an additional threshold, also applying to any entity that "does business" in California and generates at least $25 million in annual gross revenue.[30]

Exemptions. These comprehensive state privacy laws also each exempt certain types of entities and/or data from coverage. These exemptions are detailed in the table below, which notes whether the relevant exemption applies to: (a) entities that are regulated by a particular law; (b) data regulated by the particular law; or (c) activities regulated by the particular law.

Exception	CCPA	VCDPA	CPA	UCPA	CTDPA
Children's Online Privacy Protection Act ("COPPA")		Entity[31]	Data[32]	Entity[33]	Entity[34]
Fair Credit Reporting Act ("FCRA")	Activity[35]	Activity[36]	Activity[37]	Activity[38]	Activity[39]

[29] *See, e.g.*, VCDPA § 59.1-576(A).

[30] CCPA § 1798.140(d)(1)(A). As of the date of this paper, the meaning of "doing business" in California is an open issue.

[31] VCDPA § 59.1-576(D).

[32] CPA § 6-1-1304(2)(j)(IV).

[33] UCPA § 13-61-102(3).

[34] CTDPA § 3(c).

[35] CCPA § 1798.145(d).

[36] VCDPA § 59.1-576(C)(10).

[37] CPA § 6-1-1304(2)(i).

[38] UCPA § 13-61-102(2)(j).

[39] CTDPA § 3(b)(11).

Exception	CCPA	VCDPA	CPA	UCPA	CTDPA
Gramm-Leach-Bliley Act ("GLBA")	Data[40]	Data, Entity[41]	Data, Entity[42]	Data, Entity[43]	Data, Entity[44]
Medical Information and Protected Health Information	Data[45]	Entity, Data[46]	Data[47]	Data[48]	Data[49]
Nonprofit organization[50]	Entity[51]	Entity[52]		Entity[53]	Entity[54]

[40] CCPA § 1798.145(e).

[41] VCDPA § 59.1-576(B)(ii).

[42] CPA § 6-1-1304(2)(j)(II).

[43] UCPA § 13-61-102(2)(k).

[44] CTDPA § 3(a)(5).

[45] CCPA § 1798.145(c).

[46] VCDPA § 59.1-576(B)(iii), (C)(1).

[47] CPA § 6-1-1304(2)(a).

[48] UCPA § 13-61-102(2)(g), (4).

[49] CTDPA § 3(b)(1).

[50] Note that the state laws' definitions of "nonprofit organization" differ.

[51] *See* CCPA § 1798.140(d) (defining "business" to exclude nonprofit organizations).

[52] VCDPA § 59.1-576(B)(iv); *see also* § 59.1-575 (defining "nonprofit organization" to mean "any corporation organized under the Virginia Nonstock Corporation Act (§§ 13.1-801–946) or any organization exempt from taxation under §§ 501(c)(3), 501(c)(6), or 501 (c)(12) of the Internal Revenue Code").

[53] UCPA § 13-61-102(2)(d); *see also* § 13-61-101(23) (defining "nonprofit corporation" to include domestic nonprofits organized under the Utah Revised Nonprofit Corporation Act and foreign nonprofits that are incorporated under laws other than Utah's and would qualify as nonprofits if formed under Utah law).

[54] CTDPA § 3(a)(2); *see also* § 1(17) (defining "nonprofit organization" to mean "any organization that is exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent corresponding internal revenue code of the United States, as amended from time to time.").

Exception	CCPA	VCDPA	CPA	UCPA	CTDPA
Business Information[55]		Data[56]	Data[57]	Data[58]	Data[59]
Human Resources Information[60]		Data[61]	Data[62]	Data[63]	Data[64]

[55] "Business Information" includes information that reflects a transaction or communication between a business and another entity's employees, owners, directors, officers, and contractors, solely within the context of due diligence or providing or receiving a product or service.

[56] *See* VCDPA § 59.1-575 (defining "consumer" to not include "a natural person acting in a commercial or employment context").

[57] *See* CPA § 6-1-1303(6)(b) (defining "consumer" to exclude "an individual acting in a commercial or employment context").

[58] *See* UCPA § 13-61-101(10) (defining "consumer" to exclude "an individual acting in an employment or commercial context").

[59] *See* CTDPA § 1(7) (defining "consumer" to exclude "an individual acting in a commercial or employment context or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency").

[60] "Human Resources Information" includes information about job applicants, employees, owners, directors, officers, medical staff, and contractors, so long as that information is used solely within that person's role or former role with respect to the business. This exception also extends to emergency contact information and personal data of relatives necessary to administer benefits.

[61] VCDPA § 59.1-576(C)(14).

[62] *See* CPA § 6-1-1303(6)(b) (defining "consumer" to exclude "an individual acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context").

[63] *See* UCPA § 13-61-101(10) (defining "consumer" to exclude "an individual acting in an employment or commercial context").

[64] *See* CTDPA § 1(7) (defining "consumer" to exclude "an individual acting in a commercial or employment context or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency").

Obligations for business contact data. As is apparent in the above table, the CCPA is the only of the above comprehensive state privacy laws that does ***not*** exempt business information and human resources/employee information from coverage.[65] Business contacts of California businesses must be notified of the business's information practices and must be notified that they can exercise rights granted by the CCPA, as related to information about them. Similarly, California businesses must notify applicants and employees of their information practices and recognize the exercise of certain rights granted by the CCPA in regard to information about such applicants and employees.

Data Security. These comprehensive state privacy laws require businesses or controllers to establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices must be appropriate to the volume and nature of the personal data the business or controller will process.[66]

Sensitive Data. These comprehensive state privacy laws generally impose heightened obligations and sometimes restrictions on processing "sensitive data" or "sensitive personal information." Though each state law defines "sensitive data" or "sensitive personal information" differently, each definition, at minimum, defines information revealing race, ethnicity, religion, or citizenship or immigration status as "sensitive."[67] The CCPA's definition of "sensitive personal information" is the broadest of the states, including personal information revealing any account log-in in combination with a code allowing access to that account, in addition to other data elements.[68] The CCPA, VCDPA, and CTDPA also classify precise geolocation information as sensitive data.[69]

Just as the states do not define "sensitive data" uniformly, neither do they impose uniform requirements or restrictions on processing such data. In Utah, consumers must receive notice and have an opportunity to opt out prior to the collection and processing of any sensitive information.[70] In California, consumers have the right to limit use and

---

[65] *See* CCPA § 1798.145(n)(3) (noting the CCPA's exemption for business contacts information and human resources information became inoperative on January 1, 2023).

[66] *See* VCDPA § 59.1-578(A)(3).

[67] CCPA § 1798.140(ae); VCDPA § 59.1-575 (defining "sensitive data"); CPA § 6-1-103(24); CTDPA § 1(27); UCPA § 13-61-101(32).

[68] CCPA § 1798.140(ae). Common data elements considered "sensitive" under comprehensive laws include race and ethnicity information, religious affiliation, and sexual orientation.

[69] *Id.*; VCDPA § 59.1-575 (defining "sensitive data"); CTDPA § 1(27).

[70] UCPA § 13-61-101(32).

disclosure of sensitive personal information to only those uses and disclosures that are necessary for certain business purposes, such as: (a) activities to ensure security and integrity; (b) performing services on behalf of a business; and (c) activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business.[71] The remaining states take a more restrictive approach, requiring businesses to secure opt-in consent prior to processing information classified as "sensitive."[72]

Assessments. Most comprehensive state privacy laws require data controllers (such as a franchisor or franchisee) to conduct data protection assessments ("DPAs") when the controller processes personal information for certain purposes. The VCDPA, CPA, and CTDPA all require controllers to conduct DPAs for the following processing activities: (1) processing personal data for purposes of targeted advertising; (2) sales of personal data; (3) processing personal data for purposes of profiling, where such profiling presents a reasonably foreseeable of legally significant effects; (4) processing sensitive data; and (5) and processing activities involved personal data that present a "heightened risk of harm" to consumers.[73]

These comprehensive laws require assessments to identify and weigh the benefits that may flow from the processing to the controller, consumers, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be put in place by the controller to reduce such risks. Controllers must also factor the following into assessments: use of de-identified data, the reasonable expectations of consumers, the context of the data processing, and the relationship between the controller and the consumer.[74]

These laws also provide that controllers must make the required DPAs available to their state Attorney General upon request.[75] The CCPA directs the state's new privacy agency, the CPPA, to issue regulations requiring businesses whose processing activities present a "significant risk to consumers' privacy or security" to: (1) perform an annual cybersecurity audit, and (2) submit to the CPPA on a regular basis a risk assessment with respect to personal information processing, including whether the processing involves sensitive personal information.[76] As of the date of this paper, these regulations have not

[71] CCPA § 1798.140(ae).

[72] VCDPA § 59.1-578(A)(5); CTDPA § 6(a)(4); CPA § 6-1-1308(7).

[73] VCDPA § 59.1-580(A); CPA § 6-1-1309(2); CTDPA § 8(a).

[74] VCDPA § 59.1-580(B); CPA § 6-1-1309(3); CTDPA § 8(b).

[75] VCDPA § 59.1-580(C); CPA § 6-1-1309(4); CTDPA § 8(c).

[76] CCPA § 1798.185(a)(15).

yet been promulgated by the CPPA. The UCPA does not make specific reference to DPAs or other assessments.

Global Privacy Controls / Universal Opt-Out Mechanisms. Some comprehensive state privacy laws contain provisions related to "global privacy controls" or "universal opt-out mechanisms," which are browser extensions or other device-based settings, that allow consumers to "broadcast" their opt out preferences related to data sales, sharing, and targeted advertising across the Internet. The proposed regulations currently under consideration by the CPPA would require businesses to recognize and honor global privacy controls.[77]

On the other hand, Colorado and Connecticut take graduated approaches to such controls. The CPA will allow businesses to honor universal opt-out mechanisms at their discretion from July 1, 2023 until July 1, 2024. After the latter date, Colorado businesses will be required to universal opt-out mechanisms.[78] Similarly, Connecticut will require businesses to honor universal opt-out preference signals starting on January 1, 2025.[79] The VCDPA and UCPA do not address global privacy controls.

Contractual Obligations. Each of these comprehensive state privacy laws requires data controllers or businesses to enter into contractual agreements with data processors, service providers, contractors, or other third parties who process personal information on behalf of and at the direction of the controller.[80] Though specific contractual requirements vary with each state law, in general, data processors must be prohibited from using personal data for any purpose other than providing enumerated services to a controller.[81] While the majority of states use "processor" as an umbrella term to describe various entities that may process personal data on behalf of a controller, California takes a unique approach by separately defining "service provider," "contractor," and "third party," and prescribing distinct contractual requirements for each type of entity.[82]

---

[77] *See* Cal. Privacy Prot. Agency, *Final Regulations Text* § 7025 (Feb. 3, 2023), https://cppa.ca.gov/meetings/materials/20230203_item4_text.pdf.

[78] CPA § 6-1-1306(1)(a)(II).

[79] CTDPA § 5.

[80] CCPA §§ 1798.110(d), 140(j), (ag); VCDPA § 59.1-579(B); CPA § 6-1-1305(5); UCPA § 13-61-301(2); CTDPA § 7(b).

[81] CCPA §§ 1798.110(d), 140(j), (ag); VCDPA § 59.1-579(B); CPA § 6-1-1305(5); UCPA § 13-61-301(2); CTDPA § 7(b).

[82] VCDPA § 59.1-579(B); CPA § 6-1-1305(5); UCPA § 13-61-301(2); CTDPA § 7(b); *cf.* CCPA § 1798.140(ag), (j), (ai).

Enforcement and Rulemaking. Each of these comprehensive state privacy laws are enforceable by the respective state's Attorney General.[83] Generally, these laws require businesses to be provided a certain time period to cure alleged violations. These cure periods range from 60 days (CPA, CTDPA) to 30 days (VCDPA, UCPA). On January 1, 2025, the CPA's mandatory cure period will expire, while the CTDPA's cure period will become available at the discretion of the Connecticut Attorney General.

Beginning July 1, 2023, the CCPA will be enforced by the California Attorney General and the CPPA, the latter of which is also charged with drafting implementing regulations under the statute. The CCPA contains a limited private right of action related to certain data breaches, subject to a mandatory 30-day cure period.[84] For enforcement actions initiated by the CPPA, the agency will have discretion to issue an opportunity to cure alleged violations of the law.

The CPPA has initiated a rulemaking process to enact regulations to implement the CCPA. On February 14, 2023, after giving the public two opportunities to comment on different drafts of proposed rules, the agency sent the "final" regulatory package to the California Office of Administrative Law ("OAL") for review. The regulations may become effective after OAL approves them and formally transmits them to the California Secretary of State. These regulations remain in development, with the CPPA projecting April 2023 as the earliest possible date regulations could become effective. The CPPA also has initiated preliminary phases of another rulemaking related to cybersecurity audits, risk assessments, and automated decision-making under the CCPA by releasing a discussion draft of an invitation for preliminary comments on such subject areas.[85]

The CPA is the only other comprehensive state privacy law of those mentioned above that grants rulemaking authority to a state agency under the statute. Unlike the CCPA, the CPA does not authorize creation of a separate regulatory agency, but rather, directs the Colorado Attorney General to issue regulations as necessary to further the purposes of the statute. The Colorado Attorney General announced that his office had sent the "final" regulatory package to the Colorado Secretary of State on March 15, 2023, with an expectation that the rules will take effect on July 1, 2023.[86]

---

[83] CCPA § 1798.155; VCDPA § 59.1-584; CPA § 6-1-1311; UDPA § 13-61-402; CTDPA § 11.

[84] CCPA § 1798.150(b).

[85] *See* Cal. Privacy Prot. Agency, *Discussion Draft: Invitation for Preliminary Comments on Proposed Rulemaking – Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking* (Feb. 3, 2023), https://cppa.ca.gov/meetings/materials/20230203_item5.pdf.

[86] Colo. Att'y Gen., *Colorado Privacy Act (CPA) Rulemaking*, (last updated Mar. 15, 2023),https://coag.gov/resources/colorado-privacy-act/.

B. Federal Privacy Prospects in Congress

Efforts to pass comprehensive federal privacy legislation have been ongoing to date. Two central issues legislators continue to debate with respect to a federal privacy approach are preemption and enforcement. Members of Congress have been unable to reach consensus on whether a federal privacy law should preempt existing state laws or in the alternative stand alongside them (adding yet another set of requirements for companies to meet when processing personal data). Legislators have also not reached agreement on whether the enforcement vehicle for violations should rest with the FTC and state Attorneys General or if it should include a private right of action.

In 2022, Congress considered the American Data Privacy and Protection Act ("ADPPA") under H.B. 8152.[87] The ADPPA passed the House Energy and Commerce Committee, but it never went to the full House of Representatives floor for a vote. If enacted, the bill would have established certain data minimization requirements and prohibitions related to covered data processing. The ADPPA also would have also created consumer rights to access, correct, and delete covered data. In addition, the bill included a private right of action and would not have completely preempted existing comprehensive state privacy laws.

January 2023 marked the beginning of the 118th Congress. After elected representatives were sworn in as Members of the U.S. Senate and U.S. House of Representatives, congressional leaders began working on Committee assignments for new and existing Members. The two main congressional committees of jurisdiction over privacy-related issues are the Senate Commerce Committee and the House Energy and Commerce Committee. For the 118th Congress, Senator Maria Cantwell (D-WA) is the Chair of the Senate Commerce Committee, and Senator Ted Cruz (R-TX) is the Ranking Member. For the House Energy and Commerce Committee, Representative Cathy McMorris-Rodgers (R-WA) is the Chair, and Senator Frank Pallone (D-NJ) is the Ranking Member.

C. The Federal Trade Commission's ("FTC's") Advance Notice of Proposed Rulemaking

While it is unclear whether a federal privacy bill will advance through Congress, the FTC has indicated its intention to promulgate rules in the privacy space. On August 22, 2022, the FTC issued an Advance Notice of Proposed Rulemaking ("ANPR") relating to commercial surveillance and data security.[88] Through the ANPR, the FTC sought "public comment on the harms stemming from commercial surveillance and whether new

---

[87] American Data Privacy and Protection Act of 2022, H.R. 8152, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

[88] Fed. Trade Comm'n, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (Aug. 22, 2022).

rules are needed to protect people's privacy and information."[89] The FTC defined "commercial surveillance" as "the business of collecting, analyzing, and profiting from information about people," [90] and expressed concern that such surveillance could result in harm to consumers if companies fail to adequately secure consumers' personal data or if surveillance systems are addictive and negatively affect the mental health of children.[91]

Despite bringing hundreds of enforcement actions against companies for privacy and data security violations in the 20 years leading up to the ANPR, the FTC argued that "enforcement of the FTC Act alone may not be enough to protect consumers."[92] Rather, the FTC argued, "rules that establish clear privacy and data security requirements across the board and provide the Commission the authority to seek financial penalties for first-time violations could incentivize all companies to invest more consistently in compliant practices."[93]

To that end, the ANPR asked 95 questions, including

- Which practices do companies use to surveil consumers?
- Which measures do companies use to protect consumer data?
- How, if at all, do these commercial surveillance practices harm consumers or increase the risk of harm to consumers?
- Are there some harms that consumers may not easily discern or identify? Which are they?
- Are there some harms that consumers may not easily quantify or measure? Which are they?
- Has the Commission adequately addressed indirect pecuniary harms, including potential physical harms, psychological harms, reputational injuries, and unwanted intrusions?
- Which, if any, commercial incentives and business models lead to lax data security measures or harmful commercial surveillance practices? Are some commercial incentives and business models more likely to protect consumers

---

[89] Fed. Trade Comm'n, Press Release, *FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices*, (Aug. 11, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices [hereinafter FTC Privacy ANPR Press Release].

[90] 87 Fed. Reg. 51273, 51277.

[91] FTC Privacy ANPR Press Release.

[92] 87 Fed. Reg. 51273, 51278-51280.

[93] *Id.*

than others? On which checks, if any, do companies rely to ensure that they do not cause harm to consumers?[94]
- How do companies collect consumers' biometric information, including fingerprints and facial images?
- How cost-effective is contextual advertising as compared to targeted advertising?
- In which circumstances is consumer consent likely to be effective?
- In which contexts are transparency or disclosure requirements effective?

But not all stakeholders agree that the FTC should use an ANPR to create rules regarding consumer data privacy and security. Some, like then-Commissioners Noah Joshua Phillips and Christine S. Wilson in their dissents,[95] as well as the U.S. Chamber of Commerce in its comments,[96] assert that legislating comprehensive national rules for consumer data privacy and security is a complicated undertaking, that national consumer privacy laws pose consequential questions, and that Congress – not the FTC – should be responsible for enacting a national privacy law.[97] Many stakeholders believe that

---

[94] *Id*. at 51281-51285. The FTC received over 1,250 comments on the ANPR, which can be viewed at https://www.regulations.gov/docket/FTC-2022-0053 (last visited Feb. 10, 2023).

[95] 87 Fed. Reg. 51273, 51293-51299.

[96] U.S. Chamber of Com., *Comments on Advance Notice of Proposed Rulemaking; Extension of Comment Period, Federal Trade Commission; Trade Regulation Rule on Commercial Surveillance and Data Security Commercial Surveillance ANPR* (Nov. 21, 2022), https://www.regulations.gov/comment/FTC-2022-0053-1029.

[97] Then-Commissioner Phillips explained in his dissenting statement regarding the ANPR,

> The ANPR kickstarts the circumvention of the legislative process and the imposition upon the populace of the policy preferences of a majority of unelected FTC commissioners. The Supreme Court recently noted "a particular and recurring problem [of] agencies asserting highly consequential power beyond what Congress could reasonably be understood to have granted." Apparently the FTC is next up to the plate. Our Section 18 authority to regulate "unfair or deceptive acts or practices" goes only so far; and the ANPR contemplates reaching well beyond, including to common business practices we have never before even asserted are illegal. Reading the FTC Act to provide the Commission with the "sweeping and consequential authority" to mandate changes across huge swaths of the economy will test the limits of our congressional delegation.

Noah J. Phillips, *Dissenting Statement Regarding the Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking* 4 (Aug. 11, 2022) (references omitted),

Congress should enact preemptive federal legislation that would clearly define prohibited data practices that make personal data vulnerable to breach or misuses, while preserving the benefits that come from the responsible use of data.[98] Moreover, with at least five U.S. states already having enacted comprehensive privacy legislation and bills pending in numerous other states, then-Commissioners Phillips and Wilson and the Chamber of Commerce argued that FTC rulemaking would add to the patchwork of laws and regulations governing privacy and data security in the United States.

D. Other Federal Agencies

The FTC is not the only federal agency that has initiated a process related to data privacy in recent months. For example, in late 2022, the Consumer Financial Protection Bureau ("CFPB") published an outline of proposals and alternatives under consideration related to access and portability of consumer financial records.[99] In addition, in January 2023, the Federal Communications Commission issued a notice of proposed rulemaking related to preventing "digital discrimination of access to broadband internet access services."[100] Similarly, in January 2023, the National Telecommunications and Information Administration issued a request for comment on "privacy, equity, and civil rights" to inform a report the agency plans to publish on "whether and how commercial data practices can lead to disparate impacts and outcomes for marginalized or disadvantaged communities."[101] As a result, various federal agencies are considering privacy regulations or privacy-related matters that could impact franchisors, franchisees, their customers, or their suppliers in years to come.

---

https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Phillips%20Dissent%20to%20Commercial%20Surveillance%20ANPR%2008112022.pdf.

[98] *See, e.g.*, Privacy for America, *Principles for Privacy Legislation*, (last visited Mar. 28, 2023), https://www.privacyforamerica.com/overview/principles-for-privacy-legislation/.

[99] Consumer Fin. Prot. Bureau, *Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights, Outline of Proposals and Alternatives Under Consideration* (Oct. 27, 2022), https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf.

[100] Fed. Comm. Comm'n, Implementing the Infrastructure Investment and Jobs Act: Prevention and Elimination of Digital Discrimination, 88 Fed. Reg. 3681 (Jan. 20, 2023).

[101] Nat'l Telecomm. & Info. Admin., Privacy, Equity, and Civil Rights Request for Comment, 88 Fed. Reg. 3714 (Jan. 20, 2023).

III. Franchise System Data Privacy and Protection Programs - Brand Standards, Joint Employment, and Vicarious Liability

While the increasingly complex web of privacy laws poses challenges for all businesses, franchise systems, in particular, face unique issues in navigating the changing privacy law landscape due to the interconnected relationship between the franchisor, its franchisees, suppliers, and end consumers.

A. Impact of Data Breach on the Reputation of the Franchise Brand – Recognizing Privacy and Data Security as a Brand Standard

A franchisor's trademark is often considered to be its most valuable asset. And a core feature of a successful franchise system is the creation and delivery of a uniform product or service provided to customers through many independently owned and operated businesses operating under the franchisor's trademark.[102] Achieving this level of consistency generally requires that the franchisor exert some degree of monitoring or control over various facets of the franchisee's business. Moreover, the Lanham Act,[103] requires a trademark owner, such as a franchisor, to exercise adequate control over the use of its trademarks to protect the integrity of the mark - or risk loss of ownership of the marks.[104] As a result, franchisors typically create and implement "Brand Standards" or requirements regarding the "look, feel, and quality standards to which franchisees must adhere and which give the brand its identity and, hopefully, value."[105]

Traditionally, "Brand Standards" have included, among other things, detailed requirements and specifications for signage, décor, trade dress, uniforms, products used or sold in the franchise, product quality, customer service, and technology, such as point-

---

[102] *See, e.g.*, Instructional Sys. Inc. v. Comput. Curriculum Corp., 614 A.2d 124, 151 (N.J. 1992) (citations omitted).

[103] 15 U.S.C. §§ 1051-1141.

[104] *Id.*; *see also* Kerl v. Dennis Rasmussen, Inc., 682 N.W.2d 328, 337-38 (Wis. 2004) ("The 'control' of a franchisor does not consist of routine, daily supervision and management of the franchisee's business, but, rather, is contained in contractual quality and operational requirements necessary to the integrity of the franchisor's trade or service mark.")

[105] Bethany L. Appleby & Andrew P. Bleiman, *I Want It My Way: Brand Standards Disputes in Franchise Systems* 2, AM. BAR ASS'N (Nov. 2, 2022); *see also* Patterson v. Domino's Pizza, LLC, 60 Cal. 4th 474 (Cal. 2014) (finding that "[b]y following the standards used by all stores in the same chain, the self-motivated franchisee profits from the expertise, goodwill, and reputation of the franchisor").

of-sale or reservation systems.[106] On the other hand, franchisors generally avoid imposing detailed requirements about or exerting control over a franchisee's day-to-day operations (such as the hiring, firing, compensation, training, and discipline of employees) to, among other reasons, avoid vicarious or employment liability based on the actions of their franchisees. Similarly, franchisors generally require franchisees to "comply with applicable law," and avoid any requirements or guidance that might be construed as legal advice. Historically, data privacy was viewed as part of the franchisee's obligation to know and comply with "applicable law" with minimal, if any, specific requirements imposed by the franchisor.

Over the past 15-20 years, however, the franchising community has increasingly recognized that data privacy and data security are integral to brand integrity and more akin to Brand Standards like product quality or customer service than to day-to-day operations, such as employee hiring or discipline. Franchisors appeared to be moving in that direction at least from the mid-2000s as a result of heightened risk of data breaches and the resulting impact on the brand.[107] Franchisors also realized that the advent of PCI-DSS compliance requirements, the enactment of new privacy laws worldwide, and an understanding that franchisor assistance and control over point-of-sale systems, centralized reservation systems, payment card systems, and marketing and loyalty programs could lead to franchisor liability for franchisee privacy violations and date security breaches.[108]

In addition, a series of cases against franchisors alerted the franchising community that franchisors could not necessarily escape liability for franchisee data privacy or data security issues simply by pointing to the franchisee's failure to comply with applicable law. For example, in 2012, the FTC filed a claim against Wyndham Worldwide Corporation and subsidiaries, alleging, among other issues, that the franchisor's and its affiliates' "failure to maintain reasonable security allowed intruders to obtain unauthorized access to the computer networks of Wyndham Hotels and Resorts, LLC, and several hotels

---

[106] Appleby & Bleiman, *supra* note 105, at 2.

[107] *See, e.g.*, Catherine Boschee, Thomas Epstein, & Karin Simonson, *Implementing a Franchise-Wide Data Protection Program* 25-29, INT'L FRANCHISE ASS'N (2007) ("Although we do not wish to minimize the seriousness of this [vicarious liability] issue . . . the authors believe that compliance with data protection laws and privacy policies is a significant brand and quality issue, and that the franchisor can find its brand destroyed overnight if it does not require consistent, fair and lawful data practices across the franchise system.").

[108] *See* Michael K. Lindsay & Mark S. Melodia, *Data Protection and Privacy in Franchising: Who is Responsible?* 3, AM. BAR ASS'N (Oct. 16, 2013).

franchised and managed by Defendants."[109] Similarly, the FTC's 2014 enforcement action against Aaron's, Inc. (the franchisor) based on allegations that its franchisees engaged in deceptive trade practices by installing tracking "spyware" on their customers' rented computers sent shockwaves through the franchise community.[110]

In addition to the alarms that litigation often sounds, franchisors have increasingly recognized that a data breach can cause significant reputational harm to the franchise brand and the franchise system as a whole, especially since customers and media tend to associate a data privacy violation or data security breach with the brand and the franchisor – even if the violation or breach Is 100 percent attributable to a franchisee.[111] And the reputational harm caused by a data breach can be significant. For example, the Ponemon Institute, which issues an annual report on the cost of a breach and quantifies the potential losses, estimated that estimated "lost business" costs due to a data breach (*i.e.*, costs associated with business disruption and revenue losses from system downtime; cost of lost customers and acquiring new customers; and reputation losses and diminished goodwill) averaged $1.42 million worldwide in 2022 (or 32.6 percent of the total estimated average worldwide cost of $4.35 million for a data breach in 2022). [112]

---

[109] Complaint for Injunctive and Equitable Relief, F.T.C. v. Wyndham Worldwide Corp., No. 2:12-cv-1365 (D. Ariz. Aug. 9, 2012) (emphasis added); F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015); *see also* Keith v. Back Yard Burgers of Nebraska, Inc., No. 8:11CV135, 2012 WL 1252965 (D. Neb. 2012) (denying franchisor's motion to dismiss claim that franchisor was vicariously liable for a franchisee's printing of computer-generated receipts showing credit card expiration dates in violation of the Fair and Accurate Credit Transaction Act of 2003 based on allegations that the franchisor's point-of-sale system requirements and policies led to its exercise of actual control over the franchisee's operations, and that the franchisor was directly involved in and controlled the day-to-day operations).

[110] Aaron's, Inc., No. C-4442 (F.T.C. Mar. 11, 2014); *see, e.g.*, Len MacPhee, Paul Reeve, Shelly O'Callaghan, & Sally King, *Data Privacy and Security: Can Any Brand Sleep at Night?* 11, INT'L FRANCHISE ASS'N (2015); David B. Ramsay, *Data Security: Evolving Legal Duties and Challenges for Franchise Systems*, 20(3) J. INTERNET L. 3, 7-8 (2016). For a discussion of more recent data privacy and data security cases involving franchise systems, *see infra,* Part VI.

[111] *See* Ramsey, *supra* note 110, at 4 ("[A] breach at the franchisee level, having little or nothing to do with actions by the franchisor, may cause immense harm to the reputation of the entire brand in the eyes of the public, and can have an immediate and drastic impact on the entire franchise system.") (citation omitted).

[112] Ponemon Institute, *Cost of a Data Breach Report 2022* 9-12 (2022), https://www.ibm.com/downloads/cas/3R8N1DZJ. The Ponemon Institute calculates data breach by using "activity-based costing" to identify and assign a cost according to actual

For these reasons, many franchisors now treat data privacy and data security as Brand Standards and establish system-wide privacy and data security programs, which may include all or some of the following features:

- Requirement that franchisees establish and implement a data privacy and data security plan[113]
- Limitations on franchisee use of personal data of customers during and after the term of the franchise agreement
- Cybersecurity insurance requirements
- Requirements to use approved vendors and technology to address privacy and data security issues, including software, training, and incident response
- Providing sample forms
- Limitations on franchisee marketing,, including by email or text
- Providing training and guidance and/or recommending training conducted by third parties
- Reservation of the right to audit franchisees' data privacy and security practices

B. Joint Employment (and Other) Liability Arising Out of Franchisee Operations

At the same time privacy laws and franchise privacy programs have expanded, the franchising industry has been upended by another issue – the swinging pendulum of standards used to determine issues of joint employment (*i.e.*, where an employee is found to be employed by two or more putative employers) and employment misclassification (*i.e.*, where an employee has been misclassified as an independent contractor). As a result of these shifting standards, some franchisors have reevaluated the support and services that they provide to franchisees in an effort to avoid exercising (or retaining authority to exert) too much control of their franchisees and being exposed to liability for a franchisee's actions.[114] This trend of reducing or eliminating services and support

---

use for the following activities: detection and escalation, notification, post-breach response, and lost business. *Id.* at 54.

[113] *See infra,* Part IV for a detailed discussion about establishment of a Privacy Program.

[114] *See* Joyce Mazero, Karen Boring Satterlee, Eric H. Karp, Leonard H. MacPhee, Jess A. Dance & William W. Sentell, *Drawing Lines in Franchisor Support – Is It Necessary and Where Are the Lines to Draw in Today's Joint-Employment Environment?* 38 FRAN. L.J. 327, 347–49 (2019).

provided to franchisees contradicts and creates a tension with the move by franchisors to develop more comprehensive, systemwide data privacy and protection programs and impose new requirements on franchisees.

Further complicating the issue for franchisors, the states and federal government use different tests for evaluating joint employment and misclassification claims (although most focus to some degree on the franchisor's actual or reserved control over the franchisee and its employees).[115] The following is a brief overview of some of the more common tests:

- National Labor Relations Board ("NLRB") Joint Employment Rule– Most in the franchise industry are well-acquainted with the tortuous path that the NLRB has followed over the past several years in a quest to settle on a standard for joint employment beginning. To summarize:
    - Beginning in 1984, the NLRB focused on the actual exercise of "direct and immediate" control over the essential terms and conditions of a worker's employment, including hiring, firing, discipline, supervision, and direction.[116]
    - In the 2015 *Browning-Ferris Industries of California* ("BFI") decision, the NLRB reversed the long-standing precedent and held that either the reserved right to control (even if unexercised) or indirect control (such as through an intermediary) could be sufficient to establish a joint-employer relationship[117]
    - The April 2015 *Freshii* Advice Memorandum applied the same joint employment standard that the NLRB would announce in the BFI case and concluded that the franchisor of the Freshii system was not a joint employer because it did not directly or indirectly control the core

[115] A detailed discussion of joint employment, misclassification, and other potential claims against franchisors based on franchisee operations is beyond the scope of this paper. For more information *see, e.g.*, Sally Lee Foley, Thomas L. Gravell, & Nicolas Guibert de Bruet, *Joint Employers and the National Labor Relations Board*, 40 FRAN. L.J. 7 (2020); Theresa D. Koller & Norman M. Leon, *Independent Contractor or Employee? The Current State of the Ever-Changing Law and its Impact on Franchising*, AM. BAR ASS'N (2020); Mazero, et al., *supra* note 114; Stephen D. Aronson, Matthew B. Harris, Stuart Hershman, Nick R. Rotchadl, & Brian B. Schnell, *Joint Employer/Vicarious Liability Practical Applications in Enforcing System Standards Without Exercising Too Much Contr*ol, INT'L FRANCHISE ASS'N (2017); Mary-Christine Sungaila & Martin M. Ellison, *Joint Employer Liability in the Franchise Context: One Year After Patterson v. Domino's*, 35 FRAN L.J. 339 (2016).

[116] TLI, Inc., 271 N.L.R.B. 798 (1984) *overruled by* Browning-Ferris Indus. of Cal, Inc., 362 N.L.R.B. 186 (Aug. 27, 2015).

[117] 362 N.L.R.B. at 187.

terms and conditions of employment of its franchisees' employees.[118]

- In the 2017 *Hy-Brand Industrial Contractors* decision, the NLRB overruled *Browning-Ferris* and reinstated the previous standard requiring "direct control."[119]
- In 2018, the NLRB vacated *Hy-Brand* based on a finding that one of the board members should have recused himself from the case due to a potential conflict.
- The U.S. Court of Appeals for the D.C. Circuit affirmed the *Browning-Ferris* decision in 2018.[120]
- The NLRB issued a final rule in 2020, which reinstated the pre-*Browning* requirement that a putative employer exercise direct control over the employees.
- On April 22, 2022, the D.C. Circuit upheld McDonald's settlement with the NLRB in connection with the NLRB's 2014 complaint that McDonald's was a joint employer of its franchisees' employees – without making a finding on the joint employment issue.[121]
- On September 7, 2022, the NLRB published a Notice of Proposed Rulemaking, which would reinstate the *Browning-Ferris* standard requiring only "reserved" or "indirect" control.[122]

- Formal Control – whether the putative employer: (1) had the power to hire and fire the employees, (2) supervised and controlled employee work schedules or conditions of employment, (3) determined the rate and method of payment, and (4) maintained employment records.[123]

---

[118] Nat'l Lab. Rel. Bd. Office of General Counsel, Advice Memorandum, Nutritionality, Inc. d/b/a Freshii, Cases 13-CA-134294, 13-CA-138293, and 13-CA-142297 (Apr. 28, 2015), nlrb.gov/case/13-CA-134294?order=status&sort=desc. When the Freshii memorandum was issued, the new joint employment standard, which was later adopted in *Browning-Ferris Industries*, had been proposed.

[119] 365 N.L.R.B. No. 156 (Dec. 14, 2017).

[120] Browning-Ferris Industries of California, Inc., v. Nat'l Lab. Rel. Bd., 911 F.3d 1195, 1222 (D.C. Cir. 2018).

[121] Fast Food Workers Comm. v. Nat'l Labor Rel. Bd., 31 F.4th 807 (D.C. Cir. 2022).

[122] Standard for Determining Joint-Employer Status, 87 Fed. Reg. 54641 (Sept. 7, 2022).

[123] Pope v. Espeseth, Inc., 228 F. Supp. 3d 884 (W.D. Wis. 2017).

- In *Pope v. Espeseth, Inc.*,[124] employees of a window washing franchisee alleged that the franchisor and its franchisee were joint employers of the franchisee's window cleaner employees under the Fair Labor Standards Act ("FLSA"). The case turned on an evaluation of the second factor of the formal control test – whether the franchisor supervised and controlled the franchisee's employees via the detailed requirements of the operations manual. The court concluded that the franchisor did not have control over the employee's working conditions and was not their employer based, in part, on a finding that: (1) the franchisee was not required to follow the manual as drafted by the franchisor; (2) was free to adapt the manual and recommended forms, and (3) set its own employee policy.[125]

- In a 2018 decision, the U.S. District Court for the Southern District of New York rejected the New York Attorney General's argument that Domino's and its affiliates were joint employers of their franchisees' employees under the FLSA based, in part, on the following factors: (1) Domino's did not exercise control over hiring of employees despite requiring franchisees to run a criminal background check with an approved vendor; (2) quality control, compliance monitoring, and addressing customer complaints did not constitute control of the employees' employment conditions; and (3) Domino's ability to access the franchisee's employment records through the proprietary PULSE software system did not mean that Domino's maintained the employment records, but rather that access and review of the records was merely an extension of quality control procedures).[126]

---

[124] 228 F. Supp. 3d 884 (W.D. Wis. 2017)

[125] *Id*. at 889-91.

[126] *In re* Domino's Pizza Inc., 16-CV-2492, 2018 WL 4757944 (S.D.N.Y. Sept. 30, 2018); *But see* Parrott v. Marriott, Case No. 17-10359, 2017 WL 3891805 (E.D. Mich. Sept. 6, 2017) (denying Marriott's motion to dismiss claim that Marriott was joint employer of franchisee employees based on finding that the following allegations suggested that Marriott maintained a level of control that could "translate into a joint employment arrangement": (1) giving food managers discount rates at Marriott hotels; (2) exercising a substantial degree of supervision over the work of food managers; (3) controlling operations through corporate managers and auditors who review and compel compliance; (4) supervising and controlling work schedules for food managers; (5) controlling workplace conditions by requiring franchises to comply with food and beverage standards; and (6) imposing standardized procedures for hiring food managers).

- Economic Realities Test – evaluation of: (1) opportunity for profit or loss depending on managerial skill; (2) investments by the worker and the employer; (3) degree of permanence of the work relationship; (4) nature and degree of control (considers employer's control, including reserved control over the performance of the work and economic aspects of the working relationship); (5) extent to which the work performed is an integral part of the employer's business; (6) skill and initiative; and (7) additional factors.[127]

- "ABC" Test – If a person provides services to the putative employer, they will be considered an employee, unless the putative employer demonstrates that all three of the following conditions have been met: (A) the worker is free from the control and direction of the hirer in connection with the performance of the work (both under the contract and the work in fact); and (B) the worker performs work that is outside the usual course of the hiring entity's business; and (C) the worker is customarily engaged in an independently established trade, occupation, or business of the same nature as that involved in the work performed.[128]

Given the vicissitudes surrounding joint employment, misclassification, and other potential liability, franchisors have become increasingly circumspect about issuing broad mandates and providing any support or services that could be viewed as an exercise of control over franchisee operations. As noted above, however, many franchisors recognize that they must establish privacy and data security standards for franchisees and impose some controls due to the significant risk of liability and reputational harm from privacy violations and data breaches.[129] Studies, like the annual Ponemon Institute "Cost of a Data Breach," which quantify the overall cost of a data breach (and include reputational harm as one of the costs), may strengthen the argument that a franchisor-mandated data privacy and security program is the type of control necessary to protect the integrity of the

---

[127] Dep't of Lab., Employee or Independent Contractor Classification under the Fair Labor Standards Act, 87 Fed. Reg. 62218, 62220-21 (citing U.S. v. Silk, 331 U.S. 704 (1947) and Rutherford Food Corp. v. McComb, 331 U.S. 722 (1947)).

[128] *See* Dynamex Operations West, Inc. v. Superior Court, 4 Cal. App. 5th 903, 955-56 (2018); *see also* Koller & Leon, *supra* note 115, at 19-54 (discussing the ABC test and variations among states, along with the difficulties the test poses for franchise systems).

[129] See Mazero, *et al.*, *supra* note 114, at 356 ("The potential harm to a brand resulting from data breach and similar system-damaging events at a unit dictates that franchisors establish mandatory policies . . . for data security, data breach, and crisis management . . . Although this control over a non-employment aspect of unit operations may be used as an argument to establish joint employer status, the potential for catastrophic harm to the brand warrants the risk.")

trademark and brand rather than an exercise of control over a franchisee's day-to-day operations.[130]

IV. Establishing and Evaluating Privacy Programs

Against this background, which includes both an international and domestic patchwork of privacy laws and regulations, both franchisors and franchisees are exposed to significant regulatory and reputational risk (as well as opportunity) in the privacy space. Franchisors that collect and process personal data must develop and maintain a privacy program that complies with all applicable laws. At the same time, as noted above, they must ensure that franchisees also comply with applicable privacy laws because – as is always the case in the franchise space – if a franchisee violates a privacy law and the issue garners media attention, consumers will not differentiate between a violation by the franchisee and a violation by the franchisor, and the brand as a whole may suffer reputational harm. Moreover, regulators may question whether the franchisor had adequate guard rails in place for franchisees' use of personal data or whether the franchisor turned a blind eye to franchisees' conduct if that conduct benefited the brand as a whole. Likewise, franchisees should make sure that franchisors are operating within the confines of applicable privacy laws for similar reasons: a violation of privacy law that attracts attention from media and consumers could diminish the value of the franchise.

With these concerns in mind, a franchisor should develop a robust privacy program, and a potential franchisee should: (1) evaluate the sophistication of franchisor's privacy program: and (2) if the franchisee collects personal data independently from the franchisor, develop its own privacy program.

In the franchise context, there may be two primary entities that collect personal data: the franchisor and the franchisee. For example, a franchisor may collect personal data to operate a loyalty program, while a franchisee may separately collect customers' personal data as permitted by the franchisor. While the franchisor may bear the regulatory risk associated with collecting customers' personal data, both the franchisor and the franchisee bear the same reputational risk associated with a franchisor collecting personal data from customers. Accordingly, a potential franchisee should assess whether a franchisor has an established privacy program before deciding whether to enter into a business relationship with the franchisor. And a franchisee that collects personal data separately from the franchisor should ensure that it has its own well-developed privacy program.

Developed privacy programs (by either a franchisor or franchisee) should follow several well-established principles:

[130] *See supra* note 108 and accompanying text.

A. Provide Notice about the Collection of Personal Data

Many laws require businesses that collect personal data to disclose what personal data they collect, how they process that data, with whom they share that personal data, and for how long they retain that data.[131] These laws also require businesses that collect personal data to provide this notice prior to the point of collection.[132]

From a commercial perspective, it is critical that a business's privacy notice be accurate. When a business prepares its privacy notice, the business should canvass every business team to help ensure that the privacy notice captures and describes the ways in which each team is collecting and using personal data, and does not unintentionally inhibit future innovative uses. For example, how is the marketing team collecting and processing personal data? Is the team collecting personal data directly from customers? Is the team buying demographic data? Is the team sending marketing emails and/or text messages to customers? How is the data analytics team collecting and processing personal data? Is the team buying data about customers? Is the team using artificial intelligence to determine which customers are likely to purchase a product within the next 30 days and then sending those customers promotional emails containing a discount code? How is the social media team collecting and processing personal data? Have they deployed cookies and pixels that allow both first-party and third-party tracking? Only once a thorough review of how every team collects and processes personal data has been completed can the business compile an accurate privacy statement. After that, if a business team subsequently wants to begin collecting personal data for a new purpose or wishes to begin collecting a new category of personal data, the business should ensure that the privacy notice and related privacy practices do not prohibit those activities, and where needed, make updates to apply to new data going forward.

B. Minimize the Collection of Personal Data

Although it may be tempting for a business to collect as much personal data as possible, businesses are increasingly encouraged to limit the collection of personal data to only the personal data that the business may use for legitimate business purposes and that the business has disclosed in its privacy notice.[133] The rationale for minimizing the collection of personal data is multi-fold. First, if a business is collecting personal data in the hope that one day, the business will determine a use for that data, the business would have to disclose in its privacy notice that it is collecting the personal data, but the business would be unable to describe a valid use for that data. Second, businesses that store personal data are always at risk of suffering a data breach. By minimizing the amount of data it holds, a business can minimize the harm that will result from a data breach. Finally, a business that collects personal data should have established retention and deletion

---

[131] *See supra* note 27 and accompanying text.

[132] *Id*.

[133] *See, e.g.*, CCPA §§ 1798.100(a)(1) & (c).

schedules that ensure that the business retains the data only as long as necessary for legitimate business purposes.

C. Obtain Consent as Required by Law

Many privacy laws require businesses to offer consumers the ability to opt in to, or opt out of, the use of personal data. For example, a business cannot send marketing emails to a resident of the European Economic Area unless the business has asked the individual to opt-in to receive those emails, and businesses must allow residents of the United States to opt-out of receiving marketing emails.[134] A business that engages in marketing must be able to both track the applicable requirements and develop the technology required to comply with those requirements. For example, if a business has customers from multiple countries, the business will need to understand the consent rules in each country, build tick boxes that appear during the customer journey to capture consent, maintain a back-end system to record customers' preferences, and offer customers the ability to change their preferences.

The business also must consider where during the customer journey it wishes to seek consent from customers. For example, for businesses that both sell products and operate loyalty programs, does the business want to seek consent during the purchasing journey, or does the business want to seek consent when a customer joins the loyalty program? One risk of seeking consent during the purchasing journey is that it may be an obstacle to completing the transaction, but the possible benefit of seeking consent at that time is the ability to capture consent from the largest possible group of individuals.

In practice, the challenges of capturing consent and ensuring that a business only sends marketing emails to customers that they are legally permitted to market to may mean that a franchisor decides that it will control all email marketing campaigns on behalf of the brand. By taking this approach, the franchisor does not have to fear that a franchisee will send marketing emails to a customer who has either opted out of, or not consented to, receiving such emails. But in some franchise systems, the franchisor runs a national marketing program and permits franchisees to engage in local marketing. In such scenarios, the franchisor and the franchisee need to have a clear understanding of what constitutes a "marketable" customer. For example, if a customer has unsubscribed from receiving marketing emails from the franchisor, the franchisee would be exposing itself to regulatory and reputational risk if it were to send marketing emails to that customer. As a result, the franchisor and the franchisee should consider coordinating closely regarding which customers are "marketable."

D. Ensure Vendors Protect Personal Data

Businesses that collect personal data have an obligation to protect that data. Because privacy and cybersecurity are typically considered two different topics, this paper

[134] GDPR, article 6; Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act, 15 U.S.C. § 7704(a)(3).

does not discuss the details related to the critical need for businesses that collect personal data to have a robust cybersecurity program. But we will address businesses' obligation to protect personal data when they share that data with third parties, such as vendors. A business should include data protection provisions in every contract with vendors with which the business shares personal data. These provisions should limit the vendor to only processing the personal data as directed by the business, prevent the vendor from sharing the personal data with any third parties, and require the vendor to meet certain cybersecurity standards of protection for the data. Often, these provisions are drafted as a separate "data processing addendum" which is appended to the underlying contract between the parties.

The provisions also should require the vendor to immediately notify the business if the vendors suffers a data breach. "Breach" should be defined expansively, as many laws do, to include both the loss of personal data and unauthorized access or potential access to personal data.[135] A business should require this notice from its vendors because although the vendor may have suffered the breach, the business likely will suffer reputational harm should the breach become public if the public cannot distinguish between the business and its vendors. For example, if the media reports that the personal data of thousands of a business's customers was available on the dark web, the public may not understand that the business did not suffer a cyber incident but rather the data appeared on the dark web because a vendor used by the business was compromised. Accordingly, to try to minimize reputational harm, the business may want to prepare holding statements and take other actions to address the incident.

E. Respect Data Subject Rights

Many countries and states afford individuals "data subject rights." These rights include, but are not limited to, the right of access and the right to erasure. The right of access means that an individual may ask a business for a copy of all personal data that business holds about the individual; the right to erasure means that an individual may ask a business to erase all of the personal data the business holds about the person.[136] (The business may, however, retain any data it must retain as required by law.) A business must be prepared to fulfill requests from individuals who seek to exercise these rights. Doing so often requires a business to complete a thorough inventory of its systems to identify where it holds personal data so that it can both pull that personal data to respond to an access request and delete that data in response to an erasure request from every system where the data is held. The business must also fulfill these requests within the limited time frame permitted by the applicable law.

A franchisor and a franchisee also must understand in which systems their customer data is held. For example, if a customer makes an access request to a franchisor, the franchisor should provide all of the data that the franchisor holds about the

[135] *See, e.g.*, N.Y. Gen. Bus. Law § 899-AA.

[136] *See, e.g.*, CCPA §§ 1798.105, 1798.110.

customer and should also either collect additional data about the customer that is held separately by the franchisee and produce that data to the customer or inform the customer that the franchisee may also hold data about the customer and instruct the customer on how to submit an access request to the franchisee. Conversely, if a customer makes an access request to a franchisee, the franchisee should produce to the customer the data that the franchisee holds about the customer but also should notify the customer that the franchisor may hold additional data about the customer and instruct the customer on how to submit an access request to the franchisor.

F. Training

In many businesses, numerous employees may have access to customers' personal data. It is both required by some laws and a good idea to provide training to those employees to ensure that they have a need for access to such data, and process and protect that data properly. The goal of such training should be to heighten employees' awareness of privacy issues so that they are able to spot such issues and escalate them to the right team within the business. For example, training should educate employees about whether obligations exist to provide notice to consumers about the collection of personal data prior to the point of collection; the need to limit the sharing of personal data; and the need to restrict the ability of vendors to process personal data.

In the franchising context, franchisees should determine the appropriate amount of training that they need to provide to their employees and should abide by any training requirements established by the franchisor's Brand Standards. The franchisor may limit its requirements to the obligation for franchisees to comply with applicable law and train employees to do so as well, or the franchisor may provide more detailed and specific training requirements for franchisees' employees. As noted above, the franchisor will likely consider questions of joint employer liability in determining the extent of its involvement in training franchisees' employees and establish requirements according to its assessment of risk in that area.

V. Use of Personal Data Regarding Customers

One hot topic among franchisors and franchisees is the question of use of personal data associated with customers. Customer data has value for analytics and marketing purposes. But simply because the employee of a franchisee may touch personal data associated with a customer does not mean that the franchisee "owns" the data. In addition to observing legal requirements under applicable laws, franchisors and franchisees must abide by the disclosures they make regarding personal data use in their consumer-facing privacy notices. Such notices should include information about the categories of personal data processed and the purposes for processing such data, in addition to other disclosures regarding how the entity will use the personal data it collects.

Franchisees and potential franchisees should be sure that they understand which policies govern the collection and use of the personal data associated with customers and, if the franchisor's policies govern the data, what (if anything) the franchisee may do with that data. For example, the franchise agreement or operations manual ("Operations

Manual") may include language that makes clear that during the term of the franchise agreement, only the franchisor may use the personal data that is collected from customers and that after the term of the agreement, the franchisee may only retain and use personal data of customers as necessary to fulfill outstanding orders. As discussed above, franchisees and potential franchisees also should understand whether they are permitted to collect personal data from customers separate and apart from the relationship that they have with the franchisor

VI. Litigation Trends

As jurisdictions grant citizens additional privacy rights, as people begin to prioritize privacy, and as plaintiffs' class action attorneys revitalize and reinterpret old laws, there has been a clear uptick in privacy-related litigation. Whereas companies always had to ensure that they were not engaging in unreasonable data security practices, companies now also should focus on whether their practices of providing notice and obtaining consent when necessary are sufficient and would withstand scrutiny in court.

A. Unreasonable Data Security Practices

The Federal Trade Commission has not hesitated to sue companies that it alleges have unreasonable data security practices. As noted above, in 2012, the FTC sued Wyndham Hotels and Resorts, alleging that Wyndham's security practices had unfairly exposed consumers' payment card information.[137] Wyndham settled that case, agreeing to establish a comprehensive information security program designed to protect cardholder data, conduct annual information security audits, and maintain safeguards in connections to its franchisees' servers.[138] The FTC touted this settlement, with then-FTC Chairwoman Edith Ramirez stating, "This settlement marks the end of a significant case in the FTC's efforts to protect consumers from the harm caused by unreasonable data security. Not only will it provide important protection to consumers, but the court rulings in the case have affirmed the vital role the FTC plays in this important area."[139]

Since settling the Wyndham case I n2015, the FTC has brought numerous cases in this space. For example, in October 2022, the FTC filed a complaint against Chegg Inc., an education technology provider, alleging that Chegg had failed to protect the

---

[137] *See supra* note 109 and accompanying text.

[138] Stipulated Order for Injunction, F.T.C. v. Wyndham Worldwide Corp., No. 2:12-cv-1365 (Dec. 11, 2015).

[139] Fed. Trade Comm'n, Press Release, *Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk*, (Dec. 9, 2015), https://www.ftc.gov/news-events/news/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment-card-information-risk.

personal information it collected from users and employees.[140] Among other issues, the FTC alleged that the company had failed to properly protect users' personal data and that as a result, Chegg suffered multiple data breaches that exposed the personal information of about 40 million users and employees, including users' email addresses, dates of birth, sexual orientation, and disabilities, as well as financial and medical information about Chegg employees.[141] Chegg ultimately entered into a Consent Agreement with the FTC whereby Chegg agreed to implement a comprehensive information security program, limit the data Chegg collects and retains, offer users multifactor authentication to secure their accounts, and allow users to request access to and deletion of their data.[142] These actions by the FTC illustrate the willingness of the FTC to act against companies that have lax security practices that lead to data breaches and the exposure of consumers' and employees' personal data.

But the FTC is not the only actor in the data breach space. Class action litigation also is a significant risk for companies that do not have what are deemed to be reasonable data security practices. After Marriott acquired Starwood, Marriott discovered in 2018 that for four years, hackers had exploited vulnerabilities in Starwood's network to access and steal customer data.[143] In total, 133.7 million Starwood guest records were compromised, including names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, date of birth, gender, arrival and departure information, reservation dates, and communication preferences.[144] For some customers, the information also included payment card numbers and payment card expiration dates. In May 2022, class certification for potential trial was granted, and as of the date of this paper, the case is still pending in the U.S. District Court for the District of Maryland.[145]

B. Privacy Claims Based on Other State and Federal Laws

In addition to bringing actions based on lax security practices, consumers and employees also have started to bring privacy claims based on a number of other state and federal laws, including Illinois's Biometric Information Privacy Act (BIPA), the federal Video Privacy Protection Act (VPPA), and the California Invasion of Privacy Act (CIPA).

---

[140] Complaint, Chegg, Inc., No. C-4782 (F.T.C. Oct. 31, 2022).

[141] *Id.* at 2-4.

[142] Decision and Order, Chegg, Inc., No. C-4782 (F.T.C Jan. 25, 2023).

[143] *In re* Marriott Int'l, Inc., Customer Data Security Breach Litigation, 341 F.R.D. 128, 138-39 (D. Md. 2022).

[144] *Id*.

[145] *Id*. at 172 (acknowledging that "this Court is one of the first to certify Rule 23(b)(3) classes involving individual consumers complaining of a data breach").

(1) Illinois's Biometric Information Privacy Act

In 2008, Illinois was the first state to pass a biometric data privacy law. The BIPA requires, among other things, informed consent prior to the collection of biometric data, such as fingerprints and face, hand, and retina screens, and mandates data protection obligations and retention guidelines. The BIPA also created a private right of action for individuals harmed by BIPA violations and provided statutory damages for such violations.[146] Beginning in 2015, plaintiffs began bringing both employee-based and consumer-based class action lawsuits. The employee-based claims largely alleged BIPA violations in connection with the use of time-management systems that collected biometric data.

These claims have resulted in both significant settlements and jury verdicts. In 2020, Facebook agreed to a $650 million settlement in the BIPA class action lawsuit, *Patel v. Facebook, Inc.*, to resolve claims it collected social networking website user biometric data without consent.[147] This settlement was one of the largest consumer privacy settlements in U.S. history.

Two years later, in October 2022, the first-ever jury verdict in a BIPA class action lawsuit was returned in *Rogers v. BNSF Railway Company*. In *Rogers,* the lead plaintiff asserted that BNSF had improperly required employees entering BNSF's facilities to provide their biometric information through a fingerprint scanner, and the court certified a class of more than 44,000 drivers who had their fingerprints scanned at one of BNSF's four Illinois facilities.[148] Although BNSF tried to shift liability to the vendor that actually collected the drivers' biometric data, [149] the jury found BNSF liable for violating the BIPA and determined that the Company had intentionally or recklessly violated the BIPA approximately 45,600 times.[150] Based on the jury's finding, the court calculated damages

---

[146] 740 Ill. Comp. Stat. 14/20 (2018).

[147] *In re* Facebook Biometric Information Privacy Litigation, Case No. 15-cv-0747-JD, 2020 WL 4818608 (N.D. Cal. 2020) (aff'd by *In Re* Facebook Biometric Information Privacy Litigation*,* Case No. 21-15553, 2022 WL 822923 (9th Cir. 2022)).

[148] Rogers v. BNSF Railway Co., Case No: 1:19-cv-03083, 2022 WL 787955 (N.D. Ill. 2022) (denying BNSF's motion for summary judgment).

[149] *Id*. at *3.

[150] *See* Eunice Park, *The AI Bill of Rights: A Step in the Right Direction*, 65 ORANGE CTY. LAW. MAG 25, 29 (Feb. 2023) (citations omitted).

using the maximum statutory amount of $5,000 for each violation and awarded damages in the amount of $228 million.[151]

More recently, in *Ronquillo v. Doctor's Associates*[152] and *Rushing v. McAlister's Franchisor SPV and Focus Brands*[153] two federal district courts in Illinois have denied franchisor motions to dismiss claims of alleged BIPA violations made by franchisee employees against the franchisor. In both *Ronquillo* and *Rushing*, the plaintiff employees alleged that the franchisors had violated the BIPA because the franchisor-mandated point-of-sale systems "captured, collected disseminated, or otherwise used" their biometrics without their informed consent.[154] In evaluating a similar claim in *Kyles v. Hoosier Papa and Papa John's International*, the U.S. District Court for the Northern District of Illinois denied Papa John's International (the franchisor's) motion to dismiss based on a finding that the plaintiff employees plausibly" alleged that Papa John's International had "control" and "possession" of their biometric data within the meaning of BIPA based, in part, on assertions that Papa John's: (1) had developed the point-of-sale system used by the franchisees; (2) required franchisees to use fingerprint scanning features "whenever possible"; (3) retained remote access to the system; and (4) regularly downloaded and used data from the system (such as to crate reports of which franchisees and workers do not use the system's fingerprint scanner) had "because.[155]

(2) Video Privacy Protection Act

Plaintiffs recently have latched onto VPPA as another basis for privacy class action claims. The VPPA was enacted in 1988, after the failed Supreme Court confirmation hearing of Robert Bork. During that hearing, a news outlet published Bork's movie rental history. Although the history did not contain any salacious content, Congress moved quickly to make it illegal for "video tape service provider[s]" to disclose personally identifiable information about renters, purchasers, or subscribers of "prerecorded video cassette tapes or similar audio visual materials" to third parties.[156]

---

[151] Judgment in a Civil Case, Rogers v. BNSF Railway Company, Case No: 1:19-cv-03083, (N.D. Ill. Oct. 12, 2022).

[152] 597 F. Supp. 3d 1227 (N.D. Ill. 2022);

[153] Case No. 22-CV-649-SMY, 2023 WL 2163388 (S.D. Ill. 2023).

[154] *Id*.; *see also Ronquillo* at 1230.

[155] Kyles v. Hoosier Papa and Papa John's International, Case No. 1:20-cv-07146, 2023 WL 2711608 (N.D. Ill. 2023) at *3-4.

[156] Video Privacy Protection Act of 1988, 18 U.S.C. § 2710.

After lying dormant for more than 30 years, plaintiffs' lawyers resurrected the VPPA in 2022.[157] Since then, plaintiffs have filed more than 100 proposed class actions against companies based on the companies' use of one of Meta's pixels.[158] Specifically, plaintiffs allege that website operators that use the Meta pixel violate the VPPA because the pixel discloses to Meta information about the videos that visitors to the website watch.[159] Plaintiffs, however, have not limited their claims to websites, like Hulu and HBO, which are in the business of providing video content to their customers. Claims also have been brought against Chick-Fil-A, ESPN, Weight Watchers, and other companies that are not primarily in the business of providing video content.[160]

While the law in this area is not settled – questions like are website operators "video tape service providers?" and is video content on a website "prerecorded video cassette tapes or similar audio visual materials?" persist – companies that operate websites should be aware of the risk of litigation and should consult with counsel to determine the extent to which they are willing to use pixels that send information about users' engagement with video content to third parties and what, if any, actions they can take to mitigate risk from using these pixels.

(3) California Invasion of Privacy Act

Plaintiffs have also homed in on the use of other website technologies, such as session replay technology and chat functionality. Session-replay software allows website operators to better understand how users interact with a website by recording the pages and content that a website visitor views, the visitor's mouse movements and keystrokes,

---

[157] Jean Mooney, *Defending Claims under the Video Privacy Protection Act*, WESTLAW TODAY (Jan. 18, 2023), https://today.westlaw.com/Document/I2b31cf8997b611ed8636e1a02dc72ff6/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1.

[158] *See* Stephanie Duchesneau, Meredith Halama, Nicola Menaldo, Charles Sipos, & James Snell, *Be Kind, Don't Rewind: The VPPA's Reemergence in Privacy Class-Action Litigation*, JD SUPRA (Mar. 20, 2023), https://www.jdsupra.com/legalnews/be-kind-don-t-rewind-the-vppa-s-1816696/,

[159] A pixel is a piece of code that allows companies to track visitor activity on their website. Companies frequently use pixels and other tracking devices to better understand the actions visitors to their site take and the effectiveness of their advertising. Companies also use pixels and other tracking devices to send information about site visitors to third parties, like Meta, so Meta can perform analytics on that data so the companies can send targeted advertising to specific customer segments.

[160] *See* Mooney, *supra* note 157 (identifying typical allegations in VPPA complaints based on use of Meta pixels).

and the search information the visitor puts into the website.[161] Website operators use such software to better understand, and then improve, website visitors' experiences. Chat functionality allows website visitors to chat, in real-time, either with a computer program, known as a chatbot, or a real person.

A plaintiff in Pennsylvania alleged that a company's use of session replay technology on its website violated Pennsylvania's Wiretapping and Electronic Surveillance Control Act (WESCA) on the grounds that Pennsylvania is a two-party consent state, and the plaintiff had not consented to her session activity being recorded.[162] The U.S. District Court for the Western District of Pennsylvania originally granted the website owner's motion for summary judgment, holding that WESCA did not apply because: (1) there was no "interception" of information under WESCA since a marketing technology company was a direct party to the communication; and (2) even if an interception occurred, it was outside of Pennsylvania since the information was received in Virginia and interpreted in Ohio; however, the U.S. Court of Appeals for the Third Circuit disagreed and remanded the case for further proceedings on the question of whether the plaintiff had granted consent for the use of session replay software.[163]

Similarly, plaintiffs in California recently have filed several putative class actions alleging violations of the California Invasion of Privacy Act, California's wiretapping statute.[164] These plaintiffs allege that a third-party provider of chat functionality that has real-time access to website chat communications without the website user's knowledge or consent is violating CIPA, and that the website operator is "aiding and abetting" that vendor's violation of CIPA.[165]

---

[161] *See* Carroll v. Chick-fil-A, Inc., Case No. 3:23-CV-00314 (N.D. Cal. 2023); Cantu v. WW.com LLC, Case No. 2:22-cv-07977 (C.D. Cal. 2022); Swartz v. ESPN, Inc., Case No. 1:22-cv-01523 (M.D. Pa. 2022); *see, e.g.*, Mooney, *supra* note 157 (noting that in 2022, class action plaintiffs filed suit under the VPPA based on use of Meta pixels against "dozens of defendants including the Boston Globe, NFL, NPR, Paramount, Sony Group, and AMC Networks.").

[162] See Popa v. Harriet Carter Gifts, Inc., 544 F. Supp.3d 535 (W.D. Pa. 2022) (vacated and remanded by Popa v. Harriet Carter Gifts, Inc., 52 F.4th 121 (3d Cir. 2022).

[163] Popa v. Harriet Carter Gifts, Inc., 52 F.4th 121 (3d Cir. 2022).

[164] Cal. Penal Code § 632.

[165] *See* Cody v. Lacoste USA, Inc., 8:23-cv-00235 (C.D. Cal. 2023); Byars v. Sterling Jewelers, Inc., Case No. 5:22-cv-01456 (C.D. Cal. 2022); Byars v. Goodyear Tire and Rubber Co., Case No. 5:22-cv-01358 SSS (KKx) (C.D. Cal. Feb. 3, 2023); Byars v. Hot Topic, Inc., Case No. EDCV 22-1652 JGB (KKx), 2023 WL 2026994 (C.D. Cal. Feb. 14, 2023).

As with the VPPA litigation, the law relating to CIPA claims is not settled. But the rash of putative class actions should cause website operators to consult with counsel and consider whether they are providing visitors to their sites with adequate notice of the personal data that is being collected on the site, how that data is being used, and with whom it is being shared and whether, and in what form, they should obtain consent from site visitors.

VII. Conclusion

Data privacy and data security are likely to be important matters for franchise systems in the foreseeable future. Given the potential harm that data privacy violations and data security breaches can cause to a franchise brand and reputation, franchisors and franchisees both must remain vigilant as they navigate the murky waters of 21st Century data privacy and security laws.