February 3, 2021

The Honorable Jerry Klein
Chairman
Committee Industry, Business and Labor
North Dakota State Senate
Bismarck, North Dakota 58505

Dear Chairman Klein,

We write to share our views on proposed legislation before your committee this legislative session, which could unintentionally harm innovative companies in North Dakota. ACT | The App Association (the App Association) is the leading trade group representing small mobile software and connected device companies in the app economy, a $1.7 trillion ecosystem led by U.S. companies and employing 7,720 people in North Dakota.[1] Our member companies create the software that brings your smart devices to life and make the connected devices that are revolutionizing healthcare, education, public safety, and virtually all industry verticals. They propel the data-driven evolution of these industries and compete with each other and larger firms in a variety of ways, including on privacy and security protections. We have serious concerns with the proposal you are considering, SB 2333. We believe SB 2333 would devalue the services we purchase from software platforms while jeopardizing security as well as intellectual property (IP) and privacy protections for consumers.

In today's connected world, small software companies need three things from the platforms they use: easy access to a global market, the ability to offload overhead (like managing credit cards and preventing piracy), but most importantly, ensuring consumer trust. Consumer trust is fundamental for competitors in the app economy, especially for smaller firms that may not have substantial name recognition, and platforms have responded to this need (and competed with each other) in developing novel transparency and trust mechanisms.[2]

Before the entry of large software platforms like the Apple App Store and the Google Play store—and the mobile operating systems that power smart devices—software distribution was a more complex and costly undertaking for developers. The software ecosystem ran on personal computers and required companies to develop and market as well as carve out a supply chain that was far from streamlined. During this time, app companies were not only required to write code for their products, but they were also responsible for printing boxes and CDs, hiring third parties to handle financial transactions, employing legal teams to protect their IP, and contracting with distributors to provide access to retail store shelves in ways that promote and secure trust in their product. Even after the internet made it possible to distribute software electronically, generating consumer trust in software was unavoidably and often prohibitively expensive: developers spent up to 50 to 70 percent of their revenue on distribution, paying for magazine ads, marketing costs to publishers, and literally buying shelf space a big retailers. This is incredibly expensive when

[1] ACT | The App Association, State of the U.S. App Economy: 2020, *available at* https://actonline.org/wp-content/uploads/2020-App-economy-Report.pdf.

[2] Martens, Bertin, "An Economic Policy Perspective on Online Platforms," Institute for Prospective Technological Studies, Digital Economy Working Paper 2016/05. 2016.

1401 K Street NW Suite 501
Washington, DC 20005

202.331.2130 @ACTonline
ACTonline.org /actonline.org

compared to fees of 15 percent for developers making $1 million or less on Apple's App Store or 30 percent for higher-grossing apps and apps across the other major platforms.[3]

Beyond cost reductions, consumers are now depending on mobile devices to store their most important information, and the ability to protect that data is vital. SB 2333 puts users' most vital data at risk. Today's software ecosystem depends on strong privacy, security, and IP protections at the platform level, therefore proposals to require platforms to allow circumvention of these protections would harm consumers and app economy competitors alike. Platforms currently work to keep apps that violate user trust out of their stores. In particular, apps that promote pornography, assist stealing music and movies, and allow for the illicit stalking or tracking of a person are banned. Those three categories of apps are also known vectors for malware and other software that either steals and sells personal data or uses the device resources in unexpected ways. SB 2333 creates an easy avenue for applications that would do real harm to consumers.

SB 2333 would circumvent the general prohibitions on such content by a platform and would render parental controls enabled by those platforms ineffective. In another example, there is strong demand for stolen content, especially during the pandemic as consumers are streaming content at home. Now, more than ever, we need to empower platforms to help content creators enforce their IP rights. Unfortunately, this proposal would help IP infringers circumvent the measures platforms use to sniff out IP theft and help IP owners eliminate the infringing content.

Just as the proposal would allow several questionable forms of content and activities—from which platforms currently protect consumers—it would also open new avenues for cyber attacks and privacy violations that would undermine the offerings of our member companies. For example, some bad actors market their device monitoring apps designed to track children's mobile device use as a way to track anyone, including adults, without their knowledge or permission. These "stalker apps" operate outside the bounds of what is allowable in app stores or mobile operating systems by accessing troves of personal data including location, messaging, and calls. Stalker apps put domestic abuse victims at further risk for harassment and harm by their abusers. In 2019, The Federal Trade Commission (FTC) acknowledged the dangers of allowing third-party apps access to bypass manufacturer restrictions in its first ever action against a purveyor of so called "stalker apps", Rentina-X. The FTC stated in its enforcement action that "the purchasers were required to bypass mobile device manufacturer restrictions, which the FTC alleges exposed the devices to security vulnerabilities and likely invalidated manufacturer warranties."[4]

Requiring platforms to allow the installation of unapproved content would impede the ability of platform operators to ubiquitously update devices' functionality and security. This requirement would make an attack like the one involving SolarWinds easier, as that breach involved the

[3] Mark Gurman, *Apple to Cut App Store Fees in Half for Most Developers*, BLOOMBERG, (November 18, 2020), https://www.bloomberg.com/news/articles/2020-11-18/apple-to-cut-app-store-fees-in-half-to-15-for-most-developers.

[4] Press Release, Fed. Trade Comm'n, FTC Brings First Case Against Developers of "Stalking" Apps (Oct. 22, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/10/ftc-brings-first-case-against-developers-stalking-apps.

installation of software onto personal devices.[5] A key element of our member companies' ability to reach their markets is this built-in trust, which the proposal could significantly erode as unsecured apps find their way onto the devices of our members' clients and customers. Those developers who seek to reach consumers and clients outside the software platforms (or in addition to providing apps on the platforms) can provide robust offerings as progressive web apps or on the internet. Software is not inaccessible even if its characteristics make it difficult to offer on the various software platforms; legal cannabis sellers, for example, make their products and services available off the platforms, even though payment processing using federally insured depository institutions is illegal and therefore unavailable on the platforms.[6] However, for our member companies and other small companies innovating in the app economy and creating jobs in North Dakota, much of the platforms' value derives from their ability to create a trusted space for consumers, developers, and content creators alike.

We appreciate this opportunity to weigh in as you work to ensure that public policy strikes the right balance to best promote competition and consumer protection. We strongly support public policy that enables the free market to create trusted software spaces that address privacy, security, and IP threats for consumers and for software developers to compete, create jobs in North Dakota, and provide innovative products and services.

Sincerely,

Morgan Reed
President

ACT | The App Association
1401 K Street NW (Suite 501)
Washington, District of Columbia 20005

Cc:
The Honorable Doug Larsen
The Honorable Randy A. Burckhard
The Honorable Curt Kreun
The Honorable Richard Marcellais
The Honorable Shawn Vedaa

[5] Isabella Jibilian, *Here's a Simple Explanation of How the Massive SolarWinds Hack Happened and Why it's Such a Big Deal*, BUSINESS INSIDER, (December, 24, 2020), https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

[6] Caleb Danzinger, *It's Complicated: Can you Sell Cannabis Online?*, CANNABIS & TECH TODAY, (June 30, 2020), https://cannatechtoday.com/its-complicated-can-you-sell-cannabis-online/.