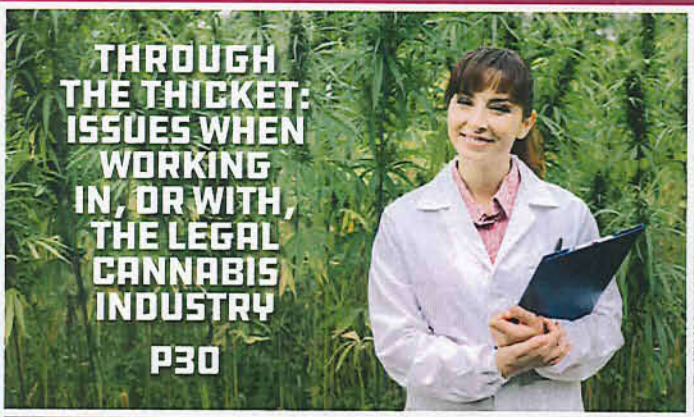
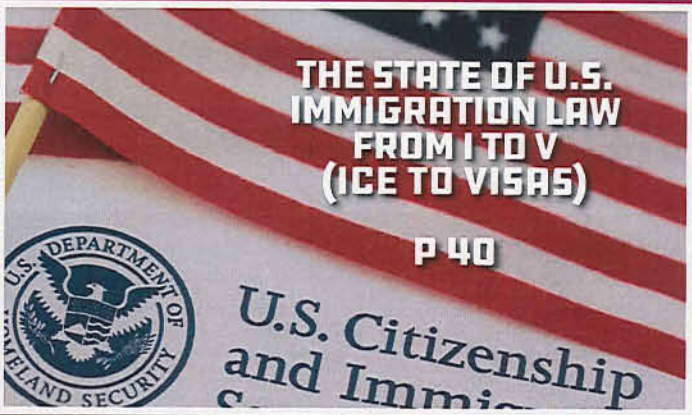
SPRING 2019

US LAW



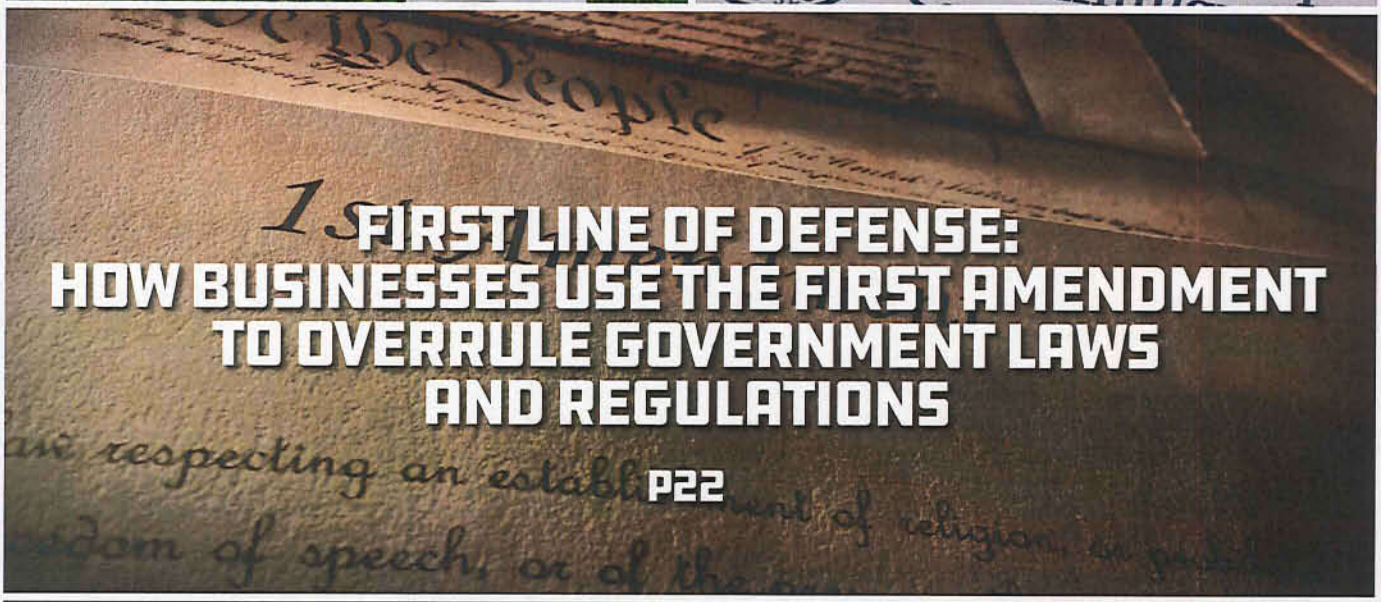
THROUGH THE THICKET: ISSUES WHEN WORKING IN, OR WITH, THE LEGAL CANNABIS INDUSTRY

P30



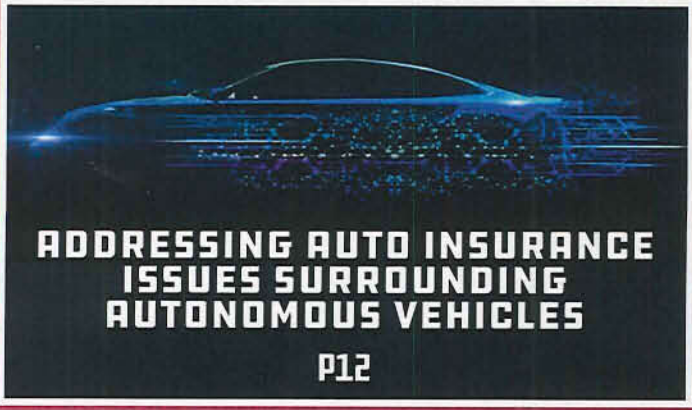
THE STATE OF U.S. IMMIGRATION LAW FROM I TO V (ICE TO VISAS)

P 40



FIRST LINE OF DEFENSE: HOW BUSINESSES USE THE FIRST AMENDMENT TO OVERRULE GOVERNMENT LAWS AND REGULATIONS

P22

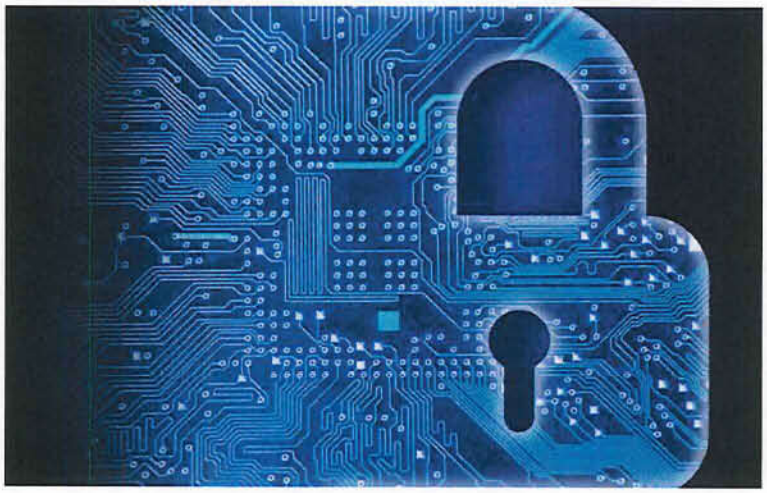


ADDRESSING AUTO INSURANCE ISSUES SURROUNDING AUTONOMOUS VEHICLES

P12

EXPAND AND CONTRACT: DEVELOPMENTS IN WORKER'S COMPENSATION EXCLUSIVE REMEDY

P20



Developing Data Privacy Law and the Standard for "REASONABLE SECURITY MEASURES"

Hilary Wells and Holly White Lewis Roca Rothgerber Christie LLP

Legislation regarding data privacy has exploded over the past few years. Gone are the days of data protection requirements only applying to the finance and health care sectors. Individuals and companies across all sectors face new and expanded requirements to protect and properly maintain personal identifying information. The FTC, exercising its enforcement powers under Section 5, is targeting businesses it believes are employing unreasonable security practices. To complicate matters even further, because Congress has failed to enact a uniform data protection statute, the individual states are taking up the charge to protect personal information, each in a slightly different manner. This article will analyze the newly enacted data protection laws in the United States and offer guidance regarding the developing standard of care, known as "reasonable security measures."

Nearly 10 states have recently enacted expanded data privacy legislation, which has already become effective or will become effective early next year. These states include Alabama (SB 381, effective June 1, 2018), Arizona (HB 2145, effective August 3, 2018), California (A.B. 375, effective January 1, 2020), Colorado (HB 1128, effective September 1, 2018), Louisiana (Act No. 382, effective August 1, 2018), Nebraska (LB 757, effective July 18, 2018), Ohio (SB 220, effective November 2, 2018), Oregon (SB 1551, effective June 2, 2018), and South Dakota (SB No. 62, effective July 1, 2018). Most of these laws broaden the definition of "personal information" and increase notification obligations. Some states now mandate deletion of personal information when it is no longer needed, and impose hefty civil penalties for non-compliance.

Many of these newly enacted statutes, including those enacted in Alabama, California, Colorado, Louisiana, Nebraska and Oregon require the individual, business or entity maintaining personal information to use "reasonable security measures." Other states that use "reasonable security measures" for their data protection standard include Arkansas, Illinois, Maryland, Nevada and New Mexico. Ohio has taken a unique approach by focusing on compliance through voluntary action and offers a breach litigation safe harbor to covered entities that meet the law's cybersecurity standards. Conversely, California and Colorado have some of the broadest and

strictest statutes in the country. Colorado requires covered entities to affirmatively delete and protect personal information as well as investigate breaches and potential breaches and adhere to strict notification standards. California's new law provides that consumers have the right to request the deletion of personal information, opt out of the sale of personal information and access the personal information in a "readily usable format" that enables it to be easily transferred to third parties. Businesses are concerned that this law could threaten companies that generate revenue from targeted advertising over internet platforms, such as social media companies, Google and even internet service providers.

The term "reasonable security measures" is becoming part of the data protection lexicon. Thus, it is important to understand what this term means and how to comply. Reasonable security is not a new concept. The Uniform Commercial Code has used the term "security procedure" in connection with wire transfers since 1989.

"Security procedure" is defined in Section 4A of the Uniform Commercial Code as:

> A procedure established by agreement of customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication. *A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices. Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer is not by itself a security procedure.*

Further, Uniform Commercial Code Section 4A provides:

> If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if (i) the security procedure is a commercially reasonable method of providing security against authorized payment orders, and (ii) the bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer. *Commercial reasonableness of a security procedure is a question of law to be determined by considering the wishes of the customers expressed to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated.*

This early Uniform Commercial Code definition of a commercially reasonable security procedure would become a springboard for the interpretation of "reasonable security measures" contained in the recently enacted data privacy legislation. The standard relies heavily upon the industry practice in which the individual, business or entity operates. Thus, it is important to be aware of what your particular industry requires with respect to cybersecurity. For example, the Federal Financial Institutions Examination Council ("FFIEC") has released regulatory guidance regarding online banking, outlining what kind of security controls need to be in place, such as multifactor authentication and back-end fraud detection controls. The FFIEC is a formal United States government interagency body composed of five banking regulators that is "empowered to prescribe uniform principles, standards and report forms to promote uniformity in the supervision of financial institutions." Courts rely heavily on this type of guidance to determine whether "reasonable security measures" have been implemented by an organization.

The National Institute of Standards of Technology has developed a Cybersecurity Framework for how private sector organizations in the United States can access and improve their ability to prevent, detect and respond to cyberattacks. The first version of the framework was published in 2014 and was originally aimed at operators of critical infrastructure. Version 1.1 of the framework was released to the public on April 16, 2018, and includes guidance on how to perform self-assessments, additional detail regarding supply chain risk management, and how to interact with supply chain stakeholders. The NIST framework is generally viewed as an industry best practice, but it has faced criticism because complete implementation requires a high level of investment.

The NIST Cybersecurity Framework is divided into three parts: "Core," "Profile," and "Tiers." The NIST Framework's Core structure consists of five functions (1) Identify, (2) Protect, (3) Detect, (4) Respond and (5) Recover. Each of these functions is then broken down into categories, subcategories and informative references. The "Profile" element of the framework is where an organization typically begins. The organization develops a "Current Profile" to outline its cybersecurity activities and the outcomes it is achieving. It can then develop a "Target Profile," or simply utilize a baseline profile tailored to its particular sector or type of organization. The "Tiers" are used by an organization to clarify how it views its cybersecurity risk and the degree of sophistication of its management approach.

The FFEIC guidance and the NIST Cybersecurity Framework are good resources for determining if your organization is meeting the standard of care with respect to "reasonable security measures." However, assessing cybersecurity risk must be a dynamic process, as the risks are always changing and evolving. What constitutes a "reasonable security measure" this year may not be considered as such next year. Thus, an organization should have a core structure in place that is flexible and appreciates that "reasonable security measures" are not a static concept but one that must continue to evolve and develop to meet the challenges of the changing cybersecurity landscape.

Hilary Wells is a partner in Lewis Roca Rothgerber Christie's Litigation Group and serves as the chair for the Data Protection and Cybersecurity team. She has represented a wide-range of businesses including banks, financial advisors, private equity companies, insurance companies and health care providers.

Holly White is a partner in Lewis Roca Rothgerber Christie's Litigation Group. Her practice is primarily focused on contractual disputes between large commercial entities and insurance companies. She approaches litigation thoughtfully and strategically, with the intent of obtaining the best and most efficient outcome for her clients based on her analysis of the specific facts of each individual case.