June 9, 2015

The Honorable Fred Upton
Chairman
Committee on Energy and Commerce
2183 Rayburn House Office Building
Washington, D.C. 20151

The Honorable Frank Pallone, Jr.
Ranking Member
Committee on Energy and Commerce
237 Cannon House Office Building
Washington, D.C. 20515

The Honorable Michael C. Burgess, M.D.
Chairman
Subcommittee on Commerce, Manufacturing, and Trade
2336 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce, Manufacturing, and Trade
2367 Rayburn House Office Building
Washington, D.C. 20515

Re: The Student Digital Privacy and Parental Rights Act, H.R. 2092

Dear Chairman Upton, Ranking Member Pallone, Subcommittee Chairman Burgess and Ranking Member Schakowsky:

We write to express our support of the Student Digital Privacy and Parental Rights Act (H.R. 2092), and to respectfully urge the House Energy and Commerce Committee promptly to hold a hearing on this bill. This bipartisan proposal, introduced by Congressmen Luke Messer and Jared Polis on April 29th, would provide much-needed safeguards for the privacy and security of students' personal information in today's digital world.

Education technology is an integral component of classroom instruction and K-12 school operations across the country. According to a 2013 report by Fordham Law School's Center on Law and Information Policy (CLIP), 95 percent of school districts rely on cloud computing services for a diverse range of functions, from tracking student performance to providing services such as cafeteria payments and transportation planning. As schools, teachers, and students increasingly use online services, EdTech providers are collecting, generating, and maintaining large amounts of sensitive student information. Students' privacy and wellbeing cannot be ensured without clear and enforceable rules requiring private companies to protect the confidentiality, security and integrity of their student data systems.

Federal law has not kept pace with the rapid adoption of EdTech and it is unclear to what extent it safeguards students' personal data from misuse, commercial data mining, or unauthorized access. We need innovative approaches to protect students and empower parents.

The Student Digital Privacy and Parental Rights Act sets sensible baseline rules for K-12 websites, online services, and apps to protect the privacy and security of students' personal information:

- It prohibits targeted advertising to students or parents on these school services, as well as collection and use of student data for targeted advertising elsewhere.
- It prohibits the sale of students' personal information.
- It prohibits the creation of personal profiles of students except for school purposes.
- It prohibits disclosure of students' personal data to third parties except in limited circumstances, and requires third party recipients to comply with robust data protection standards.
- It requires the EdTech company to implement procedures for data security, including preparing a response to a data breach. This mirrors federal laws for other types of data, like the Health Insurance Portability and Accountability Act and Gramm-Leach-Bliley Act.
- It requires companies to delete student data after 45 days at the school's request or the parent's request, and to purge student data after a year unless a school or parent has directed the company to maintain the data.
- It also provides parents with rights to access and correct information about their children, and permits parents and students to download student-created work.
- It requires clear public disclosure of the types of student information collected, the purposes for which the information is used or disclosed, and the identity of any third-party recipients.
- It gives the Federal Trade Commission (FTC) rulemaking and enforcement authority. Legislation that gives the FTC this regulatory power would better incentivize EdTech providers to practice responsible data collection, use and sharing practices.
- It would not preempt stronger state student privacy laws. This will allow for states to innovate on student privacy to afford their students enhanced privacy protections.

While H.R. 2092 would provide strong protections for students' personal information, it still permits use of EdTech for personalized and adaptive student learning purposes. Moreover, it permits use of aggregated, de-identified information for research and product improvement. It also allows schools to retain data if retention is for an educational or administrative purpose. This bill strikes an appropriate balance so students can benefit from online learning products, while minimizing risks inherent in the digital age.

Student digital privacy is undoubtedly a civil liberties concern; children should not have to trade their privacy for an education. It is also a civil rights concern; we increasingly read stories of Big Data fostering negative profiling and discrimination. Students – especially those disproportionately subject to profiling *offline* – must be able to trust that the services they interact with online will not perpetuate such discrimination.

The enactment of a strong Student Digital Privacy and Parental Rights Act to govern the growing EdTech industry, along with modernization of the Family Educational Rights and Privacy Act to update rules for schools' use and disclosure of student data, will take critical steps to comprehensively safeguard schoolchildren's privacy in the 21st century.

We applaud H.R. 2092's thoughtful approach to protecting students' digital lifecycle and hope Congress will swiftly enact this much-needed legislation. To this end, we strongly encourage you to hold an early hearing on H.R. 2092 and to move this bill through the legislative process as quickly as possible.

Respectfully submitted,

Center for Democracy & Technology
Center for Digital Democracy
Common Sense Media
Consumer Action
Consumer Federation of America
Consumers Union
Consumer Watchdog
Electronic Frontier Foundation
National Consumers League
Privacy Rights Clearinghouse