..... moves to amend H.F. No. 1370 as follows:

Delete everything after the enacting clause and insert:

"ARTICLE 1

DEEP FAKE TECHNOLOGY

Section 1. **[604.32] CAUSE OF ACTION FOR NONCONSENSUAL DISSEMINATION OF A DEEP FAKE DEPICTING INTIMATE PARTS OR SEXUAL ACTS.**

Subdivision 1. **Definitions.** (a) As used in this section, the following terms have the meanings given.

(b) "Deep fake" means any video recording, motion-picture film, sound recording, electronic image, or photograph, or any technological representation of speech or conduct substantially derivative thereof:

(1) that is so realistic that a reasonable person would believe it depicts speech or conduct of an individual; and

(2) the production of which was substantially dependent upon technical means, rather than the ability of another individual to physically or verbally impersonate such individual.

(c) "Depicted individual" means an individual in a deep fake who appears to be engaging in speech or conduct in which the individual did not engage.

(d) "Intimate parts" means the genitals, pubic area, partially or fully exposed nipple, or anus of an individual.

(e) "Personal information" means any identifier that permits communication or in-person contact with an individual, including:

(1) an individual's first and last name, first initial and last name, first name and last initial, or nickname;

(2) an individual's home, school, or work address;

(3) an individual's telephone number, email address, or social media account information; or

(4) an individual's geolocation data.

(f) "Sexual act" means either sexual contact or sexual penetration.

(g) "Sexual contact" means the intentional touching of intimate parts or intentional touching with seminal fluid or sperm onto another individual's body.

(h) "Sexual penetration" means any of the following acts:

(1) sexual intercourse, cunnilingus, fellatio, or anal intercourse; or

(2) any intrusion, however slight, into the genital or anal openings of an individual by another's body part or an object used by another for this purpose.

Subd. 2. **Nonconsensual dissemination of a deep fake.** (a) A cause of action against a person for the nonconsensual dissemination of a deep fake exists when:

(1) a person disseminated a deep fake with knowledge that the depicted individual did not consent to its public dissemination;

(2) the deep fake realistically depicts any of the following:

(i) the intimate parts of another individual presented as the intimate parts of the depicted individual;

(ii) artificially generated intimate parts presented as the intimate parts of the depicted individual; or

(iii) the depicted individual engaging in a sexual act; and

(3) the depicted individual is identifiable:

(i) from the deep fake itself, by the depicted individual or by another individual; or

(ii) from the personal information displayed in connection with the deep fake.

(b) The fact that the depicted individual consented to the creation of the deep fake or to the voluntary private transmission of the deep fake is not a defense to liability for a person who has disseminated the deep fake with knowledge that the depicted individual did not consent to its public dissemination.

Subd. 3. **Damages.** The court may award the following damages to a prevailing plaintiff from a person found liable under subdivision 2:

(1) general and special damages, including all finance losses due to the dissemination of the deep fake and damages for mental anguish;

(2) an amount equal to any profit made from the dissemination of the deep fake by the person who intentionally disclosed the deep fake;

(3) a civil penalty awarded to the plaintiff of an amount up to $100,000; and

(4) court costs, fees, and reasonable attorney fees.

Subd. 4. **Injunction; temporary relief.** (a) A court may issue a temporary or permanent injunction or restraining order to prevent further harm to the plaintiff.

(b) The court may issue a civil fine for the violation of a court order in an amount up to $1,000 per day for failure to comply with an order granted under this section.

Subd. 5. **Confidentiality.** The court shall allow confidential filings to protect the privacy of the plaintiff in cases filed under this section.

Subd. 6. **Liability; exceptions.** (a) No person shall be found liable under this section when:

(1) the dissemination is made for the purpose of a criminal investigation or prosecution that is otherwise lawful;

(2) the dissemination is for the purpose of, or in connection with, the reporting of unlawful conduct;

(3) the dissemination is made in the course of seeking or receiving medical or mental health treatment, and the image is protected from further dissemination;

(4) the deep fake was obtained in a commercial setting for the purpose of the legal sale of goods or services, including the creation of artistic products for sale or display, and the depicted individual knew that a deep fake would be created and disseminated in a commercial setting;

(5) the deep fake relates to a matter of public interest; dissemination serves a lawful public purpose; the person disseminating the deep fake as a matter of public interest clearly identifies that the video recording, motion-picture film, sound recording, electronic image, photograph, or other item is a deep fake; and the person acts in good faith to prevent further dissemination of the deep fake;

(6) the dissemination is for legitimate scientific research or educational purposes, the deep fake is clearly identified as such, and the person acts in good faith to minimize the risk that the deep fake will be further disseminated; or

(7) the dissemination is made for legal proceedings and is consistent with common practice in civil proceedings necessary for the proper functioning of the criminal justice system, or protected by court order which prohibits any further dissemination.

(b) This section does not alter or amend the liabilities and protections granted by United States Code, title 47, section 230, and shall be construed in a manner consistent with federal law.

(c) A cause of action arising under this section does not prevent the use of any other cause of action or remedy available under the law.

Subd. 7. **Jurisdiction.** A court has jurisdiction over a cause of action filed pursuant to this section if the plaintiff or defendant resides in this state.

Subd. 8. **Venue.** A cause of action arising under this section may be filed in either:

(1) the county of residence of the defendant or plaintiff or in the jurisdiction of the plaintiff's designated address if the plaintiff participates in the address confidentiality program established by chapter 5B; or

(2) the county where any deep fake is produced, reproduced, or stored in violation of this section.

Subd. 9. **Discovery of dissemination.** In a civil action brought under subdivision 2, the statute of limitations is tolled until the plaintiff discovers the deep fake has been disseminated.

EFFECTIVE DATE. This section is effective August 1, 2023, and applies to dissemination of a deep fake that takes place on or after that date.

Sec. 2. **[609.771] USE OF DEEP FAKE TECHNOLOGY TO INFLUENCE AN ELECTION.**

Subdivision 1. **Definitions.** (a) As used in this section, the following terms have the meanings given.

(b) "Candidate" means an individual who seeks nomination or election to a federal, statewide, legislative, judicial, or local office including special districts, school districts, towns, home rule charter and statutory cities, and counties.

(c) "Deep fake" means any video recording, motion-picture film, sound recording, electronic image, or photograph, or any technological representation of speech or conduct substantially derivative thereof:

(1) that is so realistic that a reasonable person would believe it depicts speech or conduct of an individual who did not in fact engage in such speech or conduct; and

(2) the production of which was substantially dependent upon technical means, rather than the ability of another individual to physically or verbally impersonate such individual.

(d) "Depicted individual" means an individual in a deep fake who appears to be engaging in speech or conduct in which the individual did not engage.

Subd. 2. **Use of deep fake to influence an election; violation.** A person who disseminates a deep fake or enters into a contract or other agreement to disseminate a deep fake is guilty of a crime and may be sentenced as provided in subdivision 3 if the person knows or reasonably should know that the item being disseminated is a deep fake and dissemination:

(1) takes place within 90 days before an election;

(2) is made without the consent of the depicted individual; and

(3) is made with the intent to injure a candidate or influence the result of an election.

Subd. 3. **Use of deep fake to influence an election; penalty.** A person convicted of violating subdivision 2 may be sentenced as follows:

(1) if the person commits the violation within five years of one or more prior convictions under this section, to imprisonment for not more than five years or to payment of a fine of not more than $10,000, or both;

(2) if the person commits the violation with the intent to cause violence or bodily harm, to imprisonment for not more than one year or to payment of a fine of not more than $3,000, or both; or

(3) in other cases, to imprisonment for not more than 90 days or to payment of a fine of not more than $1,000, or both.

Subd. 4. **Injunctive relief.** A cause of action for injunctive relief may be maintained against any person who is reasonably believed to be about to violate or who is in the course of violating this section by:

(1) the attorney general;

(2) a county attorney or city attorney;

(3) the depicted individual; or

(4) a candidate for nomination or election to a public office who is injured or likely to be injured by dissemination.

EFFECTIVE DATE. This section is effective August 1, 2023, and applies to crimes committed on or after that date.

Sec. 3. **[617.262] NONCONSENSUAL DISSEMINATION OF A DEEP FAKE DEPICTING INTIMATE PARTS OR SEXUAL ACTS.**

Subdivision 1. **Definitions.** (a) For purposes of this section, the following terms have the meanings given.

(b) "Deep fake" means any video recording, motion-picture film, sound recording, electronic image, or photograph, or any technological representation of speech or conduct substantially derivative thereof:

(1) that is so realistic that a reasonable person would believe it depicts speech or conduct of an individual; and

(2) the production of which was substantially dependent upon technical means, rather than the ability of another individual to physically or verbally impersonate such individual.

(c) "Depicted individual" means an individual in a deep fake who appears to be engaging in speech or conduct in which the individual did not engage.

(d) "Dissemination" means distribution to one or more persons, other than the individual depicted in the deep fake, or publication by any publicly available medium.

(e) "Harass" means an act that would cause a substantial adverse effect on the safety, security, or privacy of a reasonable person.

(f) "Intimate parts" means the genitals, pubic area, anus, or partially or fully exposed nipple of an individual.

(g) "Personal information" means any identifier that permits communication or in-person contact with an individual, including:

(1) an individual's first and last name, first initial and last name, first name and last initial, or nickname;

(2) an individual's home, school, or work address;

(3) an individual's telephone number, email address, or social media account information; or

(4) an individual's geolocation data.

(h) "Sexual act" means either sexual contact or sexual penetration.

(i) "Sexual contact" means the intentional touching of intimate parts or intentional touching with seminal fluid or sperm onto another individual's body.

(j) "Sexual penetration" means any of the following acts:

(1) sexual intercourse, cunnilingus, fellatio, or anal intercourse; or

(2) any intrusion, however slight, into the genital or anal openings of an individual by another's body part or an object used by another for this purpose.

(k) "Social media" means any electronic medium, including an interactive computer service, telephone network, or data network, that allows users to create, share, and view user-generated content.

Subd. 2. **Crime.** It is a crime to intentionally disseminate a deep fake when:

(1) the actor knows or reasonably should know that the depicted individual did not consent to the dissemination;

(2) the deep fake realistically depicts any of the following:

(i) the intimate parts of another individual presented as the intimate parts of the depicted individual;

(ii) artificially generated intimate parts presented as the intimate parts of the depicted individual; or

(iii) the depicted individual engaging in a sexual act; and

(3) the depicted individual is identifiable:

(i) from the deep fake itself, by the depicted individual or by another individual; or

(ii) from the personal information displayed in connection with the deep fake.

Subd. 3. **Penalties.** (a) Except as provided in paragraph (b), whoever violates subdivision 2 is guilty of a gross misdemeanor.

(b) Whoever violates subdivision 2 may be sentenced to imprisonment for not more than three years or to payment of a fine of $5,000, or both, if one of the following factors is present:

(1) the depicted individual suffers financial loss due to the dissemination of the deep fake;

(2) the actor disseminates the deep fake with intent to profit from the dissemination;

(3) the actor maintains an Internet website, online service, online application, or mobile application for the purpose of disseminating the deep fake;

(4) the actor posts the deep fake on a website;

(5) the actor disseminates the deep fake with intent to harass the depicted individual;

(6) the actor obtained the deep fake by committing a violation of section 609.52, 609.746, 609.89, or 609.891; or

(7) the actor has previously been convicted under this chapter.

Subd. 3a. **No defense.** It is not a defense to a prosecution under this section that the depicted individual consented to the creation or possession of the deep fake, or the private transmission of the deep fake to an individual other than those to whom the deep fake was disseminated.

Subd. 4. **Venue.** Notwithstanding anything to the contrary in section 627.01, an offense committed under this section may be prosecuted in:

(1) the county where the offense occurred;

(2) the county of residence of the actor or victim or in the jurisdiction of the victim's designated address if the victim participates in the address confidentiality program established by chapter 5B; or

(3) only if venue cannot be located in the counties specified under clause (1) or (2), the county where any deep fake is produced, reproduced, found, stored, received, or possessed in violation of this section.

Subd. 5. **Exemptions.** Subdivision 2 does not apply when:

(1) the dissemination is made for the purpose of a criminal investigation or prosecution that is otherwise lawful;

(2) the dissemination is for the purpose of, or in connection with, the reporting of unlawful conduct;

(3) the dissemination is made in the course of seeking or receiving medical or mental health treatment, and the image is protected from further dissemination;

(4) the deep fake was obtained in a commercial setting for the purpose of the legal sale of goods or services, including the creation of artistic products for sale or display, and the

depicted individual knew, or should have known, that a deep fake would be created and disseminated;

(5) the deep fake relates to a matter of public interest and dissemination serves a lawful public purpose;

(6) the dissemination is for legitimate scientific research or educational purposes; or

(7) the dissemination is made for legal proceedings and is consistent with common practice in civil proceedings necessary for the proper functioning of the criminal justice system, or protected by court order which prohibits any further dissemination.

Subd. 6. **Immunity.** Nothing in this section shall be construed to impose liability upon the following entities solely as a result of content or information provided by another person:

(1) an interactive computer service as defined in United States Code, title 47, section 230, paragraph (f), clause (2);

(2) a provider of public mobile services or private radio services; or

(3) a telecommunications network or broadband provider.

EFFECTIVE DATE. This section is effective August 1, 2023, and applies to crimes committed on or after that date.

ARTICLE 2
AGE-APPROPRIATE DESIGN CODE

Section 1. **[13.6505] ATTORNEY GENERAL DATA CODED ELSEWHERE.**

Subdivision 1. **Scope.** The sections referred to in this section are codified outside this chapter. Those sections classify attorney general data as other than public, place restrictions on access to government data, or involve data sharing.

Subd. 2. **Data protection impact assessments.** A data protection impact assessment collected or maintained by the attorney general under section 325O.04 is classified under section 325O.04, subdivision 4.

Sec. 2. **[325O.01] CITATION; CONSTRUCTION.**

Subdivision 1. **Citation.** This chapter may be cited as the "Minnesota Age-Appropriate Design Code Act."

Subd. 2. **Construction.** (a) A business that develops and provides online services, products, or features that children are likely to access must consider the best interests of children when designing, developing, and providing that online service, product, or feature.

(b) If a conflict arises between commercial interests of a business and the best interests of children likely to access an online product, service, or feature, the business must prioritize the privacy, safety, and well-being of children over the business's commercial interests.

Sec. 3. **[325O.02] DEFINITIONS.**

(a) For purposes of this chapter, the following terms have the meanings given.

(b) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with that other legal entity. For these purposes, "control" or "controlled" means: ownership of or the power to vote more than 50 percent of the outstanding shares of any class of voting security of a company; control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company.

(c) "Business" means:

(1) a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners; and

(2) an affiliate of a business that shares common branding with the business. For purposes of this clause, "common branding" means a shared name, servicemark, or trademark that the average consumer would understand that two or more entities are commonly owned.

For purposes of this chapter, for a joint venture or partnership composed of businesses in which each business has at least a 40 percent interest, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal data in the possession of each business and disclosed to the joint venture or partnership must not be shared with the other business.

(d) "Child" means a consumer who is under 18 years of age.

(e) "Collect" means buying, renting, gathering, obtaining, receiving, or accessing any personal data pertaining to a consumer by any means. This includes receiving data from the consumer, either actively or passively, or by observing the consumer's behavior.

(f) "Consumer" means a natural person who is a Minnesota resident, however identified, including by any unique identifier.

(g) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice.

(h) "Data protection impact assessment" means a systematic survey to assess and mitigate risks to children who are reasonably likely to access the online service, product, or feature that arise from the data management practices of the business.

(i) "Default" means a preselected option adopted by the business for the online service, product, or feature.

(j) "Deidentified" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable natural person, or a device linked to such person, provided that the business that possesses the data:

(1) takes reasonable measures to ensure that the data cannot be associated with a natural person;

(2) publicly commits to maintain and use the data only in a deidentified fashion and not attempt to reidentify the data; and

(3) contractually obligates any recipients of the data to comply with all provisions of this paragraph.

(k) "Likely to be accessed by children" means an online service, product, or feature that it is reasonable to expect would be accessed by children based on any of the following indicators:

(1) the online service, product, or feature is directed to children, as defined by the Children's Online Privacy Protection Act, United States Code, title 15, section 6501 et seq.;

(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 contains 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 clause (2);

(5) the online service, product, or feature has design elements that are known to be of interest to children, including but not limited to 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.

(l) "Online service, product, or feature" does not mean any of the following:

(1) telecommunications service, as defined in United States Code, title 47, section 153;

(2) broadband service, as defined in section 116J.39, subdivision 1; or

(3) the sale, delivery, or use of a physical product.

(m) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. Personal data does not include deidentified data or publicly available information. For purposes of this paragraph, "publicly available information" means information that (1) is lawfully made available from federal, state, or local government records or widely distributed media, and (2) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.

(n) "Precise geolocation" means any 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 1,850 feet, except as prescribed by regulations.

(o) "Process" or "processing" means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(p) "Profiling" means any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(q) "Sale," "sell," or "sold" means the exchange of personal data for monetary or other valuable consideration by a business to a third party. Sale does not include the following:

(1) the disclosure of personal data to a third party who processes the personal data on behalf of the business;

(2) the disclosure of personal data to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer;

(3) the disclosure or transfer of personal data to an affiliate of the business;

(4) the disclosure of data that the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience; or

(5) the disclosure or transfer of personal data to a third party as an asset that is part of a completed or proposed merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business's assets.

(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 data by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

(s) "Third party" means a natural or legal person, public authority, agency, or body other than the consumer or the business.

Sec. 4. **[325O.03] SCOPE; EXCLUSIONS.**

(a) A business is subject to this chapter if the business:

(1) collects consumers' personal data or has consumers' personal data collected on the business's behalf by a third party;

(2) alone or jointly with others, determines the purposes and means of the processing of consumers' personal data;

(3) does business in Minnesota; and

(4) satisfies one or more of the following thresholds:

(i) has annual gross revenues in excess of $25,000,000, as adjusted every odd-numbered year to reflect the Consumer Price Index;

(ii) alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal data of 50,000 or more consumers, households, or devices; or

(iii) derives 50 percent or more of its annual revenues from selling consumers' personal data.

(b) This chapter does not apply to:

(1) protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Code of Federal Regulations, title 45, parts 160 and 164, established pursuant to the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and the Health Information Technology for Economic and Clinical Health Act, Public Law 111-5;

(2) a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Code of Federal Regulations, title 45, parts 160 and 164, established pursuant to the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, 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 clause (1);

(3) 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 or pursuant to human subject protection requirements of the United States Food and Drug Administration; or

(4) a business whose principal business is the origination of journalism, and which has a significant portion of its workforce consisting of professional journalists.

Sec. 5. **[325O.04] BUSINESS OBLIGATIONS.**

Subdivision 1. **Requirements for businesses.** A business that provides an online service, product, or feature likely to be accessed by children must:

(1) before any new online services, products, or features are offered to the public, 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;

(2) biennially review all data protection impact assessments;

(3) document any risk of material detriment to children that arises from the data management practices of the business identified in the data protection impact assessment required by clause (1) and create a timed plan to mitigate or eliminate the risk before the online service, product, or feature is accessed by children;

(4) within five business days of a written request by the attorney general, provide to the attorney general a list of all data protection impact assessments the business has completed;

(5) within seven business days of a written request by the attorney general, provide the attorney general with a copy of any data protection impact assessment;

(6) 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 business or apply the privacy and data protections afforded to children to all consumers;

(7) 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 business can demonstrate a compelling reason that a different setting is in the best interests of children;

(8) provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service, product, or feature;

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

(10) enforce published terms, policies, and community standards established by the business, including but not limited to privacy policies and those concerning children; and

(11) provide prominent, accessible, and responsive tools to help children, or if applicable their parents or guardians, exercise their privacy rights and report concerns.

Subd. 2. **Data protection impact assessments; requirements.** (a) A data protection impact assessment required by this section must:

(1) identify the purpose of the online service, product, or feature; how it uses children's personal data; and the risks of material detriment to children that arise from the data management practices of the business; and

(2) address, to the extent applicable:

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

(ii) 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;

(iii) 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;

(iv) 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, contact on the online product, service, or feature;

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

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

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

(b) A data protection impact assessment conducted by a business for the purpose of compliance with any other law complies with this section if the data protection impact assessment meets the requirements of this chapter.

(c) 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.

Subd. 3. **Prohibitions on businesses.** A business that provides an online service, product, or feature likely to be accessed by children must not:

(1) use the personal data of any child in a way that the business knows, or has reason to know, is materially detrimental to the physical health, mental health, or well-being of a child;

(2) profile a child by default unless both of the following criteria are met:

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

(ii) either of the following is true:

(A) 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 with which a child is actively and knowingly engaged; or

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

(3) collect, sell, share, or retain any personal data that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged, or as described below, unless the business can demonstrate a compelling reason that the collecting, selling, sharing, or retaining of the personal data is in the best interests of children likely to access the online service, product, or feature;

(4) if the end user is a child, use personal data for any reason other than a reason for which that personal data was collected, unless the business can demonstrate a compelling reason that use of the personal data is in the best interests of children;

(5) 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 business 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;

(6) 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;

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

(8) use any personal data collected to estimate age or age range for any purpose other than to fulfill the requirements of subdivision 1, clause (6), or retain that personal data longer than necessary to estimate age. Age assurance must be proportionate to the risks and data practice of an online service, product, or feature.

Subd. 4. **Data practices.** (a) A data protection impact assessment collected or maintained by the attorney general under subdivision 1 is classified as nonpublic data or private data on individuals under section 13.02, subdivisions 9 and 12.

(b) 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 this section does not constitute a waiver of the privilege or protection.

Sec. 6. **[325O.05] ATTORNEY GENERAL ENFORCEMENT.**

(a) A business that violates this chapter may be subject to an injunction and liable for a civil penalty of not more than $2,500 per affected child for each negligent violation, or not more than $7,500 per affected child for each intentional violation, which may be assessed and recovered only in a civil action brought by the attorney general in accordance with section 8.31. If the state prevails in an action to enforce this chapter, the state may, in addition to penalties provided by this paragraph or other remedies provided by law, be allowed an

amount determined by the court to be the reasonable value of all or part of the state's litigation expenses incurred.

(b) Any penalties, fees, and expenses recovered in an action brought under this chapter must be deposited in an account in the special revenue fund and are appropriated to the attorney general to offset costs incurred by the attorney general in connection with enforcement of this chapter.

(c) If a business is in substantial compliance with the requirements of section 325O.04, subdivision 1, clauses (1) to (5), the attorney general must, before initiating a civil action under this section, provide written notice to the business identifying the specific provisions of this chapter that the attorney general alleges have been or are being violated. If, within 90 days of the notice required by this paragraph, the business cures any noticed violation 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 business is not liable for a civil penalty for any violation cured pursuant to this section.

(d) Nothing in this chapter provides a private right of action under this chapter, section 8.31, or any other law.

(e) Nothing in this chapter may be interpreted to impose liability in a manner that is inconsistent with United States Code, title 47, section 230, or otherwise infringe on the established rights and freedoms of children.

Sec. 7. **AGE-APPROPRIATE DESIGN; ATTORNEY GENERAL.**

$142,000 in fiscal year 2024 and $142,000 in fiscal year 2025 are appropriated from the general fund to the attorney general to enforce the Minnesota Age-Appropriate Design Code Act.

Sec. 8. **EFFECTIVE DATE.**

(a) Sections 1 to 6 are effective July 1, 2024.

(b) By July 1, 2025, and as required by section 5, a business must complete a data protection impact assessment for any online service, product, or feature likely to be accessed by children offered to the public before July 1, 2024, unless that online service, product, or feature is exempt under paragraph (c).

(c) Sections 2 to 6 do not apply to an online service, product, or feature that is not offered to the public on or after July 1, 2024."

Delete the title and insert:

"A bill for an act

relating to data privacy; addressing individual privacy rights regarding the dissemination of fake content and images; providing for the Minnesota Age-Appropriate Design Code Act; providing for penalties; appropriating money; proposing coding for new law in Minnesota Statutes, chapters 13; 604; 609; 617; proposing coding for new law as Minnesota Statutes, chapter 325O."