Western States Take Steps to Safeguard Data Privacy

Given the increase in cyber-attacks, several U.S. states have introduced and passed legislation on data breach notifications and data privacy. This national trend has some resemblance to the protections provided by Europe's data privacy legislation that went into effect at the end of May 2018, known as the General Data Protection Regulation (GDPR).

In the West, **Colorado**, **Arizona**, and **Oregon** have highlighted and expanded the definition of personal information to be protected. During this year's session, the Colorado General Assembly unanimously passed House Bill (HB 1128) 1128 that expands the categories of personal information covered by the state's data breach notification law and allows businesses 30 days to inform customers if their private data has been compromised. The bill was signed into law by Governor John Hickenlooper in June. Sponsor of the bill, Rep. Wist, said, "what I want to do is reduce identity theft, pure and simple." In Arizona, Governor Doug Ducey signed similar legislation in April (HB 2154). In addition to someone's name and social security number, information such as a private key that is unique to an individual and is used to authenticate or sign an electronic document, for example, has been added. In June, Oregon's amended data breach notification law (SB 1551) went into effect. Among other changes, the amended law requires a notice to affected Oregon residents within 45 days of determining that a security breach occurred and expands the scope of those who must provide notice of a security breach to anyone who "otherwise possess" personal information.

A recent study ranked U.S. states by online data privacy protections. The study evaluated each state based on customer data, social media, employee communications, law enforcement agencies access to data and more. In the U.S., **California** emerged as the winner, complying with 75 percent of the criteria and **Utah** followed in second place with 60 percent.

Home to Silicon Valley and tech giants, California is the only state to include an inalienable right to privacy in its constitution. California's legislative efforts this year went beyond breach notification. In September, Governor Jerry Brown signed into law an amended version (SB 1121) of the California Consumer Privacy Act of 2018 (CCPA), which was originally enacted in late June 2018. The CCPA "is being heralded by many as a 'first in the nation' privacy regime" and has been referred to as a "U.S. state's adoption of the European Union GDPR." Christin McMeley, a

Washington D.C. attorney who represents cable industry clients on privacy and information security matters, called the new law "a really big deal." Starting in 2020, Californians will have the right to learn what businesses know about them, as well as provide consumers the right to request that businesses delete personal information and restrict businesses from selling that information, among other provisions. Additional amendments may be forthcoming between now and the time the CCPA becomes enforceable in 2020.

The sizeable collection of people's personal information exposes them to privacy and security risks. As a result, lawmakers nationwide have expressed concerns about personal security within the evolving digital age and are pursuing modifications to data privacy laws.

2018 Cost of a Data Breach Study: Global Overview

IBM and the Ponemon Institute LLC released a study that includes research from more than 2,200 IT, data protection, and compliance professionals from 477 companies around the world who experienced a data breach within the past year. The study found that a data breach is not simply a malicious or criminal act, it found that over half was due to human error (27%) or a system glitch (25%). In the U.S., the financial burden of a breach averaged $7.91 million. However, if the company contained the breach in less than 30 days, they saved over 1 million. Find out more by clicking on the following to access the *2018 Cost of a Data Breach Study: Global Overview*.

Revitalizing Privacy and Trust in a Data-driven World

Enacting data-breach legislation, while well-intentioned, has been advised by experts to consider strengthening data security practices. *The Global State of Information Security Survey (GSISS) 2018* revealed 9 focus areas to advance privacy risk management. These include more participation among CEO's and business leadership, committing to an information security strategy, including personal data encrypting and management, protecting cross-border data flows, and building trusted networks. Based on responses from 9,500 executives in 122 countries and territories, this report found an overall deficit in data-use governance, offers insightful statistics and references a considerable amount of useful cybersecurity resources.