Posts on Facebook by Schools and Districts and the Potential Risks to Students' Privacy

Joshua M. Rosenberg¹, Macy Burchfield¹, Conrad Borchers², Benjamin Gibbons³, Daniel Anderson⁴, and Christian Fischer²

¹University of Tennessee, Knoxville

²University of Tübingen, Germany

³Emory University

⁴University of Oregon

Abstract

For many schools and districts in the United States, Facebook has emerged as an important communication tool. Facebook has been used for many purposes including sharing timely information, building a sense of community, and highlighting staff and students. However, neither researchers nor, we think, most schools and districts have paid enough attention to how their Facebook use may pose a risk to the privacy of the individuals—often students who are minors. One of our recent social media studies showed that between 15 and 20 million photos of students have been shared on strictly publicly accessible Facebook pages of public schools and districts. We estimated that at least 150,000 of these photos—and perhaps as many as a million or more—depict students who are identifiable by name and school and/or district. In this article, we review some of the risks to students that might result from their identification through social media posts and offer practical steps that schools and districts can take to minimize these risks.

Introduction

For many schools and school districts around the county, a Facebook page or Twitter account serves as a tool for updating the community about events, highlighting the accomplishments of staff and students, and, during a pandemic, sharing essential information (Michela et al., 2021; Rosenberg & Nguyen, 2021). You may have liked posts from such pages or accounts yourself! Because of its community-oriented nature, social media posts by official school accounts are often fully accessible to the public. While rapid technological advancements allow for increasingly sophisticated analyses of social media and image data, the privacy implications of public schools' use of social media remain unclear. We recently tried to shed light on the extent to which students are identifiable in Facebook posts of public schools and districts and pinpointed the potential risks of that data (Burchfield et al., 2021).

Our Research on Schools and Districts' Use of Facebook

Over the past year, we (a group of researchers and educational data scientists) have explored how schools and school districts use social media to communicate. We have been impressed by the unabashedly positive and uplifting messages shared by the accounts associated with these K-12 educational institutions. In so being, we noticed a pattern that gave us a moment's pause: Many of these public posts included the names and faces of students. Moreover, because these were posts by schools and districts, they were identifiable photos that were also implicitly tied to a particular place. While privacy has been a focus of some research on social media use (e.g., Fiesler & Proferes, 2018), no research to our knowledge has investigated privacy in the context of social media use by K-12 educational institutions. We note that while any individual crafting a post is doubtless with the intent to recognize or even celebrate individual students—indeed, many identifiable posts were to announce students' accomplishments—an unintentional effect could be that students' privacy is impacted in unseeable and often unknowable ways.

How Might This Data be Used in Ways That Are Harmful to Students?

While school districts may not have reason to think that individuals or organizations may use these identifiable posts of students for nefarious ends, there is the risk that photos of students linked to their name and school (district) could be used to threaten individual students or groups of students now or in the future. Indeed, it is hard to predict how identifiable photos of students could be used; we already know that facial recognition algorithms can use images to predict characteristics of people, such as their political identity (Kolinski, 2021). It is not beyond the pale to imagine predicting other characteristics of students, including those that could be more damaging if predicted (correctly or incorrectly) and revealed than one's political identity, mental

health, or sexual orientation which could result in personal, educational, or employment-related discrimination.

As one example, algorithms exist that were designed to infer the sexual orientation of individuals from facial images (Wang & Kosinski, 2018). We note that the development and use of such algorithms is one example of a contested use of facial recognition. While the validity and ethical integrity of such algorithms are still subject to debate, they demonstrate how technological advancements pose unknown risks to individuals with publicly available personal data. Furthermore, it is widely documented that Facebook creates “shadow” profiles for individuals depicted in photos, but without accounts (Hautala, 2018; Garcia, 2017; Tufekci, 2018). Facebook also has a robust facial recognition program that they describe in the help section of their website (Facebook, 2021). Thus, Facebook, along with others who may legally or illegally access publicly available social media data that they can sell to others who construct algorithms (Confessore, 2018), may already be harvesting and using facial recognition data on students to commercially benefit from recognizing them--and potentially their identity. Finally, malicious actors could possibly use such posts to target individual students (e.g., cyber-stalking), and criminals might also systematically collect (and/or link with) information on individuals through social media to write highly customized—and thus convincing—fraud emails, which is often referred to as “spear-phishing”. In sum, the risks to individual students may appear small, but the risks to a small number of students over time may be great, and difficult to predict due to rapid technological advancements and open questions pertaining to the ethical boundaries and regulations of artificial intelligence.

How widespread is the potential issue? We found that there have been a remarkable 18 million posts on Facebook from United States schools and school districts. Importantly, 9.3 million posts included one or more images (Burchfield et al., 2021). In our research, we manually examined 100 randomly sampled posts containing photos (from the larger collection of more than nine million posts). For these, we counted the number of photos that made students’ faces visible. Then, we sought to find out how many of these photos were named. In all, we detected 187 student faces in the 100 posts we analyzed; of those 187, five were identified in such a way that it was clear what the students’ name was (and vice versa; what the photo of the student who was named was).

While these numbers for the sample (of 100 posts) we analyzed are small, when we consider the entire set of posts, they became more notable. We carried out an inferential analysis using the ratio of photos and identifiable photos per post and a Binomial distribution and estimated that there are between around 15 and 20 million photos of students’ faces shared on the pages of schools and districts. Making an inference from our sample to the population of posts, we estimated the number of students’ faces that we identified were consistent with there being between 150,000 and more than one million students’ faces shared in the entire population of

posts. In short, there are very many photos of students' faces being shared in publicly accessible ways, and many of these students—perhaps as many as one million—are shared in ways that allow the students' faces to be identified by name (and, by school or district).

Implications of Our Research on Students' Privacy on Social Media

What should we make of these findings? The scale of Facebook is huge. Even a small proportion of posts that identify a few students accumulate over time and across school and district pages to posting tens of millions of photos of students, possible identification of hundreds of thousands of students. These posts may (likely?) represent the largest public collection of identifiable photos of students (and minors). Importantly, and disturbingly, these posts are accessible by anyone in the world—even individuals without a Facebook account who simply visit the page of a school or district (into the indefinite future) or do so with the intent of collecting and reselling this data (Confessore, 2018). Moreover, given the nature of data shared on Facebook, these posts are also likely to persist on the Internet for a long time (perhaps indefinitely).

It is a strange feature (and perhaps a “bug”) of social media that posts, doubtlessly many written with only the aim of lauding a student and allowing others in the school or district community to do the same, could mean that students' privacy is placed at risk. In some ways, the blurred boundaries between the personal and professional life on social media contribute to this issue: We are accustomed to sharing (identifiable) pictures of ourselves and our family members and friends through social media. The key differences are that the pages of schools and districts are not, like our own posts, restricted to those who we wish to see our posts, and students and parents have restricted agency regarding what and how much is posted. Moreover, 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 people (and parents) realize (Burchfield et al., 2021)—and this information might make a difference in a parent or child's decision regarding the sharing of their information.

In this way, K-12 institutions' use of Facebook represents a form of context collapse between the private and professional sphere, the phenomenon of social media encouraging individuals to communicate to and with multiple audiences (i.e., friends and colleagues at work) via the same medium, breaking down historical and traditional barriers between interacting across these different audiences (Marwick & boyd, 2011; Vitak et al., 2012).

Our goal in this research is not to suggest that K-12 institutions should stop using social media. Through our research, we have been uplifted by how schools and districts used - and use - social media, particularly during the COVID-19 pandemic, when we have seen the many ways

districts have continued to provide (and communicate about) the services they provide. We do, however, hope to prompt reflection and changes in how institutional social media platforms are used, as we discuss next.

What Schools and Districts Can Do to Protect Students' Privacy on Social Media

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

1. *Refrain from posting students' full names.* One step that schools and districts can take is to refrain from posting students' full names (first and last names); this step will likely reduce the risk to identify students substantially. A compromise may be to 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 but risks to their privacy may be reduced.
2. *Consider posting non-portrait photos.* Portrait—yearbook-style—photos that clearly depict most of the students' faces are likely the choice of many schools and districts when determining which photo to share as such photos focus clearly on the students being recognized. However, this feature is why such photos may present the greatest potential identifiability risk to students: It is easy to make out who the student is - both for humans as well as algorithms. The careful selection of photos that depict a student at an awards ceremony, athletics event, or in a group with many people may make it more difficult to identify a student (and may reduce the risk to students' privacy). In addition, such photos may be less likely to be accessed (legally or not) for use in a facial recognition database.
3. *Ask parents to opt-in—rather than opt-out—to the sharing of their child's information.* Some schools and districts have an opt-out policy, which places the responsibility (and burden) of contacting their child's school or district to indicate that they would prefer for photos and other information about their child to *not* be shared through media, including the school's or district's website and their social media platforms. Opt-in policies require parents to decide to have their children's information shared through these channels. This may minimize any perception of coercion (or conformity, as parents may feel that their child will be disadvantaged if they choose to opt-out from this media release policy) that parents may feel around agreeing for photos and other information about their child to be shared. This concern relates to our next two recommendations.
4. *Allow parents to request for photos of their children to be removed from their school's or district's page.* As we (as a society) become more attuned to some of the detrimental effects of using social media, including privacy risks (and for other reasons), some parents may wish for photos of their children to be removed—even in the case of photos posted long ago! While this may not be a common occurrence, we suggest that schools and districts create and communicate about how photos can be removed by request (even by parents who opted-in to media releases).

5. *Consider educating parents at the time they opt-in to the sharing of their child's information about what content will be shared—and how it will be shared.* Related to asking parents to opt-in to media release policies, it may be possible that many parents are unaware of the breadth and fully-public nature of the posts on many social media platforms, including (in most cases—and in the case of *all* of the Facebook pages included in our study) posts on Facebook, Twitter, and Instagram. Schools and districts may choose to use this article or other resources (see Swisher, 2019, Tufekci, 2018) that highlight some of the privacy risks associated with social media use. Because of this, schools and districts may take the opportunity to inform and educate parents about the specific ways in which photos and other information will be shared. Such communications can provide a positive context for schools and districts that wish to establish the norm of not sharing highly identifiable information through official school or district pages. We acknowledge that an opt-in system may be a greater administrative burden for schools and districts, but perhaps that burden can emphasize the gravity of the situation (and the potential risks) involved.
6. *Considering making school or district pages private.* This step requires an additional administrative burden for those managing a page - the need to approve requests from others to join the page. Though not foolproof, this additional step would, at least, make it so that posts are not publicly accessible.

To sum up, we urge schools and districts to be cautious when it comes to posting identifiable information about students on social media. While it may not pose legal issues in some districts (or resistance from parents), there are privacy threats to students that may be serious now or in the near present. Moreover, an ethical (and, potentially, a legal) perspective suggests that students - minors - may not yet fully understand how their likeness is being used and shared by their educational institution, and we should be cautious given the responsibility we have to protect and care for them.

Lastly, what can and should individual educators do? Our study (and therefore any recommendations we would like to make) do not pertain to individual educators' uses of social media. While some of the issues we have discussed are comparable between schools' and districts' social media use and the use of social media by individual educators, the risks are smaller, in our view, because the reach and audience of individual educators are, in many cases, smaller than schools and districts--and it is more challenging (for us and others) to collect this kind of information from individual educators at scale. Nevertheless, some of the recommendations we have made likely apply to educators sharing news and updates from their classrooms via social media, and we also urge critical reflection and careful planning about these uses of social media.

Conclusion

Social media is here to stay We truly see this as a boon to educators and educational institutions seeking to communicate with parents, students, and the community more effectively using tools that many individuals are already using, especially during times of crisis in which timely communication is vital. However, with millions of photos—and hundreds of thousands (and potentially millions) of identifiable photos that are both connected to particular locations (and times)—the risks to students at present and in the future are non-negligible and should prompt pause and reflection around how we in education use social media. This is especially the case given the public nature and ease of accessibility of posts on Facebook; posts that are accessible to so many in the community, but also unfortunately to those who may wish to cause harm.

So, as you view a post by your school or district, continue to interact and connect! Our aim is not to stop that, but to prompt a moment's reflection, especially on the part of those responsible for posting from their school's or district's social media page: Recognizing possible risks to students and taking small steps to protect students' privacy may make a difference now and in the future. As technologies and modes of communications advance, issues beyond the benefits of these tools also emerge, with privacy being perhaps a key one for us as educators to consider going ahead.

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*.
- Confessore, N. (2018). Cambridge Analytica and Facebook: The scandal and the fallout so far. <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>
- Facebook. (2021). What is the face recognition setting on Facebook and how does it work? <https://www.facebook.com/help/122175507864081>
- Garcia, D. (2017). Leaking privacy and shadow profiles in online social networks. *Science Advances*, 3(8).
- Hautala, L. (2018). *Shadow profiles: Facebook has information you didn't hand over*. CNET. <https://www.cnet.com/news/shadow-profiles-facebook-has-information-you-didnt-hand-over/>
- Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, 13(1), 114-133.
- Michela, E., Rosenberg, J. M., Sultana, O., Burchfield, M., Thomas, T., & Kimmons, R. (2021, April). “Life will eventually get back to normal”: School districts’ Twitter use in response to COVID-19. Presentation at the American Educational Research Association Annual Meeting, Orlando, FL.
- Kosinski, M. (2021). Facial recognition technology can expose political orientation from naturalistic facial images. *Scientific reports*, 11(1), 1-7.
- Rosenberg, J. M., & Nguyen, H. (2021). How K-12 school districts communicated during the COVID-19 pandemic: A study using Facebook data. In In Dowell, N., Joksimovic, S., Scheffel, M., & Siemens, G. (Eds.), *Proceedings of the 11th International Conference on Learning Analytics & Knowledge*. Association for Computing Machinery.
- Swisher, K. (2019). Be paranoid about privacy. *The New York Times*. <https://www.nytimes.com/2019/12/24/opinion/location-privacy.html>

- Tufekci, Z. (2018). Facebook's surveillance machine. *The New York Times*.
<https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html>
- Quodling, A. (2018). Shadow Profiles-Facebook Knows about You, Even If You're Not on Facebook. *The Conversation*, 13. <https://theconversation.com/shadow-profiles-facebook-knows-about-you-even-if-youre-not-on-facebook-94804>
- Vitak, J., Lampe, C., Gray, R., & Ellison, N. B. (2012). " Why won't you be my Facebook friend?" strategies for managing context collapse in the workplace. In *Proceedings of the 2012 iConference* (pp. 555-557).
- 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.