SOCIAL MEDIA AND STUDENTS' PRIVACY:

WHAT SCHOOLS AND DISTRICTS SHOULD KNOW

Sharing good news about students on public social media accounts could have negative unforeseen consequences.

By Joshua M. Rosenberg, Macy Burchfield, Conrad Borchers, Benjamin Gibbons, Daniel Anderson, & Christian Fischer

For many schools and school districts around the United States, a Facebook page or Twitter account serves as a tool for updating the community about events, highlighting the accomplishments of staff and students, and, especially during a pandemic or other crisis, sharing essential information (Michela et al., 2021; Rosenberg & Nguyen, 2021). Because their purpose is to reach the community, official school social media accounts are often fully accessible to the public. But what does this mean for student privacy, especially in a time when rapid technological advancements allow for increasingly sophisticated analyses of social media and image data? While some research on social media use has focused on privacy (e.g., Fiesler & Proferes, 2018), no research to our knowledge has investigated it in the context of K-12 educational institutions. We have made some initial steps into building a research base by examining the extent to which students are identifiable in Facebook posts of public schools and districts and pinpointing the potential risks of that data (Burchfield et al., 2021).

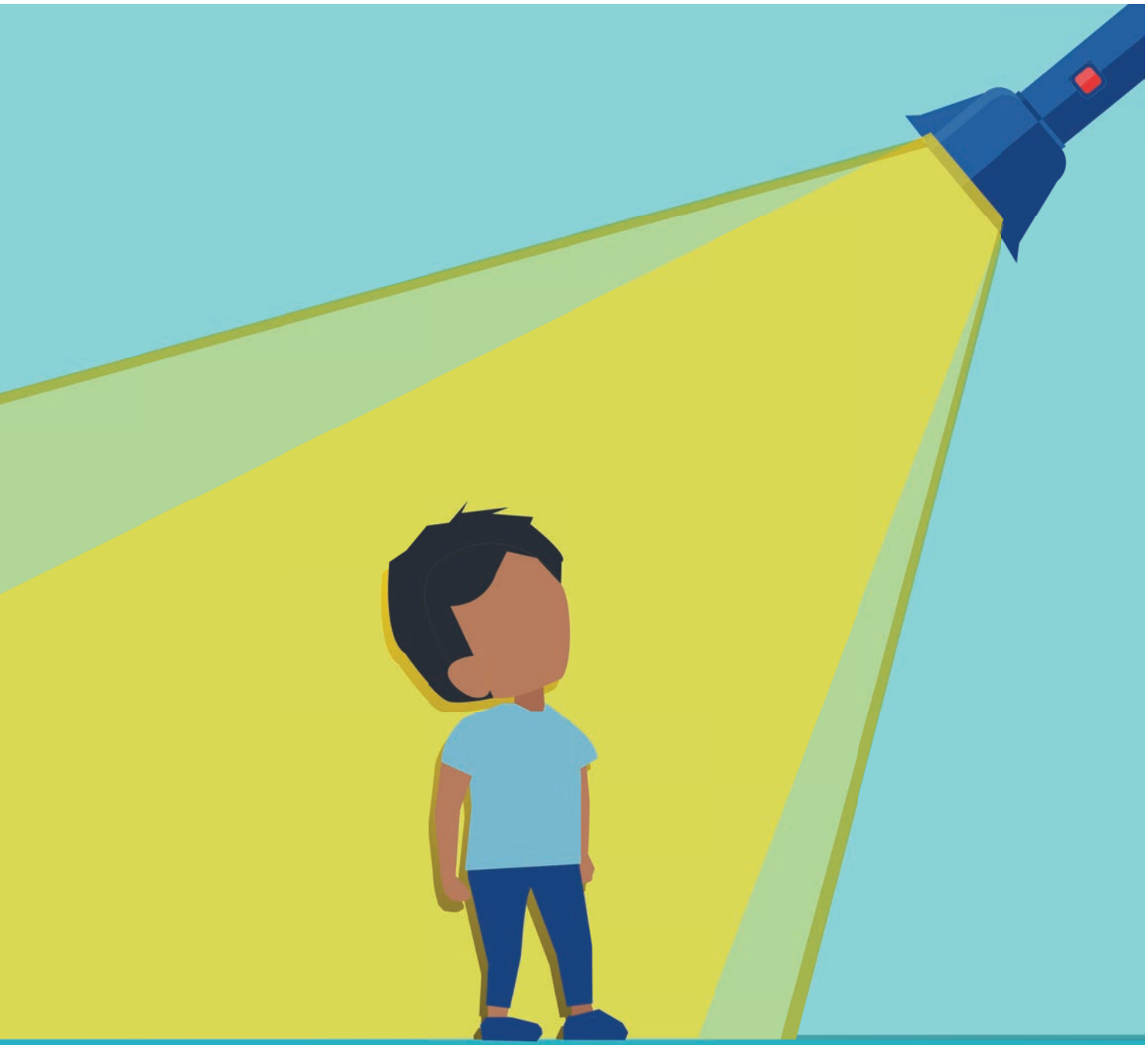
Over the past year, we have explored how schools and school districts use social media to communicate, and we have been impressed by the unabashedly positive and uplifting messages K-12 educational institutions shared on their accounts.

JOSHUA M. ROSENBERG (jmrosenberg@utk.edu; @jrosenberg6432) is an assistant professor of STEM education in the Department of Theory and Practice in Teacher Education and a faculty fellow at the Center for Enhancing Education in Mathematics and Sciences at the University of Tennessee, Knoxville. He is a coauthor of *Data Science in Education Using R* (Routledge, 2020). **MACY BURCHFIELD** (macyburchfield@gmail.com; @macyburchfield) is an undergraduate researcher at the University of Tennessee, Knoxville. **CONRAD BORCHERS** (conrad.borchers@student.uni-tuebingen.de; @conradborchers) is an undergraduate student of psychology at the University of Tübingen, Germany. **BENJAMIN GIBBONS** (ben.gibbons@emory.edu; @bdgibbo) is a student at Emory University, Decatur, GA. **DANIEL ANDERSON** (daniela@uoregon.edu; @datalorax_) is a research associate professor at the University of Oregon, Eugene. **CHRISTIAN FISCHER** (christian.fischer@uni_tuebingen.de; @FischerTubingen) is an assistant professor of educational effectiveness at the University of Tübingen, Germany.

However, many of these public posts included the names and faces of students, and because these were posts by schools and districts, the photos were implicitly tied to a particular place. Those who create these posts doubtless want to recognize or even celebrate individual students — indeed, many posts were to announce students' accomplishments — but they could be unintentionally compromising students' privacy in unseeable and often unknowable ways.

Potential harm to students

While school districts may not have reason to think that individuals or organizations may use these posts of students for nefarious ends, it is hard to predict how identifiable photos of students could be used now or in the future. We already know that facial recognition algorithms exist that use images to predict such characteristics as political identity (Kosinski, 2021) or sexual orientation of individuals



GETTY IMAGES

from facial images (Wang & Kosinski, 2018). It is not beyond the pale to imagine using photos to make such predictions (correctly or incorrectly) in ways that could result in personal, educational, or employment-related discrimination. While the validity and ethical integrity of such algorithms are still contested, their existence demonstrates how technological advancements pose unknown risks to individuals with publicly available personal data.

Furthermore, Facebook also has a robust facial recognition program that they describe in the help section of their website, and it is widely documented that Facebook creates "shadow" profiles for individuals depicted in photos, but without accounts (Garcia, 2017; Hautala, 2018; Tufekci, 2018). Thus, Facebook, and others who access publicly available social media data, and who often sell it to others (Confessore, 2018), may already be harvesting and using facial recognition data on students for commercial gain.

Finally, malicious actors could use posts to target and cyberstalk individual students or to systematically collect information on them to write highly customized — and thus convincing — fraud emails (a practice often referred to as "spear-phishing"). In sum, the risks to individual students may appear small, but they could easily increase over time. Which students could be targeted and how is difficult to predict, especially given the rapid technological advancements and open questions about ethical boundaries and regulations for social media data.

How widespread is the risk? We found that there have been a remarkable 18 million posts on Facebook from U.S. schools and school districts, and 9.3 million posts included one or more images (Burchfield et al., 2021). In our research, we randomly sampled 100 of these 9.3 million posts with images and found 187 student faces, five of which we could easily connect with student names.

While five names and photos of students from 100 posts may seem like a small number, when we consider the entire set of posts, it becomes more notable. Extrapolating from our sample, we estimated that around 15-20 million photos of students' faces have been shared on schools' and districts' Facebook pages, and between 150,000 and 1 million-plus student names and faces have been shared in the entire population of posts. In short, there's an abundance of publicly accessible photos of students' faces being shared in publicly accessible ways, with-perhaps as many as 1 million being shared in ways that allow the students' faces to be identified by name (and school or district).

> Limiting public access to pages reduces the possibility that people with no connection to the school system can find photos of students.

Implications for schools' social media use

The scale of Facebook is huge. Public posts on Facebook may represent the largest collection of identifiable photos of students (mostly minors), and these posts are accessible by anyone in the world — even individuals without a Facebook account who visit the page of a school or district. Moreover, given the nature of data shared on Facebook, these posts are likely to persist on the Internet for a long time (perhaps indefinitely).

It is a strange feature of social media that posts written with the aim of lauding a student and encouraging others in the school or community to do the same could mean that students' privacy is placed at risk. And it's understandable that the people creating these posts would make this mistake. We are accustomed to sharing identifiable pictures of ourselves and our family members and friends through social media, but we have control of the privacy settings on our personal accounts and can, therefore, restrict who sees those posts. The pages of schools and districts, on the other hand, are usually public, and students and parents have limited agency regarding what and how much is posted. While many K-12 institutions require parents and students to sign a waiver before publicly sharing their child's name and face, our research has revealed that the accessibility of photos of students may be far greater than most parents realize (Burchfield et al., 2021). Having more complete information about the risks might make a difference in a parent or child's decision regarding the sharing of their information.

Our goal in this research is not to suggest that K-12 institutions stop using social media. As we've conducted our research, we have often been impressed by how schools and districts use Facebook, Twitter, and other tools, particularly during the COVID-19 pandemic, when it has been so important to maintain communication with students and families. We do, however, hope to prompt reflection about and changes in how social media platforms are used.

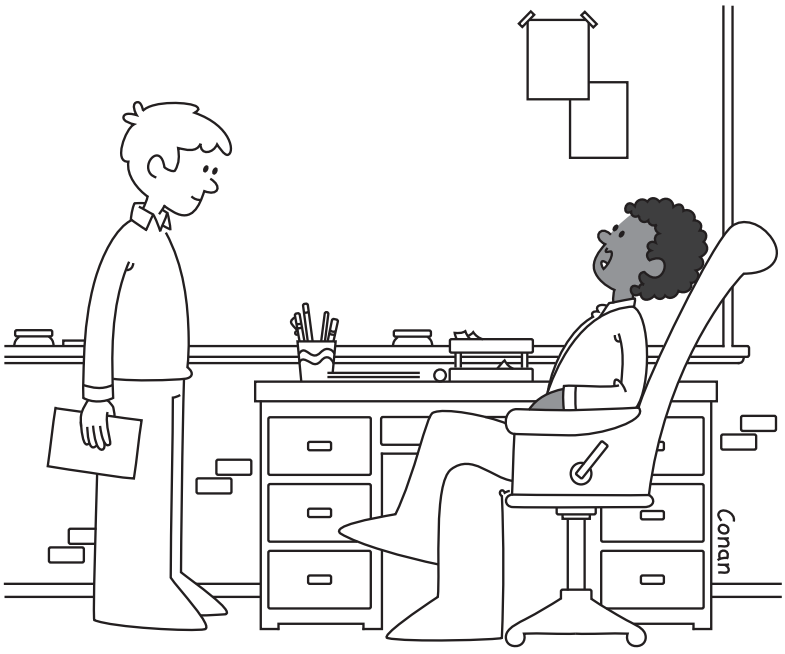
When images on Facebook and other platforms are easily accessible to parents, friends, and members of the local community, they are also accessible to those who wish to cause harm.

How to protect student privacy

What can and should schools and districts do? We offer several practical suggestions:

Refrain from posting students' full names. This will substantially reduce the risk that students can be identified by bad actors. Schools wishing to laud students might post the students' first name only, or their first name with the first initial of their last name, so that a student can still be recognized and congratulated by friends and neighbors but risks to their privacy are reduced.

Consider posting non-portrait photos. Many schools and districts tend to post yearbook-style photos that clearly depict the faces of students whose accomplishments they want to recognize. However, such photos are particularly risky precisely *because* it is so easy (for humans and algorithms) to identify the given students. Selecting photos that capture students from a distance (for example, at an awards ceremony or athletic event, or in a group with many other people) can reduce the risk to their privacy, and such photos may be less likely to be accessed (legally or not) for use in a facial recognition database.



"It certainly is a comfortable chair, but I still don't think it's the answer to our teacher retention problem."

Ask parents to opt in (rather than requiring them to opt out) to sharing their child's information. Some schools and districts have an opt-out policy, which asks parents to contact their child's school or district to indicate that they would prefer that the school *not* share photos and other information about their child through media, including the school's or district's website and social media accounts. Opt-in policies take the opposite tack, requiring parents to give the school permission to share images of and information about their children. This may create an extra administrative burden for the school, but making sharing a little less seamless can emphasize the gravity of the situation (and the potential risks) involved. Plus, it minimizes parents' fear that their child will be disadvantaged if they choose to opt out from the media release policy.

Make it easy for parents to request that photos of their children be removed. As parents become more attuned to some of the detrimental effects of using social media, including privacy risks, they may want the school to take down photos of their children — even those posted long ago. While this may not happen very often, we suggest that schools and districts create a simple and straightforward way for parents to make these requests. Even parents who've opted in to media releases should be able to request that specific photos be removed or to change their minds and opt out of all photos.

Educate parents about what information will be shared and how. When asking parents to opt in or out of social media sharing, schools and districts should fully inform them about the specific ways in which photos and other information will be shared. Further, because many parents are unaware of potential risks to their children's privacy, schools and districts should take the opportunity to educate them about this topic (by sharing this article or other relevant resources; e.g., Swisher, 2019, Tufekci, 2018).

Consider making school or district pages private. Although not foolproof, limiting public access to pages (by setting them to private on Instagram or Twitter or creating a private page or group on Facebook) reduces the possibility that people with no connection to the school system can find photos of students. However, this step requires an additional administrative burden for those managing a page because they will need to approve requests from others to join the page.

In sum, we urge schools and districts to be cautious when it comes to posting identifiable information about students on social media. Even when such sharing is entirely legal and does not provoke resistance from parents, the privacy implications for students may be serious, now or in the near future. Minor students in particular may not yet fully understand how their likeness is being used and shared by their educational institution, and the adults in their lives have a responsibility to protect and care for them.

Finally, since our study focused only on schools' use of students' images and information, we cannot share specific recommendations for teachers who use social media to communicate about their work. We suspect that the risks are smaller, in this case, because the online reach of individual teachers tends to be much smaller than that of schools and districts. Still, we would urge them to be cautious when sharing news and updates from their classrooms on social media.

Finding the balance

Social media is here to stay, and for the most part we see it as a boon for educators and educational institutions, enabling them to communicate with parents, students, and the community more effectively, especially during times of crisis. However, schools have already posted millions of photos (hundreds of thousands of which allow anyone to connect a student's face with their name and location at a particular time), and the risks to students' privacy are significant. When images on Facebook and other platforms are easily accessible to parents, friends, and members of the local community, they are also accessible to those who wish to cause harm.

Our goal is not to stop schools from posting helpful information or sharing good news about students. But we do want those in charge of schools' social media policies and accounts to understand the risks and take steps to protect students' privacy. As such technologies evolve, we should all be careful to weigh their costs along with their benefits. ■

References

Burchfield, M., Rosenberg, J.M., Thomas, T., Borchers, C., Gibbons, B., & Fischer, C. (2021). Is student privacy "quick and easy"? Investigating student images and names on K-12 educational institutions' Facebook postings. In S. Hsiao and S. Sahebi (Eds.), *Proceedings of the 11th International Conference on Educational Data Mining* (pp. 619-624).

Confessore, N. (2018, April 4). Cambridge Analytica and Facebook: The scandal and the fallout so far. *The New York Times*.

Fiesler, C. & Proferes, N. (2018). "Participant" perceptions of Twitter research ethics. *Social Media+ Society, 4* (1).

Garcia, D. (2017). Leaking privacy and shadow profiles in online social networks. *Science Advances, 3* (8).

Hautala, L. (2018, April 11). Shadow profiles: Facebook has information you didn't hand over. *CNET*.

Kosinski, M. (2021). Facial recognition technology can expose political orientation from naturalistic facial images. *Scientific Reports, 11* (1), 1-7.

Michela, E., Rosenberg, J., Kimmon, R., Sultana, O., Burchfield, M.A., & Thomas, T. (2021). "We are trying to communicate the best we can": Districts' communication on Twitter during the COVID-19 pandemic. *OSF Preprints*.

Rosenberg, J.M. & Nguyen, H. (2021). How K-12 school districts communicated during the COVID-19 pandemic: A study using Facebook data. In N. Dowell, S. Joksimovic, M. Scheffel, & G. Siemens (Eds.), *Companion Proceedings of the 11th International Conference on Learning Analytics & Knowledge* (pp. 118-120).

Swisher, K. (2019, December 24). Be paranoid about privacy. *The New York Times*.

Tufekci, Z. (2018, March 19). Facebook's surveillance machine. *The New York Times*.

Wang, Y. & Kosinski, M. (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of Personality and Social Psychology, 114* (2), 246.

GETTY IMAGES