February 7, 2025

Honorable Senator Jeff Barta, Chairman
Senate Industry and Business Committee
State Capitol
600 East Boulevard Avenue
Bismarck, ND 58505

RE: North Dakota SB 2380 – Opposition (as Drafted)

Dear Chair Barta and members of the Committee:

ACT | The App Association is a global trade association for small and medium-sized technology companies. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology.

We appreciate the committee's consideration of our input as you work to address and protect limit minors' access to the harmful content found on the internet. We acknowledge the bill sponsors' and committee's concerns that the internet is a vastly complex arena, and children's access to the internet requires the utmost level of care. **We oppose SB 2380** and believe that the current language of North Dakota SB 2380 fails to achieve the legislative intent.

We also believe that **SB2380 directly shields known bad actors in the children's and youth privacy spaces such as Meta, Roblox, Snapchat, Epic Games, and Match Group by shifting the responsibility owed to their individual users and parents of younger users solely to the app stores**. We are hesitant to support proposed children's online safety legislation proposed and supported by companies facing millions of dollars in fines for violating children's privacy.[1]

Section 1: Tools Currently Available and Alternative Solutions for Consideration

While the intention behind SB2380 is to protect minors from accessing harmful online content and social media, the act would unintentionally create a state-wide obstacle for all users of mobile devices. The proposed approaches are both less effective and inadvertently less effective and more cumbersome than current methods of shielding minors from inappropriate content online.

For example, when parents set up smart devices for their children now, they can configure the device so that access to certain online content is only possible via the parents' or guardians' permission (see example below). App stores enforce these preferences, blocking any downloads that parents and guardians disallow as well as any downloads of apps designated as outside the age range of the child user of the device, regardless of parental permission. Parents may adjust the settings that apply to the

[1] https://www.nytimes.com/2023/11/25/technology/instagram-meta-children-privacy.html

device, including to allow a child that is close to their ninth birthday to download an app meant for children aged nine and above.

Under this framework, the parent is in charge of a device assigned to their child. They can parent as they see fit, and the developers providing these capabilities design their user interfaces according to parental preferences, rather than according to government officials' assessment of compliance. As such, parental control tools on offer today are in a constant process of improvement and refinement, which is better for parents and developers than freezing them in place to serve the goals of record-keeping and enforcement avoidance that come with a government regime contemplated in the legislative proposal.

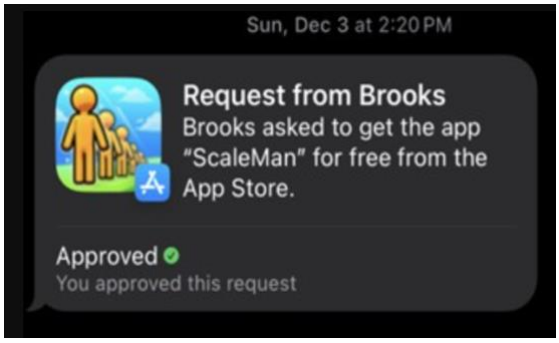

Figure 1: Screenshot of a notification sent to a parent of a request for their child to download an application to the child's device.

App developers currently must accurately indicate the age appropriateness of their apps when distributing through one of the official app stores—or else be subject to removal from the app stores. The internet is full of content that is harmful or inappropriate for minors. To mitigate the risk and limit access to harmful content, developers and device manufacturers implement tools that allow parents to configure devices for their children.

When configuring the device, parents can eliminate any possible access to the browser itself, confining their children's experience to apps that are approved for their ages (apps with browser access are strictly for 17 and over on the app stores).[2, 3, 4] Parents and guardians should not need to comply with layers of government red tape just to effectuate a much weaker level of control than what they currently have over their children's online experience.

To the extent the committee wishes to see a framework giving parents flexible, meaningful control over their kids' online experiences via their smart devices, this already exists, and any government

[2] Step-by-step guide to turning on device level filters currently available for Apple iPhones and tablets: https://support.apple.com/en-us/105121

[3] Step-by-step guide to turning on device level filters currently available on Samsung Galaxy phones and tablets: https://www.samsung.com/us/support/answer/ANS10003399/

[4] Step-by-step guide to turning on device level filters currently available for Apple iPhones and tablets on the Motorola phone - https://en-us.support.motorola.com/app/answers/detail/a_id/156314/~/parental-controls---moto-g-play

regime to change it would inevitably add costs for developers and headaches for parents. The failures to protect children's privacy that exist today—and which the proponents of the bills cite—are decidedly outside the purview of app stores and smart devices and solely on social platforms, including those the proponents provide. The solution is two-fold, but largely rests with more education to parents, guardians, and educators to know and deploy all tools that are currently available.

SB2380 would produce a disproportionate impact on small and medium-sized tech companies. Small and medium-sized tech companies and developers, like our members, play a crucial role in helping manufacturers turn an ordinary phone or tablet into a smart device – through the creation of the apps and other layers of software that work with the physical devices. These businesses are at the forefront of creating new ways of empowering parents and guardians to enable access to educational and beneficial content for their children via smart devices in a way that keeps parents at the center of their children's online experience and maximizes their ability to protect them. In the current ecosystem, a developer of a stargazing app with five employees can list their software as appropriate for children aged 12 and above (if on iOS)[5] or 10 and above (if on Google Play or another platform)[6] for example. Parents may wish to allow access for their 12-year-old, or they could decline access. This is solely at the parent's discretion.

If SB2380 is enacted, however, the parent has effectively no choice in the matter, the issue having been decided for them by the government. The child must be identified as "under 13," pursuant to the app store's age verification requirement. On notice as to the child's status, the developer would then be obligated to follow the requirements laid out in SB2380.

For example, it would need to provide the parents with "profile visibility settings, including the ability to determine whether the child has limited the public visibility of their profile;" "reporting notices, including the ability to be notified when a child submits a report to the application concerning a potential violation of its terms and policies;" and various other mandates that are designed for social networks, not stargazing apps.

Even without the "developer" (social media) mandates in the bill, the actual knowledge as to a child's under-13 status effectively removes the ability for developers to offer things like stargazing apps to general audiences. They can either choose to market to "children," subjecting themselves to verifiable parental consent (VPC) requirements under the Children's Online Privacy Protection Act (COPPA),[7] or they can completely shut off access to their services by children, setting the cutoff at age 18 just to be safe. Of course, the latter is much more likely to be the case, and there are two consequences of this:

[5] https://developer.apple.com/help/app-store-connect/reference/age-ratings/
[6] https://www.esrb.org/ratings-guide/.
[7] COPPA applies to operators of commercial websites and online services "directed to children under 13," https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.

1) your 12-year-old no longer has the privilege of accessing high-quality stargazing apps that traverse bona fide app review and therefore are subject to meaningful parental controls via platform-level settings; and

2) 12-year-olds are unlikely to accept this fate and will access low-quality versions of the software operating in legal grey or black markets unchecked by app store constraints and completely outside this legislature's and parents' purview. Meanwhile, the good actor stargazing apps have likely lost much of their consumer base, left exclusively with consumers who have verified explicitly and pursuant to bureaucratic mandate that they are over 18. In a less likely scenario, they may have convinced their investors to allow them to become a VPC paperwork shop first and foremost, relegating the stargazing function to the backseat of their business plan priorities.

Adding to the VPC compliance costs, the bill itself would put the ball in the developer's court to maintain a paper trail on parents' consent to simply download the app (COPPA is not predicated on "downloads," it is predicated on collection of information—two completely separate things). Under the proposal, the app store's flag indicating parental consent only applies to the initial download. Parents often revoke consent, but this revocation must be effectuated between the parent and the developer under the proposal, since app stores have no functional ability to delete software from an individual's device. Under current law, parents effectuate this permission withdrawal by deleting the app—and decline permission for future downloads. But under SB2380, the developer would be the record-keeper for the entire age verification-predicated parental consent mechanism contemplated in the bill (even though deleting the app is a far easier method). This is an inevitable consequence of mandating age verification as a precondition of using the internet in the first place, since each link in the chain knows the age of the person and must act according to that knowledge. It follows that attempts to limit liability solely to app stores cannot succeed and would ultimately create significant legal uncertainty for small businesses in the app economy.

Whether the developer decides to exclude any consumer under 18 or not, under SB2380, the stargazing app would be less credibly competitive with larger rivals with big compliance budgets. It would be saddled with a new reality of frustrated parents, red tape, and legal uncertainty. This would be true for virtually all apps with high educational utility, including those used by school districts and therefore subject to the Family Educational Rights Privacy Act (FERPA), designed for kids, teens, and adults. It is simply unclear how SB2380 would conflict with or work around school district norms and FERPA requirements, and it is unlikely the resulting legal uncertainty could be waved away with savings clauses or rules of construction. The introduction of this level of legal uncertainty weighs far more heavily on small businesses like the five-employee stargazing app, providing a relative advantage to its larger competitors with legal departments and compliance resources.

The app store age verification language being considered by the committee, instead of supporting the innovative spirit in the digital ecosystem, undermine the ongoing progress that our businesses and developers are making.

SB2380 incorrectly assume that homes are multi-device homes, and that all children and youth have their own devices. One chief assumption in many of the age verification proposals is that all children

and all homes are multidevice homes. It is quite common for parents to use their own logins for a household laptop or tablet that they allow their kids to use. In instances like this, children may bypass all of the consent requirements that could be established by these proposals.

App stores and social media platforms are not one in the same, and not all apps are social media apps. App stores are like a mall filled with shops (apps) each selling various items for various audiences. Social media companies are a tiny fraction of the millions of individual businesses in this mall. The proposal to require the "mall" (app stores) to send a notification to every single shop (app and website) that a child entered the mall when only a small portion of shops have harmful or adult-specific items unnecessarily punishes all of the other shops in order to help solve a problem that is unique to a handful of stores (social media companies). That problem is the currently unchecked use by children under the age of 13 on social media platforms in violation of federal child privacy laws, for which social media platforms are liable. This letter from Senators Bill Cassidy and Ed Markey details the lengths to which some platforms go to skirt the law's requirements and helps explain why proposals like the ones being considered by the committee would help bad actors evade this responsibility even as it would add costs for small business app developers and red tape for parents.[8]

The legislative proposal mandating app store age verification is being pushed by huge platforms facilitating massive social networks with poor track records on protecting children's privacy. During an October 2, 2024, South Dakota hearing on this same legislative proposal, Nicole Lopez, the global director of youth safety policy at Meta (valued at ~$1.5T), named Roblox (valued at ~$28B), Match Group (valued at ~$10B), and Snapchat (valued at ~$17.5B) as the major industry supporters for app store level age verification. The unfortunate reality, is that these trillion- and billion-dollar companies have a history of violating various laws design to protect children who have used their platforms to access harmful content online.[9, 10,11]

Social media companies have their own community. Social media companies are businesses that require each and every user to create an account to have access to a digital community where the users can communicate with each other through messaging, shared photos, and comments on posts, among other things intentionally created for both teen and adult crowds, and they have the responsibility to protect their users. This responsibility includes restricting account creation of minors and compliance with data governance laws and limiting targeted advertisements.

[8] https://www.markey.senate.gov/imo/media/doc/markey_cassidy_letter_to_meta_on_states_coppa_complaint_-_120523pdf.pdf

[9] https://www.businesswire.com/news/home/20231107766120/en/Multiple-Families-Sue-Roblox-Corporation-for-Exploiting-Children-Online

[10] https://nmdoj.gov/press-release/attorney-general-raul-torrez-files-lawsuit-against-snap-inc-to-protect-children-from-sextortion-sexual-exploitation-and-other-harms/

[11] https://www.documentcloud.org/documents/24080032-state-ags-v-meta

Many of the social media companies are also standalone websites. This means that that even if the social media companies leave an app store, laptop and smartphone users could still create social media accounts on these specific companies' websites. This proposal does not take this into account.

Children are extremely tech savvy. Most young children are tech savvy and can be one lunch discussion or sports practice away from learning how to bypass any kind of app store parental verification and age gating mechanisms.

Possible Alternatives

- **Education, awareness, and activations**. We encourage consideration of allocating state resources into education and training programs to help spread awareness of built in parental monitoring and control features that already exist. We welcome the chance to partner with the state's startup and tech ecosystem by providing resources that can assist in training parents, grandparents, and others on current apps and tools that limit and monitor minors' access online. We believe efforts like these would help enable better protections without imposing impractical requirements on parents, developers, and manufacturers.

- **Public-private partnerships and standards development:** The internet and technology are global by nature, and it is nearly impossible to geofence requirements on parents, developers, students, and children in a state's border. To this end, the tech sector has historically worked to develop mutually agreed upon industry practices at a global level. This allows agreements and complete solutions to move at the speed of innovation, rather than the speed of government. We believe that it will take the entire ecosystem joining forces to properly create an online environment where children can be protected. This would also include state specific public-private partnership between government agencies, school districts, the legislature, and more small businesses building tools that facilitate the protection of privacy and kids' online safety.

We encourage the committee to explore these alternative approaches, and we offer to be an active contributor to these solutions. By working together to foster digital literacy, awareness, and parental empowerment, we can create a safer environment for minors without stifling innovation or burdening small businesses.

Thank you for your time and consideration. We trust that you will carefully evaluate the points raised and remove the bill from consideration while focusing alternative ways to support both the protection of minors and the growth of the app economy in North Dakota.

Sincerely,

Caleb D. Williamson
State Public Policy Counsel
ACT | The App Association