Minnesota Consumer Data Privacy Act (2023)
House File 2309
Rep Steve Elkins

Section 1: Data Practices Act Considerations (1.18)
Classifies data collected by the AG to enforce this Act as non-public under the Data Practices Act.

Section 2: Names the bill the "**Minnesota Consumer Data Privacy Act" (1.12)**

Section 3: Definitions (1.17)
There are 4 pages of definitions, and they are a critical part of the bill. These definitions are aligned with the definitions in existing data privacy laws in California, Virginia, Colorado, Connecticut and Utah and it's extremely important to the business community that we maintain this consistency across states.

Before reading the bill, one should familiarize oneself with these foundational definitions:

Role Players
- Consumers
- Controllers (companies that create data)
- Processors (companies that process data for Controllers)

Categories of Data
- Personal Data
- Sensitive Data (and its subcategories)

Things that can be done with data
- Profiling (e.g., calculating a credit score)
- Sale
- Targeted Advertising

The definition of "Sensitive Data" is especially important because companies must obtain the Consumer's approval before selling Sensitive data (Opt-in). Data that is not "sensitive" can be sold unless the Consumer indicates that they don't want it sold (Opt-out).

Note: There is only one case where a definition in this bill is different than in the other states: Specific Geolocation at line 4.26. I don't think that the definition used in the other states is enforceable in practice.

Section 4: Exclusions (5.12)
1. **Subd 1**: Small businesses are outside of the bill's scope
2. **Subd 2**: Governments are outside of the bill's scope (in Minnesota they are covered by the Data Practices Act).
   Data that is already covered by other, mostly federal, data privacy laws, such as:
   - HIPAA or the MN Heath Records Act (Health Care)
   - Fair Credit Reporting Act (FCRA) (Credit Reporting)
   - Gramm-Leach-Bliley (GLB) (Personal Finance)
   - FERPA (Education)
   - Children's Online Privacy Act (COPA) (Children's data)
   - Other similar laws

   … are governed by those laws, instead. *(note: businesses are always looking for expansions of these carve outs.)*

Section 5: Responsibilities According to Role (8.4)
This section outlines the general responsibilities of Controllers and Processors to protect the privacy and security of Consumer data.

Section 6: Consumer Personal Data Rights (9.28)
This is the heart of the bill. It outlines the following Consumer rights with respect to the data that Controllers have about them.

1. **Subd1 (9.28)**: Consumers have the right to have Controllers:
    1. Tell them what kinds of personal data they have about them
    2. Correct inaccurate personal data
    3. Delete personal data about them
    4. Provide a copy of their personal data
    5. Opt-out of having their personal data Sold, used in Targeted Advertising or used to Profile them
    6. Answer questions about …
        1. the decision resulting from the profiling,
        2. the reasons why the profiling resulted in the decision
        3. the accuracy of the data used to profile them

        ... and to correct inaccuracies in the data used to profile them and have the profiling re-run (note: this is a right that is not included in the other states' laws.)

2. **Subd 2 (10.25)**: Describes how Consumers can invoke these rights
3. **Subd 3 (11.1)**: Describes an anticipated "universal opt-out" mechanism that Consumers can invoke through personal settings at the platform level (e.g., when using a web browser such as Chrome, Bing or Firefox) to indicate that they don't ever want their data processed or sold by any Controller that collects data from them via that platform.
4. **Subd 4 (11.26):** Requires Controllers to provide a convenient means to exercise these rights, and requires Controllers to act on Consumer requests within a reasonable amount of time. Requires Controllers to verify that the party making the request is, in fact, the Consumer before acting on the request, while protecting the Consumer's Personally Identifying Information.
5. **Subd 5 (13.9):** Describes a required appeals process

Section 7: Processing Deidentified or Pseudonymous Data (14.1)
This section describes the responsibilities of Controllers and Processors in the handling of Deidentified and Pseudonymous data.

Deidentified data and Pseudonymous data are defined in the Definitions, but, in a nutshell, Deidentified data is personal data from which all personally identifying information (PII) that could be used to identify the Consumer (e.g., name, address, date of birth, SSN, DL #, etc.) has been stripped away. Pseudonymous data is personal data which never included any PII, only anonymous identifiers (e.g., a device id, online advertising id or a random number id that cannot be associated with a Consumer without additional information possessed only by the Controller). (Sometimes a Pseudonymous ID is added to Deidentified data.)

This section is important because a great deal of the personal information collected over the internet is Pseudonymous, while much of the data collected and sold by Controllers to third parties is first Deidentified. However, there are a variety of techniques by which the identities of the related Consumers can be revealed by reverse-engineering the data. Therefore, I added paragraphs (d) (14.28) and (e) (14.31) to my version of the bill to prohibit processors and third parties from doing so.

Section 8: Responsibilities of Controllers (15.1)

1. **Subd 1 (15.2): Transparency Obligations.** Requires clearly written privacy notices for Consumers.
2. **Subd 2 (16.26): Use of Data.**
   a-c Restricts Controllers to only collecting the data that they need to conduct business with the Consumer and nothing more.
   d Requires Controllers to secure and protect the Consumer's data
   e Prevents the processing of "Sensitive" data without the Consumer's consent
   f Requires Controllers to provide a mechanism for Consumers to revoke their consent
   g Further limits the use of children's data
3. **Subd 3 (17.22): Nondiscrimination**. Prohibits use of the Consumer's data to engage in discriminatory practices. Prohibits Controllers from requiring Consumers to relinquish their rights under this act to obtain lower prices or better services. Prohibits the sale of the Consumer's data to a third party to participate in customer loyalty programs, except to the extent necessary to provide program rewards.
4. **Subd 4 (18**.13) **Waiver of Rights Unenforceable**. States that the Consumer's rights under this Act cannot be waived.

Section 9: Data Privacy and Protection Assessments (18.16)

Requires the Controller to conduct and maintain an assessment of the policies and procedures used to comply with the provisions of this Act, including their policies that implement the foundational principles of "Privacy by Design" and procedures used to secure Consumer Data. This assessment must be provided to the Minnesota Attorney General upon request.

Section 10: Limitations and Applicability. (20.14)

Describes limitations needed to comply with other legal requirements or exceptions that are in the public interest.

Section 11: Attorney General Enforcement. (22.25)

Provides for enforcement by the Minnesota Attorney General. *(The bill does **not** provide a "right of private action", which is a lightning rod for business and has not been provided in any of the other state laws that have passed, to date.)*

Section 12: Preemption of Local Law, Severability (23.8)

Preempts local governments from regulating in this subject area. Allows severability should any of the provisions of the Act be ruled invalid by the courts.

Section 13: Effective Date (23.15)

Sets the effective date at July 31, 2024 with a few exceptions that are consistent with the effective dates in Colorado and Connecticut, the most recent states to pass similar laws. m