5RIGHTS FOUNDATION

The Minnesota Age Appropriate Design Code

Minnesota State Representative Kristin Bahner (DFL) has introduced the ***Minnesota Age Appropriate Design Code Bill*** to offer privacy and safety to Minnesota children online. With this Bill, Minnesota has the chance to lead the way in making the digital world safe for American children. Data protection for children radically changes the way digital companies engage with children and offers them privacy and safety by design.

The Bill is practicable and realistic, drawing on the UK's Age Appropriate Design Code (AADC) and subsequent law and regulation internationally.

This short note provides frequently raised concerns and responses.

MN AADC: Carefully crafted to avoid constitutional and pre-emption pitfalls

In 2022, the California legislature adopted a new law that represents a paradigm shift in terms of tech regulation. The California Age Appropriate Design Code (CA AADC), modeled after a substantially similar law in the United Kingdom, demands that big tech bears some responsibility for the harms online platforms cause children and teenagers.

Of the more than 30 bills pending in state legislatures across the country that seek to address online harms facing children and teenagers, the AADC represents the most carefully calibrated framework that considers competing interests and legal principles. The law was designed specifically with what states could legally regulate in mind, and the distinction between federal and state responsibilities.

NetChoice, representing the Big Tech lobby, recently filed a lawsuit seeking to prevent the CA AADC from taking effect. Tech's legal arguments are tired, old arguments they have used elsewhere and are not applicable here.

- **The AADC is a data protection bill, not a content moderation bill, and does not violate the First Amendment**

  First, the lawsuit contends that the CA AADC violates the First Amendment. NetChoice argues that several provisions of the Bill constitute a "prior restraint on speech" – in other words, these provisions allow the government to prohibit speech or other expression before it happens. The truth is that the bill does not dictate, or even discuss, anything about third-party content companies should put up or take down - it incentivizes heightened safety and privacy for kids upstream, by requiring high default privacy settings at the point of design. To the extent the law implicates content on platforms, it does so in a permissible content-neutral manner, not based on any particular viewpoint.

  For example, the lawsuit complains that the CA AADC requires that companies implement their own content moderation rules. However, it is the companies themselves that decide whether to have those rules, if any, and what they contain. This type of content-neutral law does not violate the First Amendment.

- **The AADC does not violate Section 230 of the Communications and Decency Act**

  Second, as for the lawsuit's contention that the CA AADC would be preempted by federal law, specifically Section 230 of the Communications and Decency Act, even Google's counsel in the recent hearing for the Supreme Court case *Google v. Gonzalez* conceded that although Section 230 gives platforms immunity from lawsuits about third party content they host, it does not immunize them from harms

flowing from their own choices. This is precisely why the CA AADC focuses squarely on things within platform control, such as algorithmic design, prioritization mechanisms, and personal data collection and use. It smartly encourages platforms to make data management choices that prioritize privacy and safety over wringing out every possible dollar of profit regardless of the social cost--all based on things the platforms can control. It thus is not preempted by Section 230.

- **The AADC uses common legal terms and concepts, ensuring that the bill is not unconstitutionally vague or overbroad**

  Third, the lawsuit contends that the CA AADC is both overbroad and impermissibly vague. As examples of this contention, the lawsuit points to words in the statute such as "material," "reasonable to expect," "compelling," and "substantially similar", among others. Each of these terms are widely used legal terms of art frequently found in statute and case law, and readily interpreted by courts and businesses alike. The lawsuit specifically alleges that the term "likely to be accessed" is unconstitutionally vague, and argues that the five factors for consideration are "ambiguous". Far from being ambiguous, the five factors require an AG or court to consider, given the totality of the circumstances, whether a business falls within the scope of the bill. A totality of the circumstances analysis to determine the application of a law is regularly employed when a one-size-fits all statute is inappropriate. In the case of the internet with it's diversity of sites, apps, businesses, consumers, and online products, a one-size-fits all approach does not adequately address harms youth are experiencing online.

  For example, NetChoice argues that "routinely accessed by a significant number of children" is vague. But assigning a percentage of children to that particular factor would ignore the fact that children regularly visit sites of vastly different sizes. For example, YouTube has monthly viewership over 2 billion users, and 81% of American parents with children under the age of 11 claim their children watch YouTube. Compare these numbers with Napaautoparts.com, which is surely visited by 16-18 year olds with an interest in repairing their cars. Napa, however, has a monthly viewership of approximately 522,000. 1% of Napa's viewership is 5,200 users, whereas 1% of YouTube's is 20 million. Thus, it is not hard to see how using a hard percentage to determine the bill's scope would bring in smaller businesses that reasonable minds could agree are not likely to be routinely accessed by a significant number of children, while also excluding sites that exploit millions of children's data regularly. Further, using a gross number does not take into account smaller sites that are regularly visited by children and use children's information in particularly disturbing ways, such as pro-suicide or pro-anorexia sites.

MN AADC: Privacy and Age Assurance

The AADC creates an age estimation requirement that is based on the risk a platform's data management practices present to youth using the online product. Some of common misconceptions about age estimation are addressed below.

- **Contrary to industry arguments, the MN AADC will improve privacy for youth online**

  The MN Age Appropriate Design Code (AADC) is drafted to improve the privacy of young Minnesotans. For example, the MN AADC requires that companies:

  - Make their privacy notices 'plain speak' and easy to read, so that young users (and parents) understand what they do and can make better decisions about which apps and websites to use.
  - Provide easy to use, responsive tools that allow children (and parents) to make a complaint if something has gone wrong with their privacy.

- Stop using 'dark patterns' to manipulate young users into handing over more data when they sign up to a service.
- Stop companies from collecting unnecessary geolocation data from youth, as well as from selling and sharing kids' data unnecessarily.
- Undertake a Data Protection Impact Assessment about their product, which includes identifying potential risks of harm that arise from a platform's data management practices and mitigate those risks *before* the online product is available to children.
- Default youth accounts to 'high privacy settings'.

- **The MN Age Appropriate Design Code does not automatically require age estimation**

  The MN AADC does not call for automatic age verification, nor will every platform have to check your ID to open an account. This is a falsehood often peddled by opponents of the Code.

  Instead, the MN AADC requires digital services to estimate the age of their users under 18 "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."

  Age estimation needs to be proportional to the risks a service presents. This means two things:

  1. If products, services, or platforms are safe, always handle data in secure ways and default all users to strong privacy settings, they do not need to estimate or verify users' age at all.

  2. If companies want to use data in ways that does not comply with the MN AADC, they need to balance the level of risk with the level of certainty they need about a user's age. For example, if they publish people's locations live for anyone in the world to see (a very risky practice) they might need very strong age verification techniques to ensure they are not sharing the location of users under 18. If they're practices are less risky, like publishing pictures of users online for only approved friends to see, they can use lighter age estimation techniques, like asking users their age when they create an account or profile.

  The MN AADC also limits how companies may use any personal information collected to estimate age or age range for any purpose other than fulfilling the age verification requirements. Specifically, the MN AADC provides that companies may only use information collected to estimate a user's age for that purpose and may not retain that personal information longer than necessary to estimate age.

- **If companies need to estimate a user's age, there are many techniques available that have limited privacy impacts**

  If a company does not want to create high privacy settings by default for all users, then they need to assure themselves of the user's age so that they are not capturing the data of children and teens in ways that does not comply with the Code. There are many privacy preserving ways to do this. This includes estimating age by:

  - Asking users to enter their age (or asking twice, if a child made up a fake date of birth, they may forget it the second time). This is often called self-declaration.

- Using data the companies already collect and analyze to estimate the age range of users, such as data about what videos they watch or what other materials they engage with.

- Asking users to get an adult or two to vouch for their age, by sending them a simple link to confirm. This is often called social vouching.

Since many platforms, like Instagram, TikTok, Facebook, among others, already have age requirements for users, most of these companies already engage age verification practices, which may or may not be privacy protective. Contrary to opposition arguments that the MN AADC would require the collection of more information about users, the MN AADC would actually provide additional privacy protections by requiring age estimation methods that are proportionate to risk, limiting how the companies use age estimation data, and requiring that data's deletion.

MN AADC: Enforcement and the Right to Cure

- **The MN AADC is exclusively enforced by the State's Attorney General**

  The MN AADC is exclusively enforced by the Attorney General and does not include a private right of action. As a *design* bill, legal action for violations need not be based in harm to an individual child, but are rather based on product design decisions that could affect every child in the state. Accordingly, as a matter of public policy, the bill appropriately tasks the State with enforcement.

  The bill requires that online platforms likely to be accessed by children, as defined, must complete a data protection impact assessment (DPIA), which identifies any risk of harm to children that can result from the data management practices of the platform, and mitigate or eliminate those risks before making the online product available to children. Businesses must turn over a DPIA and related information within 3 or 5 days, as specified, to the Attorney General upon request. The Attorney General may request a business's DPIA for a variety of reasons, including, but not limited to: to ensure they are complying with the Code's requirement that such an assessment be conducted, because of complaints received from citizens regarding a certain business's practices, or because reporting or media investigations of business practices.

  The MN AADC would subject businesses that violate the Code to an injunction and 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.

- **To incentivize compliance, the MN AADC includes a limited right to cure.**

  The MN AADC includes a 90 day right to cure only for businesses "in substantial compliance with the requirements" of DPIA provisions of the Code. When the Attorney General's office determines a business meets this substantial compliance requirement, they must, before initiating a civil action, provide written notice to the business identifying the specific provisions of the MN AADC that the Attorney general believes have been violated. The business then has 90 days to correct the noticed violation and provide the Attorney General with a written statement that the alleged violations have been cured and sufficient measures have been taken to prevent future violations. If these steps are taken, the business is considered to have cured the violation and not liable for civil penalty that would have otherwise resulted.

The right to cure is designed to encourage the tech industry to continue to innovate within the requirements of the Code and highlights the MN AADC's intent to work with, rather than against, the tech industry. Accordingly the Code will not penalize companies trying to comply with the requirements of the MN AADC, but rather provide them an opportunity to correct violations, as long as they are making the effort to offer safe and private online spaces to youth.

The right to cure also makes the MN AADC more affordable from both a compliance and enforcement perspective. By allowing this option for businesses in substantial compliance, the Attorney General does not have to go through costly investigation and/or litigation before ensuring the intent of the bill: safe and privacy protective online spaces for youth. Rather the right to cure allows the Attorney General and businesses acting in good faith to collaboratively achieve the desired outcome.

Finally, the right to cure does not allow businesses to violate the MN AADC until caught and avoid penalties. Because the right to cure only applies to businesses in substantial compliance with the MN AADC, only businesses that have taken proactive steps to comply with the Code are offered the benefit of limited liability. A business that ignores the requirements of the MN AADC and continues to operate business as usual would not be offered this benefit – rather the Attorney General could immediately file a civil suit against the company for their violation of the Code.