ACLU
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
Northern California

Californians for Justice

CENTRAL VALLEY PARTNERSHIP

CAIR
SACRAMENTO VALLEY / CENTRAL CALIFORNIA

DOLORES HUERTA FOUNDATION FOR COMMUNITY ORGANIZING
ORGANIZE

FRESNO BARRIOS UNIDOS
Advocacy • Education • Wellness

GSA NETWORK

HMONG INNOVATING POLITICS

SIREN
SERVICES, IMMIGRANT RIGHTS & EDUCATION NETWORK

Sent via electronic mail

December 15, 2020

Robert G. Nelson
Office of the Superintendent
Fresno Unified School District
2309 Tulare Street
Fresno, CA 93721
Bob.nelson@fresnounified.org

Dear Superintendent Nelson,

We write to express civil rights and civil liberties concerns with Fresno Unified School District's ("FUSD" or "District") requirement that students utilize online monitoring software while participating in distance learning. Specifically, we are concerned that FUSD's requirement that students use Gaggle on both district-issued and personal laptops, Chromebooks, and other electronic devices to attend class and submit assignments violates the California Electronic Communications Privacy Act ("CalECPA") and disproportionately harms marginalized students. Given these concerns and the reality that surveillance technologies like Gaggle are not proven to promote school safety, we demand that the District end this requirement.

In response to the COVID-19 pandemic, school districts across the state transitioned to distance learning as a safety measure to prevent the spread of the novel coronavirus. School districts across the state began the 2020-21 academic year with distance learning and, on account of recent legislation, will be permitted to offer distance learning in the 2020-21 school year to comply with public health orders and to permit medically fragile students to learn from home.[1]

[1] Cal. Educ. Code § 43503.

As a result, students rely on computers, tablets, and other electronic devices to attend classes, complete assignments, participate in extra-curricular activities, communicate with psychologists and other health professionals, and socialize with their peers. With this unprecedented full transition to remote learning, some school districts have partnered with online safety management vendors to aid administrators in monitoring students' activities while using District-provided hardware and software. These vendors claim that their products protect student safety and ensure their well-being by blocking potentially harmful content and monitoring student communications and files for violations of student digital safety policies such as cyberbullying. While we recognize that distance learning during a global pandemic has no precedent, it is critical that local education agencies uphold the privacy and free speech rights of students and families in developing solutions to address online learning. FUSD's current requirement that students utilize Gaggle while engaging in distance learning contravenes these rights.

FUSD asserts that it recently partnered with Gaggle to help the District meet its legal obligations under the Child Internet Protection Act ("CIPA"), a voluntary program that imposes certain requirements on schools to receive discounted communications services and products, including internet safety policies and technology protection measures.[2] Gaggle monitors students' activities while they use District-provided software such as Microsoft Teams, Microsoft Office 365 email, and OneDrive. For FUSD students, Gaggle is automatically integrated with this software, which all students are *required* to use in order to attend class and submit assignments.[3] Accordingly, both students who receive District-issued devices and students who opt to use their personal devices for remote learning are required to allow Gaggle access to their devices to monitor their online activity. This monitoring includes machine-learning technology that blocks potentially harmful content and images; flagging of keywords in communications and internet searches that may indicate a student's intent to harm themself or others; and human review of blocked content and flags by Gaggle and school district personnel to evaluate incidents and conduct any necessary follow up, including contacting law enforcement in some cases.[4]

We are aware of several FUSD students and parents who are rightfully skeptical of this online monitoring, citing privacy and free speech concerns. They further contend that they did not provide FUSD with consent to monitor their children's online activity via Gaggle. The District

[2] Federal Communications Commission, *Children's Internet Protection Act (CIPA)*, https://www.fcc.gov/consumers/guides/childrens-internet-protection-act.

[3] Shayla Girardin, *School districts outline plans to keep virtual classrooms secure from hackers*, ABC30 ACTION NEWS (Aug. 11, 2020), https://news.gaggle.net/how-it-works?utm_campaign=2020%20Overview%20Video&utm_source=gaggle.net&utm_medium=web (reporting that "Fresno Unified is using Microsoft Teams as their primary platform, which requires everyone to have a login. . . . Another key investment is Gaggle, an online tool looking for anything that may cause concern. 'As in cyberbullying, it looks for porn, for anything in email, in the files that they store, in the team chat,' explained [Fresno Unified Chief Tech Officer Kurt] Madden, 'So anything that they're doing in teams or storing.'"). *See also* Gaggle, *How It Works*, https://news.gaggle.net/how-it-works?utm_campaign=2020%20Overview%20Video&utm_source=gaggle.net&utm_medium=web.

[4] *Id*. *See also* Fresno Unified School District, *A Strategic Plan for Reopening Schools 2020-2021* 8 (July 31, 2020), https://www.fresnounified.org/wp-content/uploads/A-Strategic-Plan-for-Reopening-Schools.pdf ("Gaggle uses key phrases and technology to identify inappropriate language, bullying and harassment, inappropriate sexual content and even situations that might lead to self-harm. . . . If a school administrator is unavailable, Gaggle will contact local public safety in life threatening situations.")

has stated that it obtained consent from its students' parents/guardians to use Gaggle through the FUSD Technology Acceptable Use policy[5], which students and parents/guardians sign at the start of each academic year. While families recall signing this policy in previous school years, they state that they did not receive or sign any such policy for the 2020-2021 school year. Even if students and parents/guardians were notified of the District's plans to use Gaggle during distance learning and asked to sign a form consenting to the district's monitoring of their child's activity, it does not appear they could opt out without detriment, as consenting to Gaggle monitoring has been described as a requisite for their children's eligibility to attend school within FUSD.

1. California law prohibits monitoring of electronic devices without student consent.

Under the California Electronic Communications Privacy Act ("CalECPA"), a "government entity"—including a public school or any person acting on its behalf—may only "access electronic device information" under a narrow set of circumstances.[6] Absent a court order or exceptional circumstances, accessing electronic device information requires the consent of the "authorized possessor" of the device.[7] Your policy, which allows the school to access electronic device information on school-issued devices or software that are required for educational purposes, is in violation of this requirement.

Neither the school's ownership of the device nor the student's "acceptance" of the mandatory terms of use change this conclusion. CalECPA is very clear that it is the *authorized possessor's* consent that is necessary, not the owner's, unless the device is "reported as lost or stolen."[8] Moreover, consent for government search must be "freely and voluntarily given."[9] Accepting terms presented as mandatory in order to fully participate in public education —especially during a pandemic, when remote classes require the use of electronic devices—does not meet that standard.

If a school wishes to monitor the use of or otherwise access data on a school-issued device or account, it may directly ask the student and their parent or guardian. But it may not condition full participation in school or school-sponsored activities, including the use of school-issued electronic devices, on access to the device in the student's possession. Any such policy that impermissibly conditions participation in the educational program on consenting to invasive digital searches violates California law.

2. Compliance with California law is consistent with the Children's Internet Protection Act.

Under the Children's Internet Protection Act ("CIPA"), schools (and other institutions) with "computers having Internet access" that wish to apply for and receive grants or discounts through

[5] Fresno Unified School District, *District Technology Acceptable Use Policy*, https://mk0informationtrwene.kinstacdn.com/wp-content/uploads/AUP-English.pdf.

[6] Cal. Penal Code § 1546.1(c).

[7] *Id.* § 1546.1(c)(4).

[8] *Id.* § 1546.1(c)(4) & (c)(5).

[9] *Schneckloth v. Bustamonte*, 412 U.S. 218, 228 (1973) (quoting *Bumper v. North Carolina*, 391 U.S. 543, 548 (1968)). *Schneckloth* and *Bumper* interpreted consent within the context of the Fourth Amendment, which CalECPA was designed to codify and build upon.

the E-rate program must “enforce[e] a policy of Internet safety for minors that includes monitoring the online activities of minors.”[10] However, this provision is not in tension with CalECPA’s prohibition on monitoring school-issued devices without meaningful consent. Nor would it matter if it were, as schools may not decline to comply with California law.

To date, there is no evidence that CIPA certification has been conditioned on a program of monitoring devices that are not in the actual possession of the school, including school-owned devices issued to students. Instead, CIPA certification and access to grant monies has been granted based on monitoring of devices, including computers and networks, that are in the possession of the school itself. Moreover, the FCC states this monitoring “does not require the tracking of Internet use by minors” such as accessing logs of web pages visited by a student using a school-issued device.[11] As such, California schools can apply for E-rate discounts and CIPA certification without monitoring school-issued devices in the possession of students, thus avoiding any tension with CalECPA.

Even if such tension existed, however, schools cannot simply choose not to comply with California statutory law in order to apply for voluntary discounts through a federal program. CalECPA’s mandate applies to all “government entities,” which includes public school districts. CIPA certification is voluntary. If there were any conflict, a school’s obligation to follow CalECPA unquestionably take precedence.

3. Gaggle Is Not A Proven and Effective Measure to Improve School Safety

We understand that the District purchased Gaggle with the goal of protecting students from harms associated with using online technology, including protecting students from cyberbullying or self-harm. However, Fresno Unified has not offered any sound evidence that Gaggle would significantly benefit student or school safety. To the contrary, the only support for the claim that Gaggle purports to safeguard children’s safety is offered only by the company itself and is not supported by sound, independent research.

Independent research has consistently shown that surveillance methods have not proven to be effective at preventing violence on school campuses.[12] There is even less data supporting the efficacy of surveillance software like Gaggle in preventing bullying, harassment, and self-harm among students.

Generally, surveillance technology is not effective at making students safer and has the potential to harm students. The Center for Democracy and Technology and the Brennan Center for Justice report that the technology used by schools to purportedly address school safety concerns are largely “unproven, have known technical limitations, are difficult to audit, and almost certainly

[10] 47 U.S.C. 254(h)(5)(B).

[11] Federal Communications Commission, *Children’s Internet Protection Act (CIPA)*, https://www.fcc.gov/consumers/guides/childrens-internet-protection-act.

[12] James H. Price and Jagdish Khubchandani, *School Firearm Violence Prevention Practice and Policies: Functional or Folly?* VIOLENCE AND GENDER 154-167 (Sep. 2019), http://doi.org/10.1089/vio.2018.0044; Jack Gillum & Jeff Kao, *Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students*, PROPUBLICA (Jun. 25, 2019), https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/..

produce false positives that could subject students to unnecessary scrutiny and interactions with law enforcement."[13] They further report that technology meant to monitor students' online activity, including monitoring to prevent cyberbullying or self-harm, is not reliable, explaining that:

> These tools are largely experimental and have significant technical limitations and accuracy problems. Some of these tools rely on a predetermined "library" of words or phrases that could indicate potential risks of harm. However, many words associated with harm (such as "bomb" or "shoot") are extremely common and have meanings that are entirely context-dependent. These types of tools will produce many false positives, overwhelm schools with information, and subject far too many students to unnecessary surveillance given their limited efficacy.[14]

We understand that the COVID-19 pandemic has necessitated an unprecedented reliance on technology to communicate with students and families and to provide instruction during distance learning. However, we cannot rely on technology while ignoring civil rights and civil liberties concerns.[15]

Instead of investing in technology like Gaggle that is not independently proven to be an effective component of a comprehensive school safety plan, we urge the District to instead invest its resources in evidence-based best practices to promote school safety. To protect students against cyberbullying, the most effective strategy schools can use is to promote a positive school climate, which "is consistently associated with lower rates of bullying and cyberbullying behaviors."[16] Last year, the Learning Policy Institute's Linda Darling-Hammond highlighted multiple evidence-based measures that are effective in promoting school safety, none of which include surveillance measures or harsh discipline for students:

> A recent body of research shows that a better way to make schools truly safe is to invest in student supports, including social and

[13] Center for Democracy & Technology & Brennan Center for Justice, *Technological School Safety Initiatives: Considerations to Protect All Students* 1 (June 2019), https://cdt.org/wp-content/uploads/2019/06/2019-05-24-School-safety-two-pager-Final.pdf. *See also* Center for Democracy & Technology & Brennan Center for Justice, *Social Media Monitoring in K-12 Schools: Civil and Human Rights Concerns* 1 (Oct. 2019), *https://www.brennancenter.org/sites/default/files/2019-10/CDT%20Brennan%20Statement%20on%20School%20Social%20Media%20Monitoring.pdf;* Todd Feathers, *Schools Spy on Kids to Prevent School Shootings, But There's No Evidence It Works*, VICE (Dec. 2019) https://www.vice.com/en/article/8xwze4/schools-are-using-spyware-to-prevent-shootingsbut-theres-no-evidence-it-works ("Some vendors claim to have prevented school shootings and intervened to save thousands of suicidal children. There is, however, no independent research that backs up these claims.")

[14] Center for Democracy & Technology and Brennan Center for Justice, *Social Media Monitoring in K-12 Schools: Civil and Human Rights Concerns*, 1 (Oct 2019), https://cdt.org/wp-content/uploads/2019/10/CDT-Brennan-School-Social-Media-Monitoring.pdf.

[15] *See, e.g.,* ACLU's letter to the California Department of Education and California Senator Connie Leyva about education technology and civil liberties concerns (May 19, 2020) (available at https://www.aclusocal.org/sites/default/files/acluca_20200519_edtech_civil_liberties.pdf).

[16] U.S. Department of Education, *Final Report on the Federal Commission on School Safety* 24 (Dec. 2018), https://www2.ed.gov/documents/school-safety/school-safety-report.pdf.

> emotional learning and mental health supports; community involvement, including access for children to health and social services supports that address the trauma many experience; and professional development for teachers and school staff.
>
> Teaching students how to recognize and manage their emotions, access help when they need it, and learn problem solving and conflict resolution skills can make a huge difference in school safety. A meta-analysis of more than 200 studies found that schools using social-emotional learning programs focused on these skills make schools decidedly safer, reducing bullying and poor behavior, as well as supporting increased school achievement. A second meta-analysis found that these benefits are sustained over time, positioning students and their schools for greater success.[17]

Because Gaggle and surveillance programs like it are not independently proven to promote school safety and because such technology leads to invasive intrusions into student privacy, we demand that the District cease its use of Gaggle and invest in measures that are proven to promote school safety while respecting civil rights and civil liberties.

4. Surveillance Technologies Disproportionately Impact Students of Color and Students Within the LGBTQ+ Community

We also urge the District to cease use of online monitoring technologies like Gaggle because they disproportionately impact students of color and students within the LGBTQ+ community.

Surveillance technologies have been shown to disproportionately and erroneously flag activity from these groups. For example, language algorithms not only produce mostly useless data and rarely succeed in preventing violence, but also often erroneously single out people of color.[18]

A recent nationwide survey of K-12 parents found that while parents generally welcome technology for distance learning, “African American parents reported higher levels of concern on issues of unauthorized access of student online activity or communication online (43% “very concerned,” compared to 35% overall) and scenarios where student data could be shared with

[17] Linda Darling-Hammond, *Want Safe Schools? Start with Research-Based Discipline Policies*, Learning Policy Institute (May 2019), https://learningpolicyinstitute.org/blog/want-safe-schools-start-research-based-school-discipline-policies.

[18] *See, e.g.*, Barton Gellman and Sam Adler-Bell, *The Disparate Impact of Surveillance*, The Century Foundation, (2019), https://tcf.org/content/report/disparate-impact-surveillance/?agreed=1; James H. Price and Jagdish Khubchandani, *School Firearm Violence Prevention Practice and Policies: Functional or Folly?* Violence and Gender at 154-167 (Sep. 2019), http://doi.org/10.1089/vio.2018.0044; Anna Woorim Chung, *How Automated Tools Discriminate Against Black Language*, MIT Center for Civic Media (Jan. 24, 2019). https://civic.mit.edu/index.html%3Fp=2402.html. *See also*, Natasha Duarte, Emma Llanso, and Anna Loup, *Mixed Messages? The Limits of Automated Social Media Content Analysis,* Center for Democracy & Technology (Nov. 28, 2017) https://cdt.org/insight/mixed-messages-the-limits-of-automated-social-media-content-analysis/.

law enforcement (61% “very” or “somewhat concerned,” compared to 56% overall).”[19] To the detriment of students and families, reliance on surveillance technology can lead to increased student contact with law enforcement, even when there is no true threat to student safety. Such contact that unnecessarily exposes children to the criminal legal system is known as the school-to-prison/deportation pipeline and these types of surveillance programs serve as the digital component to this pipeline. Instead of strengthening this harmful pipeline, school districts like FUSD should work to dismantle it.

Finally, students might hesitate to look for help or support online if they know they are being surveilled by their school. This may have a disproportionate negative effect on LGBTQ+ students, who might avoid searching health resources or youth-friendly LGBTQ+ content if they know doing so can trigger an alert to school officials.

Again, we recognize that distance learning during a global pandemic has no precedent and appreciate the District’s commitment to providing instruction during the pandemic. However, it is critical that FUSD uphold the civil rights and civil liberties of students and families in its technology program. For these reasons, we demand that FUSD end the required use of Gaggle. We welcome an opportunity to further discuss these matters.

Sincerely,

Jennifer Jones
Technology & Civil Liberties Fellow
ACLU Foundation of Northern California

Ana Mendoza
Education Equity Staff Attorney
ACLU Foundation of Southern California

Ashley Rojas
Executive Director
Fresno Barrios Unidos

Daniel O’Connell, PhD.
Executive Director
Central Valley Partnership

Maricela Gutiérrez
Executive Director
SIREN (Services, Immigrant Rights &
Education Network)

Sukaina Hussain
Outreach Director
CAIR Sacramento Valley/Central California

Katie Moua
Fresno Lead Community Organizer
Hmong Innovating Politics

Rosa De León
Strategy Director
Californians for Justice

Cecilia Castro
Deputy Director
Dolores Huerta Foundation

Ginna Brelsford & Geoffrey Winder
Co-Executive Directors
GSA Network

Cc: Kurt Madden, Chief Technology Officer for Fresno Unified School District

[19] Center for Democracy & Technology, *Student Data and Information Privacy: A Survey of Parents of K-12 Students* (Sep. 2020) https://cdt.org/wp-content/uploads/2020/09/CDT-Parent-Student-Data-Privacy-Report-Slides.pdf .