ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

August 3, 2015

VIA EMAIL

Mr. ---
Superintendent
Roseville City School District

Ms. ---
Director of Technology
Roseville City School District

Re: Protecting the Online Privacy of District Students

Dear Mr. --- and Ms. ---:

We have been retained by -- to represent him in further discussing his interest in protecting his daughter's online privacy in light of the district's decision to use Chromebooks and Google Apps for Education (GAFE) in the classroom. As you know, -- -- will start fourth grade at Sargeant Elementary this fall.

Mr. -- is pleased that you have agreed to provide -- with a non-Google hardware and software option for the upcoming school year. The district will purchase a non-Google device (that cannot be taken home), and communication between the district and -- that would have otherwise been through Gmail will instead be sent to an email address provided by Mr. --. A non-Google option is consistent with the accommodations her third grade teacher made: -- used her teacher's Apple computer and the Firefox browser to access a variety of websites linked on her teacher's webpage.[1]

Computers and the Internet can provide valuable educational experiences for students and teachers alike, and we commend Roseville City School District for bringing technology into the classroom. However, the use of Chromebooks and GAFE puts students' privacy at risk. We fear that the district has not fully considered the equally important interests in protecting student privacy and teaching students to be savvy and safe technology users.

The district has a responsibility to help protect students' privacy in light of Google's data practices and federal and state privacy laws (as we discuss below). We urge you to permit --, and all students – if their parents so decide – to use alternative devices, software and websites, for the upcoming school year and every year.

[1] *See* Roseville City School District webpage for Christina Bartell, http://www.rcsdk8.org/apps/pages/index.jsp?uREC_ID=164321&pREC_ID=links&type=u&id=&sREC_ID=u164321&hideMenu=&linkLabel=American%2BSymbols.

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

I. Google Collects and Uses a Variety of Student Personal and Behavioral Data

Although Google provides very useful services, it is also a commercial data company that is eager to win loyal users. Roseville City School District is helping recruit those users by having students use Google hardware and software/"cloud" products. **The district is teaching students that it is appropriate to give up their personal information in exchange for "free" services, without also teaching them how to protect their privacy online.**[2]

When students log into Google,[3] whether through the Chromebook or through GAFE directly, students are sharing personally identifiable information with the company. They use their full first and last name to identify themselves as account holders; their first name initial and full last name are part of their Gmail username (along with their year of graduation and the last three digits of their student ID number); and their birthdate is their password.[4]

Notwithstanding the Student Privacy Pledge,[5] once students log in, Google tracks virtually everything they do online.[6] Google then uses this behavioral data for a variety of purposes, including for the serving of targeted advertisements.[7]

---

[2] Researchers at Fordham Law School conducted a study looking at the cloud service contracts of school districts. Regarding free services, the researchers wrote, "[T]he personal information of students is likely being commercialized in some way to support the provision of the service to the district." Joel Reidenberg et al., "Privacy and Cloud Computing in Public Schools," Fordham Law School, p. 56 (Dec. 13, 2013), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip. *See also* Farai Chideya, "No Child Left Un-Mined? Student Privacy at Risk in the Age of Big Data," *The Intercept* (June 27, 2015), https://firstlook.org/theintercept/2015/06/27/child-left-un-mined/.

[3] The Google Chrome OS Terms (http://www.google.com/chromebook/termsofservice.html) are the terms of service for the Chromebook operating system. Section 8 *Privacy and your personal information* references the general Google Privacy Policy (https://www.google.com/policies/privacy/) and the Chrome Privacy Notice (https://www.google.com/intl/en/chrome/browser/privacy/), which relates to the Chrome OS and the Chrome browser.

[4] "Student Computer Access Login Directions," http://www.rcsdk8.org/pdf/Computer%20Access%20Login%20Directions14_15.pdf.

[5] Google signed onto the Student Privacy Pledge created by the Future of Privacy Forum and the Software and Information Industry Association, http://studentprivacypledge.org/?page_id=45. The pledge became operational January 1, 2015 and likely does not apply to the district's GAFE contract, which is dated July 2013: the pledge is meant to apply to "new contracts and policies going forward," and only to "existing contracts as updated over time."

[6] The Chrome Privacy Notice states under *Information Google receives when you use Chrome* that Chrome can track a user's location; additionally: "Google will store certain information, such as history, bookmarked URLs as well as an image and a sample of text from the bookmarked page, passwords and other settings, on Google's servers in association with your Google Account. Information stored with your Account is protected by the Google Privacy Policy." The Google Privacy Policy states under *Information we collect/Information we get from your use of our services*, "We collect information about the services that you use and how you use them," where collected information can include "your usage data and preferences, Gmail messages, G+ profile, photos, videos, browsing history, map searches, docs,

In April 2014, Google said it would permanently disable the display of ads *within* GAFE and remove all ads scanning in Gmail for Apps for Education, "which means Google cannot collect or use student data in Apps for Education services for advertising purposes."[8]

However, the company conspicuously did not promise that *all* data collection would be turned off when students are logged into GAFE, or that it would not collect data for *other purposes*. Google previously confirmed that "the company 'scans and indexes' the emails of all Apps for Education users for a variety of purposes, including potential advertising" but "would not say whether those email scans are used to help build profiles of students or other Apps for Education users."[9]

Additionally, it is likely that the company collects data on students when they are logged into Google but navigate outside of GAFE.[10] In so doing, the company can serve ads to students on non-GAFE Google services such as YouTube or on third-party websites that use Google's ad services.[11]

II. California Law

A. SOPIPA Contains Significant Loopholes

We understand that you decided against providing -- with a non-Google option beyond fourth grade primarily because the Student Online Personal Information Protection Act (SOPIPA) will be operative January 1, 2016.[12] But SOPIPA does not absolve the district of its responsibility to help protect students' online privacy.

SOPIPA defines "covered information" as information "created or provided by a student, or the student's parent or legal guardian," "is created or provided" by the school or district, or is

---

or other Google-hosted content," as well as "any content as it flows through our systems" (https://www.google.com/policies/privacy/example/collect-information.html).

[7] Google Privacy Policy *How we use information we collect*.

[8] Bram Bout, "Protecting Students with Google Apps for Education," Official Google for Work Blog (April 30, 2014), http://googleforwork.blogspot.com/2014/04/protecting-students-with-google-apps.html.

[9] Benjamin Herold, "Google under fire for data-mining student email messages," Education Week (March 14, 2014), http://thenotebook.org/blog/147017/google-under-fire-data-mining-student-email-messages.

[10] One log-in credential (i.e., username and password) applies to all Google products. Thus the Google Privacy Policy under *How we use information we collect* states, "We may combine personal information from one service with information, including personal information, from other Google services." However, the company promises not to add information about user interactions with non-Google websites obtained through its ad network: "We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent." *See also How DoubleClick Ad Exchange works with AdWords*, https://support.google.com/adwords/answer/2472739?hl=en.

[11] *Types of cookies used by Google*, https://www.google.com/policies/technologies/types/.

[12] Student Online Personal Information Protection Act (S.B. 1177) (2013-2014), to be codified at Business & Professions Code § 22584, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1177.

gathered by the service provider "and is descriptive of a student or otherwise identifies a student."[13] Thus, SOPIPA covers not only traditional personally identifiable information such as name, birthdate and student ID number, but also online behavioral data such as "search activity."

SOPIPA includes important privacy protections for K-12 students, but it also includes a significant loophole. Among other things, the law prohibits an educational service provider from engaging in targeted advertising on its own website or any other website "when the targeting of the advertising is based upon any information, including covered information and persistent unique identifiers, that the operator has acquired" from a student's use of the website.[14] A service provider also may not "use information, including persistent unique identifiers, created or gathered by the operator's site, service, or application, to amass a profile about a K–12 student except in furtherance of K–12 school purposes."[15]

However, SOPIPA expressly "does not apply to general audience Internet Web sites, general audience online services, general audience online applications, or general audience mobile applications, *even if login credentials created for an operator's site, service, or application may be used to access those general audience sites, services, or applications*."[16]

Thus, SOPIPA will prohibit Google from serving targeted ads within GAFE (which it has already said it has stopped doing) and from serving targeted ads through its ad network on third-party websites *based on* student behavioral data obtained from the use of GAFE.[17] But when students are logged into Google and navigate outside of GAFE, SOPIPA will likely permit the company to collect student behavioral data for a variety of purposes, including serving ads.

Additionally, SOPIPA may allow Google to collect a broad array of browser data when students are logged into the Chromebook (i.e., Chrome OS/Chrome browser). The law defines "operator" as an operator of "an Internet Web site, online service, online application, or mobile application." It is not clear if a device or browser fits into these categories.[18]

Thus, SOPIPA has ensured that Google may continue to amass loyal users who are accustomed to logging into Google, losing their privacy and being commoditized outside of the educational environment.

---

[13] Section (i).
[14] Section (b)(1).
[15] Section (b)(2).
[16] Section (m) (emphasis added).
[17] Similarly, the Student Privacy Pledge says that companies will "not use or disclose student information *collected through* an educational/school service (whether personal information or otherwise) for behavioral targeting of advertisements to students" (emphasis added).
[18] Section (a).

B. California Constitution Guarantees a Right to Privacy and an Education

The California Constitution guarantees both the right to privacy and the right to an education:

> "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."[19]

> "A general diffusion of knowledge and intelligence being essential to the preservation of the rights and liberties of the people, the Legislature shall encourage by all suitable means the promotion of intellectual, scientific, moral, and agricultural improvement."[20]

The California Supreme Court held, "California has assumed specific responsibility for a statewide public education system open on equal terms to all."[21] Schools and districts, therefore, should accommodate students who have a right to benefit from technology in the classroom without giving up their privacy.

III. FERPA Requires Written Parental Consent

The federal Family Educational Rights and Privacy Act (FERPA) protects students' "education records" including personally identifiable information.[22] The information students use to log into Google – name, student number, and birthdate – all qualify for protection under FERPA.[23] The law also protects information about students' online activity when that information is tied to personally identifiable information: as the U.S. Department of Education wrote, FERPA protects behavioral "metadata" unless it has been "stripped of all direct and indirect identifiers."[24]

FERPA generally prohibits educational institutions that receive federal funds from sharing protected student information with third parties without written parental consent.[25]

---

[19] Cal. Const. art. I, § 1 *Inalienable rights*.
[20] Cal. Const. art. IX, § 1 *Encouragement of education*.
[21] *Butt v. California*, 4 Cal. 4th 668, 680 (1992).
[22] "Education records" are defined as "those records, files, documents, and other materials which contain information directly related to a student and are maintained by an educational agency or institution or by a person acting for such agency or institution." 20 U.S.C. § 1232g(a)(4)(A).
[23] 34 C.F.R. § 99.3.
[24] U.S. Dept. of Education, Privacy Technical Assistance Center, "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices" (Feb. 2014) pp. 2-3, http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf ["DOE Whitepaper"]. *See also* U.S. Dept. of Education, Family Policy Compliance Office, "FERPA General Guidance for Parents," http://familypolicy.ed.gov/content/ferpa-general-guidance-parents.
[25] 20 U.S.C. § 1232g(b)(1).

We understand that you believe the district need not obtain written parental consent before students use Chromebooks/GAFE because the GAFE contract cites FERPA's "school official" exception.[26] We disagree.[27]

A. The "School Official" Exception Is Inapplicable

FERPA sets forth three specific criteria for the "school official" exception to be valid.[28] The district has not met them.

First, the district may only share protected student information with "school officials . . . who have been determined by such agency or institution to have legitimate educational interests."[29] Specifically, a contractor like Google must meet criteria set forth in the district's annual notification of FERPA rights.[30]

The Roseville City School District's Annual Parent Notice for 2014-2015 states, "Access to a pupil's records will only be granted to those with a legitimate educational interest."[31] However, the document does not list any criteria for what counts as a "school official with a legitimate educational interest" in protected student information, nor does it notify parents that Google might qualify.

The district website has posted a one-page letter from Marco Baeza, former Director of Technology, that notifies parents of the district's intention to use Google Apps for Education, but the document does not mention the adoption of Chromebooks.[32] Additionally, while the letter states that federal laws govern technology use, the document does not explicitly invoke the "school official" exception for Google. Finally, the document claims that the district "does not disseminate student's educational records to third parties." As explained above, this claim is inaccurate.

---

[26] Google Apps for Education Agreement, Section 7.4 (Effective Date 2013-07-13).
[27] An important related question is: Are there contract terms that specify that Google will be considered a "school official" when protected student information is shared with the company when students log into Google via a Chromebook (i.e., Chrome OS or Chrome browser)?
[28] We do not take issue with the fourth requirement of the "school official" exception: the contractor "Performs an institutional service or function for which the agency or institution would otherwise use employees." 34 C.F.R. § 99.31(a)(1)(i)(B)(1); DOE Whitepaper p. 4.
[29] 20 U.S.C. § 1232g(b)(1)(A). *See also* 34 C.F.R. § 99.31(a)(1)(i).
[30] DOE Whitepaper p. 4.
[31] Roseville City School District Annual Parent Notice 2014-2015, *Pupil Records/Notification of Privacy Rights of Pupils*, http://www.rcsdk8.org/ourpages/auto/2012/8/17/42846092/Annual%20Parent%20Notice%2014-15.pdf.
[32] Roseville City School District, Letter to Parents/Guardians about Google Apps for Education from Marco Baeza, Director of Technology (July 2014), http://www.rcsdk8.org/ourpages/auto/2012/8/17/42846092/Google%20Apps%20for%20Education.pdf ["Baeza letter"].

The second and third criteria of the "school official" exception can be considered together. A contractor may receive student education records without written parental consent if the company "Is under the direct control of the agency or institution with respect to the use and maintenance of education records."[33] And the contractor "cannot use FERPA-protected information for any other purpose than the purpose for which it was disclosed."[34]

The district could meet these two criteria with a contract that explicitly establishes direct control and sets strict limits on use of protected student information. Unfortunately, the GAFE contract does not do so.

The GAFE contract provides:

> Each party will: (a) protect the other party's Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to Affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential. Each party (and any Affiliates, employees and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfill its obligations under this Agreement, while using reasonable care to protect it.[35]

The GAFE contract further provides that "Customer Data is considered Customer's Confidential Information," where customer data is defined as "data, including email, provided, generated, transmitted or displayed via the Services by Customer or End Users" – that is, by the district or the students.[36] The contract also permits the district to "suspend or delete End User Accounts at any point in time."[37]

These confidentiality provisions do not amount to direct control. The GAFE contract does not explicitly limit what student data Google may collect and what Google may do with that data. Nor does the contract clarify the interaction between its terms (or lack thereof) and Google's liberal privacy policies discussed above. We also have not seen the Chromebook contract with Google (if there is one).

Additionally, the Baeza letter states that GAFE "gives the District control over applications and content, restrict [sic] access to non-approved applications or content, and allows administrators to establish policies specifying who their users can communicate with via email." However, giving the district control over how *students* use GAFE is not the same as controlling what protected student information is shared with or collected by *Google* and what Google may do with that information.

---

[33] 34 C.F.R. § 99.31(a)(1)(i)(B)(2); DOE Whitepaper p. 4.
[34] 34 C.F.R. § 99.31(a)(1)(i)(B)(3); DOE Whitepaper pp. 4-5.
[35] Section 7.1.
[36] Section 16.
[37] Section 1.5.

Because these three key criteria have not been met, FERPA's "school official" exception does not apply to Google and thus written parental consent is required before Roseville City School District students may use Chromebooks and Google Apps for Education.

The district apparently concluded this as well, at least initially. The district requested that parents acknowledge receipt and understanding of the Baeza letter for the 2014-2015 school year.[38] The Baeza letter itself provides, "If you do **not** consent to your child's participation in this program . . . please contact your child's teacher or principal as soon as possible."[39]

While Mr. -- sincerely appreciates you agreeing to provide -- with a non-Google option for the upcoming school year, we urge you to reconsider your legal conclusion that the district is not required to first obtain written parental consent.

B. The District Has Publicly Acknowledged Risks to Students' Online Privacy

Even if the "school official" exception applies to Google, the district itself has admitted that use of online services may put student privacy at risk and, accordingly, has led parents to expect that they would be able to opt out.

The Baeza letter admits the risks of using an online service: "the possibility exists that a student's personal information and educational records stored in Google Apps for Education may be accessible to someone other than the Student or the District *by virtue of the online environment*. Accordingly, parents may ask for their child's account to be removed at any time."[40]

Additionally, the district website includes an FAQ related to Google Apps for Education: "Are Google Apps for RCSDKIDS mandatory to use? No, but we encourage staff to explore their use with each other and with students."[41]

Parents have relied on the district's public assertions that they may choose not to have their children use Chromebooks/GAFE. The district should stand by that commitment.

---

[38] Parent/Guardian Receipt of Notification 2014-2015, http://www.rcsdk8.org/ourpages/auto/2012/8/17/42846092/Receipt%20of%20Notification_14-15.pdf.
[39] Emphasis in original.
[40] Emphasis added.
[41] http://www.rcsdk8.org/apps/pages/index.jsp?uREC_ID=240810&type=d&pREC_ID=556678.

IV. COPPA Requires Parental Consent

The Baeza letter correctly states that the federal Children's Online Privacy Protection Act (COPPA) applies to technology use in the district.[42] However, the letter implies that COPPA is satisfied because "[t]he District does not collect personal student information for commercial purposes." This is not correct because COPPA applies to Google and not the district. Google must obtain "verifiable parental consent" before collecting personal information from children under 13.[43]

COPPA defines "personal information" as both traditional personally identifiable information and online behavioral data. The definition includes the child's first and last name; online contact information; screen or user names that function as online contact information, persistent identifiers; and "information concerning the child . . . that the *operator collects online from the child* and combines with an identifier described above."[44]

Earlier this year the FTC issued new guidance on the applicability of COPPA to schools. The Commission made clear that if "an operator intends to use or disclose children's personal information for its own commercial purposes in addition to the provision of services to the school, it will need to obtain parental consent."[45] Specifically, a school district should ask: "Does the operator use or share the information for commercial purposes not related to the provision of the online services requested by the school? For instance, does it use the students' personal information in connection with online behavioral advertising, or building user profiles for commercial purposes not related to the provision of the online service?" If the answer to these questions is "yes," the district "cannot consent on behalf of the parent."[46]

As discussed above, when students are logged into Google and navigate outside of GAFE, it is likely that Google collects student behavioral data to, at the very least, serve them ads within non-GAFE Google services such as YouTube or on third-party websites that use Google's ad services. Thus, Google must obtain parental consent to collect and use students' personal data. Any suggestion to the contrary, from the district or Google, is misleading at best.

---

[42] 15 U.S.C. §§ 6501-6506; 16 C.F.R. Part 312 (July 1, 2013), https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.
[43] Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions," Section A.1, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.
[44] Section A.3 (emphasis added).
[45] *Id*.
[46] Section M.5.

V. The District Did Not Provide Sufficient Transparency Regarding the Google Decision

We are concerned that the district adopted Chromebooks and Google Apps for Education for student use without adequate parental notice, input, and discussion of the privacy risks.

An inquiry resulted in three documents related to a single meeting of the Roseville City School District Board of Education on May 6, 2010. The agenda for that meeting includes item 14.2, which states in its entirety:

> PRESENTATION ON THE REPLACEMENT OF THE DISTRICT'S CURRENT E-MAIL SYSTEM
> Management has been evaluating the district's current e-mail system and the need to upgrade. Replacing Exchange 2003 with Exchange 2010 is cost prohibitive. Moving to Google will be less costly and more beneficial to the district in other ways.

This agenda item did not give sufficient public notice that the district was considering adopting Chromebooks/GAFE for students. No parent keeping tabs on the board's agendas would have understood that a proposed upgrade to the district's email system actually related to a decision that would carry significant privacy risks for students.

Similarly, the minutes for agenda item 14.2 did not inform parents of the privacy implications for students: "Presentation on the Replacement of the District's Current E-Mail System – Mr. Marco Baeza, Director of Technology, provided a PowerPoint Presentation which outlined the facts, cost-saving figures, and benefits of changing from the district's current e-mail and calendar system to Google . . . ."

The PowerPoint presentation also largely discusses the need to upgrade the district's email system. Details about Google Apps for Education are not specifically mentioned until slide 13. Slide 13 contains the only privacy-related note: "no ads for faculty, staff and students." However, the presentation does not indicate that the decision to adopt GAFE for students has been or will be definitively made. Slide 16 states: "Who Is Affected? Immediately/Every employee with, or without, an email account is affected. Down the Road/Our students [and] future employees." There is no mention of adopting Chromebooks for classroom use.

Additionally, the Placer County Office of Education could not find any public meeting documents that notified parents that Roseville City School District (or other districts within Placer County) were considering adopting Chromebooks/GAFE for students. The county did share the Technology Plan for July 1, 2011-June 30, 2014, but that document nowhere mentions Chromebooks/GAFE.

We urge Roseville City School District to provide in the future adequate public notice and opportunities for public input before technology decisions are made that would affect the privacy rights of students.

VI. Solutions

A. Password Policy

We are very concerned that students' birthdates are used as their Google passwords. This is extremely bad password policy given that finding birthdates is relatively easy in the social media age. This policy teaches students to choose passwords that are both highly personal and very insecure.

The district should immediately implement a password policy that promotes the use of unique passphrases that are easy to remember but hard to guess (e.g., the tiger has red wings).[47] Older students (perhaps in middle school) can be taught more sophisticated passphrase methods, such as the "diceware" system, which creates passphrases that are memorable but not grammatically correct.[48]

Any potential increase in administrative costs will be far outweighed by the benefits. Password security is fundamental to technological literacy. By teaching students how to choose truly secure passwords, the Roseville City School District will teach its students to be smarter and safer technology users.

B. Bring-Your-Own-Device (BYOD) Policy

If you are committed to mandating the use of Google Apps for Education once -- enters fifth grade, the district should permit her (and other students) to bring her own device to class. This would enable parents to select the browser of their choice, manipulate privacy settings, and install additional privacy protective software.

You previously informed Mr. -- that a BYOD policy was infeasible "due to network expansion limitations." It is not clear what this means. If the district wants to ensure consistent use of content filters or general-purpose computer security software (e.g., antivirus or firewall software), Mr. -- would be willing to install the same or comparable software on --'s personal device. If the reference is to something else, please elaborate so we can work with you to address whatever technical concerns you have.

---

[47] *See, e.g.*, Micah Lee, "Passphrases That You Can Memorize – But That Even the NSA Can't Guess," *The Intercept*, (March 26, 2015), https://firstlook.org/theintercept/2015/03/26/passphrases-can-memorize-attackers-cant-guess/.

[48] "Diceware" is the process by which a person generates words to use in a passphrase by repeatedly generating random five-digit numbers (usually by rolling a die five times), and then picking off a long list of English words the word that corresponds to that number. *See, e.g.*, Diceware.com Dice-Indexed Passphrase Word List, http://world.std.com/~reinhold/dicewarewordlist.pdf.

C. Privacy Settings in Chrome and the Google Account

Setting aside --'s use of technology in the classroom, all students of the Roseville City School District who use Google accounts and Chromebooks should be taught to use the most privacy-protective settings.

For students' Google accounts, we recommend:

- All of the toggles on the privacy settings page (https://myaccount.google.com/privacy) should be set to the left ("paused").
- Under *Your searches and browsing activity*, make sure that "Include history from Chrome and other apps in your Web & App Activity" is unchecked.

For the Chromebook, we recommend:

- Under *Search*, uncheck "Enable 'Ok Google' to start a voice search."
- Within advanced settings (accessible by clicking *Show Advanced Settings*… near the bottom of the settings page):
    - Under *Privacy*:
        - Un-check "Use a web service to help resolve navigation errors."
        - Un-check "Use a prediction service to help complete searches and URLs typed in the address bar or the app launcher search box."
        - Un-check "Use a web service to help resolve spelling errors."
        - Un-check "Automatically send usage statistics and crash reports to Google."
        - Check "Send a 'Do Not Track' request with your browsing traffic."
    - In *Content Settings*…
        - Under *Cookies* select "Keep local data only until you quit your browser" and "Block third-party cookies and site data."
        - Under *Location* select "Do not allow any site to track your physical location."
        - Under *Protected Content* unselect "Allow identifiers for protected content (computer restart may be required)."
        - Under *Unsandboxed plug-in access* select "Do not allow any sites to use a plug-in to access your computer."

Many major websites today make use of third-party analytics and tracking services that secretly record where users go and what pages they view on the web, without users' permission. In order to reduce the effectiveness of this sort of tracking, we recommend that you teach students to use Chrome's *Incognito* mode when they are browsing non-GAFE sites. Incognito mode erases a user's cookies and browsing history whenever the window is closed. Although this does not prevent all online tracking, it does make it harder for websites to track students' web browsing across sessions. It also reduces Google's ability to link student activity on GAFE with their activity on non-GAFE websites.

Alternatively, you could install EFF's Privacy Badger add-on on all student Chromebooks.[49] Privacy Badger is a free, open-source, set-it-and-forget-it browser add-on that stops third-party trackers. If a third-party service seems to be tracking a user across multiple websites, Privacy Badger automatically blocks that service from loading any more content in Chrome.

VII. Conclusion

For the foregoing reasons, the Roseville City School District must continue to allow parents to choose whether or not their children use Chromebooks and Google Apps for Education in the classroom.

As for the students who do use Chromebooks/GAFE, the district should educate them on how to implement the most privacy-protective passwords and settings. The district would be sending a strong message in support of the technological safety and literacy of minor students.

Sincerely,
/s/
Sophia Cope
Staff Attorney
sophia@eff.org
415-436-9333 x155

cc: --
Derek Slater, Policy Manager, Google
Mark Melahn, Associate Product Counsel, Google
Jess Hemerly, Manager, Public Policy & Government Relations, Google
Sarah Holland, Senior Analyst, Public Policy & Government Relations, Google

[49] https://www.eff.org/privacybadger.