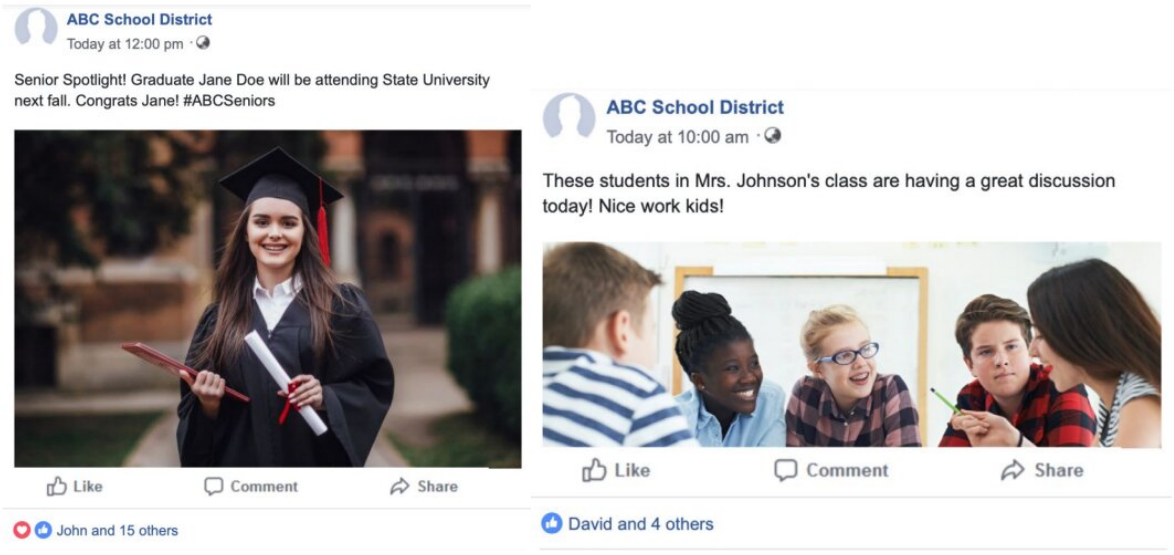
# Study: Schools' social media posts may be compromising student privacy

November 2 2022



ABC School District
Today at 12:00 pm

Senior Spotlight! Graduate Jane Doe will be attending State University next fall. Congrats Jane! #ABCSeniors

John and 15 others

ABC School District
Today at 10:00 am

These students in Mrs. Johnson's class are having a great discussion today! Nice work kids!

David and 4 others

The post on the left contains one student's name in the text of the post (Jane Doe) and one student's face in the image. This post would be coded as having one identifiable face because there is only one name and one face; thus, they can be identified together. The post in the right panel contains no student names in the text of the post but one staff last name (Johnson). The image would be coded as having three student faces, despite there being five individuals pictured because only three of the student's faces are the eyes, nose, mouth, and/or ears clear and visible. This post would be coded as having zero identifiable faces because none of the pictured students are named in the text of the post, and there is no staff face in the image to be identified with the listed name. Credit: *Educational Researcher* (2022). DOI: 10.3102/0013189X221120538

U.S. schools and school districts have shared an estimated 4.9 million posts that include identifiable images of students on public Facebook pages, unintentionally putting student privacy at risk, according to a new study. Around 726,000 of these posts are thought to identify one or more students by their first and last names. The research was published today in *Educational Researcher*.

The study examined publicly accessible posts on U.S. school and school district Facebook pages from 2005 to 2020. During that time, schools published about 18 million posts, with the annual frequency of posts, and the proportion of posts with photos, increasing each year. Public Facebook posts are accessible by all visitors to the platform, including those without a Facebook account.

"While the percentage of Facebook posts that identified students was small, the sheer volume of posts meant that hundreds of thousands of students had personally identifiable information shared by their schools," said coauthor Joshua M. Rosenberg, an assistant professor of STEM education at the University of Tennessee, Knoxville. "These findings suggest that student privacy may inadvertently be threatened by the social media activity of schools and districts."

While previous research has looked at how social media sharing by individual educators may place the privacy of students at risk, Rosenberg notes this study is the first to consider the privacy implications of social media activities undertaken by schools and districts.

Rosenberg conducted the study with Conrad Borchers (Carnegie Mellon University), Macy A. Burchfield (University of Tennessee, Knoxville), Daniel Anderson (Abl Schools), Sondra M. Stegenga (University of Utah), and Christian Fischer (University of Tübingen).

Using CrowdTangle, Facebook's tool for scholars and journalists that provides access to data on the platform's public posts, the researchers accessed public Facebook posts from all public schools and school districts in the United States. They found the posts by searching for links to Facebook pages from school and district website homepages. Thus, only schools and districts that linked to their Facebook page from their homepage were included in the sample.

The researchers found that of the 18 million posts, approximately 13.9 million included images of individuals of any age. Extrapolating from an analysis of a randomly selected sample of posts, the researchers estimated that 4.9 million of the posts had identifiable images of students, and 726,000 of these identified students' first and last names.

"The posts we studied may represent the largest existing collection of publicly accessible, identifiable images of minors," said Rosenberg. "It is likely that the photos are being accessed by a range of actors, including government agencies, predictive policing companies, and those with nefarious intent."

The study notes that government agencies in the U.S. and other countries regularly access public social media data for purposes ranging from monitoring immigration and predicting crime risks to documenting social connections. It also notes that the Australian government's online safety agency has reported that tens of millions of harmless images of minors originally shared on social media have been downloaded and saved on child exploitation sites.

"The threat to privacy will continue to grow, perhaps quickly, due to expanding facial recognition technology," said Rosenberg. He also explained that a simple reverse image search on Google could link a student to other sources of personally identifiable information online.

Rosenberg and his coauthors said there are practical steps that school leaders could take to mitigate risks. These include not including students' full names in posts; asking parents to opt in to, rather than opt out of, the sharing of their children's information on school social media; making it easy for parents to request that photos of their children be removed; and making school or district pages private.

Media companies, Rosenberg added, should consider changing the default settings for schools, automatically making pages private, which would drastically reduce the risk that student information is collected at a large scale for unintended secondary uses.

He also noted policymakers and government regulators could do more to reduce the risk that schools and other organizations that serve children will inadvertently compromise children's privacy.

"As a nation, the U.S. needs to devote greater attention and resources to mitigating the potential downsides of the pervasive sharing of children's information on social media, particularly when it is organizations such as schools and districts that are doing the sharing," said Rosenberg.

The study's authors acknowledged the importance of parent engagement efforts, including the use of social media by schools. However, they noted this must always be balanced with safety and privacy protections on multiple levels.

"While parents and schools can take steps to protect student privacy, it is also the responsibility of social media platforms and the wider society to ensure that policies and regulations keep pace with rapidly evolving technology," Rosenberg said.

**More information:** Joshua M. Rosenberg et al, Posts About Students on Facebook: A Data Ethics Perspective, *Educational Researcher* (2022). DOI: 10.3102/0013189X221120538

Provided by American Educational Research Association

Citation: Study: Schools' social media posts may be compromising student privacy (2022, November 2) retrieved 25 April 2024 from https://phys.org/news/2022-11-schools-social-media-compromising-student.html