NetChoice *Promoting Convenience, Choice, and Commerce on the Net*

Carl Szabo, Policy Counsel
NetChoice
1401 K St NW, Suite 502
Washington, DC 20005
202-420-7485
www.netchoice.org

September 1, 2015

The Honorable John Kline
Chairman
Committee on Education and the Workforce
U.S. House of Representatives
2181 Rayburn House Office Building
Washington, DC 20515

The Honorable Robert C. "Bobby" Scott
Ranking Member
Committee on Education and the Workforce
U.S. House of Representatives
2181 Rayburn House Office Building
Washington, DC 20515

The Honorable Todd Rokita
U.S. House of Representatives
1717 Longworth House Office Building
Washington, DC 20515

The Honorable Marcia L. Fudge
U.S. House of Representatives
2344 Rayburn House Office Building
Washington, DC 20515

RE: Comments on the "Student Privacy Protection Act."

Dear Chairman Kline, Ranking Member Scott, Rep. Rokita and Rep. Fudge:

NetChoice is a trade association of leading online and e-commerce businesses all of whom share the goal of promoting convenience, choice, and commerce on the net.[1] NetChoice has been actively involved in the issue of student privacy and met with dozens of legislators from across the country to discuss thoughtful and intelligent approaches to protecting student information.

We appreciate and support an update to the Family Educational Rights and Privacy Act of 1974 (FERPA)[2] to allow it to better address the issues of 21st century students. However, we worry that some of the components of the draft Student Privacy Protection Act (SPPA) could actually inhibit educational technology innovation and discourage businesses from making services available to students.

Our primary concerns are that the current draft of the SPPA:

- **Restricts Student & Parent Choice** – Any new law should preserve the right of parents and students to control what happens to data about them, including the right to transfer it.

[1] More information at NetChoice.org
[2] 20 U.S.C. 1232g

- **Misses Opportunity to Create a National Standard** – A new federal law is an important opportunity to create a national standard that will protect students and provide companies with clear guidance allowing them operate efficiently and encourage new entrants into the ed-tech space. A failure to create this national standard would only contribute to a patchwork of inconsistent student privacy laws and discourage investment and innovation in educational technology.
- **Limits Product Improvement** – The prohibition on the use of identifiable student data except to improve the student's learning outcome is overly broad. This limitation would cripple general improvements to products, including making finding and fixing many security problems illegal.
- **Creates Overly Broad Limits on Advertising** – One of the promises of educational technology is personalized learning, however the broad bans on marketing products & services could preclude a reading program from recommending books or a math program from recommending supplementary videos provided by a non-profit service.
- **Contains Overly Broad Definitions** – The definitions in the draft appear to be overly broad and may have the effect of unintentionally restricting products that are unrelated to the technology used to provide education in schools. The broad definitions of "Education Service Provider," and "Student Records" are particularly concerning.
- **Establishes Unworkable Data Breach Notification Requirements** – The proposed data breach provisions are unworkable. For example, without a harm trigger, companies will be required to report every visitor who fails to properly sign in as a security breach. If there were a breach, the three-day notice provision will require sending out notice and thus alerting criminals to security vulnerabilities long before a company would have time to properly identify the scope of the breach and fix it.

Parent & Student Choice

Parents and students should have the right to choose how data about them is used. Parents often need to access to and control of educational information for uses outside the school such as working with tutors, moving to a new school, or using other educational services. Giving them the ability to access and view their own student information is one of the guiding principles and purposes behind the creation of FERPA.[3] And the success of innovative educational products will depend upon parents and students feeling in control.

This draft contains many limitations on the use of data, and it should clearly enshrine parents' right to make choices that are right for their children – including the right to change schools or to use their student's work product or information outside of school. To address this concern, and to make businesses confident about what they must do to safely operate, we recommend adding the following to Section 7:

---

[3] *See, e.g.* Dep't of Ed., *FERPA for Parents and Eligible* Students, *available at* http://familypolicy.ed.gov/ferpa-parents-students?src=ferpa-s

> Nothing in this Act shall be construed to prohibit the use or disclosure of educational records with the affirmative consent of the school, student or the student's parent or guardian given in response to clear and conspicuous notice of the use or disclosure.

Preemption

Dozens of states have regulated or are considering regulating the use of student information in ways that will cripple innovation. Instead of maintaining a patchwork of potentially inconsistent state laws, Congress should create a national standard that simplifies regulations in this national market to create consistency for school, parents, students, and companies.

For national legislation to have a meaningful impact in the student privacy space, it must preempt inconsistent state laws. Failure to preempt would simply add more inconsistency to the existing laws in the area and further discourage organizations from innovating or investing in technology that can improve educational outcomes for all of our nation's children.

Product Improvement

Computers and software used in the classroom are not usually strictly for educational purposes. Often times they are general commercial products used for educational purposes. However, the ban on using student information "for the development of commercial products or services"[4] would make improvement of these cross-use devices and services a violation of FERPA. This restriction likely would encourage companies to prohibit the use of generally available software – for example, word processors or graphic design programs – in the classroom, leading to a decidedly inferior experience for children who are trying to learn the technology that will enable them to be successful after graduation.

The exception that personal information may be used to improve a student's academic outcome[5] is inadequate because bug fixes or other product improvements not directly tied to educational outcome would be prohibited. For example, improving the security of a product is unlikely to improve educational outcomes, but is obviously essential for good products and services.

We suggest that you remove this language.

Advertising

While we recognize that some restrictions on advertising may be appropriate in the school context, we have three recommendations:

The "marketing a product or service" ban should not prohibit adaptive learning

First, having worked with state legislators across the country, we learned that efforts to prevent interest-based advertisements often result in unintended consequences. These consequences

---

[4] Student Privacy Protection Act p. 27 line 23-24.
[5] *Id.* at p. 28 line 7-13.

included: preventing adaptive learning,[6] disallowing substitute teachers from seeing a class roster,[7] or even outlawing publication of track results in the local newspaper.[8]

As written, this law raises similar concerns to what we have seen in various state bills. The ban on "marketing a product or service" suggests that it would be illegal for a reading program to recommend books -- because books are a "product" -- or for a math program to recommend online remedial videos -- because those videos could be part of a "service."

To clarify the scope of the prohibition in section 9, we recommend the following be added to Sec.9(g)(3) based upon California's student privacy law, such that the advertising ban shall not apply to:

> (1) the use of student data, including covered information, for adaptive learning or customized student learning purposes;
>
> (2) the use of recommendation engines to recommend to a student additional content or services relating to an educational, other learning, or employment opportunity purpose within an operator's site, service, or application if the recommendation is not determined in whole or in part by payment or other consideration from a third party; or
>
> (3) responding to a student's search query, other request for information, or request for information or for feedback if the information or response is not determined in whole or in part in part by payment or other consideration from a third party.

Prohibitions on advertisements should be technology neutral and based on harm

Second, as the draft reflects, schools today allow companies to market to students, and the platform on which that advertising appears should not make a difference. Besides billboards in sports fields and advertisements in school newspapers, there are class rings, graduation gowns, and school photos where student's names, parents' information, credit card, address, phone number, ring and waist size, and other information is collected and sometimes used for marketing purposes.[9] Unless there is evidence that marketing generally is harmful to students or that marketing specific products like class rings is less harmful, both the general ban in the draft and the special provisions for things like class rings are inappropriate.

Non-targeted advertising should be permitted

Third, the draft does not clearly define marketing and advertising and their general ban as written will create confusion amongst providers and could scare new entrants away. To

---

[6] New Hampshire HB 520 (2015).
[7] *Id.*
[8] Louisiana HOUSE BILL NO. 1076 (2014).
[9] *See, e.g.,* Jostens Mobile Marketing Case Study, "For decades, Jostens relied on direct mail and calls to students' homes to remind them of upcoming Jostens appointments and deadlines for turning in payment, etc. But with postage costs rising and so many incorrect addresses and home phone numbers, Jostens wanted to find a way to cut costs and get responses to the students more effectively…. Jostens saw an opportunity to streamline the process by contacting students via text messages to their cell phones for a quick, to-the-point reminder that they are sure to see." *available* at, https://www.eztexting.com/why-ez-texting/case-studies/jostens

address the missing specificity, we recommend limiting the ban on advertising to the following generally accepted definition[10]:

> The terms 'Marketing' and 'Advertising' mean presenting advertisements to a student where the advertisement is selected based on information obtained or inferred from that student's online behavior, usage of applications, or covered information. It does not include advertising to a student (a) at an online location based upon that student's current visit to that location without the collection and retention of a student's online activities over time, or (b) in response to a single search query without collection and retention of a student's online activities over time.

Overly Broad Terms

The broad definitions of terms like "educational service provider," and "educational records" will discourage companies from entering the market because once they do unrelated activates will be regulated and unjustified burdens placed on them.

Educational Service Provider incorporates unrelated business activities

As written, the definition of "Educational Service Provider"[11] likely would mean that every component of a business was regulated by FERPA, even if just a small offshoot offers an education technology product or service.

We suggest amending the term "Educational Service Provider" so it only covers a business to the extent it is *actively engaged* in providing educational services to schools pursuant to a contract or agreement with the school.

Below is a proposed amendment similar to those adopted in states like Maryland and Nevada:[12]

> ''(5) EDUCATION SERVICE PROVIDER.—The term 'education service provider' means any provider, other than a school official or employee, of services developed for and marketed to schools, institutions of higher education, educational agency or institution employees or officers, or other individuals primarily engaged in the provision of education services, for in-school educational use <u>pursuant to a contract or agreement with an educational agency or institution, or State educational authority, to the extent the provider or individual is operating in that capacity</u>.

Educational Records includes data that is not an educational record

We are also concerned that requirements around educational records will place unnecessary burden on companies, especially when trying to comply with parents and students requests to view their records. It is impractical and unhelpful to the students and parents to provide them with all of the log and metadata that might be related to the student.

Therefore, we recommend that the definition of educational record should be amended to clarify that it only includes data created or provided by (1) the student or his parents, (2) the

---

[10] *See, e.g.* DAA, *Self-Regulatory Principles for Online Behavioral Advertising*.
[11] Student Privacy Protection Act p. 39 line 18-24, p.40 lines 1-2.
[12] *See, e.g.* Maryland HB 298 (2015), Oregon SB 187 (2015).

educational agency, or (3) personally identifies or is linked to information that personally identifies the student, similar to the California's Student Online Personal Information Protection Act.

Data breach

Unless the draft will preempt state data breach laws, new regulation is unnecessary as basically every state has breach notification laws that were created after years of hard work with industry, parents, legislatures, and attorney's general. Students and parents already enjoy robust data breach notification protections. And, the required notice in the SPPA will result in unintended consequences that will do significantly more harm than good.

First, because there is no "harm trigger," any minor breach of a security practice — such as a guest failing to properly sign-in — could require mass notification. Research has shown that excessive data breach notifications desensitize people to the actually important notices.

Second, bad actors often use real notifications as cover for sending phishing attacks disguised as official communications related to the breach in order to compromise people's accounts. Under the SPPA, unnecessary notices will increase, exacerbating this problem.

Suggested language for data breach notification in FERPA

We suggest removing the data and security breach notification altogether as the state requirements are adequate. Barring that, we strongly suggest adding a harm trigger to the legislation along with an exception for when the acquired data is already public or encrypted.[13] A "breach of security" without any evidence that sensitive data was compromised should not trigger notification requirements. Minor security flaws are routinely identified by third-party researchers (either on the service itself or in public software libraries incorporated into many services) and promptly fixed. The discovery of such an unexploited flaw could technically be a breach, but one that should not require notice.

The three-day notice requirement is unworkable. Three days will often not be enough time to identify a breach, fix it, and test the fix. Notifying the public of a breach before it has been fixed will just invite other hackers take advantage of the same problem. No other law comes close to the near immediate notice requirements that this draft proposes. We ask that you adjust the time frame to a "reasonable time" standard like the one in California law.[14]In addition to adding the harm trigger, we suggest replacing the language on page 9 lines 8-10 with the following based heavily on California Data breach notification law:[15]

> (i) Any educational agency or institution shall disclose any unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of student's personal information maintained by the educational agency or institution

---

[13] States where encryption does not require notice: Alaska, Arizona, Arkansas, California, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wyoming, District of Columbia.

[14] Cal. Civ. Code § 1798.25 - 1798.29.

[15] *Id.*

following discovery or notification of the unauthorized acquisition to any student and their parents whose non-public unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

Additional Recommendations

Creating duplicative enforcement powers leads to confusion and discourages development

The draft SPPA gives the Secretary of Education broad authority over schools, and thus vendors, and provides for extensive rulemaking authority and enforcement. These broad powers will overlap with attorney general and FTC authority causing regulatory confusion and detriment to innovation within the education industry. Attorney's general and FTC enforcement already established guidelines, experience, and precedent over privacy related matters. These new powers create duplicative governmental expenses and risks generating conflicting rules and guidelines. Moreover, introduction of another enforcement agency could discourage services from developing or making their services available to educational institutions.

If Department of Education rulemaking and enforcement is kept, then its most egregious problems should be remedied: First, the draft should provide for due process and proportional response requirements for any enforcement action. Second, a minimum ban of not less than five years[16] does not give the Secretary adequate discretion in crafting appropriate punishment for violations. Third, applying the ban to individuals who many have had nothing to do with the violation[17] is bad policy and could hurt innocent people.

Adult students don't require parental consent

The law should be clear that adult students do not need parental consent. Section 4 has a provision for adult students, but this provision does not clearly apply to the subsequent sections that continue to talk about the rights of parents, without mentioning adult students.

"Commonly accepted industry standards on privacy" do not exist

The requirement that companies meet "commonly accepted industry standards on privacy protection"[18] is vague as there are not commonly accepted industry standards. We recommend instead that the draft require "reasonable security procedures and practices."

---

[16] SPPA p. 31 line: 18.
[17] *Id.* at p. 31 lines: 15-17.
[18] *Id.* at p. 14 lines 23-25.

The research limitations are harmful to education

We also recommend removing the ban on research that is not limited to improving outcomes at the school the data came from.[19] This ban could limit valuable longitudinal studies that are critical to understanding the long-term effectiveness of educational programs.

* * *

Thank you for considering our views. We look forward to working with you on improving this update to FERPA. Please let us know if we can provide further information.

Sincerely,

Carl Szabo
Policy Counsel, NetChoice

[19] *Id.* at p. 18 lines: 15-18.