Date of Hearing: July 2, 2024

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 1283 (Stern) – As Amended June 26, 2024

AS PROPOSED TO BE AMENDED

SENATE VOTE: 35-0

SUBJECT: Pupils: use of social media

SYNOPSIS

While social media can connect students with learning opportunities, research suggests that limiting cell phone usage and social media access during the school day benefits student mental health, reduces cyberbullying, and improves academic performance. In 2019, the Legislature passed AB 272 (Muratsuchi, Ch. 42, Stats. 2019), which authorized governing bodies of schools to adopt a policy to limit or prohibit the use of smartphones by students while at school or under employee supervision. Since then, concerns surrounding student use of smartphones and social media in schools have only grown: the U.S. Surgeon General and the Governor both recently called for stronger restrictions, and the LA Unified School District adopted a ban on smartphones.

This bill would expand schools' authority beyond regulation of smartphones to include social media itself. The bill is sponsored by the Organization for Social Media Safety, which argues that this expansion is crucial to addressing the growing concerns surrounding the misuse of social media platforms in school settings, and that it will help improve students' academic performance, well-being, and safety. The bill is supported by TechNet, California Chamber of Commerce, the California State PTA, CFT — A Union of Educators & Classified Professionals, AFT, AFL-CIO, and the Los Angeles County Office of Education.

The bill is opposed by ACLU California Action and the Electronic Frontier Foundation (EFF), who raise concerns over warrantless surveillance of pupil's electronic information on smartphones and school-issued devices. While a prior version of the bill addressed their concerns, the provisions—which enabled the pupil to consent to electronic monitoring—raised concerns for this Committee and the Education Committee. As a result, the provisions were removed in the Education Committee with the understanding that the issue would be revisited in this Committee.

As proposed to be amended, the bill would:

- *Require express written parental consent in order for a governing body of a school to access the pupil's electronic information.*
- *Limit the scope of such requests to information related to specific incidents involving harassment, cyberbullying, or potential crimes.*
- *Require that written disclosure be provided to the pupil in the event the parent grants consent to such a request.*

- *Prohibit conveying electronic information to third parties unless necessary to address misconduct or required by law.*

- *Specifically prohibit the governing body from seeking, retaining, or sharing information related to the child's gender identity, gender expression, or sexual orientation unless necessary to address misconduct or required by law.*

- *Provide that the authority for such a request expires at the end of a school year.*

The amendments are set forth in full below. The bill passed the Education Committee by a vote of 6-0.

SUMMARY: This bill expands the existing authority of a local educational agency, county office of education, or charter school to adopt a policy that would either limit or prohibit the use of social media by its students while on campus or under the supervision and control of an employee. Specifically, **this bill**:

1) Authorizes the governing board of a school district, a county board of education, or the governing body of a charter school to limit or prohibit the use by its pupils of social media, as defined, while the pupils are at a schoolsite or while the pupils are under the supervision and control of an employee or employees of that school district, county office of education, or charter school.

2) Clarifies that access to a pupil's electronic information is subject to the California Electronic Communications Privacy Act (Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code).

3) Provides that a school district, county office of education, or charter school's request for voluntary disclosure of, or access to, a pupil's electronic information may be obtained only through written specific consent of the pupil's parent or guardian. Such a request must meet all of the following:

    a) The request shall identify specific categories of information and timeframes in which the information is likely to have been generated.

    b) The specific categories of information are limited to information directly related to acts of harassment, cyberbullying, or that may violate the Penal Code.

    c) The request is in response to a specific incident involving conduct or alleged conduct that falls under b).

4) If a parent or guardian grants consent to accessing the information, requires the school district, county office of education, or charter school shall, prior to accessing the information, provide a written disclosure to the pupil informing them that the parent or guardian has consented to the disclosure of, or access to, the pupil's electronic information.

5) Prohibits information obtained by the school district, county office of education, or charter school from being relayed to anyone aside from authorized staff, except as required by state or federal law.

6) Prohibits a school district, county office of education, or charter school that makes a request for electronic information from seeking to obtain information relating to a pupil's gender, gender identity, gender expression, or sexual orientation. If the school district, county office of education, or charter school discovers such information about any pupil, it must treat the information as confidential and cannot retain or share the information, except as required by state or federal law.

7) Provides that a request for access to electronic information for which consent has been granted is no longer valid after the end of the school year in which the request is made. After the ensuing school year starts, a new request may be made subject to the requirements of the bill.

8) Declares the intent of the Legislature to protect LGBTQ+ youth from policies that forcibly "out" the youth.

EXISTING LAW:

1) The governing body of a local educational agency, county office of education, or charter school may adopt a policy to limit or prohibit the use by its pupils of smartphones while the pupils are at a schoolsite or while the pupils are under the supervision and control of an employee or employees of that LEA, COE, or charter school. (Ed. Code § 48901.7(a).)

2) States a pupil shall not be prohibited from possessing or using a smartphone under any of the following circumstances:

    a) In the case of an emergency, or in response to a perceived threat of danger.

    b) When a teacher or administrator of the local educational agency, county office of education, or charter school grants permission to a pupil to possess or use a smartphone, subject to any reasonable limitation imposed by that teacher or administrator.

    c) When a licensed physician and surgeon determines that the possession or use of a smartphone is necessary for the health or well-being of the pupil.

    d) When the possession or use of a smartphone is required in a pupil's individualized education program. (Ed. Code § 48901.7(b).)

3) Under the California Electronic Communications Privacy Act (CalECPA), generally prohibits a government entity from compelling the production of or access to electronic communication information from a service provider or to electronic device information from any person or entity other than the authorized possessor of the device, absent a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to specified conditions, or pursuant to an order for a pen register or trap and trace device, as specified. (Pen. Code § 1546.1.)

4) Defines, for purposes of CalECPA:

a) "Authorized possessor" means the possessor of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device.

b) "Government entity" as a department or agency of the state or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof. (Pen. Code § 1546(i).)

c) "Specific consent" means consent provided directly to the government entity seeking information, including, but not limited to, when the government entity is the addressee or intended recipient or a member of the intended audience of an electronic communication. Specific consent does not require that the originator of the communication have actual knowledge that an addressee, intended recipient, or member of the specific audience is a government entity.

FISCAL EFFECT: As currently in print, this bill is keyed nonfiscal.

COMMENTS:

1) **Smartphones, social media, and schools.** The well-documented spike in adolescent mental health challenges since 2010 tracks "the years when adolescents in rich countries traded their flip phones for smartphones and moved much more of their social lives online—particularly onto social-media platforms designed for virality and addiction."[1] Up to 95% of youth ages 13-17 report using a social media platform, with more than a third saying they use social media "almost constantly." Although age 13 is commonly the required minimum age used by social media platforms in the U.S., nearly 40% of children ages 8–12 use social media. As of 2021, the Surgeon General notes that 8th and 10th graders spent an average of 3.5 hours per day on social media.[2]

According to the Pew Research Center, 72% of high school teachers say that students being distracted by cellphones is a major problem in their classroom.[3] While social media can connect students with learning opportunities, research suggests that limiting cell phone usage and social media access during the school day benefits student mental health, reduces cyberbullying, and improves academic performance.[4] Recognizing this, the Legislature passed AB 272 (Muratsuchi; Ch. 42, Stats. 2019), which authorized governing bodies of schools to adopt a policy to limit or prohibit the use of smartphones by students while at school or under employee supervision.

---

[1] Jonathan Haidt, "End the Phone-Based Childhood Now" (Mar. 13, 2024) *The Atlantic*, https://www.theatlantic.com/technology/archive/2024/03/teen-childhood-smartphone-use-mental-health-effects/677722/.
[2] "Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory" (May 23, 2023) p. 7, https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf.
[3] Jenn Hatfield, "72% of U.S. high school teachers say cellphone distraction is a major problem in the classroom" (Jun. 12, 2024) Pew Research Center, https://www.pewresearch.org/short-reads/2024/06/12/72-percent-of-us-high-school-teachers-say-cellphone-distraction-is-a-major-problem-in-the-classroom/.
[4] Lauraine Langreo, "Cellphone Bans Can Ease Students' Stress and Anxiety, Educators Say" (Oct. 16, 2023) *EducationWeek*, https://www.edweek.org/leadership/cellphone-bans-can-ease-students-stress-and-anxiety-educators-say/2023/10; Nikki Sweeny, "Restricting phones leads to positive student outcomes" *MSN.com*, https://www.msn.com/en-us/health/other/restricting-phones-leads-to-positive-student-outcomes/; "Banning mobile phones in schools can improve students' academic performance" (Mar. 22, 2021) *Phys.Org*, https://phys.org/news/2021-03-mobile-schools-students-academic.html.

Since then, concerns over the negative impact of student access to smartphones and social media during school have only grown. In a recent *New York Times* opinion essay, U.S. Surgeon General Vivek Murthy, calls for safety warning labels on social media platforms to address the mental health crisis among teens, he specifically urged that "[s]chools should ensure that classroom learning and social time are phone-free experiences."[5] Shortly thereafter, Governor Newsom stated, "[a]s the Surgeon General affirmed, social media is harming the mental health of our youth. Building on legislation I signed in 2019, I look forward to working with the Legislature to restrict the use of smartphones during the school day. When children and teens are in school, they should be focused on their studies — not their screens."[6] That same day, the Los Angeles Unified School District board approved a resolution to ban student use of cellphones and social media platforms during the entire school day.[7]

Two bills seek to address this issue head-on. The first is AB 3216 (Hoover, Lowenthal, and Muratsuchi), which would *require* the governing body of a school district, a county office of education, or a charter school to adopt a policy to limit or prohibit pupils' use of smartphones, except in specified circumstances, no later than July 1, 2026, and to update the policy every five years thereafter.

The second is this bill, which allows governing bodies of schools to adopt a policy to limit or prohibit the use of social media.

2) **Author's statement.** According to the author:

> As a concerned parent and legislator, I am deeply troubled by the increase in youth suicide attributed to cyberbullying and social media usage in our schools. Recent research shows the link between excessive social media exposure and heightened depression and anxiety amongst our students. Additionally, increased time on social media has been correlated with lower educational outcomes for youth. Recognizing the urgent need to protect our children and their education, I am committed to SB 1283 which helps school district's regulate the presence of social media and smartphones on school campuses statewide. It is life or death for our students and we must move quickly to mitigate the risks of smartphone addiction and online bullying during school hours, ensuring the protection of our most vulnerable Californians.

3) **Concerns regarding warrantless surveillance of electronic information.** ACLU California Action and the Electronic Frontier Foundation oppose the bill in print. They observe, correctly, that a means by which a governing body could seek to regulate social media is through the surveillance of a pupil's smartphone or a school-owned device the pupil uses:

> The premise of SB 1283 is to take local educational agencies' existing authority to "limit or prohibit" student use of smartphones and replicate it to create a new authority to regulate student social media use while they are at a schoolsite or "under the supervision and control

---

[5] Dr. Vivek Murthy, "Surgeon General: Why I'm Calling for a Warning Label on Social Media Platforms" (Jun. 17, 2024) *New York Times*, https://www.nytimes.com/2024/06/17/opinion/social-media-health-warning.html.
[6] "Governor Newsom supports efforts to get smartphones out of schools" (Jun. 18, 2024), https://www.gov.ca.gov/2024/06/18/governor-newsom-supports-efforts-to-get-smartphones-out-of-schools/.
[7] Thao Nguyen, "Los Angeles school district bans use of cellphones, social media by students" (Jun. 18, 2024) *USA Today*, https://www.usatoday.com/story/news/nation/2024/06/18/los-angeles-school-district-cellphone-social-media-ban/74144479007/.

of an employee" of the school or district. Problematically, regulating social media use is a much more complicated issue than regulating smartphones. Smartphones are physical objects, so limiting their use is as non-invasive as requiring students to put them away. On the other hand, for a school employee to regulate a student's social media usage on their smartphone while at a schoolsite, the employee would have to look through the student's phone for social media apps or messaging.

This butts up against students' right to privacy. As it was introduced, and as proposed to be amended, SB 1283 would essentially invite school employees with limited knowledge of privacy laws to violate the California Electronic Communications Privacy Act (CalECPA), which limits the ability of the government to access electronic devices without a warrant and due process. This applies in a school context – if schools want access to a smartphone's content without a student's consent, they need a warrant.

Additionally, social media can be accessed on a tablet or computer, not just on a smartphone. Most students have a school-issued tablet or computer, and SB 1283's language around "supervision" could be interpreted to give schools a broad ability to monitor student activity and student speech on school-issued devices outside of school hours, including speech they reasonably expect to be private, such as their conversations with friends while gaming. This has First Amendment and privacy implications, and we have heard from students and families that school monitoring of these kinds of activities has led to results as severe as law enforcement officers being sent to a home. These potential impacts of SB 1283 without the protections of the May 20th amendments would have disparate impact on Black and Brown students and students of low income because they are more likely to use school-issued devices for personal activities outside of school hours, as the school-issued device may be the only computer or tablet in the home.

A recent article from *Wired* details privacy and equity concerns surrounding student-monitoring software on school-issued devices:

Student-monitoring software has come under renewed scrutiny over the course of the Covid-19 pandemic. When students in the US were forced to continue their schooling virtually, many brought home school-issued devices. Baked into these machines was software that can allow teachers to view and control students' screens, use AI to scan text from student emails and cloud-based documents, and, in severe cases, send alerts of potential violent threats or mental health harms to educators and local law enforcement after school hours.

Now that the majority of American students are finally going back to school in-person, the surveillance software that proliferated during the pandemic will stay on their school-issued devices, where it will continue to watch them. According to a report published today from the Center for Democracy and Technology, 89 percent of teachers have said that their schools will continue using student-monitoring software, up 5 percentage points from last year. At the same time, the overturning of *Roe v. Wade* has led to new concerns about digital surveillance in states that have made abortion care illegal. Proposals targeting LGBTQ youth, such as the Texas governor's calls to investigate the families of kids seeking gender-affirming care, raise additional worries about how data collected through school-issued devices might be weaponized in September.

The CDT report also reveals how monitoring software can shrink the distance between classrooms and carceral systems. Forty-four percent of teachers reported that at least one

> student at their school has been contacted by law enforcement as a result of behaviors flagged by the monitoring software. And 37 percent of teachers who say their school uses activity monitoring outside of regular hours report that such alerts are directed to "a third party focused on public safety" (e.g., local police department, immigration enforcement). "Schools have institutionalized and routinized law enforcement's access to students' information," says Elizabeth Laird, the director of equity in civic technology at the CDT.[8]

Such monitoring software appears to be common in California school districts. Rocklin Unified's website, for instance, boasts the availability of "GoGuardian Parent, a mobile app designed to provide parents/guardians insight and control over their student's online activity when on school-managed devices and accounts." Among the app's features:

> **Student Activity Monitoring**
>
> - Top 5 overview of your student's online activity
> - Allow guardians to see the top five sites and documents that their students are viewing.
> - Any teacher interventions related to your student's online activity
> - Allow guardians to view how often a teacher intervened to lock their student's screen or open or close a tab.
> - 30-day overview of your student's online activity
> - Allow guardians to see their student's browsing activity across all websites for the last 30 days.[9]

This level of access to a student's information can uncover information that bears no connection to education or safety. Such information could be weaponized against vulnerable populations, particularly in the hands of school officials, such as those at Chino Valley Unified School District, who are driving efforts to forcibly "out" LGBTQ+ children to their parents through a "parental notification" system that requires officials to alert parents and guardians if the student uses a name or pronoun other than those listed on the student's birth certificate, or uses a bathroom that does not align with the gender assigned in their official records.[10]

4) **Concerns with the prior version of the bill, which recognized the pupil's right to consent to surveillance.** At the behest of ACLU California Action and the Electronic Frontier Foundation, the bill was amended on May 20, 2024, to address their concerns. As amended, the bill provided that if a school district, county office of education, or charter school requests the pupil's voluntary disclosure of or access to electronic information, the request must be accompanied by a written disclosure of the pupil's rights pursuant to the California Electronic Communications Privacy Act (CalECPA), which prohibits government entities[11] from accessing

---

[8] Pia Ceres, "Kids Are Back in Classrooms and Laptops Are Still Spying on Them " (Aug. 3, 2022) *Wired*, https://www.wired.com/story/student-monitoring-software-privacy-in-schools/.

[9] Rocklin Unified School District, "GoGuardian Parent: Rocklin Unified Gives Parents and Guardians GoGuardian Parent," https://www.rocklinusd.org/Departments/Business-Services/Technology-Services/Family-Resources/GoGuardian-Parent/index.html

[10] Mackenzie Mays and Nathan Solis, California school board battles over LGBTQ+ rights intensify after transgender vote in Chino (Jul. 21, 2023) https://www.latimes.com/california/story/2023-07-21/inland-empire-school-board-meetings-sow-chaos-over-textbooks-trans-students.

[11] "Government entity" means "a department or agency of the state or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof." (Pen. Code § 1546(i).) "A public

electronic device information by means of physical interaction or electronic communication with the electronic device, unless it does so pursuant to judicial authorization, such as a warrant or wiretap order.[12] The disclosure was required to state that (1) the school district, county office of education, or charter school is subject to CalECPA, (2) the pupil has the right to refuse to grant access to their information, and (3) the pupil has the right to consult with a parent, guardian, or attorney before granting access. Thus, the May 20th version of the bill implied that the decision whether to grant access to the pupil's electronic information belongs exclusively to the child.

This understanding of the law is rooted in CalECPA, which provides that a government entity may, without a warrant, access electronic device information "[w]ith the specific consent of the *authorized possessor* of the device."[13] "Authorized possessor" means "the possessor of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device."[14] By their plain language, these provisions appear to embrace pupils who are authorized possessors of a phone owned by their parent or guardian. But it is not clear that the Legislature, in enacting this provision, intended to enable pupils as young as kindergarteners to consent to warrantless surveillance.

Unfortunately, the solution in the May 20th version of the bill, which did not benefit from vetting by this Committee or its Senate counterpart, appeared to create more problems than it solved. Expressly granting a government entity the power to obtain consent from a pupil—who could be a young child—to access their private information, even with proper disclosures, opens the door to rampant abuses by unscrupulous officials who leverage their authority over unsuspecting children to obtain access to their information. In practice, this could lead to far more information being accessed by schools, particularly given that such authorizations could last indefinitely.

With the exception of medical emancipation statutes that grant minors over the age of 12 the ability to seek, without parental consent, certain essential—even constitutionally mandated—services such as reproductive healthcare,[15] parents and guardians are generally entrusted with overseeing the well-being of their children unless they are shown to have harmed the child. Acknowledging the very real problem of abusive officials and parents—particularly those seeking to expose the private lives of LGBTQ+ minors—it is not clear that departing from the parental authority model in this case is beneficial overall. Unlike essential medical care, there is no overriding benefit to a child being able to consent to the government accessing their private information.[16]

---

school district is a political subdivision of the State of California." (*K.M. v. Grossmont Union High School Dist*. (2022) 84 Cal.App.5th 717, 752, citations omitted.)

[12] Pen. Code § 1546.1(a), (c).

[13] *Id.* at (c)(4), emphasis added. This is distinguished from a companion provision that allows access "[w]ith the consent of the owner of the device, only when the device has been reported as lost or stolen." (*Id.* at (c)(5).)

[14] Pen. Code § 1546(b).

[15] Fam. Code § 6920 et seq.

[16] A reasonable argument can, however, be made for the converse: that minors of a certain age ought to be able to *refuse* access to their private information, even if their parents are willing to grant it. Indeed, this is the change the organizations now seek. Under the framework proposed in their letter, consent to accessing the pupil's electronic information could be obtained only by express written consent of the pupil and the pupil's guardian or parent. Such a change could arguably solve for the problem of a parent who does not have their child's best interests in mind without the unintended consequences described above. That said, this would constitute a major policy shift with ripple effects across various contexts beyond the education sphere. A policy shift of this magnitude, however justifiable, more properly warrants holistic consideration through the full legislative process.

In view of these possible unintended negative consequences, the provisions were removed from the bill in the Education Committee with the understanding that this Committee would revisit the issue. The removal of the provisions caused the ACLU and EFF to resume opposing the bill.

5) **As proposed to be amended, this bill provides specific limitations on requests for voluntary disclosure or access to a pupil's electronic information.** In view of the concerns set forth above, the author has agreed to amend the bill to impose guardrails on requests for electronic information in connection with a school's social media policy. These amendments, which were drafted in coordination with the Education Committee, do the following:

- Clarify that CalECPA applies to a pupil's electronic information.
- Require express written parental consent in order for a governing body of a school to access the pupil's electronic information.
- Limit the scope of such requests to information related to specific incidents involving potential harassment, cyberbullying, or crimes.
- Provide a written disclosure to the pupil in the event the parent grants consent to such a request.
- Prohibit conveying electronic information to third parties unless necessary to address misconduct or required by law.
- Specifically prohibit the governing body from seeking, retaining, or sharing information related to the child's gender identity, gender expression, or sexual orientation unless necessary to address misconduct or required by law. Strictly speaking, this would be covered under the provisions described above. But this provision would simply make explicit the Legislature's intent to protect children from anti-LGBTQ+ efforts.
- Provide that the authority for such a request expires at the end of a school year. This is a backstop; as described above, the request must be in response to specific incidents. Once the incident is resolved, there authority lapses. But in some cases the need to investigate or monitor could last several months. This provision ensures that the authority to access electronic information does not last indefinitely.

The amendments are as follows:

Section 48901.9 is added to the Education Code to read as follows:

(a) Access to a pupil's electronic information is subject to the California Electronic Communications Privacy Act (Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code).

(b) Notwithstanding paragraph (4) of subdivision (c) of Section 1546.1 of the Penal Code, a school district, county office of education, or charter school's request for voluntary disclosure of, or access to, a pupil's electronic information may be obtained only through written specific consent of the pupil's parent or guardian. Additionally, such a request must meet all of the following:

1) The request shall identify specific categories of information and timeframes in which the information is likely to have been generated.

2) The specific categories of information allowable under paragraph 1) are limited to information directly related to acts of harassment, cyberbullying, or that may violate the Penal Code.

3) The request is in response to a specific incident involving conduct or alleged conduct that falls under paragraph (2).

(c) If a parent or guardian grants consent pursuant to subdivision (b), the school district, county office of education, or charter school shall, prior to accessing the information, provide a written disclosure to the pupil informing them that the parent or guardian has consented to the disclosure of, or access to, the pupil's electronic information.
(d) Information obtained by the school district, county office of education, or charter school shall not be conveyed to anyone aside from authorized staff, except as necessary to address conduct that falls under paragraph 2) of subdivision (b) or as otherwise required by state or federal law.
(e) A school district, county office of education, or charter school that makes a request pursuant to subdivision (b) shall not seek to obtain information relating to a pupil's gender, gender identity, gender expression, or sexual orientation. If the school district, county office of education, or charter school discovers such information about any pupil, it shall treat the information as confidential and shall not retain or share the information, except as necessary to address conduct that falls under paragraph 2) of subdivision (b) or as otherwise required by state or federal law.
(f) A request made pursuant to subdivision (b) for which consent has been granted is no longer valid after the end of the school year in which the request is made. After the ensuing school year starts, a new request may be made subject to the requirements of this section.
(g) It is the intent of the Legislature to protect LGBTQ+ youth from policies that forcibly "out" the youth.

6) **Related legislation**. *See* Comment 1.

ARGUMENTS IN SUPPORT: CFT — A Union of Educators & Classified Professionals, AFT, AFL-CIO, writes:

> Educators within CFT are deeply troubled by the increase in youth suicide attributed to bullying and social media usage in our schools. Recent research shows the link between excessive social media exposure and heightened depression and anxiety amongst our students. Teachers have been targeted by social media posts during school hours which attempt to humiliate educators, distract from the main mission of public education, and can even lead to threats. Outside of certain sociological, historical, or governmental lessons, the use of social media by students has no utility in the public education arena, and can be quite dangerous.

ARGUMENTS IN OPPOSITION: Adopting an oppose-unless amended position, the ACLU and EFF jointly write to express concerns over the removal in the Education Committee of provisions that these organizations had worked with the author to adopt. As described above, those provisions recognized the pupil's sole right to consent to access to their electronic information, causing concerns for the Education Committee and this Committee. This Committee's amendments, set forth above, retain the parent or guardian's power to consent, but also provide for written disclosure to the pupil if the parent grants consent.

It is not clear that this will allay the concerns of these organizations, who have now adopted the stance that consent to access a pupil's electronic information ought to be obtained from both pupil and their parent or guardian—in effect, enabling the pupil to override consent granted by the parent or guardian. The organizations write as follows:

As you know, both of our organizations initially opposed SB 1283 in the Senate. We were pleased to remove our opposition on the Senate Floor in response to your office's exceptional collaboration and adoption of amendments. These amendments, which went into print on May 20, 2024, require local education agencies to provide written disclosures of a student's rights alongside any requests for a student to voluntarily disclose or give access to electronic information. ACLU California Action and EFF are deeply concerned to learn of further proposed amendments from the Assembly Education Committee that would remove this requirement from the bill. We will be compelled to leave our neutral position if these amendments are adopted.

The premise of SB 1283 is to take local educational agencies' existing authority to "limit or prohibit" student use of smartphones and replicate it to create a new authority to regulate student social media use while they are at a schoolsite or "under the supervision and control of an employee" of the school or district. Problematically, regulating social media use is a much more complicated issue than regulating smartphones. Smartphones are physical objects, so limiting their use is as non-invasive as requiring students to put them away. On the other hand, for a school employee to regulate a student's social media usage on their smartphone while at a schoolsite, the employee would have to look through the student's phone for social media apps or messaging.

This butts up against students' right to privacy. As it was introduced, and as proposed to be amended, SB 1283 would essentially invite school employees with limited knowledge of privacy laws to violate the California Electronic Communications Privacy Act (CalECPA), which limits the ability of the government to access electronic devices without a warrant and due process. This applies in a school context – if schools want access to a smartphone's content without a student's consent, they need a warrant.

Additionally, social media can be accessed on a tablet or computer, not just on a smartphone. Most students have a school-issued tablet or computer, and SB 1283's language around "supervision" could be interpreted to give schools a broad ability to monitor student activity and student speech on school-issued devices outside of school hours, including speech they reasonably expect to be private, such as their conversations with friends while gaming. This has First Amendment and privacy implications, and we have heard from students and families that school monitoring of these kinds of activities has led to results as severe as law enforcement officers being sent to a home. These potential impacts of SB 1283 without the protections of the May 20th amendments would have disparate impact on Black and Brown students and students of low income because they are more likely to use school-issued devices for personal activities outside of school hours, as the school-issued device may be the only computer or tablet in the home.

SB 1283 would also have implications for school technology infrastructure. As introduced and as proposed to be amended, this bill might allow schools to monitor activity on any device connected to the school's wi-fi or used on school grounds – including devices of parents or other non-pupils – and to add network devices that monitor traffic without due process safeguards.

For all of these reasons, ACLU California Action and EFF were pleased to work with your office on the May 20th amendments that required local education agencies to expressly communicate students' CalECPA rights alongside any request for disclosure of or access to

electronic information. This addition to SB 1283 was a critical protection to ensure local education agencies knew and took into consideration students' right to privacy under California law, and that students' disclosures were truly voluntary as required by that same law.

[. . .] Without protections around CalECPA and students' right to consent, SB 1283 would allow school districts to create policies that violate California's privacy laws, infringe on students' constitutional rights, and widen educational equity gaps.

REGISTERED SUPPORT / OPPOSITION:

Support

Organization for Social Media Safety (sponsor)
California Chamber of Commerce
California State PTA
CFT- a Union of Educators & Classified Professionals, Aft, Afl-cio
Los Angeles County Office of Education
TechNet

Opposition

ACLU California Action
Electronic Frontier Foundation

Analysis Prepared by: Josh Tosney / P. & C.P. / (916) 319-2200