American Bar Association
46th Annual Forum on Franchising

W-16: IMPLEMENTING CHALLENGING TECHNOLOGIES IN FRANCHISE SYSTEMS

Kerry Renker Green
The Wendy's Company
Dublin, Ohio

and

Manal Zakhary Hall
Dentons
Salt Lake City, Utah

and

Keri McWilliams
Nixon Peabody LLP
Washington, DC

November 1-3, 2023
Dallas, TX

TABLE OF CONTENTS

IMPLEMENTING CHALLENGING TECHNOLOGIES IN FRANCHISE SYSTEMS

I. INTRODUCTION

The introduction of contactless payment methods, mobile ordering, artificial intelligence, and other cutting-edge methods of serving customers of a franchise—all implicating the tracking and use of personal information (such as through biometric data)—can present a host of strategic and operational challenges and benefits. This paper will provide advanced guidance for addressing legal issues which may arise from these and other new technologies, including considerations as to whether technology vendors contract directly with franchisees or if franchisors obtain and pass services through to franchisees, privacy and cybersecurity, ethical use of artificial intelligence, and data governance. Finally, the paper will consider what franchise systems might expect in the future and some best practices to consider as these non-traditional methods become more widely available and demanded by consumers.

II. TECHNOLOGY LANDSCAPE IN FRANCHISING

A. The Rapidly Evolving Pace of Technology

It is amazing to think that the worldwide web recently celebrated its thirtieth public birthday.[1] Since the 1990s, technological innovations have been rapidly developed and employed in the business world creating winners and capital gains, and over time a few losers as well.[2] We have seen technological innovations come and go: intranets, fax machines, digital cameras, back of house and business management software like QuickBooks (celebrating its fortieth birthday), cell and smart phone adoption, and the advent of software as a service platforms are all just a few examples of technological advances that were once "hot commodities" and have since either become mainstays or have been phased out and become obsolete.[3]

Technological obsolescence is the concept that technologies, which were once at the frontier, become less valuable when they evolve.[4] Progress is an important part of doing business and the potential ill-effects of technological obsolescence on businesses and franchised brands cannot be ignored. When technologies cease to be relevant to voracious consumers, a franchised brand should not want to be left behind. In fact, failing to innovate and to invest in technology upgrades is a recognized serious business risk.[5]

---

[1] David Grossman, *When Was the Internet Invented? How the Web Went Public*, POPULAR MECHS. (May 16, 2023), https://www.popularmechanics.com/culture/web/a43903714/when-was-internet-invented/.

[2] Song Ma, *Technological Obsolescence* 1 (Nat'l Bureau of Econ. Rsch., Working Paper No. 29504, 2021), https://www.nber.org/system/files/working_papers/w29504/w29504.pdf.

[3] *Id*.

[4] Id.

[5] Zech Crook, *Outdated Technology Costs Businesses More Than It Saves*, PHX. BUS. J. (Nov. 15, 2018) (sponsored content), https://www.bizjournals.com/phoenix/news/2018/11/15/outdated-technology-costs-businesses-more-than-it.html.

Failing to invest in the latest technology can have significant consequences, including cybersecurity risks, wasted employee productivity, and lack of consumer confidence.[6] Customers would rather take their business elsewhere than deal with a company that uses outdated technology.[7] Moreover, in recruiting franchisees and growing a brand, the tech-savviness of a brand is viewed as a significant plus. "Younger generations rely on technology more than any other generation and have high expectations for its use."[8] If a brand's technology isn't updated, it may be missing out on some great young entrepreneurs that will fuel brand growth.[9] No franchised brand wants to lose customers or jeopardize its growth opportunities.

That said, it is not easy to keep up with technological advances in today's economy. All technological advancements have limited shelf lives and those shelf lives seem to be getting shorter over time. In 2013, well before the advent of pandemic virtuality, web-enabled services were experiencing a fourteen to eighteen month "time-to-obsolescence."[10] Mobile-first web services' time-to-obsolescence was estimated to be about twelve months.[11] At the time, mobile services were just beginning their reach to the then-new mobile voracious consumer with short user attention spans, which now have become the norm and the target consumer for many franchised brands.[12] In 2013, the average consumer was noted to reach for his or her smart phone approximately 150 times daily.[13]

Since that time, consumer use of technology has grown exponentially with even more adoption and reliance on smart phones and mobile commerce. Today, Americans touch their phones on average 2,617 times per day and will check their phone, on average once every ten to twelve minutes.[14] As of 2021, seventy-nine percent of smartphone users have used their mobile devices to make a purchase.[15] Importantly, mobile commerce is currently expected to experience

---

[6] Id.

[7] *Id.* (noting that, according to a Microsoft survey, over 90% of people surveyed said that "dealing with a company that uses outdated technology would cause them to consider taking their business elsewhere due to concerns over security, privacy, or user-friendly convenience").

[8] Jeff Brazier, *Why Franchisors Must Embrace Technology to See Growth*, ENTREPRENEUR (Mar. 1, 2023), https://www.entrepreneur.com/science-technology/for-franchise-business-growth-embrace-technology-or-bust/446074.

[9] Id.

[10] Lewis Gersh, *The Velocity of Obsolescence*, FORBES (July 29, 2013, 11:41am EDT), https://www.forbes.com/sites/lewisgersh/2013/07/29/the-velocity-of-obsolescence/?sh=5d5b4f826596. This compares to a three-to-five-year time-to-obsolescence rate that was experienced fifteen years earlier (in 1998) for the same web services.

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] Jack Flynn, *20 Vital Smartphone Usage Statistics [2023]: Facts, Data, and Trends on Mobile Use in the U.S.*, ZIPPIA.COM (Apr. 3, 2023), https://www.zippia.com/advice/smartphone-usage-statistics/#:~:text=How%20many%20times%20does%20someone,phones%20150%20times%20on%20average.

[15] Id.

a "massive CAGR" of 34.9% between 2020–2026.[16] While consumers are rapidly burning through old technology and seeking out the newest, best, and fastest way to access the goods and services they seek, it is not at all surprising that web and mobile service providers have increased productivity and sped up their "time to market" to meet these demands. In fact, it is one of the reasons why the velocity of obsolescence of many technologies supporting consumer spending has been said to be accelerating.[17]

So, it is the need to drive sales and brand growth, combined with the pressure for and actual development of new and better technologies that has caused franchise systems to rapidly innovate and to adopt new technology. More simply, as technology becomes more effective at attracting consumers, it attracts more attention by businesses.[18] The result is a flood of resources directed at driving technological developments (increased research and development budgets, the recruitment of top talent) and subsequent exploration and adoption by brands. This has all led to the many new "it" technologies being considered and adopted in various manners in franchise systems, including: (a) voice controlled technology; (b) contactless ordering utilizing digital payments; (c) app-based solutions (digital keys); (d) omni-channel marketing; (e) digital loyalty programs; (f) the metaverse; and (g) artificial intelligence-driven technology solutions (including those that capture biometric data).[19]

This paper focuses on the implementation of cutting-edge technological advancements and considers challenges in franchised brands' implementation. The following examples of cutting-edge technologies are relevant to this paper: Digital solutions (apps, mobile or contactless ordering, digital payments, digital loyalty programs), the metaverse, and artificial intelligence (or "AI"). It considers the use of each of these technologies and how the data collected through the use of each (such as biometric data) presents unique challenges.

1. Digital Solutions

Most brands wishing to employ digital solutions are looking to promote online ordering capabilities via the internet and/or mobile app. Mobile apps enable the consumer to place online orders quickly and easily and to interact with the brand.[20] Franchise brands want their consumer digital experiences to be easily interactive and as frictionless as possible, all of which requires the use and collection of personal data. Services that digital solutions facilitate can include, mobile/digital payment programs, loyalty programs (app or web), gift cards, digital promotions, coupons and discounts, and keyless entry.

---

[16] *Id.*

[17] Gersh*, supra* note 10.

[18] Allison Berman, *Technology Feels Like It's Accelerating Because It Actually Is*, SINGULARITY HUB (Mar. 22, 2016), https://singularityhub.com/2016/03/22/technology-feels-like-its-accelerating-because-it-actually-is/.

[19] *Tech Trends Affecting Franchising*, FRANCHISE GUARDIAN (Nov. 18, 2022), https://franchiseguardian.com/technology/tech-trends-affecting-franchising/.

[20] Gary R. Batenhorst, Lindsey Cooper, & Daniel Graham, *Mobile Apps, Remote Ordering, and Loyalty Programs; Risks and Opportunities*, ABA 42ND ANNUAL FORUM ON FRANCHISING W-7, at 2 (2019).

2. The Metaverse

The metaverse is a 3-D virtual world focused on the social connection among users, which can be entered via an internet browser or immersive headset where the user will appear as a digital avatar.[21] Beyond just being a fun thing to explore, the metaverse has been perceived as having great commercial potential in application, where users and (for example) order products within the metaverse (virtually) and have them delivered to them in real life. To make this purchase a reality, the metaverse needs to employ what is known as Web3 technology, a new iteration of the internet that includes virtual reality, augmented reality, mixed reality, cryptocurrencies, and non-fungible tokens among other technologies.[22]

There are multiple metaverse virtual worlds available on several platforms. Meta's Horizon Worlds is one example that enables a user to access it via Oculus VR headsets. While its future potential as a profit-center is currently under debate, in 2021 the metaverse market was estimated at almost $39 billion and was expected to rise to a staggering $679 billion by 2030.[23] It's no surprise that franchised brands have sought to explore its potential.

3. AI

Artificial intelligence (also known as "machine intelligence" and referred to herein as "AI") can be difficult to define given how rapidly this area of technology is developing. Broadly, AI refers to a technological system's ability to perform tasks that are usually associated with human reasoning such as identifying patterns in data sets.[24] Google sets the definition out in a way that recognizes its breadth in the tech space and its broad potential application for business use:

> Artificial intelligence is a field of science concerned with building computers and machines that can reason, learn, and act in such a way that would normally require human intelligence or that involves data whose scale exceeds what humans can analyze.
>
> AI is a broad field that encompasses many different disciplines, including computer science, data analytics and statistics, hardware and software engineering, linguistics, neuroscience, and even philosophy and psychology.
>
> On an operational level for business use, AI is a set of technologies that are based primarily on machine learning and deep learning, used for data analytics,

[21] Luca Piacentini, *Is the Metaverse the Next Big Thing In Franchising?*, 1851 FRANCHISE (Jan. 10, 2023), https://1851franchise.com/is-the-metaverse-the-next-big-thing-in-franchising-2720801.

[22] Laura Lorek, *Welcome to the Metaverse: Virtual Worlds and Web3 are all the Rage Right Now—but the Law is Stuck at Web1*, A.B.A. J., Oct/Nov 2022, at 16, https://www.abajournal.com/magazine/article/the-metaverse-and-web3-are-all-the-rage-but-the-law-is-stuck-at-web1.

[23] Id. at 17.

[24] Pablo J. Olmo Rodriguez, *Artificial Intelligence Law: Applications, Risks & Opportunities*, 90 REV. JUR. U.P.R. 701, 703 (2021) (citing William A. Carter, et al., *A National Machine Intelligence Strategy for the United States,* CSIS TECHNOLOGY POLICY PROGRAM, at 1 (Mar. 2018), https://www.csis.org/events/national-machine-intelligence-strategy-united-states)).

predictions and forecasting, object categorization, natural language processing, recommendations, intelligent data retrieval, and more.[25]

According to Google, the many types of AI are generally categorized by what the machine can (or should be able to) do, which include: (1) reactive machines that employ limited AI and are reactionary to different kinds of stimuli based on pre-programmed rules and cannot learn with new data; (2) limited memory AI that uses memory to improve over time by being trained with new data; (3) theory of mind AI (which does not currently exist) that can emulate the human mind and has decision-making capabilities equal to that of a human including exhibiting human-like emotional reactions; and (4) self-aware AI, which is a step above theory of mind AI, and is the "mythical machine" that is aware of its own existence and has the intellectual and emotional capabilities of a human.[26]

The application of AI in the business space provides benefits such as automation of workflows and processes so that work can be performed independently (without human oversight), the reduction of human error by eliminating manual errors in data processing, and its capability to tirelessly perform repetitive tasks.[27] More specifically, franchised brands are leveraging AI technology today in many ways, including by incorporating chatbots on their digital platforms (e.g., ChatGPT technology), utilizing AI as a content generator, performing customer profiling to understand customer demographics, creating personalized marketing and creating tools for price sensitivity optimization.[28]

While AI has been said to be "one of the most sought-after technological advancements pioneering technological growth around the world,[29] the benefits to society of technology utilizing AI platforms clearly do not come without social and commercial risks. Mr. Ali Nouri, president of the Federation of American Scientists, has warned that while AI, machine learning, and automation all bring tremendous benefits, they also pose some serious risks including "erosion of personal privacy, increased social media disinformation, and the potential for an autonomous weapons arms race."[30]

B. How Technology Can Be Introduced to a Franchised System

In order to advance a brand's business interests, it has become increasingly important to stay on the cutting edge of technological advancements. Franchise systems not only need to keep

[25] *What is Artificial Intelligence (AI)?*, GOOGLE CLOUD, https://cloud.google.com/learn/what-is-artificial-intelligence (last visited May 29, 2023).

[26] *Id.*

[27] *Id.*

[28] Jimmy St. Louis, *5 Ways Franchisors Can Leverage Artificial Intelligence*, FRANCHISEWIRE (May 11, 2023, 6:00 AM), https://www.franchisewire.com/5-ways-franchisors-can-leverage-artificial-intelligence/.

[29] Jacquelyn Bulao, *How Fast Is Technology Advancing in 2023?*, TECHJURY: BLOG (July 12, 2023), https://techjury.net/blog/how-fast-is-technology-growing/.

[30] Rodriguez, *supra* note 24, at 708.

themselves aware of current trends and advancements to attract more customers, but also to keep their franchisees up to date as well.[31]

1. Brand Interest

A franchised brand should be considering how to keep up with advancements in the tech sphere as a matter of practical necessity, as so many parts of modern franchised systems contain a technological element including training software, point of sale systems, and digital solutions for payment and customer interactivity. Further, franchised brands have been recognized expressly in some jurisdictions to have a good faith duty to "protect and enhance the value of the brand," which could mean that they must adapt to current trends, including technological trends, to meet competition.[32]

To meet competition in its efforts to meet these obligations and also to stay relevant with consumers, many brands have developed robust IT departments and appointed Chief Technology or Information Officers to oversee their operations and technological development efforts.[33] Shareholders, members, and analysts evaluating brand value regularly consider potential technological enhancements and brand technology goals in the next three to five years.[34] With all of these additional resources and the pressure from owners and shareholders for tech growth, it is no wonder that the number of inquiries as to what the new hot technology may exist to implement in a system has grown over time.

2. Franchisee Interest

Sometimes it is not the franchisor or the system that points out the need to adapt or that proposes the new technology to be used, but rather, the need is naturally raised and proposed in the field by franchisees based on what they are seeing on the ground. Franchisees are often on the frontline of customer interactions and regularly raise needs to make their interactions with customers more frictionless and for the purchasing process to be quicker. Further, with the shortage of both skilled and unskilled applicants for hourly and salaried workers in franchised systems, it is no wonder that franchisees are reaching out and asking for help.[35]

Technological enhancements such as automation may not only relieve stress for the number of employees that are needed for customer interactivity (e.g., delivery drivers in the case of autonomous vehicles), but they can also create a more engaging work environment that attracts employees.[36] That said, franchisees seeking to implement their own technology, without brand buy-in, can create brand risk by ignoring their obligations in their franchise agreement to seek

---

[31] Brazier, *supra* note 8.

[32] Dunkin' Brands Canada Ltd. v. Bertico Inc., 2015 CarswellQue 3066 (Can. Que. C.A.) (WL).

[33] Brazier, *supra* note 8.

[34] Id.

[35] Darrell Johnson, *Deciphering the Labor Market: The Numbers Behind the Labor Shortage*, MULTI-UNIT FRANCHISEE MAGAZINE, Q2, 2022, at 84, https://www.franchising.com/articles/deciphering_the_labor_market_the_numbers_behind_the_labor_shortage.html.

[36] Dave Wright, *AI and the Secret to Employee Happiness*, FORBES (Apr. 1, 2022) (Paid Program), https://www.forbes.com/sites/servicenow/2022/04/01/ai-and-the-secret-to-employee-happiness/?sh=7d66b6125a30.

approval for technological advancements and implementing weak systems that lack data security or that are wholly incompatible with system cohesion.[37]

3. Vendors Shopping Their Wares

Technology vendor start-ups have been aggressively pursuing franchised brand partners for many years. Although aggressive tech start-up investment may be slowing,[38] for decades, many tech companies came into existence riding the coattails of a multitude of professional funding sources, which poised them all for growth and acceleration.[39] For the most part, very large companies seeking a quick fix and the benefits of leveraging new streams of technologically-gathered data have been very happy to sit with these entrepreneurial technological innovators and to beta-test their products.[40]

And there has been no shortage of technology conferences and trade shows for any franchised brand to attend in order to explore new products available. One technology conference listing for 2023 tech events showcases literally hundreds of conferences, tradeshows, summits, and seminars that provide a seemingly endless list of vendors wishing to find relevance in any brands' business plan.[41] If brands will not come to the vendors to seek out new innovation, vendors will not hesitate to leverage data that they very easily know how to gather to identify any individual connected with any brand to cold-call, spam, and generally promote the adoption of their hot new product.

III. LAWS TO BE CONSIDERED IN ADOPTING NEW TECHNOLOGY INTO A FRANCHISE SYSTEM

Even with increasing opportunities and incentives to consider new technologies, franchisors and franchisees must take care to understand the legal and practical implications of the new technology that they might adopt. As technology continues to evolve, it has become increasingly apparent that the efficacy of many new technological solutions is directly correlated with the amount of data that can be used to develop the product. In many cases, this can include customer-specific information such as preferred location, visit frequency, previous orders, or geolocation; personally identifiable information such as name, address, contact information, demographics; and even biometric data such as facial recognition and fingerprints.

---

[37] *See* Gorgon Drakes & Rachel Bowley, *Franchising in a Digital World—Risks and Rewards of Implementing Consumer-facing Tech in a Franchise Network*, FIELDFISHER (Apr. 3, 2023), https://www.fieldfisher.com/en/services/franchising/franchise-commercial-law-blog/franchising-in-a-digital-world-risks-and-rewards-of-implementing-consumer-facing-tech-in-a-franchise-network (noting that the drive for centralization and uniformity in franchised systems "conflicts with the reality that franchisees are independent businesses" and will view themselves as entrepreneurs).

[38] *See* Matt Ashare, *Tech Vendor Risk Raises Vetting Stakes in Wake of SVB Crisis*, CIODIVE (Mar. 27, 2023), https://www.ciodive.com/news/Silicon-valley-bank-svb-fallout-enterprise-tech-vendor-risk/645958/.

[39] Gersh, *supra* note 10.

[40] *Id.*

[41] Bizzabo Blog Staff, *Tech Conferences: The Best Tech Events Guide for 2023*, BIZZABO (Nov. 21, 2022), https://www.bizzabo.com/blog/technology-events.

The more that any given technology relies on data and collects data, the greater the risk to the consumer that their data can be stolen, compromised, or used in unanticipated ways. Like most businesses that try to innovate, businesses in the franchise sector have not been immune to data breaches, liability based on allegations of ineffective data security practices, or accusations of impermissible use of data.[42] As a result, franchisors and franchisees must consider potential new technology with an understanding of the data privacy and security laws that might apply to their use of such technology. A history and overview of the current state of data privacy regulations in the U.S. will be helpful here.

A. Federal Data Privacy Limitations

The United States has had a number of federal privacy-related laws for years. However, the federal government's first significant attempt to regulate *general* data privacy in the United States occurred not through legislation but administrative action. The Federal Trade Commission ("FTC") filed suit against Wyndham in *FTC v. Wyndham*, citing deceptive and unfair acts or practices in connection with the Wyndham hotel chain's alleged failure to maintain reasonable and appropriate data security for consumers' personal information, in violation of Section 5 of the FTC Act[43] after intruders gained unauthorized access on three separate occasions to Wyndham's computer network, which included stored personal information of customer payment card account numbers, expiration dates, and security codes, between April 2008 and January 2014.[44]

The general structure of technology within the Wyndham system will be familiar to most franchisors and franchisees. Under its franchise agreements at the time of the FTC's complaint, Wyndham required franchisee hotels to purchase and configure to their specifications a designated computer system to handle reservations and credit card payments. The system, which stored consumers' personal information, was linked to the corporate network, including a central reservation system. The FTC alleged that after discovering the first two data breaches, Wyndham failed to take appropriate steps in a reasonable time frame to prevent further compromise of the hotel's network. The FTC further alleged that as a result of Wyndham's failure to implement "reasonable and appropriate security measures," the exposure of consumers' personal information caused substantial financial injury to consumers and businesses.

Wyndham challenged the FTC's authority to regulate cybersecurity at all and appealed the matter after being denied relief at the district court level.[45] On appeal, the Third Circuit considered two issues: "whether the FTC has authority to regulate cybersecurity under the unfairness prong of § 45(a); and, if so, whether Wyndham had fair notice its specific cybersecurity practices could fall short of that provision."[46] The court answered both questions in the affirmative.

Specifically, the court held that the FTC had the authority to bring the unfairness claim and was not required to promulgate regulations before bringing the claim. The court reasoned that the

---

[42] *See*, *e.g.*, discussion *infra* Section IV.

[43] Federal Trade Commission Act, Pub. L. No. 63-203, § 5, 38 Stat. 717, 719 (codified as amended at 15 U.S.C. § 45(a)).

[44] FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014).

[45] *Id.* at 610.

[46] FTC. v. Wyndham Worldwide Corp., 799 F.3d 236 at 240 (3d Cir. 2015).

FTC Act defines "unfair acts or practices" as those that cause or are likely to cause substantial consumer injury that are not reasonably avoidable by the consumers themselves and not outweighed by any benefits to consumers or competition. Here, the FTC adequately pled substantial, unavoidable consumer injury to support its unfair and deceptive practices claims.

The *Wyndham* case both confirmed the FTC's authority to regulate data privacy generally, and illustrated the particular challenges presented by the franchise model. When the systems within individual locations are all connected, the strength of the protection is determined by the weakest leak. One location with an outdated system, or easy-to-guess password, or personnel that fall for a malware or ransomware attack can endanger an entire brand.[47] Although the FTC has provided some non-binding guidance on best practices for data security, and federal privacy laws exist for specific types of data, there remains no comprehensive data privacy law at the federal level in the United States.[48]

B. State Data Privacy Laws

Unless and until comprehensive federal data privacy legislation is enacted, individual state data privacy laws will control.[49] As a result, franchisors operating in the Unites States will need to understand the state laws in all states in which they operate or plan to operate before the adoption of new technologies.[50]

The web of state privacy laws can be difficult to navigate for national franchised systems as each law may: (a) have different requirements; (b) apply to different populations; (c) apply only to specific types of data; (d) apply differently in specific sectors; and (e) be targeted toward different concerns. As of the writing of this paper, ten states had passed so-called "comprehensive" data privacy laws—i.e., privacy laws that are generally applicable to all businesses, designed primarily to protect consumers, and not targeted at specific sectors or

[47] See, e.g., id. at 241.

[48] *See, e.g., Start with Security: A Guide for Business,* FEDERAL TRADE COMMISSION (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf*; Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (*Oct. 2016); https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf; infra* Section III.D (summarizing federal laws applicable to certain types of data, consumer, or industries).

[49] *See generally*, Anokhy Desai, *U.S. Privacy Legislation Tracker*, INT'L ASS'N OF PRIVACY PROS., https://iapp.org/resources/article/us-state-privacy-legislation-tracker (last visited Aug. 4, 2023); Joseph Duball, *State Privacy Dispatch: Why the Floodgates Opened*, INT'L ASS'N OF PRIV. PROS: THE PRIV. ADVISOR (May 15, 2023), https://iapp.org/news/a/state-privacy-dispatch-the-floodgates-are-open/.

[50] International franchisors will also need to consider the vast array of international privacy laws such as the European Union's General Data Protection Regulation ("GDPR"). The authors limited their consideration to United States federal and state law for purpose of this paper.

specific types of data. Those states include California,[51] Colorado,[52] Connecticut,[53] Indiana,[54] Iowa,[55] Montana,[56] Tennessee,[57] Texas,[58] Utah,[59] and Virginia[60]. Many other states have legislation currently under consideration.[61]

If a franchisor has franchisees, customers, or significant operations in any state with a comprehensive data privacy law, both franchisees in the state and the franchisor must understand their obligations under the law. Key questions include: What are the thresholds for application of the law? What are the rights of persons protected by the law? What are the obligations of a person or business regulated by the law? What are the penalties for violations? And who has the responsibility for enforcement of the law? The answer to each of these questions impacts the potential risk. This Section examines the current comprehensive privacy laws that have been enacted by U.S. states.

---

[51] California Consumer Privacy Act (as amended by the Privacy Rights Act of 2020), CAL. CIV. CODE §§ 1798.100 et seq. (West, Westlaw through Ch. 1 of 2023-24 1st Ex. Sess., and urgency Legis. through Ch. 7 of 2023 Reg. Sess.).

[52] Colorado Privacy Act, 2021 Colo. Legis. Serv. Ch. 483 (West) (codified as COLO. REV. STAT. §§ 6-1-1301 et seq. (West, Westlaw through Legis. effective May 12, 2023 of the First Reg. Sess., 74th Gen. Assemb. (2023)).

[53] An Act Concerning Personal Data Privacy and Online Monitoring, 2022 CONN. PUB. ACTS No. 22-15 (codified as CONN. GEN. STAT. §§ 42-515 et seq. (West, Westlaw through all enactments of the 2023 Reg. Sess. enrolled and approved by the Governor on or before July 1, 2023 and effective on or before July 1, 2023).

[54] An Act to Amend the Indiana Code concerning Trade Regulation, 2023 Ind. Legis. Serv. Pub. Law 94-2023 (West) (to be codified as IND. CODE §§ 24-15).

[55] Iowa Consumer Data Protection Act, 2023 Iowa Legis. Serv. S.F. 262 (West) (to be codified as IOWA CODE § 715D).

[56] Montana Consumer Data Privacy Act, 2023 Mont. Laws Ch. 681.

[57] Tennessee Information Protection Act, 2023 Tenn. Pub. Acts Ch. 408 (to be codified as TENN. CODE ANN. § 47-18-3201).

[58] Texas Data Privacy and Security Act, 2023 Tex. Sess. Law Serv. Ch. 995 (West) (to be codified at TEX. BUS. & COM. § 541).

[59] Utah Consumer Privacy Act, 2022 Utah Laws Ch. 462 (West) (codified as UTAH CODE ANN. §§ 13-61-101 et seq. (West, Westlaw through the laws of the 2023 Gen. Sess. effective through May 2, 2023)).

[60] Virginia Consumer Data Protection Act, 2021 Va. Legis. Serv. 1st Sp. Sess. Ch. 35-36 (West) (codified as VA. CODE ANN. §§ 59.1-575 et seq. (West, Westlaw through the 2023 Reg. Sess. cc. 1, 18, 19, 271, 272, 342, 346, 408, 409, 741, 742 & 772)).

[61] *See generally*, Desai, *supra* note 49.

1. California

The California Consumer Privacy Act[62] came into effect on January 2020, and the amendments thereto contained in the California Privacy Rights Act[63] came into effect in January 2023. Together, these California privacy laws (together, "CCPA") form the first attempt by a U.S. jurisdiction to emulate the more stringent European Union's General Data Protection Directive ("GDPR") and allow consumers more control over their own data. The concerns animating the passage of the CCPA also animate many subsequent state data privacy efforts.

The CCPA, as enacted in 2018 contained several protections designed to give individuals more control over their personal information—including the right to: (a) know what personal data is being collected about them;[64] (b) know whether their personal data is sold or disclosed and to whom;[65] (c) say no to the sale of personal data;[66] (d) request that a business delete any personal information about an individual that was provided by that individual;[67] and (e) not be discriminated against for exercising their privacy rights.[68] The CCPA also mandates certain specific links on internet home pages for opt-out purposes.[69] The California Privacy Rights Act amended the CCPA to add a consumer right to correct any inaccurate information maintained by a business that collects personal information,[70] and a consumer right to limit the use and disclosure of sensitive information. [71]

The CCPA defines a "business" as any for-profit entity that: (a) collects the personal information of consumers, or has personal information collected on their behalf and determines the purposes and means of processing the information; (b) does business in California; and (c) meets any of the following thresholds: (1) had annual gross revenues exceeding $25,000,000 in the preceding calendar year; (2) buys, receives, sells, or shares for commercial purposes the personal information of 100,000 or more consumers or households; or (3) derives fifty percent or

---

[62] California Consumer Privacy Act, 2018 Cal. Legis. Serv. Ch. 55 (West) (codified as CAL. CIV. CODE § 1798.100, et seq. (West, Westlaw through Ch. 1 of 2023-24 1st Ex. Sess., and urgency Legis. through Ch. 7 of 2023 Reg. Sess.)).

[63] California Privacy Rights Act, 2020 Cal. Legis. Serv. Prop. 24 (West) (*amending* California Consumer Privacy Act, 2018 Cal. Legis. Serv. Ch. 55 (West) and codified as CAL. CIV. CODE § 1798.100, et seq. (West, Westlaw through Ch. 1 of 2023-24 1st Ex. Sess., and urgency Legis. through Ch. 7 of 2023 Reg. Sess.)).

[64] California Consumer Privacy Act, CAL. CIV. CODE § 1798.110 (West, Westlaw through Ch. 1 of 2023-24 1st Ex. Sess., and urgency Legis. through Ch. 7 of 2023 Reg. Sess.).

[65] *Id*. § 1798.115.

[66] *Id*. § 1798.116.

[67] *Id*. § 1798.105(a).

[68] *Id*. § 1798.125.

[69] *Id*. § 1798.135.

[70] *Id*. § 1798.106.

[71] *Id*. § 1798.121.

more of its annual revenues from selling or sharing consumers' information.[72] Importantly for franchisors and franchisees, any business that controls or is controlled by, and shares common branding with, a "business" meeting the CCPA definition is bound by the CCPA if it shares consumer personal information with that business, even if it would not independently meet the thresholds.[73] Therefore, the independent liability of a franchisee may depend on the extent of a franchisor's operations and whether the controls imposed by the franchise agreement are sufficient to show "the power to exercise a controlling influence over the management of a company."[74] Obviously, if a franchisor or franchisee meets any of the CCPA thresholds on its own, it is considered a business under the CCPA and must independently comply with the statute.[75]

In general, the CCPA is enforced by the newly created California Privacy Protection Agency.[76] Any business that violates the CCPA may be liable for an administrative fine of up to $2,500 per violation or $7,500 for each intentional violation in an administrative enforcement action brought by the California Privacy Protection Agency.[77] The one exception to government enforcement relates to data breaches. If a consumer believes that its information was "subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information" such consumer has a private right of action and can seek damages in an amount not less than $100 and not greater than $750 per consumer per incident, or actual damages, whichever is greater.[78]

2. Virginia

On March 2, 2021, Virginia became the second state to pass a comprehensive data privacy law. The Virginia Consumer Data Protection Act ("VCDPA")[79] applies to businesses that operate in Virginia, or that produce products and services that are targeted to the residents of Virginia and that during a calendar year either control or process the data of 100,000 consumers, or control or process the data of 25,000 consumers and derive more than fifty percent of their revenue from the sale of personal data.

The VCDPA introduces to state privacy laws the concept of the "controller" (the natural or legal person that, alone or jointly with others, determines the purpose and means of processing

---

[72] *Id*. § 1798.140; *see also* Scott Hall, *How Does the CCPA Impact Franchise Businesses and Relationships?*, JDSUPRA (Apr. 3, 2020), http://www.jdsupra.com/legalnews/how-does-the-ccpa-impact-franchise-12832 (analyzing potential franchisor and franchisee liability under the CCPA).

[73] CAL. CIV. CODE § 1798.140(d)(2).

[74] *Id*.

[75] *See generally, id*. § 1798.140(d)(1).

[76] *Id.* § 1798.199.10.

[77] *Id.* § 1798.150.

[78] *Id.* § 1798.155.

[79] Virginia Consumer Data Protection Act, 2021 Va. Legis. Serv. 1st Sp. Sess. Ch. 35-36 (West) (codified as VA. CODE ANN. §§ 59.1-575 et seq. (West, Westlaw through the 2023 Reg. Sess. cc. 1, 18, 19, 271, 272, 342, 346, 408, 409, 741, 742 & 772)).

personal data) as distinct from the "processor" (a natural or legal entity that processes personal data on behalf of a controller).[80] This controller and processor language create a framework for most of the state data privacy laws that follow. Under the VCDPA, the requirements are primarily imposed on the controller.

Virginia residents have a right to: (a) confirm whether a controller is processing their data and to access such data,[81] (b) correct inaccuracies in their data,[82] (c) delete personal provided by or obtained about them,[83] (d) obtain a copy of the personal data they provided in a portable format,[84] and (e) opt-out of the processing of personal data for target advertising purposes, sale purposes, or profiling in such a way that would negatively affect the consumer.[85] In addition to granting these rights to consumers, the VCDPA imposes a general requirement that controllers limit the collection of data to what is reasonably necessary for the disclosed purpose of the collection, and requires controllers to establish and implement "reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data."[86]

The VCDPA prohibits unlawful discrimination in the processing of the data and prohibits discrimination against consumers that exercise their rights under the law. The VCDPA also imposes an affirmative obligation on controllers to conduct and document a data protection assessment of certain processing activities. Importantly, there is no private right of action under the VCDPA.[87] The Attorney General of Virginia has the exclusive authority to enforce the provisions of the VCDPA and may seek civil penalties of up to $7,500 per violation.[88]

3. Colorado

Signed into law on July 7, 2021, with most provisions taking effect beginning July 1, 2023, Colorado has enacted the Colorado Privacy Act ("CPA").[89] The law applies to controllers and processors of personal data. Similar to Virginia, the CPA defines a "controller" a "a person that, alone or jointly with others, determines the purposes for and means of processing personal data" and regulates any party that conducts businesses in Colorado, and controls or processes the

[80] Virginia Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575 (West, Westlaw through the 2023 Reg. Sess. cc. 1, 18, 19, 271, 272, 342, 346, 408, 409, 741, 742 & 772) (defining "controller" and the "processor").

[81] *Id.* § 59.1-577(A)(1).

[82] *Id.* § 59.1-577(A)(2).

[83] *Id.* § 59.1-577(A)(3).

[84] *Id.* § 59.1-577(A)(4).

[85] *Id.* § 59.1-577(A)(5).

[86] Note that these obligations and similar requirements in subsequent state data privacy laws are important to consider when negotiating the vendor agreements referenced in Section VI.B.1.

[87] *Id.* § 59.1-580.

[88] *Id.* § 59.1-584.

[89] Colorado Privacy Act, 2021 Colo. Legis. Serv. Ch. 483 (West) (codified as COLO. REV. STAT. §§ 6-1-1301 et seq. (West, Westlaw through Legis. effective May 12, 2023 of the First Reg. Sess., 74th Gen. Assemb. (2023)).

personal data of 10,000 consumers or more during a calendar year, or derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 2,500 consumers or more.[90]

The CPA gives Colorado residents certain rights and imposes certain obligations on the controller of data. The key rights granted to consumers include the rights to: (a) opt-out of targeted advertising, the sale of personal data, or certain profiling;[91] (b) access the consumer's data and confirm whether the controller is processing personal data;[92] (c) correct inaccuracies in the consumer's data;[93] (d) delete the consumer's personal data;[94] and (e) obtain the consumer's data in a portable format.[95]

The CPA also imposes certain duties on controllers such as the obligation to: (a) provide consumers with clear and conspicuous method for opting out;[96] (b) respond to consumer requests within forty-five days;[97] (c) provide a detailed privacy notice, specifying the purposes for which personal data is collected and used;[98] and (d) limit the collection of data to what is needed to satisfy the disclosed purposes.[99] Importantly, the CPA also imposes a general duty of care that requires controllers to take reasonable security measures to secure personal data both during storage and use, a duty of unlawful discrimination, and a duty to avoid the processing of sensitive data.[100] There is no private right of action under the CPA; the attorney general and district attorney have the exclusive authority to enforce the CPA.[101]

4. Utah

On March 24, 2022, Utah enacted the Utah Consumer Privacy Act ("UCPA"), which becomes effective December 31, 2023.[102] With a similar framework to Virginia and Colorado, the

---

[90] Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1303(7), 6-1-1304 (West, Westlaw through Legis. effective May 12, 2023 of the First Reg. Sess., 74th Gen. Assemb. (2023)).

[91] *Id*. § 6-1-1306(1)(a).

[92] *Id*. § 6-1-1306(1)(b).

[93] *Id*. § 6-1-1306(1)(c).

[94] *Id*. § 6-1-1306(1)(d).

[95] *Id*. § 6-1-1306(1)(e).

[96] *Id*. § 6-1-1306(1)(a)(III).

[97] *Id.* § 6-1-1306(2).

[98] *Id*. § 6-1-1308(1).

[99] *Id*. § 6-1-1308(1).

[100] *Id*. § 6-1-1308(5).

[101] *Id.* §§ 6-1-1310; 6-1-1311.

[102] Utah Consumer Privacy Act, 2022 Utah Laws Ch. 462 (West) (codified as UTAH CODE ANN. §§ 13-61-101 et seq. (West, Westlaw through the laws of the 2023 General Session effective through May 2, 2023)).

UCPA imposes certain obligations on the controllers and processors of data and gives certain rights to consumers.

The UCPA applies to anyone conducting business in Utah, or producing products or services targeted toward residents of Utah that has annual revenue of $25,000,000 or more, and (a) during a calendar year, controlled or processed the data of 100,000 consumers (other than for payment transactions), or (b) controlled or processed the data of 25,000 consumers *and* derived fifty percent of their revenue from the sale of such personal data.[103] Under the UCPA, consumers have the right to: (a) confirm whether a controller is processing their personal data and to access their personal data,[104] (b) to delete the personal data that they provided to the controller,[105] (c) to obtain a copy of the personal data that they provided to the controller in a portable format,[106] and (d) to opt-out of the processing of their personal data for purposes of targeted advertising or sale.[107]

In addition, controllers under the UCPA are required to: (a) provide accessible and clear privacy notices;[108] (b) conspicuously disclose the manner in which consumers may exercise its opt-out rights;[109] (c) implement reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data and to reduce the reasonably foreseeable risks of harm to consumers;[110] (d) avoid the processing of sensitive data without taking additional steps;[111] and (e) refrain from discriminating against a consumer for exercising their rights.[112]

Notably, and notwithstanding the nondiscrimination provisions, the UCPA expressly allows the offer of different prices, rates, level, or qualities to consumers that have opted out of targeted advertising or if the offer is related to loyalty program participation.[113] This distinction will be copied by other states. The attorney general has the exclusive authority to enforce the UCPA

---

[103] Utah Consumer Privacy Act, UTAH CODE ANN. § 13-61-102(1) (West, Westlaw through the laws of the 2023 General Session effective through May 2, 2023).

[104] *Id.* § 13-61-201(1).

[105] *Id.* § 13-61-201(2).

[106] *Id*. § 13-61-201(3).

[107] *Id*. § 13-61-201(4).

[108] *Id*. § 13-61-302(1)(a).

[109] *Id*. § 13-61-302(1)(b).

[110] *Id*. § 13-61-302(2)(a).

[111] *Id*. § 13-61-302(3).

[112] *Id*. § 13-61-302(4)(a).

[113] *Id.* § 13-61-302(4)(b).

and to recover actual damages and penalties of up to $7,500 per violation but must provide an opportunity to cure the violation prior to initiating an enforcement action.[114]

5. Connecticut

On May 10, 2022, Connecticut became the fifth state to enact a comprehensive data privacy law. Like Virginia, Colorado, and Utah before it, the Connecticut Data Privacy Act ("CTDPA") imposes certain obligations on the controllers and processors of data and gives certain rights to consumers.[115]

Consumers that are protected by the CTDPA have the right to: (a) confirm whether a controller is processing their data;[116] (b) correct inaccuracies in their data;[117] (c) request that a controller delete personal data related to the consumer;[118] (d) obtain a copy of their data processed in a portable and readable format;[119] and (e) opt-out of the processing of the their data for targeted advertising, sale, or profiling.[120] The CTDPA applies to anyone conducting business in Connecticut, or producing products or services targeted to residents of Connecticut that, during the preceding calendar year, controlled or processed the data of 100,000 consumers (other than for payment transactions), or controlled or processed the data of 25,000 consumers *and* derived twenty-five percent of their revenue from the sale of such personal data.[121]

Under the CTDPA, a "controller" is a "legal entity that, alone or jointly with others determines the purpose and means of processing personal data."[122] Persons or entities that are deemed controllers under the act have certain obligations, such as the obligation to: (a) limit the collection of data to what is need to satisfy the stated purposes;[123] (b) establish and implement reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data;[124] (c) avoid the processing of sensitive

---

[114] *Id.* § 13-61-402.

[115] An Act Concerning Personal Data Privacy and Online Monitoring, 2022 CONN. PUB. ACTS No. 22-15 (codified as CONN. GEN. STAT. §§ 42-515 et seq. (West, Westlaw through all enactments of the 2023 Reg. Sess. enrolled and approved by the Governor on or before July 1, 2023 and effective on or before July 1, 2023).

[116] An Act Concerning Personal Data Privacy and Online Monitoring, CONN. GEN. STAT. § 42-518(a)(1) (West, Westlaw through all enactments of the 2023 Reg. Sess. enrolled and approved by the Governor on or before July 1, 2023 and effective on or before July 1, 2023).

[117] *Id.* § 42-518(a)(2).

[118] *Id.* § 42-518(a)(3).

[119] *Id.* § 42-518(a)(4).

[120] *Id.* § 42-518(a)(5).

[121] See generally, id. § 42-516.

[122] *Id.* § 42-515(11).

[123] *Id.* § 42-520(a)(1).

[124] *Id.* § 42-520(a)(3).

data such as biometrics;[125] (d) provide consumers with clear and conspicuous method for opting out;[126] (e) not process data for the purpose of targeted advertising, or sell data of minors; and (f)to provide a detailed privacy notice, which must specify the purposes for which personal data is collected and used.[127] Most provisions took effect July 1, 2023. There is no private right of action.[128] Depending on the technology and related standards mandated by the franchisor, a franchisor may be either a controller or processor under the CTDPA.

6. Iowa

On March 28, 2023, Iowa enacted its own comprehensive data privacy law ("IDPL"), becoming the sixth state to do so.[129] Under the new law, which will not take effect until January 1, 2025, consumers subject to the IDPL will have the right to: (a) confirm whether a controller is processing their data; (b) delete personal data provided by such consumer; (c) obtain a copy of most personal data that such consumer provided to the controller in a portable and readable format;[130] and (d) opt-out of the sale of their data.[131] Controllers must implement reasonable data security practices, and must provide reasonably accessible, clear, and meaningful privacy notices.[132]

Notably, the IDPL does not include provisions allowing consumers to correct incorrect data or to opt-out of targeted advertising. The IDPL applies to anyone conducting business in Iowa, or producing products or services that are targeted to residents of Iowa that, if during the preceding calendar year, that person either controlled or processed the data of 100,000 consumers, or controlled or processed the data of 25,000 consumers *and* derived over fifty percent of gross revenue from the sale of personal data.

In general, the obligations of controllers and processers under the IDPL are similar to those required in other states, and the IPDL has what has become a familiar framework. Therefore, the law is not expected to add a significant compliance burden to existing national

---

[125] *Id.* § 42-520(a)(4).

[126] *Id.* § 42-520(e)(1)(A)(i).

[127] *Id.* § 42-520(c).

[128] *Id*. § 11(a) (noting "The Attorney General shall have exclusive authority to enforce violations of sections 1 to 10, inclusive, of this act.").

[129] Iowa Consumer Data Protection Act, 2023 Iowa Legis. Serv. S.F. 262 (West) (to be codified at IOWA CODE § 715D) (signed into law on Mar. 28, 2023) (passed both chambers of state legislature unanimously); *see also* Anokhy Desai, *Iowa Becomes Sixth US State to Enact Comprehensive Consumer Privacy Legislation*, INT'L ASS'N OF PRIV. PROS: THE PRIV. ADVISOR (Mar. 16, 2023), https://iapp.org/news/a/iowa-becomes-sixth-us-state-to-enact-comprehensive-consumer-privacy-legislation/.

[130] An Act Relating to Consumer Data Protection, IOWA CODE § 715D(1)(c).

[131] *Id*. § 715D.3(1)(d).

[132] *Id*. § 715D.4.

brands that are in compliance with state privacy laws in other states.[133] The attorney general has exclusive authority to enforce the provisions of IDPL but must provide 90-days written notice and an opportunity to cure prior to initiating any formal enforcement action.[134]

7. Indiana

On May 1, 2023, Governor Eric Holcomb signed Indiana's Consumer Data Protection Act ("INCDPA") into law, making Indiana the seventh US state to pass comprehensive data privacy.[135] The INCDPA applies to anyone conducting business in Indiana, or producing products or services that are targeted to residents of Indiana that during a calendar year if such person either (a) controls or processes the data of 100,000 consumers who are Indiana residents, or (b) controls or processes the data of 25,000 consumers who are Indiana residents and derives over fifty percent of gross revenue from the sale of personal data.[136]

The INCDPA gives consumers the right to: (a) confirm whether or not a controller is processing the consumer's personal data,[137] (b) correct inaccuracies in the personal data that the consumer previously provided to a controller,[138] (c) delete the consumer's personal data whether provided by the consumer or obtained about the consumer,[139] (d) obtain a copy summary of the personal data that the consumer previously provided to the controller,[140] and (e) opt-out of the processing of the consumer's personal data for targeted advertising, sale, or certain profiling.[141]

Conversely, controllers under the INCDPA also have certain obligations, such as the obligation to: (a) limit the collection of data to what is adequate, relevant, and reasonably necessary for the disclosed purposes;[142] (b) avoid processing data for any purposes other than disclosed purposes;[143] (c) establish and implement reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of

---

[133] *See* Joseph Duball, *Iowa Set to Finalize Sixth US Comprehensive State Privacy Law*, INT'L ASS'N OF PRIV. PROS: THE PRIV. ADVISOR (Mar. 16, 2023) https://iapp.org/news/a/iowa-set-to-finalize-sixth-us-comprehensive-state-privacy-law/ (noting that the IDPL won't add many additional compliance hurdles it "runs closest to Utah's existing law").

[134] IOWA CODE § 715D.8.

[135] An Act to Amend the Indiana Code Concerning Trade Regulation, 2023 Ind. Legis. Serv. Pub. Law 94-2023 (West) (to be codified as IND. CODE §§ 24-15).

[136] *Id*. § 24-15-1-1(a)(2).

[137] *Id*. § 24-15-1-1(b)(1).

[138] *Id*. § 24-15-1-1(b)(2).

[139] *Id*. § 24-15-1-1(b)(3).

[140] *Id*. § 24-15-1-1(b)(4).

[141] *Id*. § 24-15-1-1(b)(5).

[142] *Id*. § 24-15-4-1(1).

[143] *Id*. § 24-15-4-1(2).

personal data;[144] (d) avoid the processing of sensitive data;[145] and (e) provide a detailed privacy notice, which must specify the purposes for which personal data is collected and used and details regarding how consumers can exercise their rights.[146]

Additionally, INCDPA imposes certain general responsibilities on controllers and processors of personal data, including the requirement for controllers to conduct a data protection impact assessment, and the obligations for processors to assist the controller in meeting its obligations.[147] Like most other states, the attorney general has exclusive authority to investigate potential violations and to enforce the provisions of INCDPA but must provide 30-days' written notice and an opportunity to cure and provide required assurances of such cure prior to initiating any formal enforcement action.[148]

8. Montana

Montana Governor Greg Gianforte signed the Montana Consumer Data Privacy Act ("MTCDPA")[149] on May 19, 2023, after unanimous passage through the state legislature. The Act will go into effect October 1, 2024.

The MTCDPA guarantees protected consumers the right to: (a) confirm whether a controller is processing their data and access the personal data being processed;[150] (b) correct inaccuracies in their personal data, consider the nature of the data, and the purposes of the processing;[151] (c) delete personal data;[152] (d) obtain a copy of most personal data that the consumer provided to the controller in a portable and readable format;[153] (e) opt-out of the processing of their data for the purposes of targeted advertising, the sale of such data, or profiling in furtherance of "solely automated decision[s] that produce legal or similarly significant effects concerning the consumer."[154] The statute requires opt-out options to be conspicuous and user-friendly.

The MTCDPA also imposes general obligations on controllers to "limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes

---

[144] *Id*. § 24-15-4-1(3).

[145] *Id*. § 24-15-4-1(5).

[146] *Id*. § 24-15-4-3.

[147] See generally, id. § 24-15-6.

[148] *Id*. § 24-15-9-3(a).

[149] Montana Consumer Data Privacy Act, 2023 Montana Laws Ch. 681.

[150] *Id.* § 5(a).

[151] *Id.* § 5(b).

[126] *Id.* § 5(c).

[153] *Id.* § 5(d).

[154] *Id.* § 5(e).

for which the personal data is processed, as disclosed to the consumer,"[155] and imposes a general obligation to establish, implement, and maintain reasonable data security practices.[156] Controllers also have an affirmative obligation to perform a data protection assessment of any processing activity that presents a heightened risk of harm to the consumer, and to share such assessments with the attorney general upon request.[157]

9. Tennessee

The Tennessee Information Protection Act ("TIPA") was signed into law on May 11, 2023, making Tennessee the ninth state to enact comprehensive data privacy and the fourth to do so just in 2023.[158] The TIPA applies to persons conducting business in Tennessee producing products or services targeting residents of Tennessee that has annual revenue of more than $25,000,000, and that either (a) control or process the personal information of 25,000 consumers *and* derive more than fifty percent of their revenue from the sale of such personal information, or (b) during a calendar year, control or process the personal information of 175,000 consumers.[159]

Unlike the laws of some other states, the TIPA seems to have been drafted with a goal of incentivizing compliance. Some provisions are now familiar from other statutes. Businesses that are controllers under the TIPA must comply with authenticated consumer requests to: (a) confirm whether a controller is processing the personal information of the consumer and access the personal information;[160] (b) correct inaccuracies in the personal information;[161] (c) delete personal information provide by or obtained about the consumer (other than de-identified data);[162] (d) obtain a copy of any personal information provided by the consumer in a reasonably accessible format;[163] or (e) opt-out of the processing of their date for purposes of selling personal information, targeted advertising, or profiling the consumer in ways that could have legal or other significant effects on the consumer. [164]

The TIPA also has general rules that govern controllers, such the requirement that controllers: (a) limit the collection of personal information to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to

---

[155] *Id.* § 7(a).

[156] *Id.* § 7(b).

[157] See generally, id. § 9.

[158] Tennessee Information Protection Act, 2023 Tenn. Pub. Acts Ch. 408 (to be codified as TENN. CODE ANN. § 47-18-3201).

[159] *Id.* § 47-18-3201 and § 47-18-3203.

[160] *Id.* § 47–18–3203(a)(2)(A).

[161] *Id.* § 47–18–3203(a)(2)(B).

[162] *Id.* § 47–18–3203(a)(2)(C).

[163] *Id.* § 47–18–3203(a)(2)(D).

[164] *Id.* § 47–18–3203(a)(2)(E).

the consumer;[165] (b) avoid processing data for any purposes other than disclosed purposes;[166] and (c) establish and implement reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal information.[167] The TIPA also has familiar language regarding the obligation of controllers to perform a data protection assessment, to use privacy policies, and to avoid discriminatory uses of data.

However, there is more language throughout the TIPA that makes it clear that the obligations are based on a fact-specific consideration of what is reasonable. The TIPA has higher thresholds that must be reached before a business becomes subject to the law, fewer restrictions on the use of de-identified data, and most notably, a safe harbor provision for those controllers and processors that maintain a voluntary privacy program. Specifically, the TIPA provides that if a controller or processor creates, maintains, and complies with a written privacy policy that reasonably conforms to the National Institute of Standards and Technology ("NIST") privacy framework (or other documented policies or standards designed to safeguard privacy), that is updated to reasonably conform with a subsequent revisions to the NIST or comparable privacy framework within two years of the publication of such revision, and generally provides a person with the substantive rights required by the TIPA, that controller or processor has an affirmative defense to any claimed violation of the TIPA.[168]

10. Texas

On June 18, 2023, Texas became the tenth state to enact a comprehensive consumer privacy law by passing the Texas Data Privacy and Security Act ("TDPSA").[169] The TDPSA will take effect on July 1, 2024—earlier than many of the other state data privacy laws.[170]

Unlike most other state privacy laws enacted to date, there are no revenue thresholds to meet before a business may be covered by the TDPSA. Rather, the TDPSA applies to a person that conducts business in Texas or produces a product or services consumed by residents of Texas, if such business processes or engages in the sale of personal data and is not a "small business" as defined by the U.S. Small Business Administration ("SBA"). Notably, the SBA includes the employees and revenues of affiliates in determining whether a business qualifies as a "small business," which means that the Texas law may potentially affect more franchisors and franchisees than other state data privacy laws.

Other components of the TDPSA are more familiar and seem to follow the Virginia framework. Under the TDPSA, a controller must comply with a consumer's request to: (a) confirm

---

[165] *Id.* § 47-18-3204(a)(1).

[166] *Id.* § 47-18-3204(a)(2).

[167] *Id.* § 47-18-3204(a)(3).

[168] *Id.* § 47-18-3213.

[169] Texas Data Privacy and Security Act, 2023 Tex. Sess. Law Serv. Ch. 995 (West) (to be codified at TEX. BUS. & COM. § 541); *see also* Joseph Duball, *Texas Latest to Add Comprehensive State Privacy Law*, INT'L ASS'N OF PRIV. PROS: THE PRIV. ADVISOR (June 2, 2023), https://iapp.org/news/a/texas-latest-to-add-comprehensive-state-privacy-law/.

[170] Texas Data Privacy and Security Act, 2023 Tex. Sess. Law Serv. Ch. 995 (West) (to be codified at TEX. BUS. & COM. § 541).

whether a controller is processing their data and access the personal data being processed;[171] (b) correct inaccuracies in their personal data, considering the nature of the data and the purposes of the processing;[172] (c) delete personal data provided by or obtained about the consumer;[173] (d) obtain a copy of most personal data that such consumer provided to the controller in a portable and useable format;[174] (e) opt-out of the processing of their data for the purposes of targeted advertising, the sale of such data, or profiling in furtherance of [a] decision that produce[s] a legal or similarly significant effect concerning the consumer."[175]

Controllers subject to the TDPSA must provide consumers with a reasonably accessible and clear privacy policy meeting certain specific requirements and including certain mandatory language.[176] Controllers must also limit the collection of personal information to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer; implement reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal information;[177] and avoid processing data for any purpose that is neither reasonably necessary or compatible with the disclosed purposes, for any discriminatory purpose, or including sensitive data without consent.[178] The Texas Attorney General has exclusive authority to investigate potential violations and to enforce the provisions of the TDPSA, but must provide 60-days' written notice and an opportunity to cure prior to initiating any formal enforcement action.[179]

C. State (and Potential Federal) Privacy Best Practices

As should be apparent from the summary above, state privacy statutes and regulations governing the use of personal data are already proliferating in a patchwork manner. As a best practice, a brand must keep abreast of new privacy laws as they are being enacted at a rapid rate and the landscape will continue to evolve in 2023 and beyond.

Moreover, federal regulation of privacy laws, and preemption of the existing and growing state patchwork of laws, is also a live possibility. Although no federal laws currently preempt the state laws described above, practitioners advising brands should closely watch for some form of federal preemption should federal legislation be enacted. Although the 2022 American Data Privacy and Protection Act ("ADPPA") had substantial promise, it was not enacted into law before the adjournment of Congress in January 2023. As more state-level laws go into effect and states become invested in the specifics of their own law, it is also possible that a federal version may

[171] *Id*. § 541.051(b)(1).

[172] *Id*. § 541.051(b)(2).

[173] *Id.* § 541.051(b)(3).

[174] *Id.* § 541.051(b)(4).

[175] *Id.* § 541.051(b)(5).

[176] *Id.* § 541.102.

[177] *Id.* § 541.101(a).

[178] *Id.* § 541.101(b).

[179] See generally, id. § 541.

not entirely preempt state requirements. Regardless, however, the release of a new draft of ADPPA is forthcoming and may have legs to gain support in 2023, in part, due to Congress' mounting concern of the collection and use of the data of minors.[180]

Proponents of a federal consumer privacy law often cite the patchwork of state laws and how it is vital to unify these for small businesses (such as emerging franchisors and individual franchisees who may have multiple units that cross state borders).[181] Many just feel it is time for the U.S. to join the many other countries around the world in enacting legislation to govern how "Big Tech" collects, stores, protects, manages, and often monetizes personal data.[182] Opponents exist for various reasons. Some are the big tech companies themselves, and some opponents are the states, such as representatives from California, that have enacted stricter legislation already occupying the space that do not want to be pre-empted. [183]

As another best practice, advisors should keep watch over state and federal efforts to manage or regulate the evolution of technology more generally. From efforts to ban or limit practices of specific platforms (for example, TikTok or Facebook) to state efforts to regulate the use of AI, the frequency of enactment of these laws is likely to only increase.[184] If a federal data privacy law is not passed in a manner that preempts state legislation in the area, the current fragmented landscape will only get messier. In addition, although AI-specific laws are still under consideration, it is entirely possible that the robust data needed to make AI systems effective may

---

[180] Steve Adler, *Revised American Data Privacy and Protection Act Due to be Released*, THE HIPPA J. (Apr. 14, 2023), https://www.hipaajournal.com/revised-american-data-privacy-and-protection-act-due-to-be-released/.

[181] See id.

[182] A.B.A. Governmental Affairs Office, *The American Data Privacy and Protection Act*, THE WASH. LETTER, Aug. 2022, https://www.americanbar.org/advocacy/governmental_legislative_work/publications/washingtonletter/august-22-wl/data-privacy-0822wl/ (noting the public's concern over Beg Tech's use of personal data").

[183] There are significant hurdles before the American Data Privacy and Protection Act, or any other bill may be passed at the federal level. *See generally*, Amy Olivero, *Reviewing the House Committee Changes to the Proposed ADPPA*, INT'L ASS'N OF PRIV. PROS: THE PRIV. ADVISOR (Sept. 16, 2022), https://iapp.org/news/a/reviewing-the-house-committee-changes-to-the-proposed-american-data-privacy-and-protection-act/; Joseph Duball, *State Views on Proposed ADPPA Preemption Come Into Focus*, INT'L ASS'N OF PRIV. PROS: THE PRIV. ADVISOR (Sept. 27, 2022), https://iapp.org/news/a/state-level-views-on-proposed-adppa-preemption-come-into-focus/; Cameron F. Kerry, *Will California be the Death of National Privacy Legislation*, THE BROOKINGS INST. (Nov. 18, 2022), https://www.brookings.edu/articles/will-california-be-the-death-of-national-privacy-legislation/; Joint Letter from Gavin Newsom, Governor of California, Rob Bonta, Attorney General of California, and the California Privacy Protection Agency, to Congressional Leaders, House Energy & Commerce Committee, United States Congress (Feb. 28, 2023) (arguing that the ADPPA should be a floor and not a ceiling), https://cppa.ca.gov/pdf/adppa_letter.pdf; Press Release, Office of Governor Gavin Newsom, Governor Newsom, Attorney General Bonta and CPPA File Letter Opposing Federal Privacy Preemption, https://www.gov.ca.gov/2023/02/28/governor-newsom-attorney-general-bonta-and-cppa-file-letter-opposing-federal-privacy-preemption/ (Feb. 28, 2023).

[184] *See e.g.,* An Act Banning Tiktok in Montana; Prohibiting a Mobile Application Store From Offering the Tiktok Application to Montana Users; Providing for Penalties; Providing for Enforcement Authority; Providing Definitions; Providing for Contingent Voidness; And Providing A Delayed Effective Date*,* 2023 Mont. Laws Ch. 681 (the Montana Tiktok ban); Sorelle Friedler, Suresh Venkatasubramanian & Alex Engler, *How California and other states are tackling AI legislation*, THE BROOKINGS INST. (Mar. 22, 2023), https://www.brookings.edu/articles/how-california-and-other-states-are-tackling-ai-legislation/.

trigger its own set of privacy challenges.[185] For example, it is likely that a future court will be asked to consider whether it is possible to grant a consumer the right to delete, as required in a number of states, if the information to be deleted has already been fed to an artificial intelligence system.[186]

As illustrated by the various state laws discussed above, the analysis required to determine which laws apply to what data can be extensive. As a best practice, national franchisors, and franchisors with national aspirations, will want to develop their technology and privacy framework in compliance with the strictest privacy regimes and to ensure that their technology vendor relationships are with companies making the same commitments.[187] These laws have the potential to significantly affect all national franchisors, and any franchisors or franchisees that derive revenue from the sale of personal data. A franchisor that mandates a new technology for a system, may contractually own the personal data collected by such system, and in any event should contractually require its vendors to comply with local privacy laws.[188]

D. Biometric Privacy Laws

One area of increasing importance is biometric privacy. Encouraged by the development of fingerprint scanning, facial recognition, and voice recognition, technology companies are eager to simplify the consumer experience by incorporating these cutting-edge technologies into their products. But many regulators have a healthy skepticism about the security of such information and the use of technologies. Already there are examples of concerning uses of this technology.[189] However, states are also grappling with the most effective way to effectively regulate this technology. Each approach has its own benefits and challenges.

1. Illinois

The Illinois Biometric Information Privacy Act ("BIPA")[190] is one such example of how state-by-state rulemaking on privacy issues that are enforced through private rights of action have the potential to create windfalls for plaintiffs' attorneys and headaches for businesses that may not be attuned to local privacy developments at the state and local level.

The BIPA came into effect on November 3, 2008. The statute was passed in the context of the increased use of biometrics, and the legislature's concern that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example,

---

[185] Zach Williams, *US States Target AI With a Medley of Regulatory Measures,* BLOOMBERG LAW (Aug. 2, 2023, 5:00 AM), https://news.bloomberglaw.com/artificial-intelligence/us-states-target-ai-with-a-medley-of-regulatory-measures (noting that AI related measures have passed in at least one dozen states).

[186] Note that in many states, the "right to delete" may not be absolute and may not apply to anonymized or de-identified data.

[187] *See also* discussion *infra* Section VI.B.1 (Contracting with Third-Party Vendors).

[188] See, e.g., Rebecca Valo, et al., *Franchising in the Age of Digitization, Robotics and Automation*, 41st ANNUAL IFA LEGAL SYMPOSIUM at 29-30 (2023) (discussing franchisor ownership of data).

[189] *See, e.g.*, Kashmir Hill & Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, N.Y. TIMES, A15, Dec. 23, 2022, https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html.

[190] Illinois Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/1, et seq.

social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[191] Because the legislature noted that the full ramifications of the technology were not fully known, it found that "regulation of the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information was warranted."[192] The BIPA's requirements are extensive but the key requirement is that any person that collects biometric information in Illinois must give proper advance notice for any such collection and obtain written consent.[193] If the entity collecting the biometric data fails to provide notice or obtain consent, an "aggrieved" person my file a claim seeking damages.[194]

In the first few years after the BIPA's passage, very few cases were filed. One source estimates that only fifteen BIPA class actions were filed between 2008 and 2016, which suggests that both that biometric-based technology was not as prevalent and that plaintiffs' attorney were not yet fully aware of the significant damages available under the law.[195] However, in 2016, the first significant class action settlement involving the L.A. Tan franchise system and L.A. Tan customers, was approved.[196] Although the amount of the settlement was only $1,500,000—which seems paltry in hindsight—it may have started a trend.

Since 2016, both the number of cases filed and the amount of damages recovered by plaintiffs have been on an upward trajectory. An estimated sixty-nine class actions were filed in Illinois in 2017, and an estimated seventy-nine were filed in Illinois in 2018.[197] In 2019, however, the Illinois Supreme Court added even more incentive for plaintiffs. An earlier 2017 Illinois Court of Appeals ruling suggested some limitations on potential BIPA liability by holding that a person was not an "aggrieved person" under Section 20 of the BIPA when the only allegation was the collection of biometric identifiers and/or biometric information without providing required

---

[191] *Id*. § 14/5(c).

[192] *Id*. § 14/5(f)-(g).

[193] Note that it is unclear under current case law whether consent, if freely given, can be effectively revoked.

[194] 740 Ill. Comp. Stat. 14/20.

[195] Seyfarth Shaw LLP, *Biometric Privacy Class Actions by the Numbers: Analyzing Illinois' Hottest Class Action Trend*, SEYFARTH: WORKPLACE CLASS ACTION BLOG (June 28, 2019), https://www.workplaceclassaction.com/2019/06/biometric-privacy-class-actions-by-the-numbers-analyzing-illinois-hottest-class-action-trend/ [hereinafter "*BIPA Class Actions by the Numbers"*].

[196] Stipulation of Class Action Settlement, Sekura v. L.A. Tan Enterprises, Inc., No. 2015-CH-16694 (Il. Cir. Ct., Dec. 1, 2016); *see also* Gabe Friedman, *First Settlement Reached Under Illinois Biometric Law,* BLOOMBERG LAW (Dec. 5, 2016, 10:27 AM), https://news.bloomberglaw.com/business-and-practice/first-settlement-reached-under-illinois-biometric-law/ (discussing the $1,500,000 million class action settlement approved between L.A. Tan and its customers).

[197] *BIPA Class Actions by the Numbers*, *supra* note 189; *see also*, *A Bad Match: Illinois and the Biometric Information Privacy Act*, ILR BRIEFLY (U.S. Chamber Institute for Legal Reform), Oct. 2021, at 4-5, https://instituteforlegalreform.com/wp-content/uploads/2021/10/ILR-BIPA-Briefly-FINAL.pdf.

disclosures and obtaining the written consent required by Section 15(b) of the Act.[198] In other words, claims could not proceed without an allegation of actual harm or damage.

However, in January 2019, the Supreme Court of Illinois reversed the decision of the appeals court, holding that a failure to comply with the BIPA's Section 15 requirements *is* the harm because it deprives a person of their statutory rights.[199] Accordingly, an individual "need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act."[200]

Without the need to identify any harm beyond the improper collection of data, this decision created a surge in BIPA litigation. In 2019, an estimated 286 BIPA claims were filed in state court in Illinois, with another 82 filed in various federal courts. In February 2023, news outlets estimated that over 2,000 cases had been filed since 2017.[201]

Also in February 2023, two new Illinois Supreme Court decisions created the conditions for an additional surge. The Illinois Supreme Court in *Cothon v. White Castle System, Inc.*[202] further expanded potential monetary liability under the BIPA by clarifying that BIPA claims accrue *each time* biometric data is unlawfully collected and disclosed.[203] The BIPA's language allows liquidated damages of up to $1,000 for "each violation" of the statute which, if the collection of data is regular and routine such as employee timekeeping or loyalty program sign-ins, could create exponential liability.[204] Although the court noted that a trial court may exercise its discretion in fashioning an award to prevent damages that would result in "financial destruction of a business," it is unclear how that would be applied in practice.[205]

In *Tims v. Black Horse Carriers*, the Illinois Supreme Court resolved the question of what statute of limitations applied to the BIPA liability, holding that the five-year statute of limitation rather than the 1-year limitation for certain privacy claims applied to the BIPA liability.[206] While not expanding the scope of ultimate liability, the *Tims* decision provides comfort to those considering filing cases where the claim would have accrued more than a year prior, and creates urgency for

---

[198] Rosenbach v. Six Flags Ent. Corp., 147 N.E.3d 125, 129 (Ill. App. Ct. 2017), *rev'd*, 129 N.E.3d 1197 (Ill. 2019).

[199] Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1206 (Ill. Jan. 25, 2019).

[200] *Id.* at 1207.

[201] Daniel Wiessner, *White Castle could face multibillion-dollar judgment in Illinois privacy lawsuit*, REUTERS, Feb. 17, 2023, https://www.reuters.com/legal/white-castle-could-face-multibillion-dollar-judgment-illinois-privacy-lawsuit-2023-02-17.

[202] Cothon v. White Castle System, Inc., No. 128004, 2023 WL 2052410 (Ill. Feb. 17, 2023).

[203] Id.

[204] *See* BIPA, 740 ILL. COMP. STAT. 14/20 (West, Westlaw through Pub. Acts 103-169 of the 2023 Reg. Sess.) (noting liquidated damages of $1,000 for each violation, and $5,000 for intentional or reckless violations).

[205] *See Cothon*, 2023 WL 2052410 at *8 (noting that the legislature intended to impose significant liability but that "there is no language in the Act suggesting legislative intent to authorize a damages award that would result in the financial destruction of a business.").

[206] Tims v. Black Horse Carriers, Inc., No. 127801, 2023 WL 1458046 (Ill. Feb. 2, 2023).

those cases in which the collection of biometric data dates back to 2018. Unsurprisingly, since the *Cothon* and *Tims* decisions, the number of new cases has seen an additional reported spike.[207]

As of the date of this paper, there have been at least seven reported decisions involving franchised systems under the BIPA, and likely many others that have been threatened or filed and settled quickly thereafter.[208]

2. All Other States

Although it might not be apparent from headlines, several other states also have biometric privacy laws. Texas and Washington have standalone biometric privacy laws.[209] Other states—including most of the states discussed in Section III.B above—have amended or enacted laws that specifically include biometric data as part of the data protected by data breach laws or other comprehensive data privacy laws. The key distinguishing factor of the BIPA is that it is the only biometric privacy law in effect that has always contained a private right of action. When enforcement is left to state attorney generals, they tend to go after the biggest companies or the most egregious violations but lack the resources to pursue all violations. Thus, the high volume of cases seen in Illinois is non-existent in other states, and the eye-popping verdicts and settlements are less frequent.

While the requirement for state enforcement leads to a lower volume of cases in general, other states may be looking to the BIPA cases to asses potential liability under their own laws.[210] In 2023, following Meta's agreement to pay $650,000,000 to settle the BIPA claims against it, the Texas Attorney General (with the help of private law firms) filed a petition against Meta for alleged violations of Texas Capture or Use of Biometric Identifier Act ("CUBI").[211] The Texas Attorney General alleged that Facebook's photo "Tag Suggestions" feature captures biometric identifiers without providing notice or obtaining consent. Subsequently, the Texas Attorney General filed a second CUBI lawsuit—this time against Google. The Texas Attorney General alleges that

---

[207] Stephen Joyce & Skye Witley, *Illinois Biometric Privacy Cases Jump 65% After Seminal Ruling*, BLOOMBERG LAW (May 2, 2023, 5:15 AM), https://news.bloomberglaw.com/privacy-and-data-security/illinois-biometric-privacy-cases-jump-65-after-seminal-ruling.

[208] Coons v. Yum! Brands, Inc., No. 21-CV-45-SPM, 2023 WL 3320149 (S.D. Ill. May 9, 2023) (Taco Bell and Yum); Kyles v. Hoosier Papa LLC, No. 1:20-CV-07146, 2023 WL 2711608 (N.D. Ill. Mar. 30, 2023) (Papa John's); Rushing v. McAlister's Franchisor SPV LLC, No. 22-CV-649-SMY, 2023 WL 2163388 (S.D. Ill. Feb. 22, 2023) (McAlisters and Focus Brands); Stauffer v. Innovative Heights Fairview Heights, LLC, No. 3:20-CV-00046-MAB, 2022 WL 3139507 (S.D. Ill. Aug. 5, 2022) (SkyZone); Ronquillo v. Doctor's Assocs., LLC, 597 F. Supp. 3d 1227 (N.D. Ill. 2022) (Subway); Smith v. Signature Systems, Inc., No. 2021-CV-02025, 2022 WL 595707 (N.D. Ill. Feb. 28, 2022) (Jimmy John's); Sekura v. Krishna Schaumburg Tan, Inc., 115 N.E.3d 1080 (Ill. App. 2018) (L.A. Tan).

[209] *See* Texas Capture or Use of Biometric Identifier Act, TEX. BUS. & COM. CODE § 503.001; Washington Biometric Privacy Protection Act, WASH. REV. CODE §§ 19.375.010 et seq.

[210] *See generally*, Andrea Peterson, *A Long-Dormant Texas Privacy Law is Finally Being Put to Use Against Tech Giants*, RECORDED FUTURE NEWS: THE RECORD (Oct. 20, 2022), https://therecord.media/a-long-dormant-texas-privacy-law-is-finally-being-put-to-use-against-tech-giants.

[211] *See generally*, Plaintiff's Petition, *Texas v. Meta Platforms, Inc.*, Case No. 22-0121 (Tex. 71st Dist. Feb. 14, 2022).

Google's products capture face geometry from photos and videos and (for Google Assistant) voiceprints from detected voices in violation of CUBI.[212]

In addition, some states or other jurisdictions may see the Illinois model as an effective enforcement mechanism that gives the state much-needed assistance with pursuing violations of biometric privacy laws. A 2023 Washington law, known as the My Health My Data Act[213] was signed by Washington Governor Jay Inslee on April 27, 2023. Although nominally intended to protect consumer health data, the definition of "health data" is broad enough to encompass biometric data. That Act will be enforced through the Washington Consumer Protection Act ("WCPA"), which authorizes class actions and contains a private right of action that allows prevailing parties to seek actual damages (including treble damages up to $25,000 per violation, in some cases), injunctive relief, and attorneys' fees.[214] The Washington attorney general also has the authority to pursue violations of the act. When the law goes into effect on March 31, 2024, Washington may become the next area of liability for biometric privacy issues. Even local jurisdictions may get involved in regulation of biometric data collection. For example, Plaintiffs' attorneys have filed a class action related to improper collection of biometric information under the New York City Biometric Identifier Information Law.[215]

E. Additional Laws to Consider

We have focused on comprehensive data privacy laws and biometric privacy laws in the U.S. both because they are evolving quickly, and because they are most likely to be implicated by data-hungry new technologies. However, franchisors should carefully consider the industries and jurisdictions in which the franchisor operates, the demographics of a brand's target customers, and the particular technology being considered for adoption, as part of analyzing what *other* laws may be implicated. International franchisors may have to navigate stricter international data privacy laws such as the GDPR.[216] Franchisors considering digital payment solutions, non-contact purchasing, or cash-free retail locations may be foiled by those jurisdictions that mandate cash acceptance out of concern for access and fairness, including Colorado, Connecticut,

---

[212] Press Release, Ken Paxton, Attorney General of Texas, Paxton Sues Google for its Unauthorized Capture and use of Biometric Data and Violation of Texans' Privacy (Oct. 20, 2022), https://www.texasattorneygeneral.gov/news/releases/paxton-sues-google-its-unauthorized-capture-and-use-biometric-data-and-violation-texans-privacy.

[213] My Health My Data Act, WASH. REV. CODE § RCW 19.375.010; *see also* Lili Burns & Jonathan Newmark, *Washington's Biometric Data Regime Advances Privacy Regulation,* BLOOMBERG LAW (May 16, 2023, 4:00 AM), https://news.bloomberglaw.com/us-law-week/washingtons-biometric-data-regime-advances-privacy-regulation.

[214] WASH. REV. CODE § 19.86.090 (West, Westlaw through all effective Legis. of the 2023 Reg. Sess. and First Spec. Sess. of the Wash. Leg.).

[215] Lauren Rosenblatt, *Amazon, Starbucks Face WA Class-Action Lawsuit Over Customer Data*, SEATTLE TIMES https://www.seattletimes.com/business/amazon-starbucks-face-wa-class-action-lawsuit-over-customer-data/ (June 8, 2023, 6:56 PM).

[216] See generally, 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, ABA 42ND ANNUAL FORUM ON FRANCHISING W-17, at 1 (2019); Caitlin Conklin, Aidan Nowak, and Travis Powers, Data Privacy in a Public World: The Impact of Data Privacy in Franchising, 42 FRANCHISE L.J. 69 at 70-75 (2022).

Delaware, Montana, Tennessee, Maine, New Jersey, Oregon, Pennsylvania, Rhode Island, and cities such as San Francisco, California, and New York City.[217]

Educational franchises and franchises that serve children and young adults must consider the Children's Online Privacy Protection Act.[218] Depending on the technology, other federal laws such as the Health Insurance Portability and Accountability Act,[219] Americans with Disabilities Act,[220] Telephone Consumer Protection Act, [221] Fair Credit Reporting Act,[222] and the Fair and Accurate Credit Transaction Act of 2003[223] along with a variety of state and local laws may each impact potential adoption of new technologies or create unintended consequences if not considered in advance.

F. Franchise Laws

A final challenge for franchisors seeking to implement new technologies in their franchise system is how to effectively disclose to prospective franchisees current technology requirements and the potential for additional change. Prospective franchisees have a material interest in understanding a franchisor's approach to technology. Existing franchisees also have a vested interest in a franchisor's plans for incorporating new technology. On one hand, a franchisor's failure to adapt can create real liabilities for a franchise system, but on the other hand, significant changes to the operating standards to incorporate new technology may require significant operational changes and cost franchisors and franchisees in training, time, and money.

More importantly, as the laws discussed above continue to evolve, franchisors may seek more control over franchisee operations to ensure that the risk to the system and goodwill remain at a manageable level. The current "Disclosure Requirements and Prohibitions Concerning Franchising and Business Opportunities" ("The Rule") was finalized by the Federal Trade Commission in 2007 when the technology landscape was very different, and that is reflected in

---

[217] *See* ATM Industry Association, https://www.atmia.com/connections/regions/united-states-americas/#cashmap (last visited Aug. 17, 2023) (map of jurisdictions with pending and enacted cashless bans).

[218] Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-6506; *see generally* Lesley Fair, *20 Million FTC Settlement Addresses Microsoft Xbox Illegal Collection of Kids' Data: A Game Changer for COPPA* Compliance, FEDERAL TRADE COMMISSION: BUSINESS BLOG (June 5, 2023) (noting that "under Section 312.4(b) of the COPPA Rule—often called the direct notice requirement—a company must provide parents with direct notice of its information practices before it collects, uses, or discloses personal information from kids; Section 312.4(d) of the COPPA Rule—often called the online notice provision—requires (among other things) that companies post a prominent and clearly labeled link to an online privacy notice explaining their information practices "at each area of the Web site or online service where personal information is collected from children.").

[219] Health Insurance Portability and Accountability Act. Pub. L. No. 104-191, § 264, 110 Stat.1936.

[220] Americans With Disabilities Act of 1990, 42 U.S.C. § 12101 et seq.; *see, e.g.,* Sullivan v. Doctor's Assocs. LLC, No. 1:19-CV-719-GHW, 2020 WL 2319295 (S.D.N.Y. May 8, 2020) (dismissing claims against franchisor based on communications between franchisee and deaf patron).

[221] Telephone Consumer Protection Act, 47 U.S.C. § 227.

[222] Fair Credit Reporting Act,15 U.S.C. § 1681 et seq.

[223] 15 U.S.C. § 1681c(g)(1); *see also* Keith v. Back Yard Burgers of Nebraska, Inc., No. 8:11-CV-135 (D. Neb. Apr. 13, 2012).

the language.[224] Today, The Rule's requirement to disclose a franchisor's requirements regarding the use of "electronic cash registers or computer systems" and the "types of data to be generated or stored in these systems" feels almost quaint.[225] While regulators clearly recognized that disclosure regarding technology requirements was warranted, it would have been impossible to predict the speed and direction of such technological change. As a result, franchisors and regulators trying to apply The Rule's framework to current technology have been largely on their own in analyzing what constitutes effective disclosure of both *current* technology requirements and the *future* changes that might be required over the lifetime of the franchise agreement.

In 2019, the context of its periodic review of The Rule, the Federal Trade Commission asked the public "[w]hat modifications, if any, should be made to [The Rule] to account for changes in relevant technology or economic conditions? What evidence supports the proposed modifications?"[226] The North American Securities Administrators Association, Inc. ("NASAA"),[227] suggested several changes with an emphasis on the ubiquity of cloud computing and the risk of data breaches and other cybersecurity threats. Among other things, NASAA argued that any revisions to The Rule should "account for the value of customer data to the franchise system and the potential value of this data to third parties," should require the franchisor to state whether the franchisor reserves the right or intends to sell or to share franchisee-generated data, and should require disclosure of the data protection obligations of the parties and duties of each in the event of a data breach.[228]

These comments were submitted in 2019, and the speed of technological obsolescence and the proliferation of new technology continues to increase. Comments made as of the date of this paper might suggest disclosure regarding the use of AI, and disclosure regarding a franchisee's right to request technology changes to comply with local laws, or to encourage the adoption of system technologies. Because customers' relationship with brand is increasingly mediated by their virtual experience, whether a franchisor-owned website, franchisor-owned app, third-party app, and even other virtual environments such as the metaverse or augmented reality, the franchisor's use (or lack of use) of these additional tools may have meaningful effects on the franchisee's bottom line. In sum, the need for effective disclosure is only intensified.[229]

Future changes to The Rule may also need to account for the use of predictive technology in franchise systems. Predictive analytics may be used to select store locations, suggest staffing

---

[224] Disclosure Requirements and Prohibitions Concerning Franchising and Business Opportunities; Final Rule, 72 Fed. Reg. 15444, 15445 (Mar. 30, 2007), codified at 16 C.F.R. Part 436, https://www.ftc.gov/sites/default/files/070330franchiserulefrnotice.pdf.

[225] *Id.* § 436.5(k)(5).

[226] Disclosure Requirements and Prohibitions Concerning Franchising, Regulatory Review; Request for Public Comment, 84 Fed. Reg. 49 at 9052 (Mar. 13, 2019).

[227] NASAA is the association of state securities administrators who are charged with the responsibility for administering state securities and franchise laws in the U.S.

[228] Letter from the North American Securities Administrators Association, Inc. submitted to the Federal Trade Commission re: Franchise Rule Regulatory Review, 16 CFR Part 436, Matter No. R511003 at page 6 (May 13, 2019).

[229] *See, e.g.*, Colleen McMillar, *Tech Trends: How 5 Brands Keep Abreast of New Technologies*, FRANCHISE UPDATE, Issue 2, 2023, at 48, https://www.franchising.com/articles/tech_trends_how_5_brands_keep_abreast_of_new_technologies.html.

with precision, provide dynamics pricing, and more.[230] Some franchisors are already making decisions using that technology in their corporate locations, but may be constrained in using the technology in franchised locations by either fear of exerting to much control and being deemed a joint employer[231] or concern about potential liability to franchisees if such AI-backed or predictive technologies make inaccurate predictions. Anecdotal evidence suggests that more and more franchisors are using or considering a variety of predictive technologies in operations.[232]

IV. EXAMPLES OF TECH IMPLEMENTATION ROLLOUT

Many franchisors have utilized new technologies to boost franchisee and franchise system performance.[233] As the current legal landscape becomes more defined, franchisors must consider their current technology suite and develop a plan for managing the risk associated with such new technologies. Several recent cases involving franchised systems highlight the risks to a franchisor of either: (a) failing to tightly control the technology and personal data collected by franchised and corporate units; or (b) failing to ensure that the policies and procedures reflect best practices in data security.

A. Data Breach Cases

As noted above, the Federal Trade Commission's claims in *FTC v. Wyndham* were based, in large part, on its allegations that the company had not been proactive about its data security. Similarly, more recent cases have seen banks, consumers, and other injured parties pursue franchisors based on data breaches that may have been tied to franchised locations using similar theories.

For example, in 2020, a district court refused to dismiss negligence claims against Sonic Corp. brought by a collection of banks based on a 2019 data breach in which a hacker accessed and downloaded customer payment data from over 300 Sonic locations.[234] Specifically, the plaintiffs claimed negligence under Oklahoma law, and *per se* negligence based on the FTC Act Section 5.

---

[230] By way of example, Taco Bell discloses in its Item 19 of its Franchise Disclosure Document issued March 27, 2023, that it uses predictive technology called "Bell Point" to assist in site selection analysis and to make sales projections. Franchisees have access to the sale projections and are provided with a confidence interval to assist the franchisee in understanding the accuracy of the data. *See* Franchise Disclosure Document, Taco Bell Franchisor, LLC, issued Mar. 27, 2023 (available at https://www.wdfi.org/apps/FranchiseSearch/MainSearch.aspx, search for "Taco Bell").

[231] For example, in allowing certain wage and hour claims by franchisee employees to proceed against McDonald's, the NLRB alleged that McDonald's inclusion of an employee scheduling tool in the franchisee technology package might be sufficient control for McDonald's to be considered a joint employer. *See generally*, Alexia Elejalde-Ruiz, *Why Should McDonald's be a Joint Employer? NLRB Starts to Provide Answers*, CHICAGO TRIBUNE (Mar. 10, 2016, 7:23 PM) https://www.chicagotribune.com/business/ct-mcdonalds-labor-case-0311-biz-20160310-story.html.

[232] Amanda Peters, *How is Artificial Intelligence Going to Impact Franchising?*, GLOBAL FRANCHISE (Mar. 6, 2020), https://www.global-franchise.com/news/is-artificial-intelligence-going-to-impact-franchising (quoting the CEO of Neighborly, who notes that the company is "enthusiastically pursuing predictive analytics as a tool to optimize our opportunities to enhance our franchisees' growth and success.").

[233] Brazier, *supra* note 8.

[234] *In re* Sonic Corp. Customer Data Sec. Breach Litig. *(Fin. Institutions)*, No. 1:17-MD-2807, 2020 WL 3577341 (N.D. Ohio July 1, 2020).

Regarding the general negligence claim, the court began its analysis by acknowledging that under Oklahoma law, there is generally *not* a duty to protect another person from criminal acts such as data breaches. However, an exception to the general rule applies if an affirmative act by a party has created or exposed another person to a recognizable high degree of risk of harm from a criminal act or misconduct, which a reasonable person would have taken into account.[235] In this case, the court concluded that Sonic Corporation and its subsidiaries and affiliates (collectively, "Sonic") had taken affirmative acts and were on notice of potential harm. The plaintiffs alleged that: (a) Sonic required franchisees to pay into a cybersecurity and technology fund, and largely controlled its franchisees' data security; (b) Sonic and its approved vendors set up the technology that franchisees used, including security settings; (c) franchisees were not permitted to modify or change the security settings Sonic created; (d) at the time of the subject data breach, twenty-three percent of Sonic locations still used significantly outdated technology including one system that was so old that the system manufacturers had stopped updates and security packages almost a decade earlier; (e) Sonic required franchisees to permanently enable remote access which allowed Sonic (and the hackers) to log into the VPN and access sites with franchisee's credit card data; and (f) Sonic permitted weak passwords for such VPN access.[236]

Sonic required that its franchisees pick from one of three approved point-of-sale vendors. Ultimately, the hackers obtained legitimate access credentials for one of those approved point-of-sale vendors and used such credentials (and VPN access) to breach the point-of-sale system of all franchisees using that vendor. Because, on a motion to dismiss, the court was required to accept the allegations as true, the court found that these actions constituted an affirmative act by Sonic sufficient to support a negligence claim. [237] In defense, Sonic argued that it was simply being a responsible franchisor, and that operation of a franchised business should not be considered an "affirmative act" sufficient to impose liability. The court agreed in theory but noted that "while Sonic's operation of a franchise is not alone sufficient, the Sonic affirmative information technology decisions arguably led to the damages Plaintiffs complain of. Simply operating a franchise operation, alone, does not create liability. But some acts taken by the franchisor can create liability."[238]

In particular, the court believed that Sonic should have been aware of the potential risk. After suffering an earlier data breach affecting primarily corporate locations, Sonic had hired a third-party reviewer to investigate and had been informed by such third-party that similar future

[235] *Id.* at *3.

[236] *Id.* at *2-3.

[237] Interestingly, while allowing the plaintiffs to proceed on their negligence claim, the court gently challenged the application of Section 5 to create liability for data breaches on a *per se* basis, noting that "[w]hile the FTC and other courts have interpreted Section 5's terms to apply to data security requirements, the statute's actual terms do not lay out positive, objective standards that, if violated, could give the standard for a negligence per se claim under Oklahoma law." *Id.* at *6.

[238] *Id.* at *4.

breached could occur.[239] The court also took note of industry-wide warnings and other high-profile data breaches that should have put the franchisor on notice.[240]

B. POS Cases

One of the challenges that franchise systems face when adopting new technology is mismatched incentives. Although franchisors have an incentive to update technology to reduce their own risk and the risk to the system, the burden of paying for the purchase, installation, and maintenance of new technology—particularly at the store level—is often partly or completely on the franchisees. If a franchisee is short on additional capital, unaware or unconcerned about system risk, or simply unconvinced that the proposed new technology will be worth the investment, struggles between franchisors and franchisee can arise. One area in which this tension frequently arises is with required point-of-sale ("POS") system changes. [241] It may be particularly acute when multi-unit operators have an obligation to update multiple stores.

In *Burger King Corp. v. Cabrera*, the franchisor-franchisee conflict over the timing for upgrading POS systems led to a termination and likely expensive litigation. [242] In April 2008, Burger King Corporation ("BKC") announced a new technology policy in which all POS systems that would be ten years old or older at the beginning of 2010 would have to be replaced with a new approved POS system by or before January 1, 2012.[243] Defendant Cabrera was a multi-unit franchise owner with POS units affected by the policy. Although Cabrera was notified of the new policy in 2008, he failed to obtain or install any of the new POS systems in any of his ten restaurants by January 1, 2010 as required.[244] Twelve days after the deadline, BKC sent a notice of default with an opportunity to cure. Although Cabrera managed to enter a contract with the approved POS vendor during the cure period (and ultimately installed the systems by April 2010), the cure period expired before he fully funded the purchase or installed any new POS systems. As a result, BKC terminated the franchise agreements. When Cabrera refused to comply with the

[239] *Id.* at *1.

[240] *Id.* at *1, *5.

[241] *See generally*, Burger King Corp. v. Cabrera, No. 10-20480-CIV, 2010 WL 5834869, at *5 (S.D. Fla. Dec. 29, 2010), *report and recommendation adopted*, No. 10-20480-CIV, 2011 WL 677374 (S.D. Fla. Feb. 16, 2011) (acknowledging the franchisor's contractual requirement to replace obsolete equipment, but denying the franchisor's request for a temporary restraining order when the franchisee has cured its default, albeit belatedly, by installing the updated point-of-sale system mandated by the franchisor). *See also* Bores v. Domino's Pizza, LLC, 530 F.3d 671 (8th Cir. 2008) (holding that a franchisor's contractual right to provide technology specifications was broad enough to require franchisees to purchase specified software from the franchisor, if the franchisor was the only source of such technology); Peterbrooke Franchising of America, LLC v. Miami Chocolates, LLC, 312 F. Supp. 3d 1325 (S.D. Fla Feb. 28, 2018) (reversing the district court's grant of summary judgment in favor of the franchisor for terminating the Franchise Agreement based on the franchisee's failure to upgrade the POS system, due to a question of fact as to whether such failure was "material").

[242] Burger King Corp. v. Cabrera, No. 10-20480-CIV, 2010 WL 5834869, at *2 (S.D. Fla. Dec. 29, 2010), *report and recommendation adopted*, No. 10-20480-CIV, 2011 WL 677374 (S.D. Fla. Feb. 16, 2011).

[243] *Id*. at *2.

[244] *Id*.

termination and simply kept operating using the Burger King name and marks, BKC filed suit for breach of contract and trademark infringement and sought a preliminary injunction.[245]

In determining whether injunctive relief was appropriate, the court first considered whether BKC was likely to succeed in showing that the failure to update technology by the deadline justified the termination. The BKC Franchise Agreement had standard language requiring franchisees to promptly comply with Burger King standards, as they may be amended.[246] It also had more specific language requiring franchisees to upgrade "obsolete" equipment. Despite this language, the court refused to grant a preliminary injunction. It found that there was a substantial factual question as to whether the existing POS system was in fact "obsolete" at the time the new policy was announced. The court noted that "[c]learly, the new POS system makes is easier for the BKC to monitor royalty payments and to audit sales. However, whether this ability makes the older POS system 'obsolete' is a much closer and debatable question that should be resolved on the full record and at trial if necessary."[247] The court acknowledged that BKC had legitimate business reasons for requiring the change and noted that the new POS system could be a critical part of BKC's efforts to stay competitive in a rapidly changing world. It also acknowledged that keeping up with new technology and inventions was good for both franchisors and franchisees. However, the court was not convinced that these business objectives rendered franchisees prior POS system obsolete.

Comparing the *Sonic* data breach case with the *Burger King* POS case makes it clear how narrow the path can be for franchisors seeking to update technology system-wide. Move too quickly and it can create franchisee expense, tension, and frustration.[248] Move too slowly, and the increased cyber security risks that are inherent in older technology can threaten the goodwill of the brand in the event of a data breach.[249]

V. THE AGILE AND ADAPTABLE FRANCHISE SYSTEM FOR AN EVER-EVOLVING TECHNOLOGY LANDSCAPE

Understandably, much of the appeal of franchised brands has, traditionally, been systematized predictability and uniformity. However, with the warp speed at which technology is now developing and evolving, this traditional view of a franchised brand is not only outdated, but even dangerous. The mandate now and, certainly, moving forward, is a franchise system that is constantly innovating, evolving, and adapting.[250] The goal, of course, is not to try to anticipate

---

[245] *Id*.

[246] *Id*. at *1.

[247] *Id*. at *6.

[248] *See generally,* sources cited *supra* note 241.

[249] For coverage of matters involving insecure franchisee technology, *see generally*, Joyce Hanson, *Franchisees Fight IHG Bid To End Suit Over Data Breach*, LAW360.COM (Jan. 18, 2023, 8:08 PM EST), https://www.law360.com/articles/1566140; Hayley Fowler, *'Easy To Hack' Wendy's Franchisee Blamed For Data Breach*, LAW360.COM (Jan. 19, 2023, 8:39 PM EST), https://www.law360.com/articles/1567308.

[250] Wouter Aghina, Karin Ahlback, Aaron De Smet, Gerald Lackey, Michael Lurie, Monica Murarka & Christopher Handscomb, *The Five Trademarks of Agile Organizations,* MCKINSEY & CO. (Jan. 22, 2018), https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-five-trademarks-of-agile-organizations.

every possible technological development, but to create an infrastructure, franchise agreement, and operations manual that will allow sufficient flexibility and franchisor discretion for continued tech development, upgrades, and modifications. The aim is a nimble franchisor that is able to anticipate and adapt quickly with minimal system disruption.[251] As we have discussed, such continued technological innovation and adaptation is increasingly of existential importance for just about every franchise system.

A. Establishing and Managing Expectations: The Importance of the Franchise Culture

Expectations are mental models of how we expect situations to work out. They serve as baselines for what we will be pleased with. Anything less than what we expect is usually a disappointment. We generally want things to work as we intend or as we suppose it would. Expectations influence behavior and feelings involving specific situations.[252]

Every franchisor—large or small, established or emerging—creates expectations among its franchisees and prospective franchisees through its unique franchise culture. This can be done consciously and deliberately, or it can be done *to* a franchise system without the franchisor even realizing that it is happening.[253] A franchise system that is nimble and adaptable is one that is strategically setting and, if necessary, proactively modifying expectations early and often.[254] These types of expectations are the result of a certain franchise culture that is well thought-out and exemplified by the franchisor at every level. "Corporate culture begins at the top and filters down through the organization."[255] This is often done by setting the system's image, standards, and values and then clearly communicating this to franchisees, as well as franchisor's management and employees.[256]

A franchise system that incorporates the importance of innovation, flexibility, and efficient adoption of changes as part of its very culture will likely be well situated to implement changes more readily and with less resistance and disruption. It will also be less likely to encounter resistance from its franchisees.

---

[251] Alejandra Alvarez, Santiago Fernandez Suarez, Nerea Joaristi, Victoria Lee, Michele Tam & Edward Woodcock, *How Can Corporate Function Become More Agile?*, MCKINSEY & CO. (Apr. 1, 2022), www.mckinsey.com/capabilities/operations/our-insights/how-can-corporate-functions-become-more-agile#.

[252] Onsight Blog, Why Managing Expectations is Important in Business, https://www.onsightapp.com/blog/why-managing-expectations-is-important-in-business# (last visited June 13, 2023).

[253] *What's the Big Deal about Franchise Culture?* FRANCHISE BUS. REV. (July 27, 2022), https://franchisebusinessreview.com/post/whats-the-big-deal-about-franchise-culture/ ("Every company has a culture, whether it is strategically planned and orchestrated, or not.")

[254] Chris Dull, Clint Ehlers, Andraya Frith & Max Staplin, *Ch-ch-ch-ch-changes: Implementing System Changes, Upgrades and New Directions Under Existing Agreements*, IFA 50TH ANNUAL LEGAL SYMPOSIUM at 3-4 (2017) ("[F]ranchisors have primary responsibility for setting brand protection standards and ensuring the system remains relevant to consumers. Franchisors must be willing to exercise such responsibility by creating a mindset for change as early as possible in the relationship…").

[255] Joe Matthews, *The Impact of Corporate Culture on a Franchisor's Success*, FRANCHISE PERFORMANCE GROUP (Jan. 31, 2020) https://franchiseperformancegroup.com/the-impact-of-corporate-culture-on-a-franchisors-success.

[256] FRANCHISE BUS. REV., *supra* note 253.

1. Existing Franchisees

For existing franchisees, managing and, if necessary, adjusting expectations, and eventually company culture, can be done through many channels, including modifications to the operations manual, system-wide communications, ongoing trainings, conferences, and conventions. If the franchise system had not previously put a lot of emphasis on the importance of technology and technological innovations, now is definitely the time to do this. The more quickly that a system's expectations can be modified, the more prepared that system will be when the time for updates and changes arrives. Given the speed with which technology is changing and updating, this cultural shift in any franchise system is essential.[257]

One way to send a clear message of the franchisor's commitment to tech innovation and development is by including franchisees in the research, development, and testing of potential innovations and ideas.[258] This can occur in the form of incentives to innovate or provide ideas of possible changes and upgrades. It can also occur through the formation of a franchisee tech advisory council that is specifically tasked with communicating with franchisees and seeking ideas for tech development and innovations.[259] These steps will not only adjust expectations and, therefore, the overall culture, but will also, as discussed further below, allow for smoother implementation when that time comes.

2. Prospective Franchisees

Franchisors have the opportunity to set expectations and understanding by prospective franchisees very early in the prospect's investigation and discovery process. This can even occur as part of the franchisor's branding itself.[260] By prioritizing technological innovation and development and making such innovation a part of the franchisor's very identity, systems can send a very clear message that this is a vital and expected part of being a franchisee. The franchisor can include language in its Franchise Disclosure Document ("FDD") to convey the message that it is a system that is very much committed to continued technological improvements and developments and that all franchisees are expected to participate and contribute to the innovation and implementation process. As discussed in more detail below, the inclusion of a technology fee (a must now), a tech implementation policy, creation of a franchisee tech advisory council, etc., are all indicators of a franchisor's emphasis on the importance of technology. These

---

[257] Brazier, *supra* note 8; Laura LaBerge, Clayton O'Toole, Jeremy Schneider & Kate Smaje, *How COVID-19 Has Pushed Companies Over the Technology Tipping Point—And Transformed Business Forever,* MCKINSEY & CO. (Oct. 5, 2020), https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever.

[258] Tanya Morrison, Charlene Wilson & Ashley Williams, Digital Transformation in a Franchise System: Keeping Up with the Technology Race Within the Bounds of Existing Franchise Agreements, IFA 52ND ANNUAL LEGAL SYMPOSIUM at 9 (2019).

[259] *Id.* ("When a franchisor seeks franchisee involvement, it allows experienced franchisees to contribute their relatable need for change, which adds to the franchisee support and advocacy for the technology change to the entire franchise system.").

[260] Trever Ackerman, *Why Company Culture is Crucial in the Franchise System,* FORBES (June 7, 2018) https://www.forbes.com/sites/forbescommunicationscouncil/2018/06/07/why-company-culture-is-crucial-in-the-franchise-system.

are the types of actions that set a tone and a franchise culture. While the franchise agreement creates the contractual obligations, the FDD can set the stage early and unequivocally.

B. The Franchise Agreement

The language of the franchise agreement is the best and most solid basis for implementation of technological innovations. The franchisor's right to implement changes to the system through the franchise agreement is supported by existing case law, even if it comes at a great financial cost to the franchisee.[261] Additionally, the application of the implied covenant of good faith and fair dealing has, generally, not been a hindrance to the implementation of changes that are intended to benefit the system as a whole.[262] Courts applying the doctrine will look to the reasonableness of the applicable system changes. Where the franchisor exhibits candor, transparency, and the interests of the system as a whole and does not act "with improper motives, or arbitrarily, capriciously, or in a manner inconsistent with the reasonable expectations of the parties[,]" the doctrine has usually supported the proposed system modifications.[263]

It is also a great place to set the tone for the franchise culture and manage expectations from the very beginning of the relationship, in the case of new or, even, renewing franchisees. The franchise agreement should include clear language that gives the franchisor flexibility and discretion in, not only instituting tech changes, but also in researching and developing new and innovative tech. This type of language would very quickly signal a system that is committed to staying ahead of the curve and its competitors. It would, thereby, also attract franchisees who are as committed to this type of innovation and not afraid of the changes and even disruptions that such changes could bring.

1. General Terms

Every system's franchise agreements in the year 2023 should be drafted to anticipate a rapidly changing technology landscape. As discussed, any business that fails to appreciate the crucial role that evolving technologies now play in the operation of its business and its bottom line risks, not only profits, but its own obsolescence, along with the obsolescence of its technology.

a. Definitions

A good starting point with general franchise agreement provisions is the definitions section.[264] Using this contractual tool to build in flexibility and discretion for the franchisor will go far in paving the way for the inevitable tech modifications and updates. This would include definitions of key terms such as: "System," "Services," "Products," "Trademarks," "Trade Secrets,"

---

[261] *See, e.g.*, Bores v. Domino's Pizza, LLC, 530 F.3d 671 (8th Cir. 2008) (franchisor could require franchisees to purchase and use only the franchisor's custom-designed integrated computer system); *see also*, JDS Grp. Ltd. v. Metal Supermarkets Franchising Am., Inc., No. 17-cv-6293, 2017 WL 2643667 (W.D.N.Y. June 20, 2017); Trail Burger King, Inc. v. Burger King of Miami, Inc., 187 So.2d 55 (D. Fla. 1966); Principe v. McDonald's Corp., 631 F.2d 303 (4th Cir. 1980), *cert. denied*, 451 U.S. 970 (1981).

[262] Robert W. Emerson, Franchise Contract Interpretation: A Two-Standard Approach, 641 MICH. STATE L. REV. 641 (2015).

[263] *In re* Sizzler Restaurants, Int'l, Inc., 225 B.R. 466, 470 (Bankr. C.D. Cal. 1998); *see also*, Robert W. Emerson, *The Faithless Franchisor: Rethinking Good Faith in Franchising*, 24 U. PENN J. BUS. L. 411, 424 (2022).

[264] Dull, et al., *supra* note 254, at 6.

"Copyrights," "Information Systems," "Confidential Information," and "Software." This is, by no means, an exhaustive list, as key terms that need to be defined with built-in flexibility will vary depending on the type of business. The salient take-away for every franchise system is to examine its system and concept closely to determine the terms that are specific to its business model that should be defined broadly to maintain the necessary flexibility and franchisor discretion.

b. System Modifications

In addition to a robust definitions section that contains as much flexibility as possible, franchise agreements need to include certain general provisions that also allow for modifications, upgrades, and system changes. For example, the following clause would permit a great deal of leeway for system modifications:

> In order to maintain the high quality and standards, methods, techniques, and specifications associated with the Franchised Business, the Trademarks, and the System, and to promote and protect the goodwill associated with the Franchise System, as well as to remain up to date with all technological advancements and innovations, Franchisor reserves the right, in its sole discretion, to change and modify the System. This includes, but is not limited to, modifications to the Manuals, System Standards, Information Systems, required equipment, and [POS/SMS] Systems. Franchisee agrees to accept and adopt such changes, modifications, or upgrades strictly in accordance with instructions and specifications from the Franchisor or as outlined in the Manuals and to bear all of the costs associated with such changes, modifications, or upgrades, including, but not limited to, the purchase of any new technology-related equipment.[265]

Also related to this systems modification provision, franchisors should avoid including a cap on the amount that a franchisee may be required to spend on such system modifications or upgrades.[266] The costs involved with technological innovations and modifications are hard to predict. Limiting language in the franchise agreements could hamper the need to stay ahead of the market and at the forefront of innovation.

c. Requirement to Follow Operations Manual

Another critical general provision in the franchise agreement is the requirement to follow the operations manual(s) as it is regularly updated and/or modified. The franchise agreement should include: (a) a broad definition of the operations manual, which can include any other manuals or guides provided by the franchisor in any form, including emails, bulletins, memos, etc.; (b) a specific reservation of rights to modify the manual; (c) a contractual obligation of franchisee to follow the manual at all times and as updated; and (d) a specifically enumerated

---

[265] Kathryn Kotel & Will K. Woods, *Operation of the Business*, in THE ANNOTATED FRANCHISE AGREEMENT 83 (Nina Greene, Dawn Newton & Kerry Olson, eds. 2018); *see also*, Dull, et al. *supra* note 254, at 6-7.

[266] David A. Beyer, Himashu M. Patel & John Dent, *Changes in System Standards - What is the Extent of Franchisor's Latitude?*, ABA 35TH ANNUAL FORUM ON FRANCHISING W-14, at 3-4 (2012).

obligation for franchisee to monitor closely any changes or revisions made to the manual and to immediately comply with all changes. [267]

d. Territorial Rights and the Metaverse

Franchisors should also examine their current alternative channels of distribution and non-traditional locations clauses with a specific eye to the ever-changing and expanding tech channels. One such channel that we have discussed is the metaverse. Franchisors considering the use of a metaverse option in their system need to assess these clauses to assure that offering a metaverse option is possible within the framework of their current territorial grants. While a deep dive into the use of the metaverse in franchising is beyond the scope of this paper, franchisors wanting to incorporate the metaverse into their system should consider drafting their franchise agreement to, at least, reserve this option in the future by: (a) defining "non-traditional locations" to also include those that operate in the metaverse or any virtual environment; (b) reserving the right to offer a similar business to the one they franchise in a virtual setting or in several different multiverses;[268] and (c) perhaps even considering including the multiverse as an alternative channel of distribution.[269]

2. Specific Provisions

Once the foundation for systemic technological changes, updates, and modifications is laid through the general provisions, the franchise agreement must now address more specific issues that go directly to the implementation of new and challenging technologies. Such specific provisions are necessary due to the general principle of contract interpretation that a specific provision dealing with a particular subject will control over a different provision dealing only generally with the same subject.[270]

a. Technology Fund/Fee

The collection of a technology fee that goes into the franchisor's technology fund has now become a must for any franchise system. A technology fund fee operates in the same way as an advertising fund fee. A franchisee pays a set amount, usually a percentage of gross revenues, into a fund that the franchisor uses for the benefit of the system by investing in new technological

---

[267] *Id*. at 5-6.

[268] According to Techtarget.com the definition of these terms is as follows:

Metaverse implies a level of deep interoperability across worlds and platforms in which assets and characters flow from one to another.

Multiverse contains multiple independent worlds that share little, if any, data.

https://www.techtarget.com/searchcio/tip/Metaverse-vs-multiverse-vs-omniverse-Key-differences (last visited on June 13, 2023).

[269] Vincent Frantz & Xheneta Ademi, *Franchising and the Metaverse,* IFA 55TH ANNUAL LEGAL SYMPOSIUM at 19-20 (2023).

[270] Burger King Corp. v. Cabrera, No. 10-20480-CIV, 2010 WL 5834869 (S.D. Fla. Dec. 29, 2010), *report and recommendation adopted*, No. 10-20480-CIV, 2011 WL 677374 (S.D. Fla. Feb. 16, 2011).

innovations to create a competitive advantage. A sample technology fund fee could read as follows:

> Franchisee must contribute ___% of its weekly Gross Revenue to the Technology Fund (the "Technology Fee"). The Technology Fee contributes to the costs of research, development, implementation, and support of new technology, as well as the modifications and updates of existing technology, including, but not limited to, platforms such as hosting, integration development, server infrastructure, application, and software development and support.

b. Information Technology Requirements

A specific clause requiring franchisees to stay current with information technology is also highly recommended:

> At Franchisor's discretion, the Franchisee shall, at its sole expense, acquire, license, use, and maintain any computer system, software, or other information technology systems, services, and equipment meeting the Franchisor's standards and specifications (collectively, the "Information Technology"), including all updates and modifications to such Information Technology.

c. Franchisee Tech Advisory Council

A franchisee tech advisory council is an excellent method for the franchisor to signal its commitment to innovation and technological development to the system, as well as inclusion and transparency regarding such innovations and system modifications. Innovation is essential for growth and being innovative should be a shared responsibility across the franchise system, not reserved just for the franchisor.[271]

Inclusion of a provision in the franchise agreement regarding the formation of such a council is both practical and strategic in that it manages expectations and contributes to a culture of innovation and agility, while also setting up the mechanism for creation of the council. A sample provision could read as follows:

> In order to provide a forum to exchange ideas and information between the franchisor and franchisee regarding the latest technological developments and ideas that would be most beneficial to the System, franchisor reserves the right to establish a Technology Advisory Council (the "Tech Advisory Council") pursuant to the terms and conditions set forth, and regularly updated, in the operations manual.

A tech advisory council can also be a great resource for innovative ideas and direction, as the franchisees are the ones most deeply immersed in the operations of the franchise businesses and often have great insights, suggestions, and feedback. Additionally, working with a franchisee council throughout the development and actual implementation of any new tech will enable the franchisor to better understand, and resolve more rapidly, any contentious issues or pushback from the system.

---

[271] Ackerman, *supra* note 260.

d. Pilot Programs

Involving franchisees in the innovation and change process can also be a valuable testing and implementation tool.[272] The inclusion of a provision regarding the use of pilot programs to test and prove out new tech prior to rollout allows the franchisor to set certain parameters and requirements for such programs. Specifically, the franchisor can set out some basic threshold parameters of franchisee participation, including: (a) a requirement to participate in additional training; (b) to, potentially, purchase new software or equipment; and (c) the expenses involved.

Franchisors should avoid including too much detail in a pilot program provision and instead refer to the operations manual for the more detailed aspects that can, of course, vary greatly depending on the tech involved. For example, the use of a pilot program in the context of developing a digital delivery app will likely present different issues and needs than the pilot program for a new CRM/POS system or use of the metaverse.[273]

e. Trade Secrets/Ownership of all Innovations

With the rapid speed of innovation and change in the technology landscape, comes a heightened need to ensure that the innovations and resulting developments, whether in the form of a new product, service, or idea, are protected. Trade secrets can be one of the franchisor's most valuable assets and while most states and the District of Columbia have adopted trade secret laws offering some protections, franchisors are best served by specifically defining what information may constitute a "trade secret" within the franchise agreement so as to leave no doubts.[274] The inquiry into whether a particular piece of information or know-how amounts to a trade secret is fact-specific.[275] Therefore, franchisors should ensure that the agreement clearly defines the information as a trade secret.

Similarly, it is essential that the franchise agreement is clear as to the ownership of all innovations and developments that franchisees may originate or to which they may contribute as part of an advisory council or otherwise. Such an ownership clause could read as follows:

> Franchisee acknowledges and agrees that all ideas, innovations, developments, or inventions, including, but not limited to, all improvements, modifications, or enhancements to any Technology, in connection with the Franchised Business (collectively, the "Innovations") is the property of the Franchisor and considered a part of the proprietary Confidential Information and/or Trade Secrets of the Franchisor. Franchisee, hereby, irrevocably assigns to the Franchisor any right, title, and interest in and to such Innovations.

---

[272] Morrison, et al., *supra* note 258, at 10.

[273] Anne P. Caiola, Brittany Johnson & Andra Terrell, *Age of Disruption: Current Issues for Restaurant Franchises*, ABA 43RD ANNUAL FORUM ON FRANCHISING W-20, at 6 (2020); Dull, et al., *supra* note 254, at 15 – 17.

[274] Himanshu Patel & Brian B. Schnell, *Accounting, Records, Reports, Audits, and Inspections; Insurance; Restrictive Covenants,* in THE ANNOTATED FRANCHISE AGREEMENT 168-169 (Nina Greene, Dawn Newton & Kerry Olson, eds. 2018).

[275] *See, e.g.*, Bimbo Bakeries USA, Inc. v. Botticella, 613 F.3d 102, 113 (3d. Cir. 2010) (holding that an employee absconding with trade secrets immediately prior to his resignation and new employment with a competitor violated Pennsylvania's trade secrets law).

C. The Operations Manual

As a regularly updated resource, the operations manual is a great place to include aspects of the system that are likely to change rapidly and often, as is the case with technology. Since just about all franchise agreements will incorporate the operations manual and thereby bind the franchisee to follow it, it serves as a very useful tool for franchisors to stay current and even ahead of the curve with technological innovations. Care should be taken, however, to ensure that the types of changes that are made through the operations manual are limited to changes that were, in fact, foreseeable at the time the franchise agreement was signed.[276] With the managing of expectations and company culture discussed above, the incorporation of more general provisions that give the franchisor lots of flexibility with technological modifications, and the inclusion of more specific provisions that directly address technology, this reasonably foreseeable standard should not be difficult to meet.

D. The Franchise Disclosure Document

In addition to being the first opportunity to set expectations, the FDD must also correctly disclose anticipated franchisee obligations in connection with tech innovation and development. While making the requisite disclosures, franchisors can also set a tone for a franchise culture that values remaining on the forefront of technological developments. For example, by including the cost of tech upgrades and improvements as a separate line item under Item 6 (Other Fees) or the inclusion of a technology fund contribution under Item 7 (Estimated Initial Investment), the franchisor is sending a very clear message of its commitment to technological innovation and adoption.

VI. THE IMPLEMENTATION PROCESS

Once the franchisor has established the contractual basis and authority for the proposed changes, it should create and send a detailed roll out plan to the entire system. Such transparency and direct communication will engender trust and greater cooperation by franchisees.

A. System-wide Communication

Franchisors should be clear in their communications about the expectations for the program, the requirements of franchisees, the specific timeline (with built-in leeway, of course) for the roll-out, and instructions for participating in the program. Presumably, if the right franchise culture and expectations have been set in advance, the entire franchise system should be well-primed and prepared for the roll-out.

A crucial part of the communication and ultimate success or failure of the technology change will depend on the reason for the changes that are being implemented. The franchisor must make a persuasive, bottom-line case for the changes—showing that the changes will benefit all. In making this business case, the franchisor should look to present the diligent and thorough research that has been conducted on customers/clients, demographics, competitors, and the

[276] Corby Anderson & Rebekah Prince, *Operating Manual, Advertising, Trademarks, and other Intellectual Property*, in THE ANNOTATED FRANCHISE AGREEMENT 127-129 (Nina Greene, Dawn Newton & Kerry Olson, eds. 2018); Beyer, *supra* note 266, at 4-7.

industry as a whole.[277] Such a bottom-line case for the changes will serve to solidify support for the changes, strengthen the franchisor-franchisee relationship, and minimize the risk of potential disputes.[278]

1. Use of Tech Advisory Council

The involvement and assistance of the franchisee advisory council will be vital at this stage.[279] If a tech advisory council has been set up and involved in the research and development of the tech improvements and upgrades thus far, then their continued involvement in the implementation will be a natural extension and will serve to continue the cooperative relationship already extant. The tech advisory council will also continue to provide the important feedback from the rest of the franchise system as the roll-out and pilot programs are progressing.

2. The Pilot Program

Pilot programs are short-term tests that can help a system learn how a larger-scale implementation might work. They provide a platform for the system to test the logistics and spot any potential deficiencies before a full roll-out.[280] If the franchisor has corporate-owned units, it might consider conducting a smaller-scale pilot program in those units first to better understand how the modifications will affect daily operations, make refinements, and document the results. Piloting, or perhaps, pre-piloting, at the corporate level also demonstrates a franchisor's good faith and confidence in implementing the change since they are leading the way and taking the risks of trial and error first.[281]

B. Logistical Considerations

There is a lot to consider in the legal landscape surrounding the implementation of new technology in a franchise system. The logistical challenges are numerous and must be addressed carefully and in a meticulous process.

1. Contracting With Third-Party Vendors

One of the earliest decisions in the roll-out of new technology is the contractual relationship with the vendors developing and implementing the new technology for the franchise system. Should the franchisor negotiate an umbrella agreement for the entire system in the franchisors name or should franchisees contract directly with the vendors? There are pluses and minuses to both approaches. Given the greater bargaining power of the franchisor entity when contracting for an entire system, it is likely to negotiate more favorable terms. However, this also means that the franchisor retains a fair amount of contractual liability that it will have to be cognizant to mitigate. Nonetheless, with this approach, the franchisor can ensure that the interest of the system

[277] Dull, et al., *supra* note 254, at 16.

[278] Morrison, et al., *supra* note 258, at 10.

[279] Beyer et al., *supra* note 266, at 10.

[280] Ron Ashkenas & Nadim Matta, *How to Scale a Successful Pilot Project,* HARV. BUS. REV. (Jan. 28, 2021), https://hbr.org/2021/01/how-to-scale-a-successful-pilot-project; Caiola, et al., *supra* note 273, at 6.

[281] Morrison et al., *supra* note 258, at 10.

as a whole, rather than the individual needs of each franchisee, are met, as well as brand integrity and system uniformity.

Additionally, technology vendor agreements can be very complex given the necessity of considering so many factors. The franchisor is certainly best equipped to address such complexities, including: (a) data security and privacy issues; (b) ownership of data generated by the applicable technology; (c) safeguarding the confidential information and intellectual property of all the parties involved; (d) important representations and warranties; (e) exclusivity provisions, as applicable; and (f) crucial indemnity and insurance issues.[282]

Thoroughly vetting any technology vendor is, of course, a must. Picking the right technology vendor is a critical decision for any franchise system. While most vendor checklists will include the big picture elements, it's essential to really delve deeply into the details to ensure that the potential vendor is the best choice for the specific needs of the system.

Some essential questions would include the following: (a) information regarding the vendor's cybersecurity policies and procedures, including their practices related to encryption and protection of data; (b) what measures are taken in the development of the applicable tech to ensure compliance with applicable privacy laws—both US and international; (c) the measures that will be included to insure protection of the franchise system's data; (d) information regarding the vendors insurance coverage—especially cyber insurance; (e) what assurances or guarantees is the vendor able to provide in the event of a data breach; and (f) will they agree to an indemnification provision.[283]

2. Proprietary Technology Development

Alternatively, a franchisor can develop its own proprietary technology. Such technology would be uniquely tailored to the system and able to specifically address the needs and concerns of franchisees. In-house development would also give the franchisor greater control over the customer experience and interface with the brand and, presumably, the ability to update and revise as needed to stay current with new developments. Ownership and control of the data could more easily rest with the franchisor with fewer logistical concerns.[284]

The cost of developing proprietary technology, however, can be prohibitive to most systems. Additionally, with the speed of advancements and innovations in this sector, the risk of such technology becoming outdated before it can offer a return on investment could be quite high. Systems would also likely need to pass this cost on to its franchisees, making the effort of system-wide implementation that much more difficult.

3. Allocation of Risk and Liability

With the roll-out of new technology comes the question of how the risk and liability for tech failure or data breaches will be allocated. It is essential to plan for such a possibility as early in

---

[282] Batenhorst et al., *supra* note 20, at 22-26.

[283] Morrison et al., *supra* note 258, at 37; Sabrina Pagnotta, *How to Create a Vendor Risk Management Checklist*, BITSIGHT BLOG (June 20, 2023), https://www.bitsight.com/blog/vendor-risk-management-checklist.

[284] Ashley Weis, *What Franchisors Should Know About Data Privacy Compliance in 2023,* FRANCHISEWIRE (Mar. 14, 2023), https://www.franchisewire.com/data-privacy-compliance-for-franchise-systems-in-2023.

the process as possible.[285] Insurance coverage by each player at every stage of the implementation process is critical. The franchisor needs to assure that the vendor chosen to develop and implement the applicable tech has ample cyber insurance coverage that provides protection for the specific work being performed by the vendor should a data breach occur during the development, testing, or implementation. Additionally, all franchisees should also be required to carry cyber insurance along with the franchisor.[286]

In addition, indemnification provisions are also essential. Such provisions should be included in the vendor contract, as well as, in all franchise agreements.

4. ADA Compliance in Emerging Technologies

One of the logistical/legal issues facing franchise systems in the implementation of new technology are challenges from consumers alleging that new tech is not compliant with the ADA, as it does not provide equal access to individuals who are hearing, vision, or otherwise impaired. The number of web accessibility lawsuits that were brought to federal court, citing Title III of the ADA, reached a new record in 2022, with plaintiffs filing 3,255 lawsuits—a twelve percent increase from 2021.[287] While a full discussion of such lawsuits is beyond the scope of this paper, as the cases and legal guidance in this area continue to develop, franchisors should factor in ADA considerations in assessing proposed new technology.[288]

VII. FUTURE CONSIDERATIONS

Given the rapidly evolving pace of technology, it is difficult to predict all that the future will hold, but there are a few issues on the horizon that most practitioners should consider.

A. Privacy Regulations Landscape Will Continue to Evolve

As noted above, ten states had already enacted their own forms of consumer data privacy protection laws by July 2023.[289] The future trend is that many more states will join those ten states in comprehensively legislating the protection of consumer data privacy. As of the date of writing, there were six states that have active bills pending for similar privacy legislation.[290]

While franchisors are left scratching their heads over how to comply with the growing patchwork of privacy laws in place, the path forward does not promise any clarity. Advisors will want to continue to look at the status of both state (and potentially federal) privacy laws at disclosure renewal season, to update data privacy addendum language requirements, and take

---

[285] JoAnn Carlton, Heather Enlow-Novitsky & Matthew Fore, *Data Security and Addressing the Risks in the Franchise System,* IFA 51ST ANNUAL LEGAL SYMPOSIUM (2018).

[286] *Id.* at 34.

[287] Level Access, https://www.levelaccess.com/blog/web-accessibility-lawsuits-2022-recap-and-what-to-expect-in2023/#:~:text=The%20number%20of%20web%20accessibility,12%20percent%20increase%20from%202021 (last visited, July 14, 2023).

[288] Batenhorst, et al., *supra* note 20, at 22-26.

[289] *See generally*, Desai, *supra* note 49.

[290] *Id.*

stock of the status of current data being shared and any updated data mapping performed by internal stakeholders. Further, disclosure renewal season isn't the only time when legal updates will need to be employed, for brands can adopt new and challenging technology and choose to enact it at any time as they take on new technology vendors providing expanded services. Variations and addenda will continue to be subjects of intense scrutiny so long as the patchwork of laws continue to grow and are not preempted by federal legislation. Whether these new addenda can amount to a material change to be required for inclusion in an amended disclosure will need to be vetted in each instance. Moreover, constant data-mapping and data governance practices will need to be employed with the implementation of each new vendor and technology. With no real relief of legislative uniformity, and only more new state legislation in sight, efforts and work in this area will only magnify as time goes on.

B. Managing Through AI/BIPA Consent

As explained, recent case law has created "annihilative liability" when a BIPA claim accrues, because these claims accrue with each "scan or transmission of biometric identifie[r]s or biometric information…"[291] With risks of each claim for a non-consensual violation totaling $1,000 or $5,000, and cumulative damages for each data capture easily potentially adding up to the billions if not consented to properly, this is a high-risk area that will have everyone reviewing their privacy policies and consent practices to be sure they meet every aspect of the BIPA's legal requirements.

AI and its implementation in franchised systems should be handled with care, as its use could easily result in data capture, such as virtual try-on technology, identify verification based on facial recognition and face tagging in social media, that implicate potential BIPA violations.[292] Vetting and working with reliable vendors who understand privacy risks and disclosure/consent concerns in this area will need to become table-stakes for any franchised brand that determines to test or implement any AI tech relying on biometric data capture. Further stressing the importance of auditing how privacy policies and data is being handled over time, including obtaining and maintaining records of written consent, will be crucial, regular touchpoints for all brand advisors.

C. Cutting-Edge Technologies and Perpetually Addressing the Existing and Changing Landscape

The risks associated with implementing challenging technology should make us all want to reach for our vendor checklists and to deeply consider the experience and wherewithal of the vendors shopping their wares to franchised brands. The cutting-edge nature of technologies franchised systems, coupled with the ever-changing legal landscape, will mean that those checklists, will need to be refreshed and re-considered regularly.

Comparing a checklist on the top "10" questions that every company should ask a vendor from 2018, to another checklist compiled in 2023 is enlightening.[293] The concept of vetting a

---

[291] Zachary Kalinowski, Garner Kropp & Tyler Newby, *BIPA's Per-Scan Damages may Create "Annihilative Liability"*, JDSUPRA (Mar. 7, 2023), https://www.jdsupra.com/legalnews/bipa-s-per-scan-damages-may-create-3773558/.

[292] *Id.*

[293] *Cf.* Lenovo, *10 Questions Every Company Should Ask When Vetting an IT Vendor*, INC. (Dec. 12, 2018) (sponsored content), https://www.inc.com/lenovo/ten-questions-every-company-should-ask-when-vetting-an-it-vendor.html, *with* Forbes Technology Council, 16 Key Considerations When Vetting a New Tech Vendor or Partner, FORBES (Apr. 4,

vendor's security practices is more prevalent in the more recent checklist, indicating a shift over time to brands regularly inquiring about a vendor's skills and experience in this area. While it is not likely that cybersecurity issues will decrease or fall off checklists, the ways to approach a vendor's experience and questions that are uniquely important to a brand will evolve over time. Future advisors should be vigilant in recommending improvements in how teams vet and select their vendors.

D. AI/Chatbots and Concerns and Advancements in the Practice of Law

Thirty-nine states have adopted a duty of competency so that lawyers must know the risks and benefits of technology.[294] Even so, in a 2021 ABA technology survey, 33% of legal professionals surveyed did not know enough about AI to answer how their firm used such technology.[295] With the advent of some brands considering targeted AI marketing for franchise recruiting or utilizing AI-enhanced chatbots to interact with potential franchise candidates, legal advisors have a duty to keep up and to understand the specific risks of the technology sought to be used, and, for example, how those risks may be compounded by implementing those technologies into longstanding recruiting processes and in light of longstanding laws governing what can and should be said to candidates considering accepting a franchise offer. The brand risks are great, but so are the ethics risks for the advisors. In the future, all practitioners will need to become expert issue-spotters of increased risks presented by AI's incorporation into brand initiatives. They will also need to follow forthcoming advancements in regulatory oversight over AI, including rapidly evolving new guidelines, reports, and press statements, such as those issued by the FTC in the last three years addressing how businesses can or should interact with consumers with respect to AI.[296]

Finally, it is worth noting that the time is already here when AI technology can be leveraged to make the practice of law, and the actual work of advising franchise brands, easier. A recent *Wall Street Journal* article explored how big law and some in-house departments are already exploiting AI tools to handle the drudgery-type of legal work typically given to entry-level lawyers.[297] Some of the tools referenced include software that can perform legal research and writing such as associated with memos and reviewing contracts, where the AI software can "sift through thousands of pages of case law in just minutes."[298] And while some brands might be skittish about uploading their confidential legal information into cloud-based products or to transfer

---

2023), https://www.forbes.com/sites/forbestechcouncil/2023/04/04/16-key-considerations-when-vetting-a-new-tech-vendor-or-partner/?sh=5e96f05f61a9

[294] Matt Reynolds, *Even with AI Certification Initiatives, Lawyers Need More Schooling on Tech*, A.B.A. J., Mar. 2, 2022, https://www.abajournal.com/web/article/even-with-ai-certification-initiatives-lawyers-need-more-schooling-on-tech.

[295] Id.

[296] Anthony E. DiResta & Zachary E. Sherman, *The FTC Is Regulating AI: A Comprehensive Analysis*, HOLLAND & KNIGHT (July 25, 2023), https://www.hklaw.com/en/insights/publications/2023/07/the-ftc-is-regulating-ai-a-comprehensive-analysis.

[297] Erin Mulvaney & Lauren Weber, *Law Firms Assign AI To Research, Drudgery*, WALL ST. J., May 12, 2023, https://www.wsj.com/articles/end-of-the-billable-hour-law-firms-get-on-board-with-artificial-intelligence-17ebd3f8.

[298] Id.

too-much responsibility to software that isn't 100% infallible, legal AI technology is tirelessly learning away and improving itself every moment of every day.[299]

While the technology is amazing, and no doubt can be leveraged to advise franchised brands more readily and cheaply, when employing any new software it will be important to understand its limitations to apply nuanced facts to the information it provides and to make sure it is being given the latest information available to be able to compute its data (such as governing case law, statutory text, or administrative codes), and to just generally make sure it isn't making mistakes.[300] The future holds interesting automation in how franchise lawyers can advise their clients, which should be approached with caution and knowledge about its limitations.

VIII. CONCLUSION

The speed of innovation is increasing rapidly, and the introduction of new technology is something that franchise systems avoid at their peril. The authors hope this paper illustrates the many complexities that need to be considered in the adoption of new technology and outlines a few potential approaches to evaluating and incorporating new technology.

[299] Daniel Schwarcz & Jonathan H. Choi, *AI Tools for Lawyers: A Practical Guide*, 108 MINN. L. REVIEW HEADNOTES (forthcoming 2023) (draft of Mar. 30, 2023 at 2-3), https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID4404017_code499486.pdf?abstractid=4404017&mirid=1. GPT-4 scored in the ninetieth percentile on the Uniform Bar Examination, including both multiple choice questions and open-ended Multistate essay questions. An earlier version of the GPT model passed four different law school final exams at a top law school with no human intervention.

[300] See id.

BIOGRAPHIES

Kerry Renker Green currently serves as Associate General Counsel, Global Franchise for The Wendy's Company. She has represented franchisors and business clients around the globe in various aspects of developing their businesses. She has drafted Franchise Disclosure Document;, overseen registration obligations; led multi-unit franchised, non-traditional, and license transactions; negotiated and closed service agreements within the IT, advertising, supply chain and logistics, and design sectors, as well as assisted with issue-spotting and navigating the many legal questions that arise in the business of franchising. Kerry also has experience litigating disputes through arbitration, trial, and appellate work in state and federal courts. Kerry currently assists in the quick service restaurant sector, focusing on global franchise advice, including domestic and international growth and issues arising at all stages of the franchise life cycle. Kerry is admitted to practice law in Ohio, before the U.S. District Court for the Northern and Southern Districts of Ohio, and the U.S. Court of Appeals for the Sixth Circuit.

Manal Zakhary Hall is of counsel at Dentons in Salt Lake City. Manal's practice focuses on all aspects of Franchise/distribution law. She regularly advises clients on a wide variety of issues, including domestic market entry, expansion and exit strategies, franchise disclosure obligations and franchise compliance programs and policies; the franchise disclosure document, individual unit franchise agreements, as well as area development and master franchise agreements; franchisee relationship issues, terminations, transfers, and dispute resolution. She assists clients with all phases of the franchise registration process in the US registration states and has assisted clients in assessing the feasibility of entering various international markets. She enjoys helping franchisors create strategies, systems, and a corporate infrastructure designed to help them scale rapidly and efficiently. Manal will also be teaching Franchise Law this fall as an Adjunct Professor at Brigham Young University J. Reuben Clark Law School.

Keri McWilliams is a Partner at Nixon Peabody LLP and co-leads their Franchise & Distribution team. She represents franchisors across numerous industries, including restaurants, retail, education, cannabis, and health and wellness, in all aspects of their corporate relationships. She works with clients to prepare and update franchise agreements and franchise disclosure documents, and provides strategic counselling on expansion and growth issues, franchise disputes, and international sales. Keri is also a leader in the franchise industry, serving as an associate editor of *The Franchise Lawyer* from 2015–2021 and as the current vice-chair of the International Franchise Association Legal Legislative Committee. She is a regular writer and presenter on franchise law topics, including as a recurring speaker and presenter for the International Franchise Association Legal Symposium, the American Bar Association Forum on Franchising, and the Georgetown University Franchise Management program. Keri has been selected by her peers for inclusion in *The Best Lawyers in America* since 2019 and is nationally ranked by *Chambers USA: America's Leading Lawyers for Business* for her expertise in the field of franchise law.