January 11, 2024

The Honorable Bonnie Westlin
Legislative Commission on Data Practices
658 Cedar St.
St. Paul, MN 55155

Re: In support of the Age-Appropriate Design Code Act (SF 2810)

Dear Chair Westlin,

For over 25 years, I served founders and venture capitalists in Minnesota as a trusted financial and investment advisor. In developing those confided relationships, I mentored senior executives, sitting alongside them, guiding product design, business strategy, and often personal leadership choices. These experiences provided insights into how companies create great client, customer, and user-focused products and services. Leading businesses excel in addressing their customers' existing problems and anticipating future needs, guiding them through a collaborative journey toward effective solutions with open and transparent communication. These businesses prioritize understanding and fulfilling the Best Interests of the Customer.

This background is critical because the Minnesota Age-Appropriate Design Code (MN AADC) provides a beneficial framework for businesses to conceptualize building Artificially Intelligent, Algorithmic, and Autonomous (AAA) based online products and services that help, rather than harm, consumers. The MN AADC has the potential to guide companies in creating human-centric innovations that focus on solving customer problems. I will expand on this potential later.

With the proper perspective, businesses can see the MN AADC as enabling ethical AI-based design that creates value for both companies and users and, through that very relationship, for the State of Minnesota.

During my role as a Fellow at ForHumanity, a non-profit civil society organization dedicated to addressing risks associated with Ethics, Bias, Privacy, Trust, and Cybersecurity in Artificial Intelligence, Algorithmic, and Autonomous (AAA) Systems, I serve as a vital member of the Priority Drafting Team. We drafted AI audit certification schemes for various international laws, including GDPR, GDPR Children's Code, the EU AI Act, the Digital Services Act, the California Consumer Protection Act, and California's AADC. We ensure a harmonized set of criteria, allowing compliance with one to equate to compliance with all.

Our approach involves an engineering-oriented translation of legal principles into business language, facilitating practical implementation. The certification scheme provides a binary (compliant/ non-compliant) set of criteria establishing the basis for independent third-party audits of AAA Systems.
Through this unique set of experiences, I submit this testimony to you in full support of the Minnesota Age-Appropriate Design Code.

The Minnesota Age-Appropriate Design Code (MN AADC) is not merely a regulatory framework but a pro-business strategy. This code stands at the intersection of consumer protection, particularly for vulnerable populations like children, and the development of robust, user-focused businesses that cater to the diverse needs of all stakeholders in Minnesota.

The MN AADC offers competitive advantages for businesses in our state. Implementing the MN AADC positions the state as a hub for innovation and ethical technology practices. Adhering to age-appropriate design principles, businesses gain a competitive edge by showcasing a commitment to user well-being, privacy, and responsible data processing. This approach aligns with evolving consumer expectations and sets a high standard for industry leaders.

The MN AADC, as a pro-business plan, fosters an environment where companies are compliant and leaders in ethical technology. It encourages innovation in product and service development while safeguarding vulnerable populations' interests, notably children. This duality creates a win-win scenario, enhancing Minnesota's reputation as a hub for technologically advanced, ethically responsible businesses.

At its core, the MN AADC champions a user-centric paradigm. By placing the needs and safety of users, especially children, at the forefront, businesses are prompted to design products and services that align with ethical standards. This enhances user trust and contributes to the development of a digital ecosystem where all stakeholders feel valued and protected.

User-centricity, as the MN AADC promotes, goes beyond compliance; it becomes a guiding principle for business operations. By fostering a culture that prioritizes the well-being of users, businesses not only fulfill their ethical obligations but also create a loyal customer base. This approach establishes a positive feedback loop, where satisfied users contribute to the growth and success of businesses committed to user-centric values.

The MN AADC represents a tremendous opportunity to take a balanced approach, for it will skew innovation in a positive upward trajectory, mitigating harms through demonstrated risk management frameworks. It is the catalyst that is good for business and a testament to a user-centric ethos. Embracing this code positions Minnesota as a pioneer in ethical technology practices, offering a unique and attractive proposition for businesses looking to thrive in an environment that values consumer protection and entrepreneurial growth.[1]

---

[1] It ensures protections like privacy by default, minimization of data collection, and transparency of automated systems. Children deserve a developmentally appropriate online experience free from exploitation. The MN AADC delivers guardrails to prevent harm.
Far from a tradeoff, the MN AADC demonstrates synergistic policymaking. Ethical digital experiences create value for both businesses and users. Minnesota has an opportunity to lead in stimulating flourishing, human-centric innovation. The MN AADC points the way forward.

It is imperative to clarify that the challenges presented in the California Courts by NetChoice, the lobbying organization for Big Tech, do not revolve around the First Amendment. Section 230 protects them from user-generated content, but it's crucial to recognize that The First Amendment has exemptions for unprotected speech.

The focus of MN AADC is not on speech or content. Instead, it centers on the methodology employed by platforms and businesses in *designing their platforms* that, in turn, deliver content, collect, and process data from vulnerable populations, and potentially influence users into actions contrary to their best interests. AADC addresses the intricate use of artificial intelligence, algorithms, and autonomous systems.

Regrettably, many businesses overlook the crucial step of understanding how their AAA Systems deliver content, recommendations, or user interactions. This step, akin to a Data Protection Impact Assessment, is fundamental.

Business leaders continue to advocate for self-regulation for data practices and AAA Systems that interact with children, including how they use speech legally. However, a notable example is Meta (formerly Facebook), which, despite internal research revealing how its content delivery systems caused harm to users under 18, chose not to alter its algorithms.

The inability of Big Tech to self-regulate is underscored by a case brought forth by 33 State Attorneys General against Meta, outlining specific internal documents, communications, and business actions. These instances serve as tangible proof, emphasizing the need for frameworks like the AADC to address ethical dimensions in content delivery and user interactions.

The following Appendix delves into the intricacies of the NetChoice vs. Bonta case, providing a comprehensive analysis and response to each of the ten sections. As we navigate the legal complexities, we must ground our understanding in the principles championed by ForHumanity. At its core, ForHumanity advocates for transparency through AI Audits. This ensures that businesses are accountable for their digital interactions with children.

The information in the Appendix scrutinizes the legal arguments and illuminates the inherent tensions between business interests and the imperative to safeguard children's digital experiences. As we explore each facet of the case, let us remember the symbiosis between innovation, commerce, and consumer protection that forms the bedrock of a digitally inclusive and secure future.

In close, while NetChoice attempts to characterize data restrictions as infringing on free speech, this claim does not withstand scrutiny. The MN AADC does not limit what businesses can say or display to children. Instead, it reasonably protects how children's personal data is collected and used behind the scenes.

Companies remain free to curate any lawful content and offer any services to children. However, they cannot exploit excessive data collection and opaque, unauthorized uses to enable dangerous targeting. Speech is not the concern - unethical data practices are.

Additionally, personal data collection and sharing extends far beyond speech protections. Reasonable regulation of data practices that enable manipulation and harm does not equate to suppressing speech.

The MN AADC strikes a fair balance between protecting children and preserving innovative services. Companies willing to justify how their data practices benefit kids can still thrive under the Act. Those relying on unchecked exploitation of children's data to turn profits should face limitations.

While no legislation is perfect, the MN AADC offers a thoughtful framework to align incentives and ethics. Some refinements may be beneficial, but data protections for children are vital. I urge upholding core safeguards while working in good faith to address concrete impacts on valuable innovation. Protecting the most vulnerable among us should be the top priority as technology rapidly evolves.

I respectfully ask the Data Practices Commission to recommend the passage of the SF 2810 in the 2024 Legislative Session.

Sincerely,

Jeffrey Kluge
CEO & Founder Holistic Ethics, LLC, and Creator of KidsTechEthics
5004 15th Ave South
Minneapolis, MN 55417
612-406-9525

APPENDIX

ANALYSIS & RECOMMENDATIONS ON THE TEN SECTIONS IN THE CA AADC

1. **The Dual Value of DPIA - Pro-Business and Pro-Child**

   The debate surrounding CAADCA's DPIA report requirement brings to light a nuanced discussion on its effectiveness, touching upon its potential benefits and perceived shortcomings. While the court raises valid concerns about its current implementation, it's crucial to recognize the inherent value that a well-crafted DPIA process can bring, acting as a catalyst for positive change in both business practices and child protection.

   Proactive Business Accountability

   The DPIA is a proactive tool that compels businesses to contemplate the potential impact of their online products or services, particularly on children. This foresight is invaluable, preventing reactive measures that often follow incidents of harm. By mandating businesses to assess and address potential risks in their design phase, the DPIA encourages a culture of responsibility and accountability.

   User-Centric Awareness

   The primary strength of the Child-Centric DPIA lies in its capacity to cultivate awareness within businesses regarding their users, particularly children. By mandating a thoughtful examination of how a business's AAA System is intended to operate and impact users, it serves as a compass for aligning digital products and services with children's unique needs, vulnerabilities, and rights.

   Mitigating Risks and Ensuring Child Safety

   The State rightly emphasizes the importance of making companies think ahead about how their products use children's data and whether their designs could pose risks. Drawing attention to past incidents, such as Snapchat's speed filter leading to reckless driving by teens, highlights the real-world consequences of overlooking potential harms in digital product design. A robust DPIA process can be a preemptive measure to identify and mitigate such risks, contributing to enhanced child safety.

   Use of the Data Protection Impact Assessment

   This framework extends beyond a mere checkbox exercise, evolving into a tool for comprehensive impact assessment. It prompts businesses to contemplate their designs' potential implications on children's well-being. This includes foreseeing and mitigating content, interactions, and data processing risks, contributing to a safer online environment for the youngest users.

Accountability Through Traceability

While the court rightly critiques the lack of immediate accountability in the current DPIA framework, it is essential to recognize the long-term accountability it establishes. The DPIA becomes a documented record of the discussions and decisions made during the design phase. In the event of harms occurring, this traceability serves as evidence, holding businesses accountable for their awareness of potential risks and their decisions not to address them adequately.

Streamlined Process

Contrary to the misconception that DPIAs must be extensive and resource-intensive, the Child-Centric DPIA framework is designed for practicality. Recognizing that businesses may have budgetary constraints, the framework offers a streamlined approach, ensuring the process remains cost-effective and accessible. This makes it a valuable resource for businesses of varying sizes and capacities.

Child-Centric DPIA Framework

Addressing concerns about the DPIA's approachability and effectiveness, initiatives like the one my firm created of KidsTechEthics developed a child-centric DPIA framework. These frameworks, rooted in the guidance from the UK GDPR Children's Code, the CA AADC, and hence MN AADC, provide businesses with a structured and accessible way to conduct assessments specifically tailored to U18 products and services. This ensures that businesses not only engage in the DPIA process but do so in a manner that aligns with the unique considerations of child-centric design.

Recommendations for Responsible Processing

Central to the framework is the inclusion of clear and actionable recommendations for responsible data processing. Instead of imposing stringent rules, it encourages businesses to adopt best practices and ethical considerations. This flexibility ensures businesses retain the freedom to innovate while upholding the fundamental principles of child-centric design.

Holistic Approach to Interaction

The Child-Centric DPIA framework transcends a narrow focus on data handling. It delves into how a business intends its AAA System to interact with its users. This holistic approach ensures that businesses not only address data privacy concerns but also consider the broader impact of their designs on children's digital experiences.

While the California court rightly demands efficacy in addressing potential harms, it is essential to recognize the dual value of DPIA—a mechanism that not only fosters responsible business practices but also acts as a proactive measure for child protection. Instead of dismissing the DPIA outright, there is an opportunity to refine and optimize its implementation to strike the delicate balance between business innovation and the paramount goal of safeguarding children in the digital landscape.

2. Balancing Age Estimation: Striking Privacy and Protection Equilibrium

Age Estimation rule underscores the delicate balance between privacy considerations and the imperative to shield children from potentially harmful content online. The State of California asserts that this rule is a pivotal measure to safeguard children, urging companies to either ascertain the age of their users or treat everyone as children concerning data protection. Conversely, NetChoice contends that this rule may inadvertently compromise user privacy by necessitating additional data collection.

The State's Perspective

The State posits that CAADCA's Age Estimation rule is a commendable effort to fortify children's online privacy. By encouraging companies to tailor their data protection measures based on user age, the rule aims to provide extra privacy safeguards for children. The intention is to create a digital environment where minors are shielded from potentially harmful content, aligning with the broader goals of the CAADCA.

Potential Concern for Businesses

The contention is that the defense's concerns about burdens on small businesses may be unfounded, given the exemption for businesses with revenue under $25 million. Additionally, the assertion that estimating age requires more data is misleading. Services and tools exist that can verify age with less data.

NetChoice's Challenge

NetChoice raises valid concerns about potential privacy invasions arising from age estimation practices. They argue that attempting to estimate a user's age could inadvertently lead to more extensive data collection, presenting privacy risks. This perspective emphasizes the need for careful consideration of the unintended consequences that may arise from implementing age estimation mechanisms.

Judicial Scrutiny

In assessing the rule's validity, the judge demands that the government demonstrates its efficacy in addressing the issues it seeks to resolve. The judge questions the practicality of age estimation, expressing reservations about its impact. There are apprehensions that estimating age might lead companies to request additional personal information, potentially infringing on user privacy rights.

The Role of DPIA

The DPIA is highlighted here as a pivotal tool in adequately applying the Age Estimation rule. It highlights the exemption for small businesses, the process of conducting a DPIA to determine user demographics, and the potential consequences for businesses neglecting this process. The example of Meta's internal research on Instagram serves as a cautionary tale, emphasizing the importance of assessing and mitigating potential harm.

Age Estimation rule's viability hinges on its ability to strike a nuanced balance between privacy considerations and the protection of children. The incorporation of DPIAs, as suggested, adds a layer of accountability and responsibility for businesses in navigating this delicate equilibrium. The ongoing debate serves as a testament to the intricacies of crafting regulations that genuinely contribute to the safety of children online without unduly compromising user privacy.

For an industry that prides itself on innovation, saying age estimation is too hard is disingenuous.

3. CAADCA's High Default Privacy Settings

High Default Privacy Settings emphasizes the pivotal role default settings hold in safeguarding children online. The rule mandates companies establish high privacy settings by default for children unless there are compelling reasons not to do so.

State's Perspective

California strongly supports this regulation, emphasizing that strict default settings are crucial to shielding kids from potential online harm. They argue that lower privacy settings could expose children to inappropriate content or solicitations from strangers, highlighting the risks of unsolicited messages. The state contends that the rule's primary purpose is to protect children from the potential harms of lax default privacy settings, aiming to create a safer online environment for minors.

Potential Concern for Businesses:

The central concern revolves around high privacy settings, primarily concerning data collection and processing rather than restricting content visibility. The argument emphasizes the importance of a duty of care businesses should uphold, particularly when dealing with vulnerable populations. These are highly trainable and detailed models, and to operate them without understanding the impact is negligent. Drawing an analogy with historical restrictions on cigarette ads to children highlights the relevance of regulating content exposure to specific demographics for the greater public welfare.

NetChoice's Challenge

NetChoice, opposing the rule, raises a concern about the uncertainty surrounding its application. The group argues that this lack of clarity might prompt some companies to block kids from accessing their services altogether, fearing unintentional rule violations. For instance, news websites might restrict access to avoid potential legal complications.

Judicial Skepticism

The judge, delving into the intricacies of the rule, expresses skepticism regarding its lack of clarity. The concern is that the uncertainty may lead companies to overzealously restrict access for children to comply with the rule, potentially impeding free speech, particularly in the case of news content. The judge acknowledges the State's point, recognizing the potential harm that can befall children with lower privacy settings. However, a critical issue emerges—the lack of clarity in the rule regarding whether it applies exclusively to accounts created by

kids or extends to any child visiting a website run by a covered business. This ambiguity becomes the crux of the debate.

Analysis

The debate over High Default Privacy Settings encapsulates the challenge of crafting regulations that balance child protection with the preservation of free speech. The judge's concerns about the rule's clarity and potential unintended consequences emphasize the need for nuanced legislation addressing the digital landscape's intricacies while safeguarding fundamental rights.

The opposing arguments skillfully divert attention from the core issue. Websites and apps extensively employ tools like cookies, pixels, and other behavior-based trackers that intricately monitor, drive targeted advertisements, and suggest personalized content. The fundamental conflict arises in the business model of these expansive platforms, where processing user data and advertising to specific demographics are key revenue generators.

Many contemporary websites provide privacy opt-ins and cookie preference acknowledgments upon entry. Individuals are given a choice at the point of entry, deciding whether to proceed and specifying their preferences.

4. CAADCA's Age-Appropriate Policy Language

The Age-Appropriate Policy Language rule mandates companies to articulate their privacy policies, terms of service, and community standards in language accessible to children. The government underscores the importance of this regulation in empowering children to make informed decisions about the online services they use.

State's Perspective

The government argues that the rule is a crucial step in addressing the current problem with businesses crafting privacy policies that are often convoluted and challenging for the general public, especially children, to comprehend. The objective is to enhance transparency and enable children to understand the terms under which they engage with online platforms.

Potential Concern for Businesses

In opposing this rule, businesses express fear of the risk of potential fines if their policies are not sufficiently clear for every child to understand. They contend that the law lacks clarity, fostering concerns about possible content censorship. Businesses worry that the ambiguous nature of the law might prompt them to modify their policies in ways that could inadvertently make it more challenging for children to comprehend.

NetChoice's Argument

NetChoice, opposing the rule, contends that the State hasn't demonstrated that the Age-Appropriate Policy Language rule is the most effective means of addressing the issue. The judge points out that the evidence presented by the State doesn't conclusively prove that

children struggle to understand privacy policies. The judge questions whether this rule is the most apt solution to the problem.

Judicial Scrutiny

The court acknowledges the government's concerns about the opaque nature of existing privacy policies. However, it raises a crucial point—the lack of clarity in the law itself. The court notes that while the government has identified a real problem with the current state of privacy policies, the law's ambiguity raises concerns about its enforceability and potential chilling effects on speech.

Analysis

This underscores the importance of having clear and easily understandable privacy policies, challenging the argument that such a requirement places an undue burden on businesses. A comparative analysis[2] of privacy policies from major companies reveals the widespread issue of using complex language in these documents. Recommending the utilization of technology, including AI systems, to simplify policy language, this approach benefits children and encourages adults to read and comprehend the policies to which they agree.

In conclusion, the discourse on Age-Appropriate Policy Language delves into the delicate balance between regulatory clarity and the genuine necessity for easily understandable privacy policies. The judge's reservations regarding the rule's effectiveness and potential implications for free speech underscore the intricate nature of navigating this intersection.

5. CAADCA's Internal Policy Enforcement

Internal Policy Enforcement rule mandates companies to ensure compliance with their own rules and Codes of Conduct, including privacy policies and guidelines for children.

State's Perspective

The government emphasizes the importance of the Internal Policy Enforcement rule in fostering consumer trust. They argue that ensuring businesses follow their own rules, especially regarding privacy and children, is vital for consumers to make informed decisions about using online services.

Potential Concern for Businesses

Businesses raise concerns about the lack of clarity in the law, fearing potential fines if their enforcement of policies doesn't align with government expectations. They argue that the

[2] https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html "We Read 150 Privacy Policies. They Were an Incomprehensible Disaster." By Kevin Litman-Navarro

rule's vagueness might lead to unintended consequences, including potential content censorship.

NetChoice's Argument

NetChoice contends that the State hasn't proven the necessity of this rule, especially in the context of free speech. The judge critiques the rule's lack of specificity, pointing out that it applies to a wide range of company rules, not just those related to children or privacy. The judge suggests that this broad application could force businesses into content-related decisions contrary to their platform's ethos.

Judicial Scrutiny

The court acknowledges the government's intention to build consumer trust. However, it raises valid concerns. According to the court, the government fails to demonstrate a direct link between a business not adhering to its rules and harm to children. The judge points out the rule's broad scope, encompassing various company policies, potentially forcing businesses into decisions that conflict with their content standards.

Analysis

NetChoice, representing some of the largest and most profitable technology businesses, contends that their industries' internal privacy policies and codes of conduct are challenging to navigate. The law does not prescribe the specific content of these policies but mandates their existence and the subsequent enforcement of consequences.

The State firmly opposes NetChoice's stance, expressing frustration at what appears to be an attempt to evade consequences for failing to adhere to self-imposed rules. Our analysis emphasizes the accountability void technology companies have enjoyed for an extended period. The argument underscores the necessity for businesses to engage in exercises like DPIAs to assess potential harm to users and advocates for holding them accountable for the policies they create. This should not be a big lift.

The Internal Policy Enforcement rule emerges as a battleground where the government seeks to establish trust, businesses seek clarity, and the court scrutinizes the potential implications of the rule. The debate transcends legalities to encompass ethical considerations, demanding accountability for the societal impacts of products and services.

6. CAADCA's Knowingly Harmful Use of Children's Data

Prohibiting businesses from knowingly using children's personal information in ways that could be materially detrimental to their physical health, mental health, or well-being. The conversation highlights concern about the broadness of the rule and its potential impact on speech.

State's Perspective

CAADCA prohibits businesses from using a child's personal information in ways they know or have reason to believe could be materially detrimental to the child's well-being. The law

doesn't precisely define what constitutes "materially detrimental," and it considers anyone under 18 as a child.

NetChoice's Challenge

NetChoice raises concerns that the rule's lack of clarity could lead businesses to bar all children from their online services rather than navigating the complexity of determining what is harmful for each age. According to NetChoice, this would impose a substantial burden on speech, surpassing what is necessary to serve the government's legitimate interests.

Judicial Scrutiny

The judge draws a parallel with a precedent case (ACLU v. Mukasey) that dealt with a rule designed to prevent harmful material from reaching minors. In that instance, the court deemed the rule overly broad and challenging to interpret, posing a risk of potential overreach. Insufficient reliance on companies to verify users' age was also a notable concern.

Applying the lessons learned from the past case, the judge expresses reservations about CAADCA's rule. The ambiguity surrounding "materially detrimental" and the broad classification of anyone under 18 as a child raises significant apprehensions. The judge is concerned that businesses might choose a blanket restriction on everyone under 18, potentially hindering access to services. In the judge's view, this could represent an overreach impacting more speech than necessary.

Analysis

Once again, opponents intertwine free speech into a point designed around processing personal data and delivering content. A well-structured business approach would involve three essential committees: an Ethics Committee, an Algorithmic Risk Committee, and a Child Data Oversight Committee. While the concept of three committees may seem overwhelming, it's essential to recognize that they serve distinct yet interrelated functions. For example, a DPIA, if completed, would provide the business with a comprehensive understanding of its delivery algorithms, revealing how recommendations are designed based on user activity. Dismissing this as too challenging overlooks the intrinsic value of understanding data processing outcomes, especially concerning content that could harm children.

This section emphasizes the intimate nature of the process, which considers many data points tailored to the user's activity. Big Tech claims that such evaluation is too hard, disregarding the importance of responsibly managing data processing and the consequential delivery of material, especially when it could harm children.

One element of this section links back to having completed a DPIA. If a business assessed how it used a subject's data and how it aligned with ethical considerations, it could foster a more responsible and informed approach to content delivery.

The second element of this section involves insights from the field of child psychology. Numerous studies, particularly those conducted by Meta's internal research teams and cited in the Bonta vs. Meta case in CA courts, supported by Minnesota's Attorney General and 31 additional Attorneys General, provide a substantial foundation. These studies shed light on purposeful behavior and create a compelling argument for the necessity of implementing guardrails, reinforcing the demand for responsible practices in the technology sector.

7. Profiling Children by Default

NetChoice's opposition to the California Age-Appropriate Design Code Act reveals contradictions undermining its credibility. On the one hand, they argue certain provisions like age estimation are too broad, violating privacy. Yet they also say definitions like "likely accessed by children" are too narrow, excluding services popular with kids. They can't have it both ways.

Similarly, NetChoice claims terms like "materially detrimental" are too vague, forcing businesses to over-censor. But they also argue profiling restrictions are too specific, preventing beneficial targeting. Again, this is an inherent inconsistency.

The truth is that NetChoice opposes any regulation, regardless of approach. They latch onto isolated micro-issues without acknowledging the Act's careful balance between flexibility and protection. Provisions like requiring child development expert consultation and data protection assessments are tailored solutions for the concerns raised.

California, as does Minnesota, has a compelling, urgent interest in protecting children online. The AADC is a narrow, measured approach to address demonstrated harms from platforms optimizing for youth engagement without regard for a child's well-being. Doing nothing poses serious risks to kids' privacy, health, and safety.

Reasonable refinements are always possible and should be considered in earnest. But hollow arguments seeking outright rejection reveal an unwillingness to take responsibility. Technology companies cannot be allowed to disregard internal research and continue conducting dangerous social experiments on children.

The AADC provides a thoughtful framework to align business incentives with ethical obligations. Children deserve no less from the digital environments shaping their development. I urge Minnesota to lead where California has pioneered, upholding child-centric design principles in law.

8 & 9. Restriction on Collecting, Selling, Sharing, and Retaining Children's Data (CAADCA § 31(b)(3)) and Unauthorized Use of Children's Personal Information (CAADCA § 31(b)(4))

Once again, NetChoice reveals contradictions in challenging the AADC's reasonable data restrictions. They argue that profiling limits are too broad, yet data collection/sharing restrictions are too narrow. They claim addressing harms requires more evidence but ignore research from the companies they represent, which document the harms that the MN AADC could prevent.

Let's be clear - excessive, unconstrained data practices enable the dangerous targeting and manipulation of children for profit. Limiting collection and unauthorized uses beyond necessities directly responds to business models exploiting youth vulnerability.

Of course, beneficial uses exist, which the AADC permits when compelling justification demonstrates serving children's interests. The business simply needs to state that reasoning in a DPIA. This careful balance allows protection while still enabling innovation. Companies unwilling to provide such justification prioritize their goals over kids' well-being.

Some refinements could strengthen safeguards while enabling more beneficial applications. But rejecting core protections is an abdication of ethical responsibility. Businesses focused on child-centric design should view the AADC as an opportunity to build trust through transparency and restraint.

Parents rightfully demand to know how their children's data is used. The AADC empowers companies to earn that trust. I urge lawmakers to stand firm against specious arguments and fearmongering. Thoughtful, nuanced legislation demonstrates your commitment to children's safety and digital rights. The path forward is industry collaboration to address real harms, not obstruction.

10. Use of Dark Patterns (CAADCA § 31(b)(7))

Harms Caused by Dark Patterns: Dark patterns, deceptive design choices deliberately crafted to manipulate users, have far-reaching implications for children in the digital landscape. These manipulative tactics can result in a range of harms, including:

1. Deceptive Advertising: Dark patterns can trick children into engaging with ads or making purchases without understanding the consequences, leading to financial harm for children and their parents.
2. Privacy Concerns: Dark patterns may encourage children to divulge more personal information than necessary, risking their privacy. This information can be exploited for targeted advertising or other potentially harmful purposes.
3. Exposure to Inappropriate Content: Dark patterns might guide children towards inappropriate or age-inappropriate content, negatively affecting their emotional well-being and exposing them to content unsuitable for their age.

4. Addictive Design: Dark patterns can create addictive user experiences, encouraging excessive screen time and interfering with offline activities, including schoolwork, physical activity, and real-world social interactions.
5. Online Harassment and Bullying: The use of dark patterns can contribute to an environment conducive to online harassment and bullying, as children may be manipulated into participating in harmful online behavior or become victims themselves.
6. Unhealthy Online Habits: Dark patterns may lead children to develop unhealthy online habits, such as constant social media checking and prioritizing online interactions over real-world relationships.
7. Impact on Mental Health: Constant exposure to manipulative design can contribute to stress, anxiety, and other mental health issues in children. The pressure to conform to online norms and the fear of missing out (FOMO) can be exacerbated by dark patterns.
8. Educational Impacts: Dark patterns in educational apps or platforms can hinder the learning experience for children, leading to confusion, frustration, and a lack of trust in digital learning environments.

Reasoning Behind CAADCA § 31(b)(7)

The inclusion of CAADCA § 31(b)(7), which prohibits the use of dark patterns to encourage harmful actions by children, is rooted in a commitment to protecting the well-being of our youth in an ever-evolving digital landscape. The reasoning behind this provision is threefold:

1. Preventing Deceptive Practices: Dark patterns are deceptive by design, often leading children to unintended and potentially harmful actions. This provision seeks to curb such deceptive practices that exploit the vulnerability of children.
2. Safeguarding Privacy: CAADCA aims to protect children's personal information from misuse and exploitation by prohibiting dark patterns that encourage children to forego privacy protections.
3. Ensuring Children's Well-being: The provision prohibits dark patterns that the business knows or has reason to know are materially detrimental to the child's well-being. This is a crucial measure to prevent actions that could harm children physically, mentally, or emotionally.

Solutions and Benefits for Children

CAADCA § 31(b)(7) offers a robust solution to mitigate the harms posed by dark patterns. The benefits for children are substantial:

1. Privacy Protection: The provision ensures that children's personal information is safeguarded by preventing dark patterns that encourage the unnecessary disclosure of sensitive data.
2. Promoting Healthy Online Habits: By prohibiting dark patterns that contribute to addictive online experiences, CAADCA encourages the development of healthier online habits, striking a balance between digital engagement and other aspects of a child's life.
3. Enhanced Educational Experiences: In the context of educational apps, the prohibition of dark patterns can improve children's learning experiences, fostering an environment of trust and reliability in digital educational tools.

4. Mental Health Safeguards: CAADCA § 31(b)(7) acts as a protective measure against dark patterns that may contribute to stress, anxiety, and other mental health issues in children, promoting a more positive online environment.

In conclusion, CAADCA § 31(b)(7) serves as a crucial component of a comprehensive framework aimed at protecting the well-being of children in the digital age. By addressing the deceptive and manipulative practices inherent in dark patterns, this provision upholds the fundamental right of children to a safe, secure, and positive online experience.

As we navigate the intricate landscape of child-centric digital design, CAADCA stands as a beacon, providing a thoughtful and measured approach to ensuring our children can explore, learn, and engage online without falling victim to deceptive practices.