1. What is your state’s law on the use of CBD oil in products to be sold to the public, i.e. cosmetics, etc.?

In Ohio, products containing cannabidiol (CBD) may only be sold through the Ohio Medical Marijuana Control Program to individuals with certain medical conditions upon the recommendation of an Ohio-licensed physician certified by the State Medical Board. Ohio House Bill 523, which legalized medical marijuana in Ohio effective as of September 8, 2016, did not distinguish between cannabis compounds, such as CBD and the more commonly known cannabinoid, tetrahydrocannabinol (THC). The Ohio State Board of Pharmacy issued formal legal guidance on this issue in August, 2018 which confirmed that any products containing CBD must comply with Ohio’s Medical Marijuana Control Program. Consequently, CBD remains a Schedule One substance under the purview of the Ohio Medical Marijuana Control Program.

However, the legal status of CBD products in Ohio will likely change soon and is now under consideration by Governor Mike DeWine. On March 28, 2019, the Ohio Senate passed Senate Bill 57 which, if passed into law, would permit the production and sale of hemp-derived CBD in Ohio, provided that such CBD products may not contain more than 0.3% THC. Senate Bill 57 was subsequently passed by the Ohio House of Representatives on July 17, 2019 and has been sent to Governor DeWine for his signature. Once signed by Governor DeWine, the bill would take effect immediately.

2. Regarding privacy issues, has your state adopted its own version of GDPR or how is your state dealing with GDPR requirements? What other privacy laws has your state adopted recently in response to concerns about the lack of protections for consumers?

Ohio has not adopted its own version of the General Data Protection Regulation (GDPR) implemented by the European Union on May 25, 2018, but it did enact the Ohio Data Protection Act (ODPA), which became effective on November 2, 2018. Unlike the GDPR, which affirmatively regulates how companies collect and protect
citizens’ personal data and information, the ODPA established an incentive-based compliance approach to cybersecurity in Ohio. Compliance with the ODPA is completely voluntary. The ODPA creates a legal safe harbor for “covered entities” (i.e., any business or non-profit entity that accesses, maintains, communicates, or handles personal or restricted information) that comply with the ODPA. Under the ODPA, if a covered entity maintains a cybersecurity program that meets the requirements set forth in the ODPA, then the covered entity has an affirmative defense against a tort action resulting from a data breach where it is alleged that the covered entity failed to implement reasonable security controls.