SENATE BILL 319

56TH LEGISLATURE - STATE OF NEW MEXICO - FIRST SESSION, 2023

INTRODUCED BY

George K. Muñoz and Mark Moores and Siah Correa Hemphill

AN ACT

RELATING TO BUSINESS; ENACTING THE AGE APPROPRIATE DESIGN CODE ACT; PROVIDING CIVIL PENALTIES.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF NEW MEXICO:

SECTION 1. [NEW MATERIAL] SHORT TITLE.--This act may be cited as the "Age Appropriate Design Code Act".

SECTION 2. [NEW MATERIAL] DEFINITIONS.--As used in the Age Appropriate Design Code Act:

A. "aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed and that is not linked or reasonably linkable to any consumer or household. "Aggregate consumer information" does not mean individual consumer records that have been de-identified;

B. "child" means a consumer who is under eighteen
years of age;

C. "collects" means buying, renting, gathering,
obtaining, receiving or accessing personal information
pertaining to a consumer by any means, including receiving
information from the consumer, either actively or passively, or
by observing the consumer's behavior;

D. "consumer" means a natural person who resides in
New Mexico, however identified, including by a unique
identifier;

E. "controller" means a person that alone or
jointly with others determines the purpose and means of
processing personal data;

F. "dark pattern" means a user interface designed
or manipulated with the substantial effect of subverting or
impairing user autonomy, decision-making or choice;

G. "data protection impact assessment" means a
systematic survey to assess risks that arise from the data
management practices of the controller to children who are
reasonably likely to access the online service, product or
feature at issue that arises from the provision of that online
service, product or feature;

H. "default" means a preselected option adopted by
the controller for the online service, product or feature;

I. "de-identified" means information that cannot
reasonably be used to infer information about, or otherwise be
linked to, an identified or identifiable individual, if the controller that possesses that information:

(1) takes reasonable measures to ensure that such information cannot be associated with an individual;

(2) publicly commits to process such information only in a de-identified fashion and not attempt to re-identify such information; and

(3) contractually obligates any recipients of such information to satisfy the criteria set forth in this subsection;

J. "likely to be accessed by children" means it is reasonable to expect, based on the following indicators, that the online service, product or feature would be accessed by children:

(1) the online service, product or feature is directed to children as defined by the federal Children's Online Privacy Protection Act of 1998;

(2) the online service, product or feature is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children;

(3) the online service, product or feature has advertisements marketed to children;

(4) the online service, product or feature is substantially similar or the same as an online service, product...
or feature subject to Paragraph (2) of this subsection;

(5) the online service, product or feature has design elements that are known to be of interest to children, including games, cartoons, music and celebrities who appeal to children; or

(6) a significant amount of the audience of the online service, product or feature is determined, based on internal company research, to be children;

K. "personal information" means information that is linked or reasonably linkable to an identified or identifiable individual; "personal information" does not include de-identified information or publicly available information;

L. "precise geolocation" means data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of one thousand eight hundred feet;

M. "process" or "processing" means an operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion or modification of personal data;

N. "processor" means a person that processes personal data on behalf of a controller;

O. "profiling" means automated processing of
personal information that uses personal information to evaluate certain aspects relating to a natural person, including analyzing or predicting aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;

P. "sell" means selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating orally, in writing or by electronic or other means, a consumer's personal information by the controller to a third party for monetary or other valuable consideration;

Q. "sensitive personal information" means personal information that includes:

(1) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status;

(2) the processing of genetic or biometric data for the purpose of uniquely identifying an individual; or

(3) precise geolocation data;

R. "share" means sharing, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating orally, in writing or by electronic or other means, a consumer's personal information by the
controller to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a controller and a third party for cross-context behavioral advertising for the benefit of a controller in which no money is exchanged; and

S. "third party" means a person who is not:

(1) the controller with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer's current interaction with the controller pursuant to the Age Appropriate Design Code Act;

(2) a service provider to the controller; or

(3) a contractor.

SECTION 3. [NEW MATERIAL] DATA PROTECTION IMPACT ASSESSMENT--MITIGATION PLAN.--

A. Before any new online services, products or features are offered to the public, a controller that provides an online service, product or feature likely to be accessed by children shall complete a data protection impact assessment for any online service, product or feature likely to be accessed by children and maintain documentation of this assessment as long as the online service, product or feature is likely to be accessed by children. A controller shall biennially review all data protection impact assessments.

B. The data protection impact assessment required
by this section shall identify the purpose of the online service, product or feature, how it uses children's personal information and the risks of material detriment to children that arise from the data management practices of the controller. The data protection impact assessment shall address, to the extent applicable, all of the following:

(1) whether the design of the online product, service or feature could harm children, including by exposing children to harmful, or potentially harmful, content on the online product, service or feature;

(2) whether the design of the online product, service or feature could lead to children experiencing or being targeted by harmful, or potentially harmful, contacts on the online product, service or feature;

(3) whether the design of the online product, service or feature could permit children to witness, participate in or be subject to harmful, or potentially harmful, conduct on the online product, service or feature;

(4) whether the design of the online product, service or feature could allow children to be party to or exploited by a harmful, or potentially harmful, contract on the online product, service or feature;

(5) whether algorithms used by the online product, service or feature could harm children;

(6) whether targeted advertising systems used
by the online product, service or feature could harm children;

(7) whether and how the online product, service or feature uses system design features to increase, sustain or extend the use of the online product, service or feature by children, including the automatic playing of media, rewards for time spent and notifications; and

(8) whether, how and for what purpose the online product, service or feature collects or processes sensitive personal information of children.

C. A controller that provides an online service, product or feature likely to be accessed by children shall, within three business days of a written request by the attorney general, provide to the attorney general a list of all data protection impact assessments the controller has completed.

D. A controller that provides an online service, product or feature likely to be accessed by children shall, within five business days, make a data protection impact assessment available to the attorney general pursuant to a written request.

E. A data protection impact assessment is protected as confidential and shall be exempt from public disclosure, including pursuant to the Inspection of Public Records Act.

F. To the extent any information contained in a data protection impact assessment disclosed to the attorney general includes information subject to attorney-client
privilege or work product protection, disclosure pursuant to Subsections C and D of this section shall not constitute a waiver of that privilege or protection.

G. A data protection impact assessment conducted by a controller for the purpose of compliance with any other law complies with this section if the data protection impact assessment meets the requirements of the Age Appropriate Design Code Act.

H. A single data protection impact assessment may contain multiple similar processing operations that present similar risks only if each relevant online service, product or feature is addressed.

I. A controller shall complete a data protection impact assessment on or before July 1, 2024 for any online service, product or feature likely to be accessed by children offered to the public before July 1, 2024.

J. A controller that provides an online service, product or feature likely to be accessed by children that has documented any risk of material detriment to children that arises from the data management practices of the controller identified in the data protection impact assessment required by this section shall create a timed plan to mitigate or eliminate the risk before the online service, product or feature is accessed by children.

SECTION 4. [NEW MATERIAL] ADDITIONAL REQUIRED ACTIONS BY
CONTROLLERS.--A controller that provides an online service, product or feature likely to be accessed by children shall:

A. estimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the controller or apply the privacy and data protections afforded to children to all consumers;

B. configure all default privacy settings provided to children by the online service, product or feature to settings that offer a high level of privacy, unless the controller can demonstrate a compelling reason that a different setting is in the best interests of children;

C. publicly provide privacy information, terms of service, policies and community standards in a prominent, precise manner and use clear language suited to the age of children likely to access that online service, product or feature;

D. if the online service, product or feature allows the child's parent, guardian or other consumer to monitor the child's online activity or track the child's location, provide to the child an obvious signal when the child is being monitored or tracked;

E. enforce published terms, policies and community standards established by the controller, including privacy policies and policies concerning children;
F. publicly provide prominent, accessible and responsive tools to help children, or, if applicable, their parents or guardians, exercise their privacy rights and report concerns;

G. consider the best interests of children when designing, developing and providing online services, products or features; and

H. prioritize the privacy, safety and well-being of children over commercial interests if a conflict arises between commercial interests of a controller and the best interests of children likely to access an online product, service or feature.

SECTION 5. [NEW MATERIAL] PROHIBITED PRACTICES.--A controller that provides an online service, product or feature likely to be accessed by children shall not:

A. use the personal information of a child in a way that the controller knows, or has reason to know, is materially detrimental to the physical health, mental health or well-being of the child;

B. profile a child by default unless:

(1) the controller can demonstrate it has appropriate safeguards in place to protect children; and

(2) profiling is necessary to provide the online service, product or feature requested, and only with respect to the aspects of the online service, product or feature.
feature with which the child is actively and knowingly engaged; or

(3) the controller can demonstrate a compelling reason that profiling is in the best interests of children;

C. collect, sell, share or retain any personal information that is not necessary to provide an online service, product or feature with which a child is actively and knowingly engaged, unless the controller can demonstrate a compelling reason that the collecting, selling, sharing or retaining of the personal information is in the best interests of children likely to access the online service, product or feature;

D. if the end user is a child, use personal information for any reason other than a reason for which that personal information was collected, unless the controller can demonstrate a compelling reason that use of the personal information is in the best interests of children;

E. collect, sell or share any precise geolocation information of children by default unless the collection of that precise geolocation information is strictly necessary for the controller to provide the service, product or feature requested and then only for the limited time that the collection of precise geolocation information is necessary to provide the service, product or feature;

F. collect any precise geolocation information of a
child without providing an obvious sign to the child for the
duration of that collection that precise geolocation
information is being collected;

G. use dark patterns to lead or encourage children
to provide personal information beyond what is reasonably
expected to provide that online service, product or feature to
forego privacy protections, or to take any action that the
controller knows, or has reason to know, is materially
detrimental to the child's physical health, mental health or
well-being; or

H. use any personal information collected to
estimate age or age range for any other purpose or retain that
personal information longer than necessary to estimate age; age
estimation shall be proportionate to the risks and data
practice of an online service, product or feature.

SECTION 6. [NEW MATERIAL] VIOLATIONS--ENFORCEMENT--

PENALTIES.--

A. A controller that violates the Age Appropriate
Design Code Act shall be:

(1) subject to injunctive relief to cease or
correct the violation;

(2) liable for a civil penalty of not more
than two thousand five hundred dollars ($2,500) per affected
child for each negligent violation; and

(3) liable for a civil penalty of not more
than seven thousand five hundred dollars ($7,500) per affected child for each intentional violation.

B. Enforcement actions pursuant to Subsection A of this section shall only be initiated by the attorney general.

C. If a controller is in substantial compliance with the requirements of Section 3 of the Age Appropriate Design Code Act, the attorney general shall provide written notice to the controller, before initiating an action pursuant to Subsection A of this section, identifying the specific provisions of that act the attorney general alleges have been or are being violated.

D. If within ninety days of the notice required by Subsection C of this section a controller cures alleged violations identified in that notice and provides the attorney general a written statement that the alleged violations have been cured and sufficient measures have been taken to prevent future violations, the controller shall not be liable for a civil penalty for any violation cured pursuant to this subsection.

E. Nothing in the Age Appropriate Design Code Act shall be interpreted to serve as the basis for a private right of action under that act or any other law.

SECTION 7. [NEW MATERIAL] EXCEPTIONS.--The Age Appropriate Design Code Act does not apply to:

A. protected health information that is collected
by a covered entity or controller associate governed by the privacy, security and breach notification rules issued by the United States department of health and human services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996;

B. a covered entity governed by the privacy, security and breach notification rules issued by the United States department of health and human services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996, to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in Subsection A of this section;

C. information collected as part of a clinical trial subject to the federal policy for the protection of human subjects, also known as the common rule, pursuant to good clinical practice guidelines issued by the international council for harmonisation of technical requirements for pharmaceuticals for human use or pursuant to human subject protection requirements of the United States food and drug administration;

D. a telecommunications service as defined in 47 U.S.C. Section 153; or
E. the delivery or use of a physical product.

SECTION 8. APPLICABILITY.--

A. The Age Appropriate Design Code Act applies to controllers in New Mexico or persons that produce services, products or features that are targeted to residents of this state and that during the preceding calendar year:

(1) controlled or processed the personal data of not less than one hundred thousand consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

(2) controlled or processed the personal data of not less than twenty-five thousand consumers and derived more than twenty-five percent of their gross revenue from the sale of personal data.

B. The Age Appropriate Design Code Act does not apply to an online service, product or feature that is not offered to the public on or after July 1, 2024.

SECTION 9. EFFECTIVE DATE.--The effective date of the provisions of this act is July 1, 2024.

- 16 -