BEARD LEGAL GROUP
EDUCATION LAW REPORT
Published in Cooperation with the Pennsylvania School Study Council, Inc.

January 2023

TikTok, TikTok: The Clock is Ticking

TikTok is a social media platform based upon user-created video content, which has captivated a generation with its addictive entertainment and subculture—and resulted in its ascent to unparalleled success and prominence. However, the platform is enveloped in controversy as the extent of its data-gathering and related implications garner greater scrutiny.

TikTok has a default setting granting TikTok broad permissions and access to the user's device, some of which are required to use certain in-App features, and which extend well beyond the scope of those required for other social media platforms. The cybersecurity consensus on TikTok is it engages in "invasive" data-gathering—well beyond the level of data-gathering associated with other Apps or social media platforms. For example, TikTok requires access to a user's camera and microphone, which is superficially understandable because it is a platform for recording and sharing videos—but access extends well beyond reasonable user expectations. Specifically, a user would expect live access to their microphone or camera to be limited to when the user presses the in-App record button—but it is not.

These permissions grant TikTok unlimited access to the user's camera, microphone, and related media files. To this end, the public evidence of intrusions of an extreme magnitude are primarily anecdotal with numerous users sharing images showing TikTok accessing such features in the background—which raises the specter of TikTok monitoring users or screen-recording a device. However, the breadth of TikTok's data-gathering is beyond speculation as Cybersecurity Engineer and Expert Thomas Perkins recently published a TikTok source-code cybersecurity analysis, which concluded TikTok accessed permissions and captured device information well beyond the permissions and data necessary for functionality—and aggressively seeks permission if a user enables manual settings for more privacy.

Perkin's article states:

> For the TikTok application to function properly, most of the access and device data collection is not required. This leads us to believe that the only reason this information has been gathered is for data harvesting. It is also notable that the device only needs to ask the user for permission to perform each of these actions once and then follow the user's preferences. The application however has a culture of persistent access or continuously asking for a decision reversal by the user. The hourly checking of location is also unnecessary. Finally, device mapping, external storage access, contacts and third-party applications data collection allows TikTok the ability to reimage the phone in the likeness of the original device.

Moreover, the privacy concerns are amplified exponentially by the common practice of connecting to wireless Internet, or "WiFi." Generally, WiFi Internet has limited defensive mechanisms, and controlled access to the network (e.g., password protection). Once WiFi is accessed, almost all of the

(Continued on Next Page)

Inside …

TikTok, TikTok: The Clock is Ticking

...Continued

data or information transmitted on that network is unencrypted and unsecured. Thus, WiFi generally results in additional vulnerability and access for data-gathering applications—including TikTok or hackers.

Furthermore, the Federal Bureau of Investigation (FBI) seems to find the more extreme concerns credible, as evidenced by FBI Director Christopher Wray's congressional testimony in which he noted national security concerns that TikTok could "control software on devices" and "technically compromise personal devices."

The aforementioned national security concerns are based upon more than TikTok's practice of aggressive data-gathering. Another principle issue is the control and origin of TikTok. Specifically, TikTok is a subsidiary of ByteDance, which is located in Beijing, China and influenced by China's authoritarian regime—which raises the concern that TikTok's data-gathering propensity is being utilized as a de facto intelligence-gathering apparatus. Furthermore, FBI Director Wray also detailed the national security concern regarding TikTok's inverted use as a mechanism to effectuate a psychological operation to manipulate users: "[the concerns] include the possibility that the Chinese government could use it to control data collection on millions of users or control the recommendation algorithm, which could be used for influence operations…" TikTok has denied ByteDance, or the Chinese Government, has access to United States user data and indicated such data is stored in the United States. However, Thomas Perkins' TikTok Report identified "TikTok IOS 25.1.1 has a server connection to mainland China which is run by a top 100 Chinese cyber security and data company…", which TikTok has also denied extends to China.

Meanwhile, TikTok has drawn the ire of other segments of the United States' federal government. (1) Congress initiated an investigation on TikTok; (2) Senators have issued a bipartisan request for the Federal Trade Commission to investigate TikTok; (3) the Federal Communications Commission (FCC) Commissioner, Brendan Carr, lambasted ByteDance (and TikTok) as "beholden" to China's government for survival and "required by law to comply with [their] surveillance demands…" and requested Google and Apple remove TikTok from their respective App Marketplaces; and (4) President Biden signed the "No TikTok on Government Devices Act" on December 30, 2022, which effectively banned the use of TikTok from federal government devices. Furthermore, there is growing bipartisan support for an absolute prohibition on TikTok due to the national security concerns surrounding the platform.

Similarly, at this time, at least thirty-two (32) states have announced state-level bans on state agencies, employees, or contractors utilizing TikTok on professional or government-issued devices. Pennsylvania is not among these states at this time; however, some Pennsylvania agencies have instituted intra-agency policies banning the use of TikTok. Due to the aforementioned vulnerability of WiFi, states and institutions have extended TikTok bans to include accessing state or government WiFi through TikTok on personal devices. Additionally, a growing number of institutions, including universities, are implementing internal policies reflecting similar restrictions.

Both ByteDance and TikTok deny the allegations of intrusive data-gathering and surveillance on behalf of the Chinese government. Similarly, the companies claim the experts' analysis of TikTok is flawed and misinformed. These denials hardly allay the growing international concernc regarding TikTok's practices—nor the micro-level implication as users inadvertently expose sensitive or personal information, or otherwise render their data more vulnerable.

School Districts are able to emulate the aforementioned preventative measures to decrease exposure to TikTok's data-gathering propensities, such as banning TikTok usage on professional devices; blocking TikTok from accessing the District's WiFi network; or prohibiting TikTok on District's devices, including cellphones.

Educational Training Opportunity

Beard Legal Group is partnering with the Central Susquehanna Intermediate Unit and hosting a Virtual Administrative Law Series.

The next session will occur:
Monday, February 13, 2023 from 9:00 a.m. until 12:00 p.m.

Session – 3
Social Media – Problems with Students and Teachers: What Every Administrator Should Know

Almost every week there is something in the news regarding issues with professional educators and/or students involving social media. There has been an explosion of litigation and court cases over the last ten years involving social media.

This presentation will cover important and relevant Court decisions involving the discipline of students and school staff regarding social media incidents.

Topics to be covered include the following:
- The types of policies that should be in place to address these issues and what needs to be included within District policies and handbooks.
- Discuss how the Courts, Arbitrators, Administrative tribunals and the Professional Practices and Standards Commission have ruled and addressed social media issues with professional educators.
- Case studies on Court decisions involving student communications on social media and the District's ability to regulate or discipline for same.
- Checklists of items that need to be in place to successfully defend against legal challenges involving social media.
- Developing professional development opportunities to minimize the impact of social media posts by students and staff.
- Tips for managing or responding to social media posts that have a negative impact on the District and greater school community.
- What school districts can legally do to address student and staff misconduct involving social media.
- Legal steps that can be taken to hold students or staff accountable for unprotected speech or communications on social media.
- Facebook, TikTok, Instagram, Snapchat, etc., and cell phones in the school setting.
- Issues regarding District established Facebook pages and other social medial accounts.

DETAILS:
- **Location**: Zoom (a link will be emailed to all registrants one week prior to the start of the event).
- **Cost**: based on membership – CSIU LEAs or Non-CSIU LEAs (any questions, please refer to contact information below).
- **Presenter**: Carl P. Beard, Esquire
- **Registration Deadline**: February 8, 2023

For registration information go to:
https://registration.csiu.org/event/id/DF036826-4834-401F-920E-2822768CC91E/view

Contact Information:
- If you have any questions regarding event content, please contact Dr. Anthony Serafini by emailing at: aserafini@csiu.org
- If you have difficulty creating a user account or have questions regarding registering for this event, please contact Audrey Jows by email at: ajows@csiu.org

Cancellation and Refund Policy:
- Refunds will not be provided to registrants who neither cancel nor attend the event.
- Confirmed registrants who are unable to attend the event may send a substitute in their place at no additional cost. Must cancel registration two weeks prior to the start date of the event.

Beard Legal Group Education Law Report

As solicitors, labor counsel and special counsel, Beard Legal Group represents more than 80 School Districts in Pennsylvania. The Firm has successfully negotiated hundreds of teacher and support staff contracts.

The Firm also represents a large area of the State for coverage of school board directors through their insurance carriers.

Our legal expertise includes: Solicitorship Services, Collective Bargaining – Teacher and Support Contracts, Employment Matters, Labor Arbitrations, Special Education Issues and Proceedings, Defense of Tax Assessment Appeals, PHRC/EEOC Complaints, Student Expulsion Hearings and Constitutional Issues.

About the Pennsylvania School Study Council

The Pennsylvania School Study Council (PSSC), a partnership between the Pennsylvania State University and member educational organizations, is dedicated to improving education by providing research information, professional development activities, and technical assistance to enable its members to meet current and future challenges. The PSSC offers professional development to the membership through colloquiums, workshops, study trips, consultation, publications, and customized services. For more information, visit the PSSC website, *www.ed.psu.edu/pssc/* or contact the Executive Director Dr. Peggy Schooling *mxs284@psu.edu.*

Subsequent Issues

If you have a school law question or topic you would like to have addressed in subsequent issues of the newsletter, please send an email to:

Carl P. Beard* *cbeard@beardlegalgroup.com*
Elizabeth Benjamin* *ebenjamin@beardlegalgroup.com*
Jennifer L. Dambeck* *jdambeck@beardlegalgroup.com*
Carl Deren Beard *cdbeard@beardlegalgroup.com*
Krystal T. Edwards *kedwards@beardlegalgroup.com*
Joseph D. Beard *jbeard@beardlegalgroup.com*

*Partner

Education Law Report is published by Beard Legal Group, P.C.

Prior issues are available on our website.

BEARD
LEGAL GROUP

MAIN OFFICE:
3366 Lynnwood Drive P.O. Box 1311
Altoona, PA 16603-1311
814/943-3304 FAX: 814/943-3430
www.beardlegalgroup.com