“Almost [one third](https://thejournal.com/articles/2014/04/08/a-third-of-secondary-students-use-school-issued-mobile-devices.aspx) of all students—elementary through high school—already use school-issued digital devices, and many of these devices present a serious risk to student privacy. They collect far more information on kids than is necessary, store this information indefinitely, and sometimes even upload it to the cloud automatically. In short, they’re spying on students—and school districts, which often provide inadequate privacy policies (or no privacy policy at all), are helping them” (Electronic Frontier Foundation, 2016). This statement on the Electronic Frontier Foundation’s website could cause any parent to march down to his child’s school and demand some answers. This is exactly what happened a few months ago in Roseville, California. Jeff, a parent of a fourth grader, made fervent objections to his daughter using Google Apps for Education. This got the attention of not just the district, but national news. Electronic Frontier Foundation has since filed a claim with the Federal Trade Commission. The question becomes, does this argument hold any merit? In short, where there has been a bit of a learning curve integrating technology safely in the classroom, including adopting Google Apps, parents can be assured that their child’s privacy is not at risk.

First and foremost, Google is not personally tracking your child. More than 50 million teachers and students are using Google Apps for Education (GAFE), especially now with the inexpensive Chromebook making technology accessible for schools. According to Futuresource Consulting, a researching firm that tracks school technology purchases, in 2012 Chromebooks made up less than one percent of all laptops in schools. Their latest data shows that Chromebooks account for 51% of sales to schools (Petersen, 2015). On a Chromebook, students are forced to use Google Apps. This presents a huge concern for parents like Jeff who believe Google is tracking their child. The Electronic Frontier Foundation’s (EFF) staff attorney, Nate Cardozo believes, “Despite publicly promising not to, Google mines students’ browsing data and other information, and uses it for the company’s own purposes. Minors shouldn’t be tracked or used as guinea pigs, with their data treated as a profit centre” (Gibbs, 2015). Cardozo and the EFF insist that the data Google is collecting will be used to target students with ads. However, this is not true. While Google admits to tracking user use, the purposes are not to collect private information. On Google’s blog it states, “The GAFE [Core Services](http://www.google.com/apps/intl/en/terms/user_features.html) -- Gmail, Calendar, Classroom, Drive, Docs, Sheets, Slides, Contacts, Groups, Vault and Hangouts -- are the heart of Google’s educational offering to schools. Students’ personal data in these Core Services is only used to provide the services themselves, so students can do things like communicate using email and collaborate on assignments using Google Docs. There are no ads in these Core Services, and student data in these services is not used for advertising purposes” (Google Apps for Education, 2015) The GAFE suite has never had ads, nor will it ever, we are assured. Google is committed to transparency of their use of data and the protection of student privacy. The collection of information is simply to make the user’s experience more effective and productive.

In addition, Chrome Sync data is not used to target ads to individual students. One of the best features of Chrome is the convenience of being able to move from one device to another, syncing information like browsing history, bookmarks and passwords by simply logging into your Chrome account. This feature called Chrome Sync is under fire by EFF. EFF claims that this is dangerous for children. When a child is at home or uses other sites like Youtube, Maps and Google News at school, their data can be collected for ad use. These sites are not considered part of the GAFE suite and contain ads. Citing Chrome Sync as a privacy violation, Google also addressed this on its blog. It states, “Personally-identifiable Chrome Sync data in GAFE accounts is only used to power features in Chrome for that person, for example allowing students to access their own browsing data and settings, securely, across devices. In addition, our systems compile data aggregated from millions of users of Chrome Sync and, after completely removing information about individual users, we use this data to holistically improve the services we provide. For example if data shows that millions of people are visiting a webpage that is broken, that site would be moved lower in the search results. This is not connected to any specific person nor is it used to analyze student behaviors” (Google, 2015). Again, Google holds true to their task of simply gathering data to improve student experiences when using Google products. Of course, in trying to put student’s first, they also recognized that not all consumers (teachers or students) would find this explanation enough. Therefore, the company reiterates that districts can turn Chrome Sync off or choose what apps to sync. Google has given so much of the GAFE control at the school district level, understanding that the needs of all students are not the same. Districts can control the use of additional Google consumer services, like Blogger, Youtube and Maps if they desire. Giving the district administrators control strengthens Google’s commitment to the integrity of student education.

Furthermore, the gaps in student privacy legislation are closing. Another real concern is not just with Google. There are so many apps and providers working with GAFE that privacy has become an issue. Khaliah Barnes, an associate director at the Electronic Privacy Information Center believes, “Students are not getting the kind of security and privacy protection they deserve” (Petersen, 2015). The laws written in the 1970’s do not require parental approval for vendors for whom school districts choose to do business. This is a bit tricky when it comes to online data. A 2013 study showed that 95% of districts relied on an online cloud service, but only a quarter of those actually informed parents. Even worse, fewer than a quarter of service agreements included what student information the district was disclosing and less than 7% restricted vendors from selling or marketing data about students. In an age of an abundance of digital information, this is really disturbing. Most parents at GAFE districts were never asked for permission, nor were they even told the school was converting. This is disconcerting and alarming to any parent, especially ones like Jeff, who are deeply concerned for the protection of privacy. However, according to an analysis by the Data Quality Campaign, in 2014, 28 student data privacy laws were signed into law across 20 states. According to edweek.org, in California, the [Student Online Personal Information Protection Act](https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1177), or SOPIPA, (SB 1177) “Prohibits operators of online educational services from selling student data and using such information to target advertising to students or to "amass a profile" on students for a non-educational purpose. The law also requires online service providers to maintain adequate security procedures and to delete student information at the request of a school or district” (Herold, 2014). This is considered one of the strictest laws passed nationwide. Therefore, even another online vendor other than Google has to abide by the rules of not collecting student information for non educational purposes, as well as delete student information when it is no longer needed. In California, another law put into effect in 2014 was AB 1594. The bill puts stricter regulations on contracts with vendors and what information they are allowed to obtain and disseminate. According to Joni Lupovitz, vice president of policy for Common Sense Media, a site dedicated to the education and advocacy of safe technology, "Together, it's really a landmark regulatory scheme. The whole idea is not to stop education technology; the idea is to create a trusted online environment so kids can just be kids and focus on learning"(Roscorla, 2014). Both of these were a leap in the right direction for the privacy of our children.

Districts are also following suit. They are wising up and not staying ignorant on who has their student data and for what purpose. In Roseville, every vendor is required to fill out a vendor compliance agreement, answering specifically to AB 1594 and agreeing to not violate the privacy of the students through sharing any information, including passwords, names and birthdays. (See [Appendix)](https://drive.google.com/file/d/0B1rwn7pWhkx-UU56NnZodi1pbzA/view?usp=sharing). Instead of using student names as identifiers in email and logins, the district has moved to using student identification numbers. Laura Assem, the Chief Technology Officer in Roseville, stated that it is vital students cannot be found online by their names. Removing the use of names is a logical step. As Assem stated, “Unfortunately, technology advances faster than legislation, but you can’t remove technology from education because it’s an accelerator” (Petersen 2015). Districts are recognizing their shortcomings with keeping kids safe, but the benefits of using technology in the classroom are still worth being patient.

GAFE provides students with an experience in the classroom and at home that has not only invigorated learning, but is preparing our students for a 21st Century world. Of course, with every new step we take in technology, there seems to be a concern. However, we must understand the benefits of using technology clearly outweigh even the most minor uncertainty. A study conducted by [Adam Schoenbart](https://www.google.com/+AdamSchoenbart1), an educator in New York who surveyed his own staff and students in 2014, the early stages of GAFE implementation at his site, found that most students and teachers found the use of GAFE had a positive impact on student learning. Of those surveyed, 65% of teachers saw a difference and 60% of students. These were just in the first years of implementation. One district in north Texas, the Arlington Independent School District (AISD) believes that by using GAFE, their collaboration as teachers improved greatly with shared Google Docs. They also improved access to technology for students across socioeconomic levels. A school district in Buffalo, New York, Amherst Central School cites Google Apps for providing individual learning opportunities (Google for Education, 2015). The testimonials seem to be plentiful on Google’s blog. More than anything, providing inexpensive ways for all students to access the internet, create content and collaborate with peers and mentors is inarguably the best option for schools.

As far as the opposition goes, there will always be those that let fear rule fact. They will argue that Google is simply lying to us; that they are storing our children’s information for use in ways we can’t even imagine. However, there is absolutely no merit to that argument. There are those that fear a security breach where our children’s information will be stolen. Unfortunately, in a digital age, that is always a valid concern, but not one that can be specifically applied to Google Apps for Education. Your Social Security number could be stolen from any of a number of secure servers by a gifted hacker. It is the risk we live with in a digital world. Understandably, prior to 2014, the laws were outdated, and companies, like Google could have used student information for profit gain in advertising or some other form. The thing is, there is no evidence it did. Rest assured though, school districts and legislatures are paying attention now. Those gaps are closing and our children are safer than ever. As we move our students to 21st Century skills, we are also moving their privacy to 21st Century security. So, let your kid check his email, work on his Slide presentation and collaborate with his buddy on a Google Doc. He’s safe. As far as dealing with the ones who still object, the Roseville father, Jeff, has come to an agreement with the district. His daughter has been issued a Macbook where she uses the internet and creates Word documents and Power Points without signing into her Google account. She is missing out on the collaborative piece, but sometimes districts have to do what’s best for every child, even if that means simply appeasing a parent.

Appendix : <https://goo.gl/ZOe0ka>

References

California Protects Student Data Privacy with Two Bills. (n.d.). Retrieved February 27, 2016, from http://www.govtech.com/education/California-Protects-Student-Data-Privacy-with-Two-Bills-.html

Gibbs, S. (2015, December 02). Google accused of spying on students in FTC privacy complaint. Retrieved February 27, 2016, from http://www.theguardian.com/technology/2015/dec/02/google-eff-ftc-privacy-chromebook-gmail-spying-students

Google for Education:. (n.d.). Retrieved February 27, 2016, from https://www.google.com/edu/case-studies/amherst-central-schools/

Google for Education:. (n.d.). Retrieved February 27, 2016, from https://www.google.com/edu/case-studies/arlington-independent-school-district/

Google for Education: The facts about student data privacy in Google Apps for Education and Chromebooks. (n.d.). Retrieved February 27, 2016, from http://googleforeducation.blogspot.com.au/2015/12/the-facts-about-student-data-privacy-in.html?m=1

Google for Education: Tools schools can trust. (n.d.). Retrieved February 27, 2016, from https://www.google.com/edu/trust/#has-google-signed-the-student-privacy-ledge

Peterson, Andrea. (2015, December 28). Google is tracking students as it sells more products to schools, privacy advocates warn. (n.d.). Retrieved February 27, 2016, from https://www.washingtonpost.com/news/the-switch/wp/2015/12/28/google-is-tracking-students-as-it-sells-more-products-to-schools-privacy-advocates-warn/

The Schoenblog. (n.d.). Retrieved February 27, 2016, from http://www.aschoenbart.com/2016/02/gafe-impact-report-part-3-summary-of.html

Student Privacy. (n.d.). Retrieved February 27, 2016, from https://www.eff.org/issues/student-privacy/