THE CONVERSATION

Academic rigor, journalistic flair

Companies use children’s data to sell them junk food and other products. Cookie image via www.shutterstock.com

How companies learn what children secretly want

August 17, 2016 10.54pm EDT

Faith Boninger

Research Associate in Education Policy, University of Colorado Boulder

Alex Molnar

Research Professor, University of Colorado Boulder

If you have children, you are likely to worry about their safety – you show them safe places in your neighborhood and you teach them to watch out for lurking dangers.

But you may not be aware of some online dangers to which they are exposed through their schools.

There is a good chance that people and organizations you don’t know are collecting information about them while they are doing their schoolwork. And they may be using this information for purposes that you know nothing about.

In the U.S. and around the world, millions of digital data points are collected daily from children by private companies that provide educational technologies to teachers and schools. Once data are collected, there is little in law or policy that prevents companies from using the information for almost any purpose they wish.

Our research explores how corporate entities use their involvement with schools to gather and use data about students. We find that often these companies use the data they collect to market products, such as junk food, to children.

Here’s how student data are being collected

Almost all U.S. middle and high school students use mobile devices. A third of such devices are issued by their schools. Even when using their own devices for their schoolwork, students are being encouraged to use applications and software, such as those with which they can create multimedia presentations, do research, learn to type or communicate with each other and with their teachers.

When children work on their assignments, unknown to them, the software and sites they use are busy collecting data.

Ads target children as they do their homework. Girl image via www.shutterstock.com

For example, “Adaptive learning” technologies record students’ keystrokes, answers and response times. On-line surveys collect information about students’ personalities. Communication software stores the communications between students, parents and teachers; and presentation software stores students’ work and their communications about it.

In addition, teachers and schools may direct children to work on branded apps or websites that may collect, or allow third parties to collect, IP addresses and other information from students. This could include the ads children click on, what they download, what games they play, and so on.

How student data are used

When “screen time” is required for school, parents cannot limit or control it. Companies use this time to find out more about children’s preferences, so they they can target children with advertising and other content with a personalized appeal.

Children might see ads while they are working in educational apps. In other cases, data might be collected while students complete their assignments. Information might also be stored and used to better target them later.

For instance, a website might allow a third party to collect information, including the type of browser used, the time and date, and the subject of advertisements clicked or scrolled over by a child. The third party could then use that information to target the child with advertisements later.

We have found that companies use the data to serve ads (for food, clothing, games, etc.) to the children via their computers. This repeated, personalized advertising is designed specifically to manipulate children to want and buy more things.

Indeed, over time this kind of advertising can threaten children's physical and psychological well-being.

Consequences of targeted advertising

Food is the most heavily advertised class of products to children. The heavy digital promotion of "junk" food is associated with negative health outcomes such as obesity, heart disease and diabetes.

Additionally, advertising, regardless of the particular product it may sell, also "sells" to children the idea that products can make them happy.

Research shows that children who buy into this materialist worldview are more likely to suffer from anxiety, depression and other psychological distress.

Teenagers who adopt this worldview are more likely to smoke, drink and skip school. One set of studies showed that advertising makes children feel far from their ideals for themselves in terms of how good a life they lead and what their bodies look like.

The insecurity and dissatisfaction may lead to negative behaviors such as compulsive buying and disordered eating.

Aren't there laws to protect children's privacy?

Many bills bearing on student privacy have been introduced in the past several years in Congress and state legislatures. Several of them have been enacted into laws.

Additionally, nearly 300 software companies signed a self-regulatory Student Privacy Pledge to safeguard student privacy regarding the collection, maintenance and use of student personal information.

However, they aren't sufficient. And here's why:

Student privacy laws are not adequate. Mary Woodard, CC BY-NC-ND

First of all, most laws, including the Student Privacy Pledge, focus on Personally Identifiable Information (PII). PII includes information that can be used to determine a person's identity, such as that person's name, social security number or biometric information.

Companies can address privacy concerns by making digital data anonymous (i.e., not including PII in the data that are collected, stored or shared). However, data can easily be "de-anonymized." And, children don't need to be identified with PII in order for their online behavior to be tracked.

Second, bills designed to protect student privacy sometimes expressly preserve the ability of an operator to use student information for adaptive or personalized learning purposes. In order to personalize the assignments that a program gives a student, it must by necessity track that student's behavior.

This weakens the privacy protections the bills otherwise offer. Although it protects companies that collect data for adaptive learning purposes only, it also provides a loophole that enables data collection.

Finally, the Student Privacy Pledge has no real enforcement mechanism. As it is a voluntary pledge, many companies may scrupulously abide by the promises in the pledge, but many others may not.

What to do?

While education technologies show promise in some areas, they also hold the potential to harm students profoundly if they are not properly understood, thoughtfully managed and carefully controlled.

Parents, teachers and administrators, who serve as the closest protectors of children's privacy at their schools, and legislators responsible for enacting relevant policy, need to recognize the threats of such data tracking.

The first step toward protecting children is to know that that such targeted marketing is going on while children do their schoolwork. And that it is powerful.