North Carolina Proposes Expansive Consumer Privacy Protections

By: Robert Van Arnam & Carmelle F. Alipio

04.20.2021

On April 6, 2021, the North Carolina General Assembly introduced **Senate Bill 569**: the Consumer Privacy Act of North Carolina (CPA), that would expand protections to consumers in the North Carolina Identity Theft Protection Act, codified at § 75-60.

1. Scope of the Proposed CPA

The proposed Act would apply to businesses that target their services to North Carolina residents. Businesses that control or process the personal data of (1) at least 100,000 consumers on an annual basis or (2) at least 25,000 consumers and derive over fifty percent (50%) of gross revenue from the sale of personal data would be required to comply.

2. Key Difference from the Identity Theft Protection Act

Unlike the current Identity Theft Protection Act, that focuses on rights and responsibilities in response to a data breach, the proposed CPA focuses on proactive measures to give consumers more control over their personal data.

The proposed CPA expands consumers rights as follows:

- **Rights of Knowledge and Access.** Consumers may request confirmation on whether a controller is processing their personal data and obtain a copy of that data.
- **Right to Correction.** Consumers may correct inaccuracies about their personal data.
- **Right to Deletion.** Consumers may request that a controller delete personal data they have provided or that a controller obtained.
- **Right to Opt Out.** Consumers may opt out of the processing of their personal data for the purposes of targeted advertising, sales, or profiling resulting from their personal data.
- **Private Right of Action -** While the Attorney General retains the right to enforce the proposed CPA, the proposed CPA provides for a private right of action. Individual consumers may institute a

civil action seeking damages and to enjoin and restrain future acts that would be in violation of the CPA. Reasonable attorneys? fees may also be awarded to the prevailing party.

3. Compliance Required by Businesses

Similar to existing data privacy regulations such as the GDPR, the proposed CPA will govern businesses according to how they handle and process data. Businesses that direct and determine the purpose for data use will be classified as ?controllers,? and businesses that process data on behalf of controllers will be classified as ?processors.? Because controllers, by definition, control how consumer data is used, non-compliance with the proposed CPA will put those businesses at risk for potentially large fines, up to $5,000 for each violation, as determined by the Attorney General.

The major compliance requirements include:

- **Responses to Consumer Requests.** Controllers are required to comply with requests by consumers to exercise any of their rights with regard to their personal data as described above. Controllers must respond to consumers without undue delay and generally within 45 days.
- **Disclosure.** Controllers must disclose to the consumer the purposes for which consumer personal data is collected.
- **Limited Data Collections.** Controllers must limit the collection of personal data to only what is ?adequate, relevant and reasonably necessary? in relation to the disclosed purposes for personal data.
- **Sensitive Data Restrictions.** If a controller did not obtain a consumer?s consent to process that consumer?s sensitive data, then the controller is prohibited from processing it. Sensitive data includes personal data relating to racial or ethnic origin, religious beliefs, health diagnosis, sexual orientation, citizenship, immigration status, biometric and genetic data, and precise geolocation data.
- **Privacy Notice.** Controllers must provide consumers with a clear and accessible privacy notice that includes the categories of personal data being processed, the purposes of such processing, how consumers may exercise their rights, and information regarding sharing consumer personal data with third parties.
- **Contracts with Processors.** Controllers must enter into contracts with processors that include processing procedures with respect to the processing performed by the processor on behalf of the controller and include specific requirements as provided in the proposed CPA.
- **Data Protection Assessments.** On at least an annual basis, controllers must conduct and document a data protection assessment of processing activities, including processing related to sale, profiling, and targeted advertising, involving personal data and an assessment of the data protections, such as cybersecurity measures, in place.

4. Looking Forward

There has been a recent push by state legislators to enact stronger data protection laws, such as

Virginia?s recent Consumer Data Protection Act, enacted in March 2021, which was previously analyzed here. While this is not North Carolina?s first attempt to expand its data protection laws, there is greater momentum now to enact a more comprehensive act. Therefore, businesses must understand their roles and likely expanded responsibilities. We will continue to monitor and report on the status of the proposed CPA.

Related People

- Carmelle F. Alipio ? 919.981.4038 ? calipio@williamsmullen.com
- Robert Van Arnam ? 919.981.4055 ? rvanarnam@williamsmullen.com

Related Services

- Intellectual Property
- Data Protection & Cybersecurity