Keeping It Off the Record: Student Social Media Monitoring and the Need for Updated Student Records Laws

ABSTRACT

An increasing number of school districts work with private companies to monitor public social media and to notify administrators of alarming student information. Although these services help address challenging school safety issues, the Family Educational Rights and Privacy Act (FERPA) and state law offer little guidance on how districts should store student social media data. This Note encourages states to pass student records laws similar to recent California legislation and urges the Department of Education to clarify the relationship between student social media and education records under FERPA. New state and federal initiatives would help ensure that third parties may not access information that inaccurately depicts a student’s current emotional state and honor individual privacy as students become more mature digital citizens.

TABLE OF CONTENTS

I. TODAY’S STUDENT: SOCIAL MEDIA, SURVEILLANCE, AND PRIVACY
   FRAMEWORKS .................................................................158
   A. Social Media Use ..........................................................158
   B. Social Media Monitoring ..................................................159
   C. Schools’ Regulation of Online Student Speech ......................161
   D. Regulating Student Privacy .............................................162

II. THE PRIVACY PATCHWORK: LITTLE GUIDANCE FOR SOCIAL
    MEDIA REPORTS ..................................................................165
   A. Social Media Reports and FERPA’s “Education Records”...166
   B. Industry Privacy Pledges and Self-Regulation ......................169

III. THE NEED FOR UPDATED STATE AND FEDERAL STUDENT
    RECORDS LAWS ................................................................171
   A. Access, Amendment, and Deletion: California’s Example ....172
      1. Positive Effects on the School-Student Relationship .... 173
      2. Positive Effects on the School-Vendor Relationship ..... 175
“Im [sic] going to be a professional school shooter.”¹ This YouTube video comment was likely the first time that authorities learned of the threatening demeanor of Nikolas Cruz, the student responsible for killing seventeen high school students and staff in Parkland, Florida, in February 2018.² After the tragedy, community members and media criticized federal and local authorities for not reacting to Cruz’s social media—a digital footprint riddled with racist slurs, violent messages, and photos of guns.³ Many wondered whether this tragedy would have occurred if someone responded to the social media threats sooner.⁴

An increasing number of serious school safety incidents are foreshadowed by online student communication.⁵ In an effort to prevent these unsafe situations, many school districts have adopted procedures for monitoring students’ social media.⁶ Some schools rely on students or school resource officers to monitor and report worrisome posts.⁷ An increasing number of school districts contract with private companies that monitor public social media and provide administrators with records of potential threats that may relate to their schools.⁸

---

² See id.
³ Id.
⁸ Aaron Leibowitz, Could Monitoring Students on Social Media Stop the Next School Shooting?, N.Y. TIMES (Sept. 6, 2018), https://www.nytimes.com/2018/09/06/us/social-media-monitoring-school-shootings.html [https://perma.cc/2WCB-X2H2] (describing how more than one hundred school districts and universities have hired social media monitoring companies within the last five years).
Social media monitoring companies comply with federal law and offer an answer to challenging safety situations. Student rights advocates, however, fear that disciplining students for information found in monitoring reports may compromise students’ rights to free speech, privacy, and due process. Moreover, if an educational entity retains monitoring reports after a threat assessment, then a student’s educational record may contain information that the Family Educational Rights and Privacy Act of 1974 (FERPA) likely does not protect from disclosure. As a result, third parties may access student information that has been taken out of its original context and inaccurately depicts a student’s online presence.

This Note analyzes social media monitoring within the context of statutory privacy frameworks. It argues that states should follow California’s lead by updating student records laws with guidance on handling information gleaned from social media monitoring services and that the Department of Education (DOE) should issue guidance on the storage of student social media information. Part I discusses student social media use, popular monitoring methods, and schools’ abilities to respond to online student speech. Part II examines how FERPA and privacy pledges fail to safeguard student privacy within the context of social media monitoring. Part III explains why states should adopt policies similar to recent California legislation and why the DOE should issue new guidance. Part IV offers concluding remarks.

9. See Leslie Regan Shade & Rianka Singh, “Honestly, We’re Not Spying on Kids”: School Surveillance of Young People’s Social Media, SOC. MEDIA + SOCY, Oct.–Dec. 2016, at 1, 7–8 (explaining that the big data collected by educational technology companies and social media monitoring companies are either compliant or not covered by current federal laws).


I. TODAY’S STUDENT: SOCIAL MEDIA, SURVEILLANCE, AND PRIVACY FRAMEWORKS

A. Social Media Use

Social media continues to be a popular medium of expression, with young users communicating through Snapchat, Instagram, and Twitter with smartphones and laptops. Many hail social media use in schools for its ability to foster positive student-to-student communication, promote creative expression, and facilitate information exchanges. However, studies suggest that social media promotes anxiety and harassment, with young students increasingly expressing concerns about online bullying. Many negative online interactions lead to physical fights in school. Many educators have begun teaching digital citizenship—responsible uses of digital media—as well as strategies to help parents monitor students’ social media use.

School threats spiked on social media after the shooting in Parkland, Florida. Every day, students are taken into custody for


15. See, e.g., Martin et al., supra note 14, at 220–23. Interestingly, this study suggests that young people attempt to maintain their privacy rights by seeking social media platforms that have short accessibility timeframes and are not popular among older people. Id. at 221–22.


17. Herold, supra note 16.

threatening to bring a bomb or a gun to school. These incidents have prompted school districts to ask teachers or school resource officers to stay abreast of school-related social media posts. Students may also use their social media accounts to show a school administrator something posted by a classmate.

**B. Social Media Monitoring**

Many school districts contract with companies that specialize in social media monitoring. These companies monitor public social media communication that occurs within a certain radius of an educational institution by using machine-learning algorithms and keywords that relate to conflict, violence, or school. Companies will then send any flagged posts within a daily report to school administrators.

For example, Social Sentinel creates a virtual boundary called a geofence around an educational institution and scans public social media within that geofence. The company can adapt its keyword search for “unique characteristics” of the community and adjust the


20. See Leibowitz, supra note 8; PBS: NEWSHOUR, supra note 7.


24. See id.

scope of its search to social media posts beyond the institution's geofence. If a social media post contains a "threat indicator," then Social Sentinel's staff reviews the language and sends a copy of the post to a school administrator through a text message or an email. School administrators may access this data, manage notification settings, update the geofence, and assign community terms from their Social Sentinel account.

Other social media monitoring services, such as Geo Listening, have similar business models. Although these companies do not offer specific recommendations on how to store social media reports, they recommend factors to consider when determining who within the school community should receive the flagged social media posts. Both Geo Listening and Social Sentinel respond to concerns about student privacy by explaining that they only access social media posts that are already public.

Because federal law requires schools to protect students from harmful online content by using filters, many districts also subscribe to services that allow school leaders to monitor student internet use generally. For example, GoGuardian allows administrators and teachers to monitor students' school-issued devices. This software

27. See id.
28. See id.
30. See CTR. FOR DIG. EDUC., BUILDING A SOCIAL SAFETY NET: HOW THREAT ALERTS CAN BRING CLARITY TO SOCIAL MEDIA ACTIVITY AND HELP KEEP SCHOOLS SAFE 7–8 (2018) (recommending that school health care professionals, guidance counselors, and security officials should be entrusted with the information and that administrators document their responses to threats so they can reflect on "how a threat response played out"); Privacy Policy, GEO LISTENING, http://geolistening.com/privacy-policy/ [https://perma.cc/M5PV-M3UP] (last visited Aug. 29, 2019) (recommending that officials purge reports after they are processed).
31. See Social Media Scanning, supra note 25; see also FAQs, GEO LISTENING, http://geolistening.com/faq/ [https://perma.cc/LQ8X-GEGC] (last visited Aug. 31, 2019) ("Most users below the age of 25 do not utilize the available privacy settings because they are seeking to be recognized for their respective posts. They have chosen to post in the public domain in exchange for popularity and a decreasing ability to communicate effectively face to face.").
32. See Children’s Internet Protection Act, 47 U.S.C. § 254(h) (2018) (requiring schools and libraries that receive discounts for internet access to block student access to obscene images, child pornography, and other content).
provides an overview of total student body data usage and individual student data usage, such as the most commonly visited sites and applications and the amount of time spent online. Schools may then export this data into an individual report. GoGuardian justifies concerns about student privacy by emphasizing that it complies with federal law and abides by industry student privacy pledges. GoGuardian does not offer specific recommendations to schools on how to retain or share student information.

C. Schools’ Regulation of Online Student Speech

Although the US Supreme Court has not addressed a school’s ability to regulate student internet activity, courts consider *Tinker v. Des Moines Independent Community School District* when analyzing an educational entity’s ability to limit student speech. In *Tinker*, the Court held that an educational entity could limit student speech if the expression presented a risk of substantial disruption or material interference with school activities. Courts extend this holding to online off campus expression when the communication created a risk of substantial disruption or material interference with school activities. For example, the US Court of Appeals for the Ninth Circuit held that a school could expel a student for threatening other students on Myspace with a school shooting. Because the Myspace messages related to future violence within the school, the school could respond. Similarly, the Fifth Circuit held that a school could discipline a student for posting threatening rap lyrics on Facebook and YouTube because the lyrics included threats to shoot a school employee and because it was

35. *See id.*

36. *Id.*


38. *See id.*


40. *See Tinker, 393 U.S. at 514 (holding that students could wear armbands to protest the Vietnam War because they did not pose a risk of substantial disruption or materially interfere with school activities).*

41. *See, e.g., Wynar v. Douglas Cty. Sch. Dist., 728 F.3d 1062, 1067 (9th Cir. 2013); Wisniewski v. Bd. of Educ. of Weedsport Cent. Sch. Dist., 494 F.3d 34, 35 (2d Cir. 2007).*

42. *See Wynar, 728 F.3d at 1067.*

43. *Id.*
reasonably foreseeable that someone would alert the school about the song. 44

Although courts generally agree that Tinker’s standard may apply to online speech outside of school, courts differ on what constitutes a substantial disruption and to what extent the online speech must relate to the educational entity. 45 Some free speech advocates fear that educational entities’ abilities to monitor public student social media may chill expression, and they argue that the Tinker standard should be carefully considered before disciplining a student for content found through any social media monitoring report. 46

D. Regulating Student Privacy

The federal government primarily regulates student privacy through FERPA. 47 FERPA aimed to address concerns about government access to personal data by limiting third-party access to school records. 48 Today, FERPA conditions the receipt of federal funds upon compliance with rules governing the availability of individual student educational records. 49 An education record is defined as information that directly relates to a student that is maintained by an educational institution. 50 It may also include records of disciplinary action taken against the student for conduct posing a safety risk. 51 This definition excludes daily classwork, teacher materials, records maintained by law enforcement, or other records made by an employee during the normal course of business. 52

Under FERPA, educational institutions may disclose information from a student’s record to third parties in three limited

---

44. See Bell v. Itawamba Cty. Sch. Bd., 799 F.3d 379, 398 (5th Cir. 2015).
46. See, e.g., Victoria Cvek, Comment, Policing Social Media: Balancing the Interests of Schools and Students and Providing Universal Protection for Students’ Rights, 121 PENN ST. L. REV. 583, 614–15 (2016) (arguing that an exception to the Tinker standard should apply when the speech is found in the public domain).
48. See Polonetsky & Tene, supra note 14, at 960 (statement of Senator James Buckley).
49. 20 U.S.C. § 1232g(a); 34 C.F.R. § 99.3 (2019).
50. 20 U.S.C. § 1232g(a)(4)(A)(i)–(ii); 34 C.F.R. § 99.3.
51. 20 U.S.C. § 1232g(h)(1); 34 C.F.R. § 99.3.
circumstances: the school official exception, the studies exception, and the audit and evaluation exception. The school official exception allows schools to disclose personal information to third parties who have a “legitimate educational interest” in the information, such as teachers, counselors, and attorneys. The studies exception allows school officials to share student information with certain researchers. The audit and evaluation exception permits schools to disclose personal information to third parties that have been authorized to use the information to develop a federal program.

Other than these three exceptions, FERPA prohibits educational institutions from disclosing personal information from a student’s educational record unless they receive written consent from the student’s parent or guardian. Every year, the school must notify guardians of their right to inspect their student’s education records and to seek amendment of any information the family believes to be inaccurate, misleading, or in violation of the student’s privacy rights. Upon a parent or guardian’s request for amendment, a school must decide whether to comply and must inform the family of their right to a hearing within a reasonable timeframe.

Since FERPA’s passage, the DOE, courts, and state officials have clarified the scope of a student’s education record. For example, a student’s record likely would not include peer-reviewed papers because they were not solely “maintained” by the teacher. Also, educational institutions may disclose noninstructional media, such as surveillance footage, to law enforcement without implicating an

---


55. ZEIDE, supra note 53, at 15.

56. Id.

57. See 20 U.S.C. § 1232g(b)(1)(A)–(C), (F); 34 C.F.R. § 99.7(a)(2)(ii).


59. 34 C.F.R. § 99.20(a)–(b).

60. See generally FAMILY POLICY COMPLIANCE OFFICE, supra note 54, at 1.

61. Owasso Indep. Sch. Dist. v. Falvo, 534 U.S. 426, 433 (2002) (“Maintain” suggests FERPA records will be kept in a filing cabinet in a records room at the school or on a permanent secure database, perhaps even after the student is no longer enrolled. . . . It is fanciful to say [that student graders] maintain the papers in the same way the registrar maintains a student’s folder in a permanent file.”); 34 C.F.R. § 99.3.
education record. Neither the DOE nor the judiciary commented on social media’s relationship to education records, but two state officials recently opined that student social media, alone, is probably not part of a student’s record because it is directly created and maintained by the student, not by the educational institution.

Two federal laws address student privacy outside the context of an education record. The Children’s Online Privacy Protection Act (COPPA) prohibits online services from knowingly marketing to or collecting data from children under thirteen unless limited exceptions apply. The Protection of Pupil Rights Amendment (PPRA) requires written consent before any student participates in an exercise that reveals information concerning a student’s psychological problems or illegal behavior. Many states have also enacted laws that address students’ online privacy. In the last five years, several states prohibited educational institutions from requiring students to allow observation of or provide passwords to personal social media accounts. These laws do not, however, regulate educational institutions that monitor student social media that already exists in the public domain.

---

62. See Rome City Sch. Dist. Disciplinary Hearing v. Grifasi, 806 N.Y.S.2d 381, 383 (Sup. Ct. 2005) (“FERPA is not meant to apply to records, such as the videotape in question which was recorded to maintain the physical security and safety of the school building and which does not pertain to the educational performance of the students captured on this tape.”); 34 C.F.R. § 99.8(b)(1)(i)–(iii).

63. See Neb. Att’y Gen. Op. No. 18–008 (Oct. 15, 2018) (“Students’ social media posts, photos and videos, etc. are not maintained by the educational agency or institution. The students creating and posting this content are not persons acting for the agency or institution. Accordingly, this content is not considered an ‘education record’ and may be disclosed at the discretion of school officials.”); Colo. Att’y Gen. Op. No. 18–01 (Jan. 11, 2018) (“Social media posts are not restricted from disclosure under FERPA . . . they are not ‘maintained’ by schools and are created by students, not school staff. . . . Thus, a school official may disclose the existence and content of social media posts.”).

64. See 15 U.S.C. § 6502(a)(1) (2018); see also Privacy Policy, supra note 30 (pledging to notify school districts upon the collection of information of children under the age of thirteen).


67. See, e.g., 105 ILL. COMP. STAT. ANN. 75/15 (West 2016) (requiring a school to “provide notification to the student and his or her parent or guardian that the elementary or secondary school may not request or require a student to provide a password or other related account information in order to gain access to the student’s account or profile on a social networking website”); MICH. COMP. LAWS ANN. § 37.274(a) (West 2018) (prohibiting an educational institution from requesting students “to grant access to, allow observation of, or disclose information that allows access to or observation of the student’s or prospective student’s personal internet account”).

68. See, e.g., WIS. STAT. ANN. § 995.55(3)(b)(2) (West 2017) (Wisconsin’s Internet Privacy Protection Law states that educational institutions are not prohibited from “viewing, accessing, or
As of now, California is the only state to explicitly address student privacy within the context of social media monitoring. In 2013, a California school district, Glendale Unified Schools, hired Geo Listening to monitor student social media for signs of suicide, violence, and substance abuse. Many parents and privacy advocates were concerned by this decision, and the California legislature responded by passing new legislation in 2015. Now, school officials who plan to gather information from social media must first notify students and guardians. The school must allow the student to amend or delete collected data and must destroy the data within a year after the student leaves the institution or turns eighteen. Educational entities must also ensure that their contracts with social media monitoring companies contain provisions that (1) prohibit the vendor from using the student information for another purpose; (2) prohibit the vendor from sharing information to anyone other than the school district, guardian, or student; and (3) require the company to destroy the information after a contract ends.

II. THE PRIVACY PATCHWORK: LITTLE GUIDANCE FOR SOCIAL MEDIA REPORTS

No state’s government, except California’s, has addressed public social media monitoring through legislation. Although social media monitoring companies comply with current law and profess to self-regulate, their practices do not help educational entity clients robustly protect student privacy because they do not offer guidance on how to store or share social media reports.

using information about a student or prospective student that can be obtained without access information or that is available in the public domain.

69. See CAL. EDUC. CODE § 49073.6(b) (West 2016).
70. See Suski, supra note 45, at 77.
71. See ASSEMBLY COMM. ON JUDICIARY, CALIFORNIA BILL ANALYSIS, ASSEMBLY COMMITTEE, 2013–2014 REGULAR SESSION, ASSEMBLY BILL 1442 (2014) (“Although schools, like any other person or entity, have the right to access social media information that is publicly posted and accessible, a school’s ability to use and act upon such information is limited by any number of legal and constitutional principles . . . . If a school district maintains the information in its school records, then the school district cannot disclose any information from those records in violation of the federal Family Educational Rights and Privacy Act.”).
72. See EDUC. § 49073.6(b).
73. See EDUC. § 49073.6(c)(2)–(3)(A).
74. Compare EDUC. § 49073.6(c)(3)(C), with CAL. BUS. & PROF. CODE § 22581(a)(1) (West 2013) (California’s “right to erase” law for minors, which allows minors to ask website operators to delete their data use).
A. Social Media Reports and FERPA’s “Education Records”

As described above, FERPA does not explicitly address whether student social media records could become part of an education record.\textsuperscript{75} One could argue that FERPA’s definition of an education record includes reports produced by companies such as Social Sentinel, because these reports contain social media that directly relate to individual students and are generated by an educational institution’s agent.\textsuperscript{76} However, educational entities and social media monitoring companies do not maintain student data in the manner that FERPA envisioned.\textsuperscript{77} Although school districts collect information about student social media activity, there is no expectation that a school official will save the report.\textsuperscript{78} School officials may elect to print out the social media report, share it with others, and preserve it in a student file.\textsuperscript{79} Then again, administrators may choose to take no action, delete the report, or simply store the report in their online service profile.\textsuperscript{80} Moreover, the DOE has not updated FERPA’s definition of “education record” since 1974; the DOE has updated some regulations to include social media, but it has not updated “education record” to include social media.\textsuperscript{81}

In fact, social media monitoring reports are similar to records that are explicitly excluded from FERPA’s framework.\textsuperscript{82} FERPA’s

\textsuperscript{75} See supra Section I.D.

\textsuperscript{76} Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g(a)(4)(A)(i)–(ii) (2018); see also 34 C.F.R. § 99.3 (2019) (defining education records as records that are directly related to a student and maintained by an educational institution).

\textsuperscript{77} See 20 U.S.C. § 1232g; Neb. Att’y Gen. Op. No. 18–008 (Oct. 15, 2018) (“Students’ social media posts, photos and videos, etc. are not maintained by the educational agency or institution. The students creating and posting this content are not persons acting for the agency or institution. Accordingly, this content is not considered an ‘education record’ and may be disclosed at the discretion of school officials.”).

\textsuperscript{78} See 20 U.S.C. § 1232g(a)(4)(A)(i)–(ii). Compare Privacy Policy, supra note 30 (recommending that officials purge social media reports after they are processed), with Owasso Indep. Sch. Dist. v. Falvo, 534 U.S. 426, 433 (2002) (“The word ‘maintain’ suggests FERPA records will be kept in a filing cabinet in a records room at the school or on a permanent secure database.”).

\textsuperscript{79} See, e.g., Amy Rock, Social Media Monitoring: Beneficial or Big Brother?, CAMPUS SAFETY (Mar. 12, 2018), https://www.campussafetymagazine.com/university/social-media-monitoring/ [https://perma.cc/QSR5-BAAK] (interviewing the University of Virginia about how it stores any Social Sentinel alerts).

\textsuperscript{80} See, e.g., CTR. FOR DIG. EDUC., supra note 30, at 8; PBS: NEWSHOUR, supra note 7.

\textsuperscript{81} See, e.g., 34 C.F.R. § 361.18(c)(2)(ii)(N) (2019) (comprehensive system of personnel development); 34 C.F.R. § 668.41(h)(3)(i)(B) (reporting and disclosure of information); 34 C.F.R. § 668.412(a), (d)(2) (2019) (disclosure requirements for gainful employment programs).

\textsuperscript{82} See 20 U.S.C. § 1232g(a)(4)(B)(i); 34 C.F.R. § 99.3 (2019) (noting that “education record” does not include “[t]he word ‘maintain’ suggests FERPA records will be kept in a filing cabinet in a records room at the school or on a permanent secure database.”).
definition of an education record excludes both administrative notes and law enforcement records.\textsuperscript{83} Similar to administrative notes, social media monitoring reports are delivered to school administrators or superintendents and may remain in their sole possession.\textsuperscript{84} Similar to law enforcement, companies like Social Sentinel and Geo Listening assess the threat level of communications to help school members, such as school security officers,\textsuperscript{85} prevent future violence.\textsuperscript{86} Although social media monitoring companies do not initiate enforcement proceedings, they may provide school security officers with investigative tools and findings.\textsuperscript{87} Thus, one could characterize social media reports as records maintained by an agent of a law enforcement agency of an educational institution.\textsuperscript{88}

Because social media monitoring reports are likely not education records, they are not protected from disclosure under FERPA.\textsuperscript{89} In other words, school administrators may share information about a student’s public social media activity with third parties without first securing parental or guardian consent.\textsuperscript{90} School administrators often claim that this is permissible, given that students choose to make the information available to the public and because the school’s safety interest overwhelms any individual student’s privacy interest.\textsuperscript{91}

\begin{small}
\begin{itemize}
\item \textsuperscript{83} 20 U.S.C. § 1232g(a)(4)(B)(i)–(ii).
\item \textsuperscript{84} See 20 U.S.C. § 1232g(a)(4)(B)(i); see also Geo Listening, SERVICE BROCHURE 2, https://geolistening.com/wp-content/uploads/2018/01/Geo-Listening-01-27-18.pdf [https://perma.cc/47YD-BJYK] (last visited Sept. 1, 2019) (“Geo Listening reviews public posts made to social networks and provides staff with timely information aligned to existing policies, so they may better respond to the social and emotional needs of their students.”); Social Media Scanning, supra note 25.
\item \textsuperscript{86} See, e.g., Social Media Scanning, supra note 25.
\item \textsuperscript{87} See id.
\item \textsuperscript{88} See 20 U.S.C. § 1232g(a)(4)(B)(i)–(ii); CTR. FOR DIG. EDUC., supra note 30, at 7 (suggesting that school superintendents receive the alerts and then inform school principals and law enforcement as needed).
\item \textsuperscript{89} See 20 U.S.C. § 1232g(a)(4)(B)(i)–(ii); CTR. FOR DIG. EDUC., supra note 30, at 7 (describing how a social media surveillance report contains information on the post, the platform, and the geographic origin).
\item \textsuperscript{90} See 20 U.S.C. § 1232g.
\item \textsuperscript{91} See, e.g., Lynn Jolicoeur & Lisa Mullins, To Detect Threats and Prevent Suicides, Schools Pay Company to Scan Social Media Posts, WBUR (Mar. 22, 2018), https://www.wbur.org/news/2018/03/22/school-threats-suicide-prevention-tech [https://perma.cc/3QE5-GWYD] (interviewing a police chief who states that he is comfortable using Social Sentinel because the posts are already set to public); Can Scanning Social Media Help
may also assert that *Tinker* and its progeny suggest that schools may respond to threatening off campus speech despite implications for individual student interests.\footnote{92}{See *Tinker v. Des Moines Indep. Cmty. Sch. Dist.*, 393 U.S. 503, 513 (1969).}

These justifications are shortsighted. First, *Tinker* addressed a school’s ability to limit student speech when that speech substantially interfered with school safety, but it did not consider how the speech could be used after the fact.\footnote{93}{See *id.*}

Moreover, social media monitoring reports create an electronic record of a student’s online activity.\footnote{94}{See, e.g., *Social Sentinel Platform*, SOC. SENTINEL, https://www.socialsentinel.com/platform [https://perma.cc/M8CR-WN5T] (last visited Aug. 29, 2019) (describing how administrators may access flagged social media through an online dashboard).}

Even if the student decides to delete an alarming social media post, a copy remains with the school administrator through an online account.\footnote{95}{See *FAQs*, supra note 31.}

In this way, schools retain ownership of student speech even after the student attempts to disassociate herself.\footnote{96}{See *Privacy Policy*, supra note 30.}

FERPA does not dictate how long educational entities should store student records, but the DOE encourages entities to destroy most data in a timely manner.\footnote{97}{See PRIVACY TECH. ASSISTANCE CTR., U.S. DEP’T OF EDUC., PTAC–IB–5, BEST PRACTICES FOR DATA DESTRUCTION 1, 4 (2014).}

Under FERPA, school districts are usually required to destroy student information within a short time frame. Although monitoring reports likely fall outside of FERPA’s scope, school districts may treat these reports similarly to how they treat other records. Therefore, it is unlikely that school districts should be allowed to indefinitely retain student social media information without explicit statutory authorization or agency guidance instructing them to do so.\footnote{98}{See *id.* at 1.}

Last year, a Florida school district responded to a public records request for information relating to Social Sentinel by providing two months of Twitter postings that Social Sentinel had flagged for the school district.\footnote{99}{Brad West, *Social Sentinel Gives Flagler Schools a False Sense of Security*, PALM COAST OBSERVER (Sept. 5, 2018), https://www.palmcoastobserver.com/article/social-sentinel-gives-flagler-schools-a-false-sense-of-security [https://perma.cc/GT5G-SMWM].}

In California, a school printed off its social media reports and used them to persuade students that their activity reflected poorly on the school.\footnote{100}{Leibowitz, supra note 8.}

These stories are worrisome, considering that many students adapt their online presences by deleting old posts or by
adjusting their privacy settings. Because schools retain a record of old student messages, their social media monitoring databases may not accurately depict a student’s current online presence and may associate that student with a past potential threat that the student has since deleted or that represents an impulsive thought from many years in the past.

Since FERPA does not protect this information from disclosure, college admissions officers, potential employers, journalists, and other private citizens may petition a school and receive information that has been taken out of its original context. This is problematic considering that the information may no longer be publicly available. Moreover, social media monitoring algorithms are imperfect because of the biases of their creators and users, and some experts fear that their keywords may disproportionately affect students who are already at risk of being subjected to harsher school discipline. Thus, allowing third parties to access student information that is no longer publicly available may perpetuate implicit biases present in the monitoring algorithm at the time of collection.

B. Industry Privacy Pledges and Self-Regulation

Social media monitoring companies profess to self-regulate student privacy by accessing only public social media, not private or closed social networks. However, these companies lack industry privacy pledges or vendor contracts that guide schools on how to store information found in social media monitoring reports.

101. See, e.g., Mary Madden, Privacy Management on Social Media Sites, Pew Res. Ctr.: Internet & Tech. (Feb. 24, 2012), http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/ (finding that 15 percent of social media users between the ages of 18–29 report having posted social media content that they later regret and that users are more frequently “pruning” their accounts).

102. See, e.g., Privacy Policy, supra note 30.


105. See FAQs, supra note 31 (“All information is gathered from public posts on social networks.”).
In 2014, the Future of Privacy Forum (FPF) and the Software & Information Industry Association (SIIA) introduced a Student Privacy Pledge (the “Pledge”) for K-12 educational technology (“edtech”) vendors. Signees agree to collect information only for authorized educational purposes, to disclose the types of information and their purpose to families, and to facilitate access and correction of student data between the school and the family. To date, almost four hundred edtech vendors have taken the Pledge, and noncompliant signees face the threat of civil enforcement by the Federal Trade Commission (FTC). Social Sentinel, Geo Listening, and other social media monitoring companies have not signed FPF’s Pledge, and they are likely ineligible. Only “school service providers” may take the Pledge. This label excludes tools that do not aid content instruction, including social media monitoring services.


107. See Provider Pledge, supra note 106.


110. See Signatories, supra note 108.

111. Student Privacy Pledge, supra note 109. Interestingly, the Pledge defines “student personal information” as data linked to an individual student’s personally identifiable information, such as a name or an address. See Provider Pledge, supra note 106. FERPA defines “personally identifiable information” more broadly as information that a reasonable person could link to a student. See Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2018); 34 C.F.R. § 99.3 (2018). Definitional inconsistencies like these may result in educational service vendors and school districts being accountable for different types of student information, especially as edtech services continue to expand in classrooms. See Eli Zimmerman, The Current State of Education Technology and Where It Is Going, EdTech (Dec. 13, 2018), https://edtechmagazine.com/k12/article/2018/12/current-state-education-technology-and-where-it-going-infographic.

112. See Student Privacy Pledge, supra note 109. The Electronic Privacy and Information Center (EPIC) has also produced a Student Privacy Bill of Rights, which contains: (1) “the right to access and amend . . . erroneous, misleading, or . . . inappropriate records”; (2) the right to limit edtech companies’ ability to collect data; (3) “the right to expect that companies and schools will collect, use, and disclose student information solely in ways that are compatible” with the data’s original context; (4) “the right to secure and responsible data practices”; (5) “the right to clear and accessible information privacy and security practices”; and (6) “the right to hold schools and . . . companies . . . accountable” for violating the Bill of Rights. Like the Pledge, the Bill of Rights is designed for edtech service providers, not social media monitoring companies. See
Although FPF’s Pledge may help keep student privacy at the forefront of educational entities’ conversations with certain classroom technology providers, such as GoGuardian,113 its requirements do not encourage social media monitoring companies to guide schools on how to store and share student social media reports. Even if a pledge specifically addressed the collection of student information from the public domain, it would not provide an adequate avenue of recovery for students and parents. Pledges are voluntary, and few educational social media monitoring companies have developed national marketing strategies or public policy platforms.114 Therefore, companies may not feel economically motivated to sign industry privacy pledges.115 Even if they did, the FTC may decide not to bring an enforcement action against a company for violating a pledge.116

Most importantly, a privacy pledge for social media companies would regulate only the companies’ actions with student social media reports—not school administrations’ actions.117 Although industry pledges and norms may help school districts find edtech providers who will engage in discussions on privacy, they do not ensure that districts develop best practices for retaining and sharing student data that other tech providers cultivate.118 Instead, privacy pledges refer educational entities to FERPA, which, as described above, does not protect this information from disclosure.119

III. THE NEED FOR UPDATED STATE AND FEDERAL STUDENT RECORDS LAWS

Because a student’s education record may contain information from social media monitoring services that is not protected from

---

113. See supra Section I.B.


115. See id.


117. See Provider Pledge, supra note 106.

118. See id.

119. See, e.g., STUDENT PRIVACY PLEDGE, supra note 109 (“The Pledge is not intended to be a comprehensive privacy policy nor to be inclusive of all the many requirements needed to comply with applicable federal and state laws.”).
disclosure, third parties may petition schools for student information that may have been taken out of its original context.\textsuperscript{120} Educational entities who use social media monitoring services should ensure that their policies mirror the practices required in California Education Code section 49073.6. The DOE should also issue guidance on social media’s relationship to education records under FERPA.

A. Access, Amendment, and Deletion: California’s Example

After Glendale Unified community members protested Geo Listening in 2013, California became the first and only state to pass legislation regarding public school social media monitoring.\textsuperscript{121} California Education Code section 49073.6 applies to any school district that adopts a program “to gather or maintain in its records any information obtained from social media of any enrolled pupil.”\textsuperscript{122} The statute defines social media broadly as any “electronic content,” including videos, photographs, blogs, podcasts, messages, and online services.\textsuperscript{123} Notably, the policy makes no distinction between private and public social media.\textsuperscript{124} The provisions do not apply to any electronic services that are used exclusively for educational purposes, such as edtech services described above.\textsuperscript{125}

Districts must provide students and their families with access to any information obtained from social media and give that student an opportunity to correct or delete that information.\textsuperscript{126} The district must also destroy all of the information gathered from the social media within a year after the student turns eighteen, or within a year after the student is no longer enrolled at the institution.\textsuperscript{127} The district must communicate to each student’s parent or guardian regarding the social media monitoring system’s general use, when the school district will destroy the data, how to access any social media reports, and how to request the removal or correction of such information.\textsuperscript{128}

\begin{enumerate}
\item See supra Section I.D.
\item \textsc{CAL. EDUC. CODE} § 49073.6(b) (West 2016).
\item \textsc{EDUC.} § 49073.6(a)(2)(A).
\item \textit{Id.}
\item \textsc{EDUC.} § 49073.6(a)(2)(B); see supra Section II.B.
\item \textsc{EDUC.} § 49073.6(c)(2).
\item \textsc{EDUC.} § 49073.6(c)(3)(A).
\item \textsc{EDUC.} § 49073.6(c)(3)(B).
\end{enumerate}
1. Positive Effects on the School-Student Relationship

States should follow California’s lead and pass similar legislation for several reasons. First, the law’s access and amendment provisions help prevent schools from disseminating old copies of student speech. Although the law does not expressly ban social media monitoring reports from incorporation in a student’s education record or from disclosure to third parties,129 it allows students to respond to narratives that could be associated with their profiles, minimizing the chance of a social media report’s use for a purpose other than ensuring school safety.130 Although the DOE has promulgated regulations that allow students and their families to inspect and request the amendment of education records,131 reiterating these principles in state law would connect these rights specifically to student social media information.

These mechanisms can also act as positive reinforcements for students who develop better digital citizenship habits as they grow older.132 If a student regrets an alarming Facebook post and deletes that information or makes her account private, then surely she deserves an opportunity to ensure that the old message does not persist in her educational file or become available during a records request. California’s requirement that educational entities destroy the digital information after a student turns eighteen or moves out of the school district ensures that this information is associated with a student for a limited amount of time and reinforces the notion that educational entities should only monitor students’ online presences to ensure the safety of their student population.133

One could argue that ongoing public safety concerns should overwhelm any privacy interest in destroying social media reports because the old data may be relevant in assessing threats that occur in the future.134 Although old reports may be relevant, they are likely not needed to gain insight into a student’s past. Schools who use social

---

129. See EDUC. § 49073.6.
130. See EDUC. § 49073.6(c)(2).
131. See 34 C.F.R. § 99.10(a) (2019); 34 C.F.R. § 99.20(a).
133. See EDUC. § 49073.6(c)(3)(A).
media monitoring services, as well as the monitoring companies themselves, often contact law enforcement when a report contains serious information. When law enforcement already has an incident report or a copy of the original communication, requiring the school to retain and provide that information is not necessary. Moreover, authorities may petition the social media application or the monitoring company to gain social media information on the student in question.

Another advantage of California’s scheme is that it could cultivate conversations about digital citizenship and emotional health among educational entities, families, and students. The notice and opportunity to review requirements increase families’ awareness of their student’s online presence. Both parents and students may review a student’s online statements, consider what they convey to present and future audiences, and reflect on what motivated the threatening speech.

Today, a good digital status is considered critical for college admission, job offers, and healthy offline relationships. By providing formal reflective opportunities for students and their families, states would recognize the need to cultivate positive digital citizenship habits in their schools.

Because California only recently adopted this law, it has not faced much controversy. Nonetheless, the law is not without potential criticisms. First, section 49073.6 does not provide an opportunity for

---


137. See EDUC. § 49073.6(c)(3)(B)(i).

138. See EDUC. § 49073.6(c)(2)–(3)(B)(i).


140. See, e.g., Sarah O’Brien, Employers Check Your Social Media Before Hiring. Many Then Find Reasons Not to Offer You a Job, CNBC (Aug. 10, 2018, 9:18 AM), https://www.cnbc.com/2018/08/10/digital-dirt-may-nix-that-job-you-were-counting-on-getting.html [https://perma.cc/DF9T-2F4N] (estimating that 57 percent of employers that check social media have found content to eliminate that person as a candidate).


142. As of July 3, 2019, EDUC. § 49073.6 has no subsequent history.
parents or students to opt out of a social media monitoring program. This perpetuates a sense of mandatory surveillance and may concern students, families, and other privacy advocates. However, an opt-out provision is not necessary. Social media monitoring services only scan social media accounts and posts that are already publicly available, so students always retain an ability to opt-out by making their accounts private.

One could criticize section 49073.6 for not specifying a private right of action for students or their parents. This concern is not unique, given that educational policies often do not provide private rights of action. Regardless, states who adopt California’s model should consider which remedies should be available to students and their families and how each state could incentivize educational entities to comply with these provisions. For instance, states could require local school boards to adopt principles that mirror the values set forth in privacy pledges and adopt an administrative hearing process to investigate allegations of noncompliance. School board policies that profess a student’s right to amend information, limit data collection, and access clear privacy practices would help guide discussions about social media monitoring within the context of FERPA and would attach broader concerns associated with social media monitoring, such as chilling speech and unreasonable searches, to local policy.

2. Positive Effects on the School-Vendor Relationship

States should also adopt California’s model to ensure that their school districts enter into protective service agreements with social

---

143. See id.
145. See Privacy Policy, supra note 30 (“If you would like to ensure that Geo Listening Monitoring Service does not monitor the content that you post through a social media platform or profile, you should ensure that your social media posts are non-public.”).
146. See EDUC. § 49073.6, CTR. FOR DEMOCRACY & TECH., STATE STUDENT PRIVACY LAW COMPRENDIUM 12 (2016).
147. See generally CTR. FOR DEMOCRACY & TECH., supra note 146, at 20, 24, 25, 28, 31, 33, 35.
148. See supra Section II.B.
149. See supra Section II.B.
150. See, e.g., Mendola, supra note 39, at 178 (“Internet surveillance could chill free speech, as students would know that their posts were monitored and consequently could choose not to express their thoughts on the Internet.”).
151. See, e.g., Shade & Singh, supra note 9, at 9 (discussing the implications of the electronic surveillance of students).
media monitoring companies. Section 49073.6 mandates that service agreements expressly prohibit the monitoring company from selling or sharing social media information with anyone other than the affected educational entities, the students, and their guardians. The social media monitoring company must destroy the information immediately after the vendor agreement’s expiration and destroy information related to a student after that student turns eighteen or moves out of the school district.

These provisions are important for school districts to require in their contracts because they encourage student privacy discussions during contract negotiations. Today, at least two Social Sentinel service agreements do not contain these provisions. Instead, the company limits its discussion of student social media information to a single paragraph in their company-wide privacy policy, which school districts must find through the company’s website. Neither the privacy policy nor the individual service agreements require the company to destroy information after a certain period of time. In contrast, Geo Listening now incorporates the provisions necessitated by section 49073.6 into its company-wide privacy policy. This policy provides a mailing address and an email address that students and families may contact to access and amend curated information, and it states that it will destroy all information after the contract’s expiration.

Admittedly, Geo Listening’s additions are minor. Without communication from school administration, it is unlikely that students and families would know their district’s specific social media monitoring vendor or investigate that vendor’s website for a privacy policy. Section 49073.6 also does not seem to have influenced Geo Listening’s individual service agreements, suggesting that the new

152. CAL. EDUC. CODE § 49073.6(c)(3)(C)(ii) (West 2016).
153. EDUC. § 49073.6(c)(3)(C)(iii)–(iv).
156. See Services Agreement: Flagler, supra note 154; Social Sentinel Privacy Policy, supra note 30.
157. See Privacy Policy, supra note 30. The company’s decision to incorporate the requirements of section 49073.6 into a company-wide privacy policy makes sense, given that Geo Listening is based in California. Id.
158. Id.
state law may not directly influence individual service negotiations. Nonetheless, minor additions to the company-wide privacy policy can help students and their families become aware of their rights under state law. States who adopt laws similar to California’s could require vendors to provide contact information directly to students and families or require educational entities to provide students and their families with a copy of the vendor’s privacy policy and service agreement.

B. Nondisclosure Under FERPA: The Need for Agency Guidance

As described above, the DOE has not updated FERPA’s definition of education record since 1974, and many privacy advocates criticize the law for not explicitly addressing electronic information that relates to students. Although the DOE has updated the definition of an education record to exclude certain documents, it has not addressed electronic student information. These factors could suggest that the DOE intends to exclude social media from FERPA’s scope, prefers that Congress legislates the issue, or does not believe it is institutionally equipped to regulate student social media information. Admittedly, it is possible that the DOE is reluctant to regulate student social media. However, the agency has not expressed this sentiment.

Federal agency action would be very helpful to educational entities because it would help ensure that student data are treated uniformly when a student transfers to a school in a new district or a new state. Guidance, specifically, would allow the term “education record” to retain definitional flexibility. Social media is an amorphous concept, and it is difficult to predict what platforms might exist in the future and whether schools and vendors will seek to monitor that information. Guidance could address today’s concept of social media,
recognize the growing popularity of social media monitoring tools, and be issued more quickly than a definitional update within a larger legislative package or the notice-and-comment rulemaking process.\textsuperscript{166} Although guidance would not confer any additional rights on students or families or impose any additional requirements for educational entities,\textsuperscript{167} it would help school districts make quick decisions regarding the storage of social media and other electronic student information.

Guidance on FERPA’s “education record” provision should clarify that schools may not disclose any information retained from student social media to third parties without parent or guardian consent.\textsuperscript{168} School administrators should rarely include social media in a student’s education file, so guidance should also include direction on when to destroy and when to retain social media threat reports. It should also provide procedures for students and families to access, amend, and request the destruction of any reports that are retained after a threat assessment. Overall, including student social media in FERPA’s definition of education record and providing guidance on the destruction on social media information would help ensure that schools do not disseminate old, inaccurate speech to third parties.\textsuperscript{169} This is especially important given the increasing number of people who demand access to student records under public records laws\textsuperscript{170} and the increasing confusion that school administrators face when balancing the protection of student electronic information and school safety inquiries.\textsuperscript{171}


\textsuperscript{167} See id.

\textsuperscript{168} See Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g(b)(1) (2018); see also 34 C.F.R. § 99.3 (“Directory information means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed.”); Frequently Asked Questions, U.S. DEPT EDUC., https://www2.ed.gov/policy/gen/guid/fpco/faq.html#q4 [https://perma.cc/TKJ3-Z6FX] (last visited Aug. 30, 2019). By including social media in the definition of an education record, the DOE would need to clarify that it is not to be construed as directory information. See Frequently Asked Questions, supra.

\textsuperscript{169} See supra Section II.A.

\textsuperscript{170} See, e.g., Daggett, supra note 163, at 92 (“Civil litigants and criminal defendants, citizens and the media exercising rights under state public records laws, researchers, and commercial entities are increasingly demanding access to student records.”).

Admittedly, DOE guidance would not address some of FERPA’s other shortcomings.\textsuperscript{172} FERPA does not provide a private right of action for students or parents,\textsuperscript{173} and the federal government rarely rescinds funds from noncompliant school districts.\textsuperscript{174} Also, school districts are not always motivated to comply with FERPA since most of their funding comes from local and state governments.\textsuperscript{175} These limitations demonstrate why both state and federal government should address social media monitoring and student privacy: State policies would ensure that school districts address data access, destruction, and remedies. New federal guidance would inject life back into FERPA and help prevent saved social media information from being shared with third parties.\textsuperscript{176} Together, new state and federal frameworks would ensure that schools neither store old online student speech, nor use it in the future for purposes other than ensuring safety.

IV. CONCLUSION

A year later, Parkland community members continue to grieve.\textsuperscript{177} School districts continue to reflect on their campus safety policies,\textsuperscript{178} with many hoping to catch the next serious threat by contracting with social media monitoring companies.\textsuperscript{179} Services like Social Sentinel and Geo Listening are well-intentioned\textsuperscript{180} and can play

\begin{footnotes}
\footnotetext{172}{See id.}
\footnotetext{173}{See Gonzaga Univ. v. Doe, 536 U.S. 273, 287–88 (2002) (holding that FERPA did not create individual rights that could be enforced under 42 U.S.C. § 1983 (2018) because the focus of FERPA’s nondisclosure provisions is the duties of institutions, not the rights of the benefited parties).}
\footnotetext{174}{See Polonetsky & Tene, supra note 14, at 967.}
\footnotetext{176}{See supra Section III.B.}
\footnotetext{179}{See, e.g., Leibowitz, supra note 8.}
\end{footnotes}
a vital role in school safety. By scanning public social media, monitoring companies help school administrators focus their energy and resources on other internal governance issues.

Admittedly, recordkeeping is only one of several issues raised by social media monitoring, as students’ rights to free speech, privacy, and due process are necessarily implicated when schools discipline students for information found in these reports. Student rights advocates must monitor the development and the effectiveness of social media monitoring practices and consider how these practices comport with jurisprudence on students’ constitutional rights.

California’s model gives states an opportunity to reiterate a student’s right to access, amend, and delete data gleaned from their public social media. At the same time, the DOE must clarify FERPA’s framework to account for schools’ increasing awareness and collection of online student speech. Together, new state and federal initiatives would help ensure that schools destroy social media reports in a timely manner and honor individual privacy as students mature into more responsible digital citizens.

Alice Haston*


182. See id.

183. See supra Part I.

184. See New Jersey v. T.L.O., 469 U.S. 325, 333, 337–41 (1985) (balancing a student’s interest in privacy against the need to maintain school order and holding that the legality of student searches hinged on a more lenient reasonableness inquiry, not a traditional Fourth Amendment analysis); Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 506, 513–14 (1969) (balancing a student’s right to free speech and determining that the speech could be limited if it posed a disruption to the school environment).

185. See supra Part III.

186. See supra Part III.

* JD Candidate, Vanderbilt University Law School, 2020; BA, University of Tennessee, 2013. The Author would like to thank her family for their support throughout her education as well as the editorial staff of the Vanderbilt Journal of Entertainment & Technology Law for their thoughtful guidance.