

White Paper
for
North Carolina Data Privacy Laws

December 3, 2023

Diane Harrell

IST 466-01

T Frazier

Executive Summary

As of now, October 2023, North Carolina has no data privacy laws. There is one Act proposed as of April 5, 2023, that will not take effect until 2024 if passed. It has a few issues that could be changed, such as the lack of protection from out-of-state businesses that the California Act (CCPA) has, and the protection of Sensitive Data as described and enforced by the Virginia Act (VCDPA). Affected individuals mentioned within this document include consumers and controllers, but they are affected in two different ways.

The proposal will help to protect the data of consumers, giving them access to controlling where their data goes and how it is used. It also requires controllers to be smarter about how they are using the individual data and puts more accountability onto them, as they will now be unable to sell data however they want, and will have to work together with the consumer to make their profit. These two entities working together will increase the safety of user data, and prevent companies from using data in ways that will harm the consumer. This will also prevent companies from using consumer data in ways that the consumer is unaware of.

Table of Contents

Introduction - Page 1

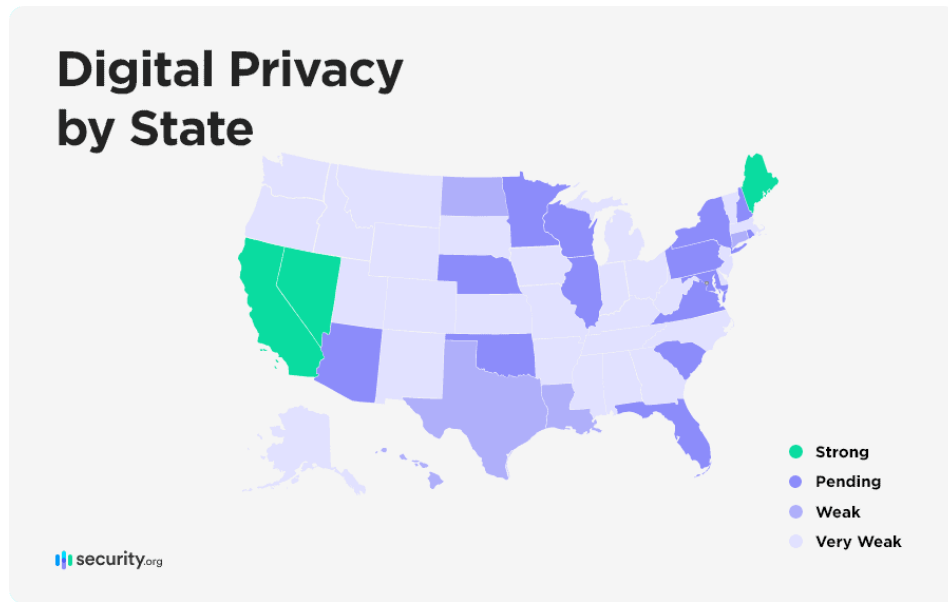
Current Policy - Page 2

Proposed Policy - Page 4

Conclusion - Page 5

Introduction

In North Carolina, there are currently no laws about data privacy, NC having only one law proposed in April of 2023 that wouldn't go into effect until at least January 2024. This policy is the only one that is looking to protect user privacy and data in North Carolina.



(Team, Security. Org., 2023)

Looking to change this, this paper will explain proposed policy changes, along with why these changes are so valuable to North Carolina's data privacy. It will also go into depth about why North Carolina should adapt more to California's Laws, and how we would benefit from doing so. These laws are important to North Carolina consumers as the right to their own personal data privacy is very important. Without it, consumer data is at risk of being sold for the use of advertisements, and revenue.

Current Policy

North Carolina currently has no data privacy laws, only the proposed Act from April 2023. This act is called the "North Carolina Consumer Privacy Act (Nahra, 2018)" and applies to any controller that conducts business in North Carolina and meets one of two requirements - controlling the personal data of 100,000 or more NC Residents, or deriving over 50% of their gross revenue from sales of personal data and controls personal data of 25k or more NC residents.

There are six substantive rights to consumers within this act (Wall et al., 2022):

1. Rights of Knowledge and Access - Consumers may confirm whether or not a business is processing the consumer's personal data and may access such data.
2. Right of Correction - Consumers may correct inaccuracies in the consumer's personal data.
3. Right of Deletion - Consumers may demand that their personal data be deleted.
4. Right to Obtain a Copy - Consumers may obtain a copy of their personal data.
5. Right to Opt-Out - Consumers may opt out of the processing of their personal data for the purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.
6. Private Right of Action - An individual consumer may institute a civil action to enjoin and restrain future violations of CPA and reasonable attorneys' fees may be awarded to the prevailing party.

The Act will require companies to adhere to the following compliances:

1. Responding to Consumer Requests - Businesses will be required to comply with CPA requests without undue delay and within 45 days.
2. Disclose - Businesses must disclose to the consumer the purpose for which consumer personal data is collected.
3. Limit Data Collection - Businesses 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 and may not exceed the disclosed purpose without consent from the consumer.
4. Obtain Consent for Sensitive Data – Businesses may not process sensitive data^[1] concerning the consumer without obtaining consent.

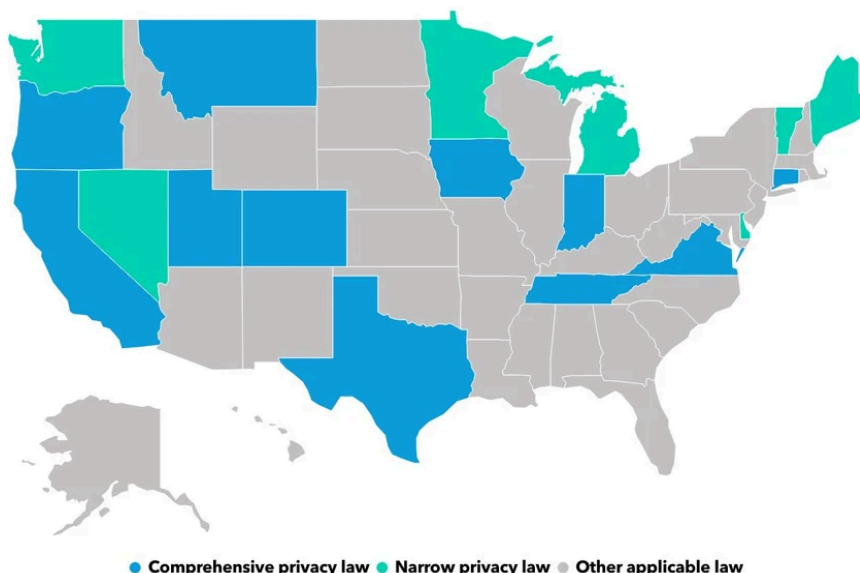
5. Privacy Notice – Businesses must provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes (1) the categories of personal data being processed, (2) the purposes of such processing, (3) how consumers may exercise their rights under CPA, (3) the categories of personal data that the business shares with third parties, and (4) the categories third parties, if any, with whom the business shares personal data.
6. Enter into Contracts – Businesses must enter into contracts with their data processors that include processing procedures with respect to the processing performed by the processor on behalf of the business and include specific requirements as by CPA
7. Conduct Data Protection Assessments – Businesses must, at least annually, conduct and document data protection assessments.

This will give individual consumers the right to their personal data privacy. It will protect individuals from targeted advertising, the sale of personal data, and profiling decisions that produce legal effects concerning the consumer. It will create a Consumer Privacy Account where all money recovered for violations of this act will be deposited.

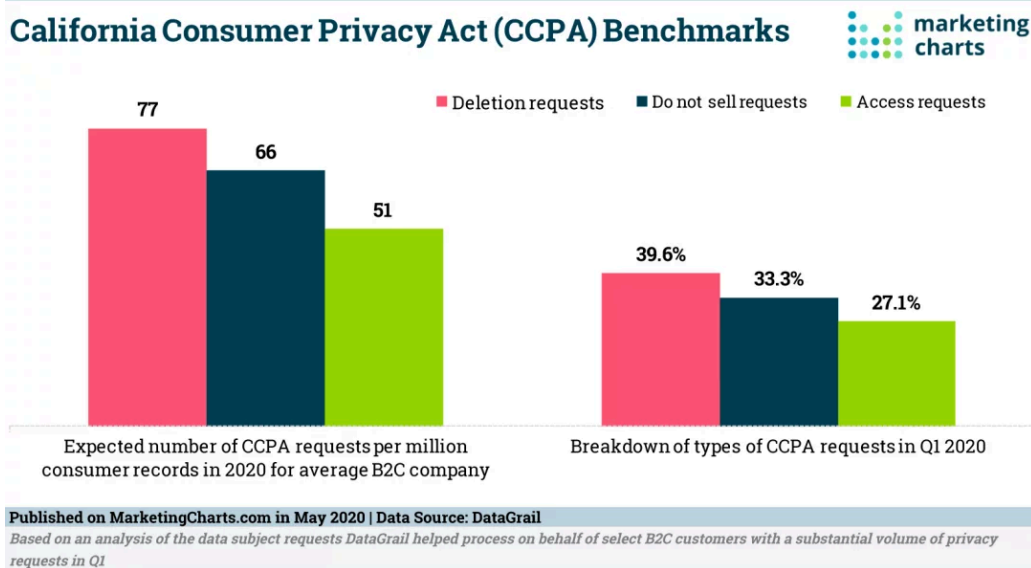
It will provide reasonable security measures, incorporating privacy designs by principles. However, it will not create a private right of action. Numerous entities would be exempt from CPA, and this act would not prohibit companies from complying with federal, state, or local laws nor would it prohibit its ability to comply with a court order or subpoena to provide information. This would not protect consumers from the collection, use, retaining, selling, sharing, or disclosure of their personal information that is deidentified or aggregate consumer information. This Act, if passed, will not take effect until January 2024.

Proposed Policy

Considering North Carolina's current lack of any instituted laws for data privacy, I believe that we should look more toward California and Virginia's data privacy laws for reference.



California was the first state to enact comprehensive data privacy legislation, via the California Consumer Privacy Act, and the California Privacy Rights Act. The CCPA was signed into law on June 8, 2018, and the CPRA was approved on November 3, 2020. Virginia was the second state to act, introducing the Virginia Consumer Data Protection Act (VCDPA) on January 1, 2023. These were both huge steps in the way of data privacy, as we saw the right to request our personal information be deleted by companies come into play.



(Lashbrook, 2020)

I believe that North Carolina would benefit from following these two acts, as the California Act gives consumers living in the state a sense of safety, as they require even businesses that operate outside of the state to keep up with their terms to protect their consumers. The CCPA requires businesses to notify consumers of the categories of personal information collected from them, and the purpose of the information that is being collected. This must happen before or during the time that information is collected. The CCPA protects consumers from discrimination based on the exertion of their rights.

The Virginia Consumer Data Protection Act ([oag.state.va.us.](https://oag.state.va.us/), 2023) went into effect on January 1, 2023. The VCDPA allows consumers to confirm that the controller is actually processing the personal information they are given, allows them to correct inaccuracies, obtain copies, and request deletion of any personal information given to the controller. Sensitive Data is also considered Personal Data under the VCDPA. Sensitive information is considered any of the following:

1. A person's racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status.
2. The processing of genetic or biometric data for the purposes of uniquely identifying that person
3. The personal data collected from a known child, which is defined as someone younger than 13
4. Precise geolocation data

The Proposed Policy would consist of all things included in the April 5th proposal, along with the above listed attributes from the California and Virginia acts.

Conclusion

As of today North Carolina still has no data privacy acts in effect. The April 5th act will help to protect users in larger ways that we are not protected right now, though it should include more points from the California and Virginia Acts. It is unfair to expect consumers to share their data with no way to control who sees it or where it goes. Taking attributes such as the CCPA's requirement for outside-of-state businesses to

comply with their act, and the VCDPA's requirements for sensitive information, and adding them to the proposed April 5th act in North Carolina would significantly help individuals in North Carolina feel safer when it comes to their data privacy and information privacy.

Works Cited

Code section group. Codes Display Text. (2018).

https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Nahra, K. J., Jessani, A. A., Ruano, G., & Kane, S. (2023). State Comprehensive Privacy Law Update – April 3, 2023. WilmerHale.

<https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20230404-state-comprehensive-privacy-law-update-april-3-2023#:~:text=relation%20to%20employment.-,Creates%20rights%20for%20individual%20consumers%2C%20including%3A%20the%20right%20to%20confirm,opt%20out%20of%20processing%20for>

GENERAL ASSEMBLY OF NORTH CAROLINA SESSION 2023. (2023).

<https://webservices.ncleg.gov/ViewBillDocument/2023/3077/0/DRS35199-LR-18B>

Team, Security. org. (2023, August 31). 47 states have weak or nonexistent consumer data privacy laws. <https://www.security.org/resources/digital-privacy-legislation-by-state/>

Wall, M., & Malik, G. (2022, September 23). Trends in privacy laws around the U.S.: A look at the pending N.C. Consumer Privacy Act. Cranfill Sumner LLP.

<https://www.cshlaw.com/resources/trends-in-privacy-laws-around-the-u-s-a-look-at-the-pending-n-c-consumer-privacy-act/>

Which states have consumer data privacy laws?. Bloomberg Law. (2023).

<https://pro.bloomberglaw.com/brief/state-privacy-legislation-tracker/>

Spainhour, E. (2019). What North Carolina businesses need to know about the california consumer privacy act. Brooks Pierce.

<https://www.brookspierce.com/publication-What-North-Carolina-Businesses-Need-to-Know-About-the-California-Consumer-Privacy-Act>

The Virginia Consumer Data Protection Act. oag.state.va.us. (2023).

<https://www.oag.state.va.us/consumer-protection/files/tips-and-info/Virginia-Consumer-Data-Protection-Act-Summary-2-2-23.pdf>

Lashbrook, J. (2020, May 14). Deletion requests most popular CCPA demand from consumers in Q1 2020. Marketing Charts.

<https://www.marketingcharts.com/customer-centric/privacy-and-security-113049>