



TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

WRITTEN TESTIMONY OF TYLER DIERS
TECHNET
MINNESOTA HOUSE OF REPRESENTATIVES
HOUSE EDUCATION POLICY COMMITTEE
REPRESENTATIVE JAMIE BECKER-FINN, CHAIR
IN OPPOSITION TO HF 1404

March 30, 2022

Good afternoon, Madam Chair and members of the Committee:

My name is Tyler Diers and I serve as the Midwest executive director for TechNet.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over four million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

I am before you today in opposition to the student data privacy provisions laid out in the proposed delete-everything amendment to HF 1404.

TechNet remains committed to working with this Committee to identify a legislative solution that protects student privacy. We strongly recommend Minnesota look to the Student Online Personal Information Protection Act (or "SOPIPA") model that has been enacted in 34 other states and includes strong protections, such as banning the sale of student data and targeted advertising in educational services, requiring strong security procedures and practices, and the deletion of student data upon request by a school. In addition, the model legislation actually creates broader protections than what is included in the current bill.

As drafted, the bill would require the technology provider to destroy or return educational data within 30 days of an expiring contract. From our perspective, service providers should only delete or export data at the request of the customer. This provision appears to put the onus on the service provider to anticipate the end of a contract and act (to delete or export data) without guidance from their customers.

Under the amendment, technology providers would also be required to establish written procedures to ensure appropriate security safeguards for educational data that would then be considered public information unless otherwise classified. Requiring providers to establish written security safeguards that are public by default would risk unnecessarily exposing sensitive data and put public education agencies, institutions, and Minnesota's students at risk.

We also have concerns with the provisions laid out in Subd. 14 which address accessing or monitoring school-issued devices. It is unclear what the restriction in this subdivision entails. Government and technology providers can be said to access and monitor devices and transmissions for a range of legitimate purposes, including ensuring that the devices are working properly.

The prohibition on "accessing or monitoring" location, any audio or visual recording, or any web-browsing activity is also extremely broad. It is unclear what behavior is prohibited and could be interpreted to mean that schools cannot access a recorded video call, for example, or any "student interactions" which could be interpreted to mean virtual classrooms or collaboration tools.

The bill also introduces several overbroad definitions. For example, "commercial purposes" is not defined beyond "including but not limited to marketing or advertising to a student or parent." With such little guidance, the burden to determine what constitutes a commercial purpose will be shifted onto providers to decipher, but with no guarantee that they made the right call. Additionally, under this bill, a technology provider is required to not "sell, share, or disseminate educational data" unless agreed upon with a public educational agency or institution.

There are numerous acceptable examples of when student data could need to be shared, including scholarships, college applications, and more. This provision again places a significant burden on technology providers to determine these criteria with limited and unclear guidance. It is our belief that schools should be able to use educational technology solutions to improve student educational outcomes, but we are concerned that the language found in the omnibus could ultimately limit student access to these solutions.

TechNet and our members that operate in the student data technology space agree with the overall goal of the provisions which aim to make student privacy a priority, which is why we work diligently with policymakers in states across the country to ensure student privacy is protected. In its current form, the proposed amendment would place a significant burden on the providers and introduce increased risk of security incidents. For these reasons, we ask you to please adopt similar provisions by over 30 states and enact the true model legislation.

Thank you in advance for your consideration on these matters, and we look forward to discussing these items in more detail at your convenience.