THE
NATIONAL LAW REVIEW

Colorado Legislature Considers Sweeping Privacy and Cybersecurity Legislation

Ballard Spahr LLP

Article By
David M. Stauss
Gregory Szewczyk
Ballard Spahr LLP
Legal Alerts

- Communications, Media & Internet
- Election Law / Legislative News

- Colorado

Monday, January 22, 2018

A bipartisan group of Colorado legislators proposed legislation that, if enacted, would significantly change the requirements for how Colorado entities protect, transfer, secure, and dispose of documents containing "personal identifying information" (PII). The proposed legislation also would expand the types of information covered by the Colorado Breach Notification Law and result in additional requirements for companies that have suffered a data breach, such as a 45-day deadline to provide notice to affected individuals.

Proposed Data Security Requirements

Perhaps most notably, the proposed legislation would require covered entities to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations."

The proposed legislation does not define what constitutes "reasonable security procedures and practices." This is not uncommon. Many states that have enacted similar legislation have failed to provide such guidance. Nonetheless, drawing guidance from analogous laws and regulations, such as Massachusetts' data security regulations, this provision could require entities to prepare written information-security and cyber-incident response plans, perform risk assessments, and

implement appropriate employee policies and administrative safeguards, among other things.

The proposed legislation also would require any person that discloses PII about a Colorado resident to a nonaffiliated third-party service provider to require "that the nonaffiliated third party implement and maintain reasonable security procedures and practices that are: (a) Appropriate to the nature of the personal identifying information disclosed to the nonaffiliated third party; and (b) Reasonably designed to help protect the personal identifying information from unauthorized access, use, modification, disclosure, or destruction."

Again, the proposed legislation is silent on what constitutes "reasonable security procedures." Examples of relevant contractual terms could include requiring entities to maintain the confidentiality of the PII, to only use PII for a specific purpose, to not share it with third parties, and to use service providers that implement procedures such as encryption of the data in transit (e.g., email or stored on thumb drives) and at rest (e.g., stored on a server) as well as access controls and data segregation.

Additionally, the proposed legislation would require public and private entities to develop a written policy for the destruction of paper or electronic documents that contain PII.

For purposes of these provisions, the legislation defines "personal identifying information" broadly as a "social security number; a personal identification number; a password; a pass code; an official state or government-issued driver's license or identification card number; a government passport number; biometric data; an employer, student or military identification number; or a financial transaction device."

Proposed Changes to Colorado's Breach Notification Law

As discussed in Chapter 1 of the *Colorado Privacy & Cybersecurity Handbook*, Colorado law requires entities to notify individuals if there is a security breach that compromises their personal information. The law currently defines personal information narrowly as an individual's first name or first initial and last name combined with any of the following data elements: a social security number; driver's license number or identification card number; or account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.

The proposed legislation would significantly expand the definition by adding four new data elements: medical information; health insurance information; biometric data; and user names or email addresses in combination with a password or security question and answer that would permit access to an online account. The proposed legislation also would eliminate the requirement that a security code, access code, or password be compromised in connection with an account number or credit or debit card number.

In addition to expanding the definition of personal information, the proposed legislation would require entities to provide notice of the data breach to individuals

"not later than forty-five days from the date of the security breach." That would modify the current law's requirement that notice be provided in the "most expedient time possible and without unreasonable delay."

The proposed legislation would continue to provide that notice is not required if the information was encrypted, but would clarify that notice would be required if the encryption key or password was compromised.

Notably, regardless of whether notice to Colorado residents is required, the proposed legislation would require entities to notify the Attorney General of "any unauthorized acquisition of unencrypted or encrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or commercial entity." That notice would need to be made "as soon as practicable but not later than seven days after discovery of the unauthorized acquisition of data if such unauthorized acquisition affected or is reasonably believed to have affected five hundred Colorado residents or more."

The proposed legislation also would set forth what must be provided in the notice, including: (1) the date, estimated date, or estimated date range of the security breach; (2) a description of the personal information that was acquired or reasonably believed to have been acquired as part of the security breach; (3) contact information for the breached entity; (4) the toll-free numbers, addresses, and websites for consumer reporting agencies and the Federal Trade Commission (FTC); and (6) a statement that the individual can obtain information from the FTC and credit reporting agencies about fraud alerts and security freezes.

Enforcement

The proposed legislation would empower the Colorado Attorney General to bring actions against entities for violating the breach notification requirements; failing to implement reasonable security procedures or not requiring nonaffiliated third-party service providers to implement them; and failing to develop a written policy for the destruction of documents containing PII. The Attorney General would be permitted to seek "relief that may be appropriate to ensure compliance with this section or to recover direct economic damages resulting from a violation, or both."

The legislation also would authorize the Attorney General to initiate a criminal investigation and prosecute any criminal violations of Colorado's computer crime statute, C.R.S. § 18-5.5-102. For a discussion of Colorado's computer crime statute, see Chapter 5 of the *Colorado Privacy & Cybersecurity Handbook*.

If enacted, this proposed legislation will substantially change the manner in which Colorado entities must treat confidential information. Colorado entities should closely monitor this proposed legislation and carefully consider how these proposed revisions may apply to their specific business and what measures may need to be taken to ensure compliance.