School posts on Facebook could threaten student privacy

Like many of us, schools are active on social media. They use their accounts to share timely information, build community and highlight staff and students. In this blog, Joshua Rosenberg discusses his US-based research showing that schools' social media activity may harm students' privacy. See here for similar findings on UK children's privacy.

As a researcher who specializes in data science in education, I and my colleagues came to the topic of student privacy unintentionally. We were exploring how schools used social media during the early days of the COVID-19 pandemic, specifically March and April of 2020. In the course of this research, we noticed something surprising about how Facebook worked: We could view the posts of schools – including images of teachers and students – even when not logged in to our personal Facebook accounts.

The ability to access pages and pictures even when we were not logged in revealed that not only could schools' posts be accessed by anyone, but they could also be systematically accessed using data mining methods, or new research methods that involve using computers and statistical techniques to discover patterns in large – often publicly accessible – datasets.

Since practically all U.S. schools report their websites to the National Center for Education Statistics, and many schools link to their Facebook pages from their websites, these posts could be accessed in a comprehensive manner. In other words, not only researchers but also advertisers and hackers could use data mining methods to access all of the posts by any school with a Facebook account. This comprehensive access allowed us to study phenomena like violations of students' privacy at a massive scale.

Risks are present

The easy access to student photos that we encountered comes despite broader concerns about individuals' privacy on social media. Parents, for instance, have expressed concerns about teachers posting about their children on social media.

Fortunately, our search of news coverage and academic publications did not reveal any harms that have come to students because their schools posted about them. However, there are a number of possible risks that identifiable posts of students could pose. For instance, would-be stalkers and bullies could use the postings to identify individual students.

Also, there are newer threats that students may face. For instance, the facial recognition company Clearview collects internet data – and social media data – from across the World Wide Web. Clearview then sells access to this data to law enforcement agencies, who can upload photos of a potential suspect or person of interest to view a list of potential names of the individual depicted in the uploaded photo. Clearview already accesses identifiable photos of minors in the U.S. from public posts on Facebook. It is possible that photos of students from schools' Facebook pages could be accessed and used by companies such as Clearview.

Even though we are not aware of these things actually happening, that is not reason to not be concerned about it. At a time when our privacy is often threatened in surprising ways, as technology journalist Kara Swisher writes, "only the paranoid survive." My fellow researchers and I think this cautious view – even a paranoid view – is particularly justified when it comes to students as minors who may not provide their explicit permission to be included within posts.

Millions of student photos available

In our study, we used federal data and an analytical tool provided by Facebook to access posts from schools and school districts. We use the term “schools” to refer to both schools and school districts in our study. From this collection of 17.9 million posts by around 16,000 schools from 2005 to 2020, we randomly selected – sampled – 100 and then coded these publicly accessible posts. We determined whether students were named in the post with their first and last name and whether their faces were clearly depicted in a photo. If both of these elements were present, we considered a student to be identified by name and school.

For example, a student in a Facebook post whose photo includes a name in the caption, such as Jane Doe, would be deemed identified.

We determined that 9.3 million of the 17.9 million posts we analyzed contained images. Within those 9.3 million posts, we estimated that around 467,000 students were identified. In other words, we found nearly half a million students on schools’ publicly accessible Facebook pages who are pictured and identified by first and last name and the location of their school.

Assessing the risks

While many of us already post photos of ourselves, friends and family – and sometimes our children– on social media, the posts of schools are different in one important sense. As individuals, we can control who can see our posts. If we want to limit it to just friends and family, we can change our own privacy settings. But people do not necessarily control how schools share their posts and images, and all of the posts we analyzed were strictly publicly accessible. Anyone in the world can access them.

Even if one considers the potential harm of this situation to be minimal, there are small steps that schools can take that could make a notable difference in whether that potential is present at all:

- **Refrain from posting students’ full names**

Not posting students’ full names would make it much more difficult for individual students to be targeted and for students’ data to be sold and linked with other data sources by companies.

- **Make school pages private**

Making school pages private means that data mining approaches similar to our own would be much more difficult – if not impossible – to carry out. This single step would drastically minimize risks to students’ privacy.

- **Use opt-in media release policies**

Opt-in media release policies require parents to explicitly agree to have photos of their child shared via communications and media platforms. These may be more informative to parents – especially if they mention that the communications and media platforms include social media – and more protective of students’ privacy than opt-out policies, which require parents to contact their child’s school if they do not want their child’s photo or information to be shared.

In sum, schools’ Facebook pages are different from our personal social media accounts, and posts on these pages may threaten the privacy of students. But using social media doesn’t have to be an either-or proposition for schools. That is to say, it doesn’t necessarily come down to a choice between using social media without considering privacy threats or not using social media at all. Rather, our research suggests that educators can and should take small steps to protect students’ privacy when posting from school accounts.

Notes

This text was originally published on The Conversation blog and has been re-posted with permission.

This post represents the views of the authors and not the position of the Parenting for a Digital Future blog, nor of the London School of Economics and Political Science.

Featured image: photo by Pixels