MINTZ

New Hampshire Establishes Privacy Protections for Student Online Personal Information

June 17, 2015 | Blog | By **Cynthia J. Larose**, Julia Siripurapu

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

California again has provided a model of privacy legislation for other states to follow. New Hampshire Governor Maggie Hassan recently signed into law **House Bill 520** (the "Bill"), a bipartisan effort to establish guidelines for the protection of student online personal information.

Who is covered by the Bill?

Modeled after California's **Student Online Personal Information Protection Act** (SOPIPA), the Bill applies to operators of Internet websites, online services (including cloud computing services), and mobile applications with ***actual knowledge*** that their website, service or application is ***used primarily*** for K-12 school purposes and was ***designed and marketed*** for K-12 school purposes ("Operators"). Like SOPIPA, the Bill imposes certain obligations and restrictions on Operators with respect to the collection, use, storage and destruction of student personal information and becomes effective on January 1, 2016. We discuss SOPIPA in more detail **here** and provide recommendations for preparing to comply with the SOPIPA requirements.

The Bill does not apply to general audience websites, online services, and mobile applications, even if login credentials created for a covered site, service, or application may be used to access the general audience sites, services, or applications. The Bill also makes it clear that it is not intended to:

- limit Internet service providers from providing Internet connectivity to schools or students and their families;
- prohibit operators of websites, online service, or mobile application from marketing educational products directly to parents so long as the marketing did not result from the use of "Covered Information" under the Bill;
- impose a duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance with the Bill on those applications or software;
- impose a duty upon a provider of an interactive computer service, as defined in **47 U.S.C. section 230**, to review or enforce compliance with the Bill by third-party content providers; or
- impede the ability of students to download, export, or otherwise save or maintain their own student created data or documents.

What information is covered by the Bill?

The Bill defines "Covered Information" very broadly to include personally identifiable information or materials, *in any media or format,* **created or provided to an Operator** by either a student (or his/her parent or guardian) while using the Operator's site, service, or application or by an employee or agent of the K-12 school, school district, local education agency, or county office of education, **as well as information gathered by the Operator** that is related to the student, such as information that is "*descriptive of a student or otherwise identifies a student, including, but not limited to, information in the student's educational record or email, first and last name, home address, date of birth, telephone number, unique pupil identifier, social security number, financial or insurance account numbers, email address, other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, other student identifiers, search activity, photos, voice recordings, or geo-location information*."

What do you have to do to comply with the Bill?

Avoid the following prohibited activities:

- Using any information (including persistent identifiers) created or collected through your site, service, or application to create a profile about a K-12 student;
- Engaging in targeted advertising (either on your site, service, or application or any other site, service, or application) when the targeting is based on any information (including covered information and persistent identifiers) that you have acquired as a result of the use of your site, service, or application;
- Selling, leasing, renting, trading, or otherwise making available a student's information (including covered information), except in connection with a sale of your business provided that the buyer continues to be bound by this restriction with respect to previously acquired student information; or
- Disclosing protected information, except where the disclosure is mandated to "respond to or participate in judicial process".

Implement and maintain the following security and deletion requirements:

- ***reasonable*** security procedures and practices (appropriate to the nature of the Covered Information) to protect Covered Information from unauthorized access, destruction, use, modification, or disclosure, and
- delete covered information if the school or district requests deletion of data under the control of the school or district.

What can you do with Covered Information?

Although, as discussed above, there are many restrictions on the use of Covered Information, Operators are permitted to:

- Use de-identified Covered Information within their sites, service, or application (or other sites, services, or applications owned by the Operator) to improve educational products and to demonstrate the effectiveness of their products or services (including in their marketing), and
- Share aggregated de-identified Covered Information for the development and improvement of educational sites, services, or applications.

Although the effective date is **January 1, 2016**, if you are an "Operator" under the Bill, this is the time to begin thinking about what kind of changes you may need to make in your processes and procedures and to put in place an implementation plan to be compliant with the Bill by its effective date.

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.

Julia Siripurapu