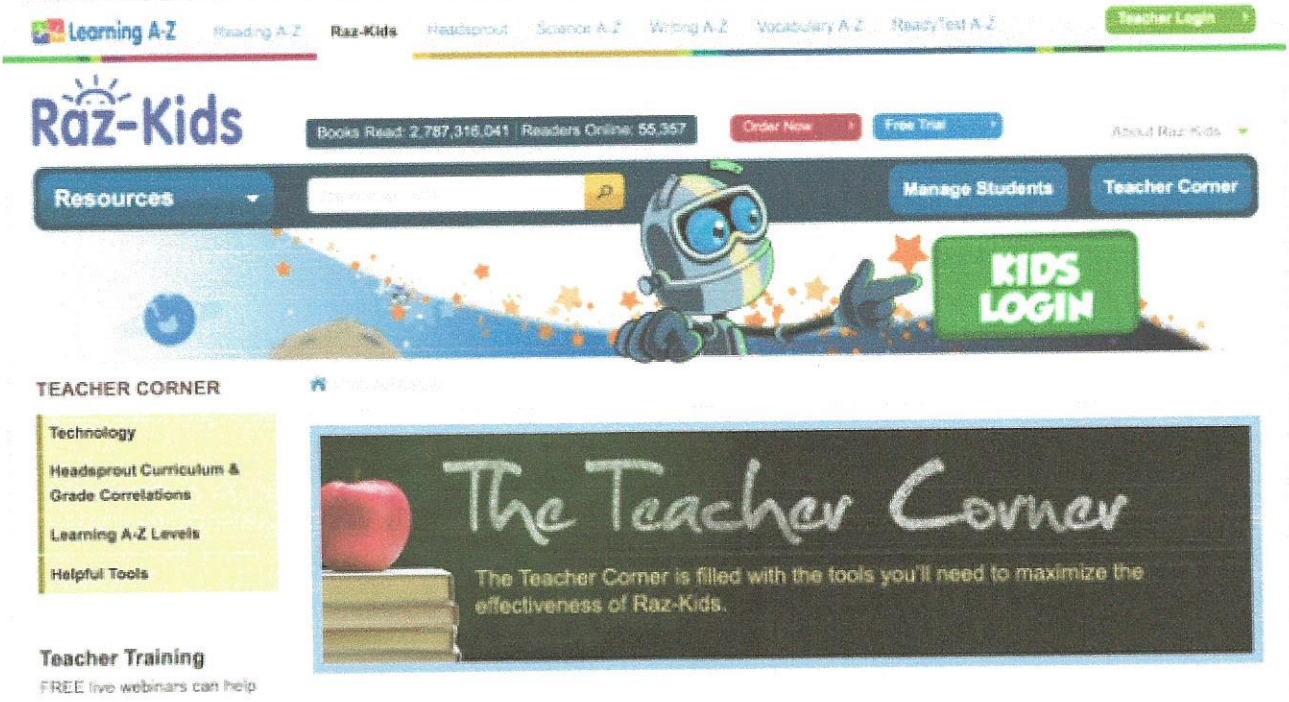
The New York Times

Digital Learning Companies Falling Short of Student Privacy Pledge



Raz-Kids.com is a popular reading program for elementary school students.

By NATASHA SINGER
MARCH 5, 2015

Last month, as part of an article about data security lapses by digital learning companies, I wrote about security vulnerabilities with Raz-Kids.com, a popular reading program for elementary school students. Since then, the service has upgraded its data security by, among other things, encrypting its student accounts.

As of Wednesday morning, however, it had not corrected some other serious security weaknesses, according to a new report from Tony Porterfield, a software engineer and father of two elementary school students who, in his spare time, tests the security practices of digital learning companies.

For instance, Mr. Porterfield noted on his blog, edtechinfosec.org, the reading program had not encrypted teacher and parent accounts. And that security weakness, he said, could potentially allow unauthorized users to obtain students' personal information — like their real names, audio recordings and reading levels.

Cambium Learning Group, the parent company of Raz-Kids, recently signed on to a nationwide student privacy pledge in which signatory companies promise to protect students' personal information.

Digital learning products can collect and analyze a wealth of detail about student use of apps and online services. The pledge was intended to reassure parents and teachers that the education technology industry was committed to safeguarding the student information it collected and to using it responsibly.

In a speech at the Federal Trade Commission in January, President Obama endorsed the student privacy pledge. More than 100 companies have signed on, including major ed tech players like Apple, Google, Houghton Mifflin Harcourt and Microsoft.

Among other things, the pledge requires signatory companies to "maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information against risks — such as unauthorized access or use."

Yet, Cambium Learning Group and several other digital learning companies signed the pledge even though, at the time they joined, they had not begun full encryption, an elementary security measure.

For school officials, teachers, parents and students, this practice may call into question the trustworthiness of the industry pledge.

"Parents and educators who don't have the training to test for themselves wouldn't be able to tell which companies have reasonable security and which do not," Mr. Porterfield said in a phone interview on Wednesday, "and that makes it hard to trust the pledge."

John Campbell, the chief executive of Cambium Learning, did not return an email seeking comment.

In an email to me last month, he wrote that the company took privacy very seriously.

"We are confident that we have taken the necessary steps to protect all student and teacher data at all times and comply with all federal and state laws," Mr. Campbell wrote in the email.

The Future of Privacy Forum, an industry-financed think tank that helped develop the pledge, is holding a series of workshops to help signatory companies understand their obligations. But that alone is unlikely to deter companies from signing on to the pledge even as they are aware of security vulnerabilities in their digital learning products.

"Security is clearly an area where ed tech start-ups have to make progress," said Jules Polonetsky, the executive director of the Future of Privacy Forum. He added: "Companies that don't provide strong security for sensitive data can be at legal risk for violating the pledge, state laws, and contractual commitments."

On Friday, the company behind Raz-Kids.com sent an email to users on its update list that described changes to the service's data security practices.

Among other things, the email recommended that users download the latest version of the Raz-Kids mobile app because the company has added a data encryption system called Secure Sockets Layer or SSL.

It said that parent access to a student account now requires a teacher's approval — a step to prevent unauthorized users from posing as parents.

And the company said it had deleted language from its student data security policy that had said the service required "student first name, student last name, and student identification number." In other words, teachers may now easily assign pseudonymous screen names — instead of using their students' real names on their accounts.