This article originally ran in the *New York Law Journal*

Privacy and Franchising: Are You Keeping Up To Protect Your Consumers and Your Franchise?

By Marc Lieberstein, Amanda Witt and Tony Glosson | September 28, 2021

The privacy laws in the United States are numerous, differ from state to state, include some federal laws, and have immediate and broad implications for franchisors and franchisees. Moreover, there are non-U.S. privacy laws that impact franchising in the United States.

In the United States, three states—California, Colorado and Virginia—have enacted what could be described as comprehensive privacy laws to protect consumers and regulate how businesses conduct themselves when collecting personal/private information from consumers. California, first with the California Consumer Privacy Act (CCPA) and then the California Privacy Rights Act (CPRA), has enacted the most comprehensive privacy law, and other states are following its model which essentially requires compliance by anyone meeting certain revenue, data volume, or organizational structure criteria, which likely includes many, if not most franchisors and/or franchisees, when they receive another party's personal or identifying information.

Unfortunately, even if you comply with California's privacy laws, you will likely not be in full compliance with any other state's privacy laws or the well-known European privacy law known as the General Data Protection Regulation (GDPR) due to the various nuances and differences between the CCPA/CPRA and those other laws.

Other states—like Illinois, Texas, Washington, Arkansas and most recently New York City, have enacted privacy laws to protect consumers from the collection of biometric and other personal identifying information that businesses collect.

Notably, New York City's legislation on biometric data, which became effective July 2021, requires businesses, i.e., franchise owners and operators, across many consumer service industries, e.g., retail, entertainment and social media, food and beverage, to make it clear to consumers that they are using and collecting biometric data.

With limited exceptions, the New York City law makes it illegal to sell or profit in any way from the collected biometric data. And like the Illinois law (i.e., the Biometric Information Privacy Act (BIPA)), the New York City law allows for individuals to sue in private actions for violations.

What does all of this mean for franchising? Well, here's a little excerpt from a franchise agreement: "You represent, warrant and covenant that you are familiar with the requirements of, …, in compliance with all consumer protection laws, data protection, privacy and cybersecurity

laws…that are applicable to your Franchise, us or you, including but not limited to the…(General Data Protection Regulation) (GDPR),…the California Consumer Privacy Act of 2018 (as amended and pursuant to regulations promulgated thereunder, collectively, CCPA)…the Telephone Consumer Protection Act of 1991 ("TCPA"), the Controlling the Assault of Non-Solicited Pornography and Marketing Act (the "CAN-SPAM Act"), the Telemarketing Sales Rule ("TSR") and the Junk Fax Prevention Act,…the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §1681 et seq., as amended by the Fair and Accurate Credit Transactions Act ("FACTA"),…the Identity Theft Red Flags and Address Discrepancies Rule,…(Cal. Civ. Code §1798.81.5, 201 Mass. Code Reg. 17.00, and Tex. TC Bus. & C. 521.052), and…Personal Data laws (such as N.Y. Gen. Bus. Law §399H) (collectively, the "Data Protection Laws")."

There really is no simple way to guarantee compliance with so many laws, but here's some general guidance for franchisors and franchisees: (1) consult with legal and privacy professionals before you start operating your business; (2) be aware that compliance with most, if not all, of these laws requires franchise businesses to provide notice to users of the services being offered, and ensuring that each user actively and actually consents to the collection and/or use of the personal identifying information; (3) confirming that the business can collect, use or sell such personal data (assuming such collection and/or use or sale is permitted by law); and (4) look to obtain insurance to cover damages resulting from any data lost due to unauthorized use, disclosure, breach or theft.

If you are thinking that your franchise business can somehow avoid having to comply, chances are you are wrong. For example, while the California CCPA appears to set a threshold of $25 million for business to comply with the privacy law, it is not clear that businesses with smaller annual revenue do not have to comply because other CCPA provisions may still cover your business. For example, a business that collects personal information of 50,000 or more California residents or households is still subject to the CCPA, regardless of whether it hits the $25 million revenue threshold.

Similarly, the privacy laws also seem to disregard the corporate realities that usually separate franchisor and franchisee, and either link them together by definition with words like "affiliate" or "control," and in that manner both franchisor and franchisee likely have to comply with the state's privacy laws regardless of whether they are physically present or doing business in that state.

Biometric privacy compliance requirements also extend outside of the franchisor-franchisee to relationships that either may have with their vendors and with whom they may share personal or private information. For example, loyalty programs, consumer-directed promotions or food

delivery services that may require a franchise party to exchange personal information are all likely subject to a state's privacy laws.

Recently, biometric privacy plaintiffs have increasingly focused on failures to comply with disclosure requirements under applicable laws, such as Illinois' BIPA requirements to post a data retention schedule and sharing disclosures. Further, plaintiffs may allege unjust enrichment if businesses profit off of biometric data in violation of applicable laws. The best way to head off these types of claims is by keeping current on your jurisdiction's requirements to avoid being caught off-guard.

Similarly, European GDPR compliance requirements continue to evolve, requiring ongoing attention from U.S.-based franchisors and franchisees in order to remain in compliance. Most recently, the European Commission released a revamped set of standard contractual clauses (SCCs) which provide a lawful basis to transfer GDPR-covered personal data to the United States or other "third countries" outside of the European Economic Area (EEA).

While many businesses had adopted the previous version of SCCs, those older SCCs have been rendered obsolete since the issuance of the updated SCCs and must be updated by Dec. 22, 2022. The prior version of the SCCs can no longer be used for new agreements after Sept. 27, 2021. The new SCCs are materially different than the prior ones and require certain analyses of laws relating to government access and the implementation of supplementary measures to protect transferred data.

Furthermore, franchisors and franchisees should be aware that the U.S.-EU Privacy Shield was invalidated by the Court of Justice of the European Union (CJEU) in the *Schrems II* decision on July 16, 2020 and may no longer be used as a transfer mechanism for personal data transferred to the United States from the EEA.

California's privacy laws, likewise, can create significant exposure for franchisors and franchisees. In addition to regulatory enforcement risks posed by California's active Attorney General's office, the CCPA provides for a private right of action for those California consumers whose data is affected by a security breach due to a company's inadequate data protection practices. With breach litigation expenses and awards rising, it is increasingly important for franchise businesses to approach data protection compliance as a top priority.

The bottom line on franchising and privacy laws is that franchisors and franchisees must keep up with the law as technology changes and with consumer expectations that the businesses with whom they deal with are not improperly using their private or personal data without their knowledge or consent. Going forward, franchise parties should consider the following steps to keep up with privacy and consumer protection laws:

- **Take stock of your actual business operation.** Evaluate your business (both online and brick and mortar) and figure out whether or not you already have data that is subject to applicable privacy laws, and/or whether you are collecting, storing, erasing or using private or personal information. If you take credit cards for payment, or ask consumers to enter their names, addresses, birthdays, you are collecting personal information that is likely subject to one or more of your state's privacy, biometric or consumer protection laws. Furthermore, credit card information is subject to compliance with the privacy Payment Card Industry Data Security Standard (PCI DSS). And keep in mind that the path to privacy mistakes usually begins with a well-meaning but mistaken statement that "we don't collect consumer information."
- **Develop a clear written procedure for responding to consumers and a breach.** Most state privacy laws, along with the GDPR, require that if a consumer learns that your business has collected their private or personal information, you must have procedures in place to respond to a consumers request to delete or at least de-identify that information. You should invest in software or other technology that enables you to locate and recognize the data, and take whatever steps are required by law to store, delete or de-identify the information.
- **Set up internal policies that enable compliance.** Franchisees and their employees must know what they can and cannot do. Since most state privacy laws require consumers to opt-in or opt out, employees need training on what they can and cannot do with the information and/or in relation to the consumer in each circumstance. Training is likely a critical component to compliance in this area, and while franchisors may not want to train franchisees or their employees directly for fear of joint employer liability, at a minimum, they should mandate that their franchisees and employees seek such training.
- **Maintain your technology and security systems.** Putting aside the obvious steps franchise businesses must take to purchase and install technology and security systems to protect consumer data, it is imperative that such systems be maintained and updated. We've all read about the proliferation of hacking and ransomware, so franchise business should be mindful of taking all reasonable steps to thwart off such attacks. Security and incident response plans, system back up protocols, and disaster recovery plans are all common and likely necessary things to have in place if you want to avoid liability or at least minimize risk and exposure to liability.
- **Update your franchise agreements and operations manual.** If you haven't done so already, your franchise agreement and operations manual should be updated to account

for compliance with the various state privacy, biometric and consumer protections laws. Franchisors need to decide whether they want to control or dictate their franchisee's compliance, as even if the franchisor attempts to shift the burden of compliance, franchisors may still be deemed in control of their franchisees and hence jointly or vicariously liable for any misuse, breach or theft of personal or private information. Indeed, if the franchise agreement mandates that upon termination all franchisee consumer and sales data is to be owned by or transferred to franchisor, there's a strong likelihood that the franchisor will be deemed to control its franchisee. To avoid this, franchisors can make suggestions and recommendations to franchisees, and provide options for their franchisees to assist them with compliance, but otherwise expressly state that they are not responsible for the franchisee's compliance, and mandate that the franchisee indemnify the franchisor for any damages associated with claims arising out of a misuse or theft of personal/private data. Purchasing cybersecurity insurance, and/or mandating that a franchisee purchase such insurance is another way for franchisors to reduce risk and minimize liability exposure.

Certainly, franchisors and franchisees can weigh the costs and risks associated with non-compliance with all the various privacy laws, but the question is: Are you willing to risk the loss in brand value, sales, and most importantly, consumer trust if you fail to comply?

Marc Lieberstein *and* ***Amanda Witt*** *are partners and* ***Tony Glosson*** *is an associate at Kilpatrick Townsend & Stockton.*