BEFORE THE UNITED STATES
FEDERAL TRADE COMMISSION

ELECTRONIC FRONTIER FOUNDATION,

Petitioner,

v.

GOOGLE, INC.

Respondent.

COMPLAINT AND REQUEST FOR INVESTIGATION, INJUNCTION, AND OTHER RELIEF

Nathan D. Cardozo
Sophia S. Cope
ELECTRONIC FRONTIER FOUNDATION
815 Eddy St.
San Francisco, CA 94109
Phone: (415) 436 9333
Fax: (415) 436 9993
nate@eff.org

I. INTRODUCTION

The Electronic Frontier Foundation (EFF) hereby petitions the Federal Trade Commission ("FTC") Pursuant to Sections 2.1 and 2.2 of regulations,[1] to investigate the privacy practices of Google for Education, a project of Google, Inc. (Google), and to commence an enforcement action against Google. EFF bases this petition on evidence that Google is engaged in collecting, maintaining, using, and sharing student personal information in violation of the "K-12 School Service Provider Pledge to Safeguard Student Privacy" (Student Privacy Pledge), of which it is a signatory.

Google is violating the Student Privacy Pledge in three ways. First, when students are logged in to their Google for Education accounts, student personal information in the form of data about their use of non-educational Google services is collected, maintained, and used by Google for its own benefit, unrelated to authorized educational or school purposes. Second, the "Chrome Sync" feature of Google's Chrome browser is turned on by default on all Google Chromebook laptops – including those sold to schools as part of Google for Education – thereby enabling Google to collect and use students' entire browsing history and other data for its own benefit, unrelated to authorized educational or school purposes. And third, Google for Education's Administrative settings, which enable a school administrator to control settings for all program Chromebooks, allow administrators to choose settings that share student personal information with Google and third-party websites in violation of the Student Privacy Pledge.

In light of the Pledge, Google's unauthorized collection, maintenance, use and sharing of student personal information beyond what is needed for education, constitutes unfair or deceptive acts or practices in violation of Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45). Accordingly, EFF respectfully requests that the FTC take prompt action including as appropriate, an investigation into Google's unfair or deceptive acts or practices and the initiation of proceedings for injunctive relief to require Google to destroy all student data so far collected, maintained, or used in violation of the Student Privacy Pledge, and to enjoin Google from further collecting and sharing such data in the future.

II. PARTIES

A. Petitioner

The Electronic Frontier Foundation (EFF) is a non-profit organization based in San Francisco, California, and works to defend civil liberties in the digital world. EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. EFF works to ensure that rights and freedoms are enhanced and protected as the use of technology grows. EFF is especially concerned when a company publically promises to adhere to certain privacy standards and fails to live up to those standards.

[1] 16 C.F.R. §§ 2.1 and 2.2.

B. Respondent

Google, Inc. is a leading technology company that owns and operates a host of different web-based, software, and hardware products, including the Google search engine, YouTube streaming video website, Chrome web browser, Chrome operating system, Android mobile operating systems, and Gmail webmail service, among others. Google's headquarters are located at 1600 Amphitheatre Parkway, Mountain View, California 94043. Google for Education is a Google project that provides inexpensive laptops (Chromebooks) to schools, which allow access to a free suite of web-based educational applications for students and classroom-management tools for teachers, known as Google Apps for Education.

III. STATEMENT OF FACTS

The K-12 School Service Provider Pledge to Safeguard Student Privacy, or the Student Privacy Pledge, was developed by the Future of Privacy Forum (FPF) and the Software & Information Industry Association (SIIA) in the fall of 2014 and became effective January 1, 2015. There are currently 200 signatories to the Student Privacy Pledge, including Google.[2]

A. Content of Student Privacy Pledge

The Student Privacy Pledge holds school service providers like Google to a number of obligations. Most relevant to this complaint, signatories commit to:[3]

- "Not collect, maintain, use or share student personal information beyond that needed for authorized educational/school purposes, or as authorized by the parent/student."

- "Not build a personal profile of a student other than for supporting authorized educational/school purposes or as authorized by the parent/student."

- "Not knowingly retain student personal information beyond the time period required to support the authorized educational/school purposes, or as authorized by the parent/student."

B. The Student Privacy Pledge is Legally Enforceable under the Federal Trade Commission Act

Under Section 5 of the FTCA, the Federal Trade Commission is "empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting

[2] STUDENT PRIVACY PLEDGE, SIGNATORIES, http://studentprivacypledge.org/?page_id=22 (last visited Nov. 5, 2015).
[3] STUDENT PRIVACY PLEDGE, PRIVACY PLEDGE, http://studentprivacypledge.org/?page_id=45 (last visited Nov. 4, 2015).

commerce."[4] In the past, the FTC has brought enforcement actions against companies that made privacy-related promises to their costumers and then violated those promises (see below, under Section V: Grounds for Relief for example enforcement actions).

The FTC has a dedicated page on its website to enforcing privacy promises that companies make to consumers. In the FTC's own words, "When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises."[5]

FTC enforceability is a central component of the Student Privacy Pledge. The Future of Privacy Forum and the Software & Information Industry Association have a website dedicated to the pledge,[6] which prominently displays three large blue buttons on the main landing page: "Read the Pledge," "See Who's Signed," and "The Pledge and Security." Clicking on "The Pledge and Security" navigates to a separate page that contains a statement by FPF and SIIA:

> A company's security and other commitments made under the Student Privacy Pledge are legally enforceable. Under Section 5 of the Consumer Protection Act, the Federal Trade Commission (FTC) can take action against companies that commit deceptive trade practices. It is a form of deception to make a public statement such as signing the Student Privacy Pledge but then implementing practices that do not conform to those public statements.[7]

Industry periodicals and prominent blogs - such as that of the Wall Street Journal[8] - have similarly represented that the Pledge is enforceable by the FTC.[9]

The Student Privacy Pledge is a promise from the signatories of the pledge to their users to commit to certain privacy standards. Google's violation of the pledge while continuing to promote itself as a signatory is an unfair or deceptive act or practice under the FTCA, and is thus subject to enforcement by the FTC.

---

[4] 15 U.S.C. § 45(a)(2).

[5] *Enforcing Privacy Promises*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last visited Nov. 6, 2015).

[6] STUDENT PRIVACY PLEDGE, http://www.studentprivacypledge.org/ (last visited Nov. 5, 2015).

[7] STUDENT PRIVACY PLEDGE, THE STUDENT PRIVACY PLEDGE AND SECURITY, http://studentprivacypledge.org/?page_id=721 (last visited Nov. 4, 2015).

[8] Alistair Barr, *Why Google Didn't Sign Obama-Backed Student Privacy Pledge*, WALL STREET JOURNAL: DIGITS BLOG (Jan. 13, 2015), http://blogs.wsj.com/digits/2015/01/13/why-google-didnt-sign-obama-backed-student-privacy-pledge/ (last visited Nov. 6, 2015) ("Google has previously been tripped up by signing industry pledges, which are legally binding in the U.S.").

[9] Grant Waterfall, *New Focus on Student Data Privacy – How to Navigate it All*, CORPORATE COMPLIANCE INSIGHTS (Aug. 14, 2015), http://corporatecomplianceinsights.com/new-focus-on-student-data-privacy-how-to-navigate-it-all/ (last visited Nov. 5, 2015) ("While compliance with the Pledge is currently voluntary, it is enforceable by the FTC under Section 5 of the Consumer Protection Act and over 150 companies have signed on to honor the Pledge to date.").

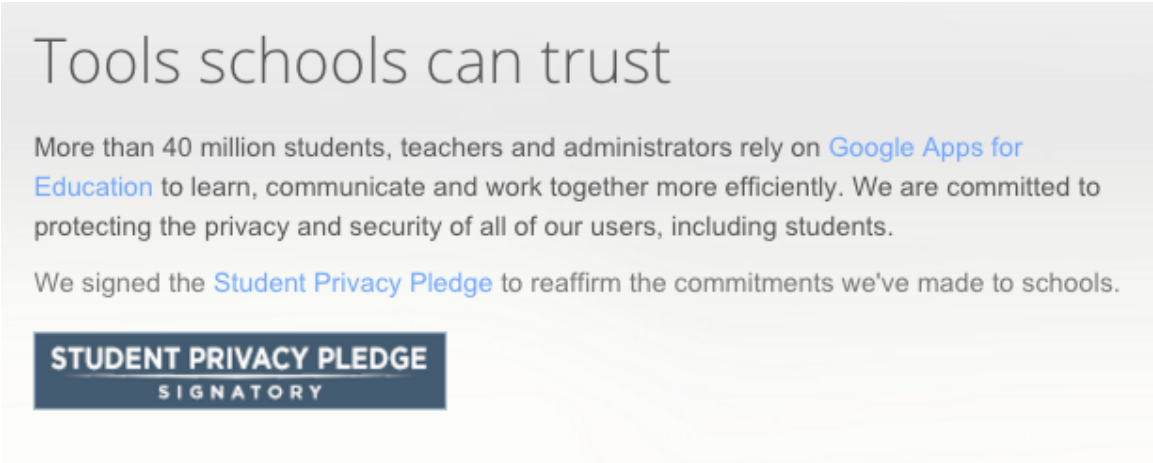
C. Google Promotes its Status as a Signatory to the Student Privacy Pledge on its Website and in the Media, and Has Received Positive Media Coverage as a Result of Signing the Pledge

1. Google's Website

a) Statements about the Student Privacy Pledge

The Google for Education website emphasizes Google's status as a signatory to the Student Privacy Pledge.

At the bottom of the Google for Education landing page is a list of links grouped by category.[10] In the "Guides" category is a link titled "Privacy & Security," which takes the viewer to a page presenting an overview of the privacy and security practices associated with Google for Education.[11] Near the top of the Privacy and Security page is a section titled "Tools schools can trust," which states that there are over 40 million users of Google Apps for Education and displays the Student Privacy Pledge's logo, highlighting Google's decision to sign the Pledge: "We are committed to protecting the privacy and security of all of our users, including students. We signed the Student Privacy Pledge to reaffirm the commitments we've made to schools."[12]



b) General Statements about Privacy

Google has also made more generic statements in support of privacy and supported privacy-related initiatives. On its official blog, Google claims to "pursue a common goal of improving privacy protections for everyone on the Internet," and stated its belief that "it's an important part of our commitment to respect user privacy while balancing a number of important

[10] GOOGLE FOR EDUCATION, https://www.google.com/edu/ (last visited Nov. 5, 2015).
[11] GOOGLE FOR EDUCATION, PRIVACY AND SECURITY, https://www.google.com/edu/trust/ (last visited Nov. 5, 2015).
[12] *Id.*

factors."[13] Google has also supported privacy awareness events such as "Data Privacy Day: Increasing Privacy Awareness and Trust," as part of what Google describes as an "ongoing constructive dialogue" with various stakeholders "to discuss how to protect user information."[14]

On its Google for Education blog, the company highlights the decision of colleges and universities to adopt its products in part because "Students can trust that they'll have a safe learning experience."[15]

2. In the Press

Unlike Microsoft and numerous other developers of digital curriculum and classroom management software, Google did not initially sign onto the Student Privacy Pledge with the first round of signatories when it was announced in the fall of 2014.[16] When questioned about its decision by the press, Google either declined to comment or simply stated that the company's policies and contracts already demonstrated a commitment to student privacy.[17] Facing sustained criticism of that decision, Google reversed course and reluctantly signed the pledge a few weeks after it went into effect in January 2015.[18]

Google has publicly promoted its decision to become a signatory to the Pledge to the press and received positive coverage for the decision. Following the decision, the company stated to the press, "[p]rotecting the privacy and security of all of our users, including students, is a top priority . . . [w]e're pleased to see the ed-tech industry come together to support this important issue and we've signed the pledge to reaffirm the commitments we've made directly to our customers."[19]

---

[13] Peter Fleischer, Global Privacy Counsel, *Why does Google remember information about searches?*, GOOGLE (May 11, 2007), https://googleblog.blogspot.com/2007/05/why-does-google-remember-information.html (last visited Nov. 6 2015).

[14] *Raising data privacy awareness*, OFFICIAL GOOGLE BLOG (Jan. 28, 2009), https://googleblog.blogspot.com/2009/01/raising-data-privacy-awareness.html (last visited Nov. 6, 2015).

[15] Michael de la Cruz, Google for Education team, *Colleges and universities find new ways to work and learn with Google for Education*, GOOGLE FOR EDUCATION BLOG (Oct. 22, 2015), http://googleforeducation.blogspot.com/2015/10/colleges-and-universities-find-new-ways-to-work-and-learn-with-Google-for-Education.html (last visited Nov. 6, 2015).

[16] Natasha Singer, *Microsoft and Other Firms Pledge to Protect Student Data*, THE NEW YORK TIMES (Oct. 7, 2015), http://www.nytimes.com/2014/10/07/business/microsoft-and-other-firms-pledge-to-protect-student-data.html?_r=0 (last visited Nov. 6, 2015).

[17] Barr, *Why Google Didn't Sign Obama-Backed Student Privacy Pledge*, WALL STREET JOURNAL: DIGITS BLOG (Jan. 13, 2015); Singer, *Microsoft and Other Firms Pledge to Protect Student Data*, THE NEW YORK TIMES (Oct. 7, 2015).

[18] The Student Privacy Pledge applies only prospectively, to new contracts that are signed (or existing contracts that are updated) after January 2015 ("This pledge is intended to be applicable to new contracts and policies going forward and addressed — where inconsistent and as agreed to by the educational institution or agency — in existing contracts as updated over time. This pledge shall be effective as of January 1, 2015." Notes, STUDENT PRIVACY PLEDGE).

[19] Sean Cavanagh, *After Initially Holding Out, Google Signs Student-Data-Privacy Pledge*, EDUCATION WEEK (Jan. 20, 2015),

Google's decision to sign the Pledge received coverage from the blogs of both the Washington Post[20] and the Wall Street Journal.[21] The decision also received coverage from smaller industry-related forums such as Education Week,[22] Connect Safely,[23] and 9TO5Google.[24]

IV. CLAIMS

A. Google Collects and Uses Student Personal Information Without Authorization When Students Are Logged In to Their Google Accounts

Google collects, maintains, and uses records of essentially everything that student users of Google for Education do on Google services, while they are logged in to their Google accounts, regardless of which device or browser they use, in violation of the Student Privacy Pledge.[25]

This includes recording students' browsing behavior on every single Google-operated site students visit regardless of its relation to schoolwork (that is, Google applications both in and out of the Google Apps for Education suite), records of what students have searched for on the Internet and the results they click on, the videos they search for and watch on YouTube, the browser extensions they have installed, and their saved passwords. Such data reveals highly personal information about students and is not necessary to deliver educational services.

Google not only collects and stores the vast array of student data described above, but uses it for its own purposes such as improving Google products and serving targeted advertising (within non-Education Google services), as Google has represented to EFF. The Student Privacy

---

http://blogs.edweek.org/edweek/DigitalEducation/2015/01/after_initially_holding_out_go.html (last visited Nov. 6, 2015).

[20] Hayley Tsukayama, *Google, Khan Academy join in student privacy pledge*, WASHINGTON POST, https://www.washingtonpost.com/news/the-switch/wp/2015/01/20/google-khan-academy-join-in-student-privacy-pledge/ (last visited Nov. 5, 2015).

[21] Alistair Barr, *Google Changes Course, Signs Student Data Privacy Pledge*, WALL STREET JOURNAL: DIGITS BLOG (Jan. 20, 2015), http://blogs.wsj.com/digits/2015/01/20/google-changes-course-signs-student-data-privacy-pledge/ (last visited Nov. 5, 2015).

[22] Sean Cavanagh, *After Initially Holding Out, Google Signs Student-Data-Privacy Pledge*, EDUCATION WEEK (Jan. 20, 2015), http://blogs.edweek.org/edweek/DigitalEducation/2015/01/after_initially_holding_out_go.html (last visited Nov. 6, 2015).

[23] Larry Magid, *Chromebooks & Google Apps appeal to schools & consumers*, CONNECTSAFELY (Apr. 3, 2015), http://www.connectsafely.org/chromebooks-google-apps-qppeal-to-schools-consumers/ (last visited Nov. 6, 2015).

[24] Ben Lovejoy, *Google changes its mind and signs student privacy pledge, says reaffirms existing promises*, 9TO5GOOGLE (Jan. 21, 2015), http://9to5google.com/2015/01/21/google-student-privacy-pledge/ (last visited Nov. 5, 2015).

[25] Unlike Claim B that is tied to students' use of the Google Chrome web browser, Claim A is applicable regardless of which web browser a student uses, so long as the student is logged in to his or her Google for Education account.

Pledge defines "student personal information" as "personally identifiable information as well as other information when it is both collected and maintained on an individual level and is linked to personally identifiable information."[26] Students' browsing data is undoubtedly personally identifiable data that is collected and maintained on an individual level, as described above.

Even when Google aggregates and anonymizes the student personal information it collects, as the company does for Google for Education core services (but not currently for data collected within non-Education Google services), Google still uses the data for its own benefit, unrelated to authorized educational or school purposes. Such use by Google is in direct contravention of the Student Privacy Pledge.[27] Not only is aggregating and anonymizing data difficult to the point of often being impossible,[28] even if the process were perfect, Google's use of students' browsing history for its own benefit and without authorization from the student or parent, runs contrary to the letter and spirit of the Student Privacy Pledge. Aggregating and anonymizing students' browsing history does not change the intensely private nature of the data – nor the fact that at the time of collection, it was tied to identifiable student accounts – such that Google should be free to use it, despite having promised not to do so without authorization from the student or parent.

B. Google Collects Student Personal Information Without Authorization by Having Chrome Sync On by Default for Chromebooks

Through the Chrome Sync feature of the Google Chrome web browser, Google is collecting, maintaining, and using student personal information in violation of the Student Privacy Pledge.

Students generally use Chromebook laptops by first logging in to their Google accounts. Chrome Sync is a feature of the Chrome web browser—and included on Chromebooks—that allows users to store information about the browser and their online sessions in the "cloud," enabling a more seamless browsing experience when switching between different devices (such as Chromebooks) that also have Chrome Sync enabled. When Chrome Sync is enabled, Google collects and stores on its servers (the "cloud") users' *entire* browsing history (not just while users are browsing within Google-owned or operated sites as described in Section A, above), bookmarks, installed extensions, and passwords, among other things.

While Chrome Sync is disabled by default on the Google Chrome stand-alone web browser that users of Apple, Windows, or Linux install on their personal computers, this is not the case for Chromebook devices. EFF has learned through conversations with Google that the "Chrome Sync" feature is *enabled* by default on all Chromebook devices, including those that are sold and distributed to schools as part of the Google for Education program. And while

[26] STUDENT PRIVACY PLEDGE.

[27] Google also stores student email content, Google Docs, and other Google-hosted content on its servers, however, unlike the information collected above, these services are necessary for Google for Education's educational purposes and are not in violation of the Student Privacy Pledge.

[28] Natasha Singer, *With a Few Bits of Data, Researchers Identify 'Anonymous' People*, THE NEW YORK TIMES: BITS BLOG (January 29, 2015), http://bits.blogs.nytimes.com/2015/01/29/with-a-few-bits-of-data-researchers-identify-anonymous-people/.

parents or students are free to turn Chrome Sync off on an individual device, it takes technical sophistication to do so.

For a non-educational user of Chrome Sync, the information collected about browsing history and bookmarks, along with information collected through Gmail and other Google applications, is used to create an individualized user profile for targeted advertising. Google asserts that it does not collect information from student users of Google for Education for advertising purposes.

However, in correspondence between EFF and Google, Google has acknowledged that it collects, maintains, and uses student information via Chrome Sync (in aggregated and anonymized form) for the purpose of improving Google products, similar to how Google uses browsing data collected within its own services as described in Section A. Google has represented to EFF that such collection is necessary for the educational purpose of Google for Education so that it may provide the student with a seamless experience, regardless of which device the student is using. But because students use their computers and access the Internet for non-academic reasons, Google invariably collects, maintains, and uses for its own benefit information "beyond that needed for authorized educational/school purposes, or as authorized by the parent/student" in direct violation of the first commitment of the Student Privacy Pledge.[29] And as described in Section A, aggregating and anonymizing the data does not somehow bring it outside of the Student Privacy Pledge's commitments.

C. Google Enables the Collection and Sharing of Student Personal Information Through Administrative Settings

1. Google Collects Student Personal Information Through Changeable Administrative Settings In Chrome and Google Apps for Education Accounts

Google offers cloud-based management systems for both the Chrome for Education[30] browser and Google Apps for Education[31] that allow school administrators to customize settings for all students and teachers in a simple, centralized way.

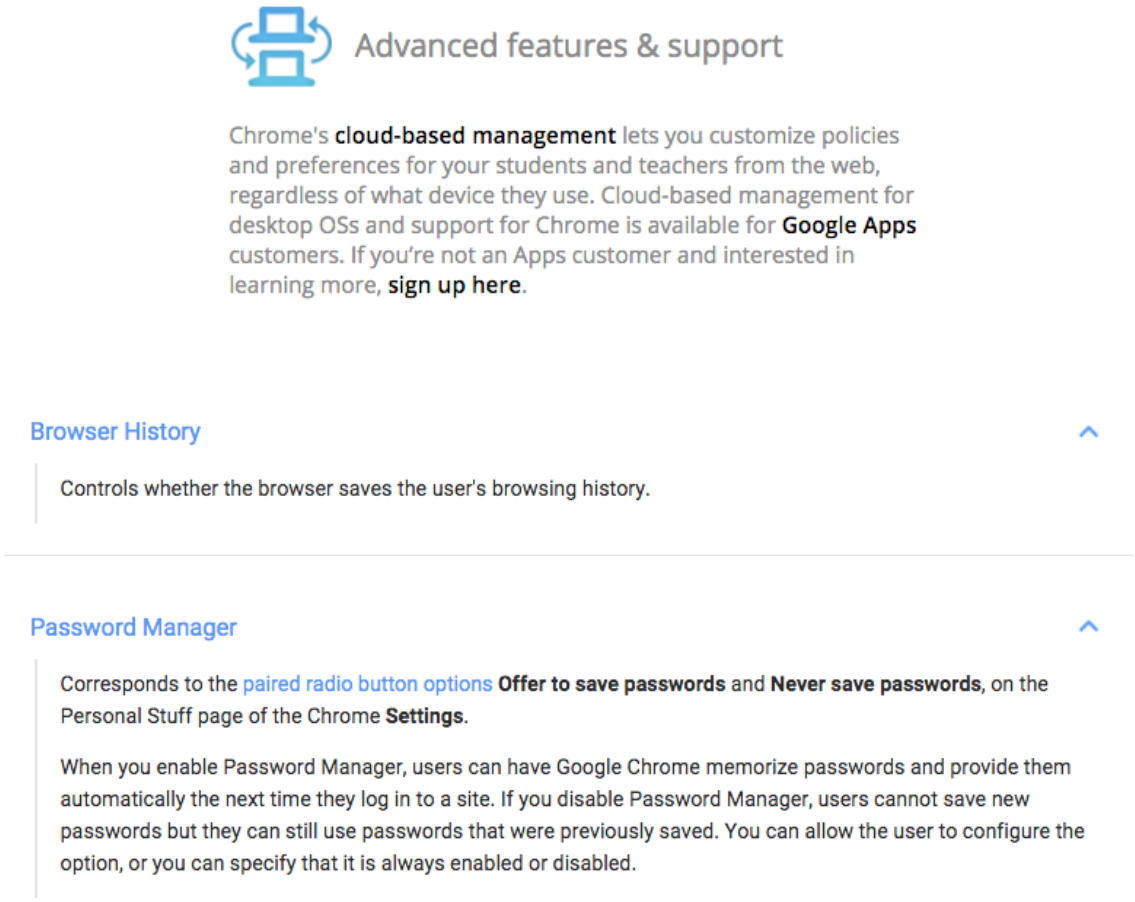
It is especially concerning that Chrome Sync is turned on by default on Google for Education Chromebook devices. However, reversing this default setting potentially would not bring Google within the bounds of the Student Privacy Pledge. This is because school administrators can individually control a whole host of settings for their student users, including

[29] STUDENT PRIVACY PLEDGE.

[30] A MODERN BROWSER FOR SCHOOLS: DEPLOY AND MANAGE CHROME FOR EDUCATION FOR YOUR SCHOOL OR DISTRICT, https://www.google.com/intl/en/chrome/education/browser/admin/ (last visited Nov. 5 2015).

[31] Google Apps for Education Administrator Help, Admin Console Feature Map, https://support.google.com/a/answer/3035631?hl=en&ref_topic=3113051 (last visited Dec. 1, 2015).

whether Chrome Sync is enabled (*i.e.*, Google will collect and store browser history and passwords on Google's servers, see images below[32]):



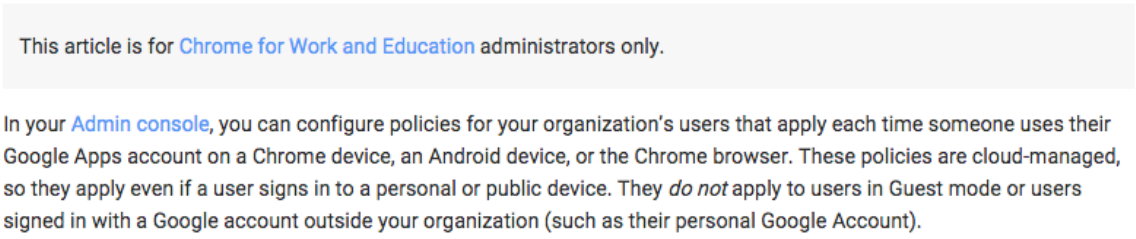
Should school administrators turn Chrome Sync on (assuming the default was *off*), Google could then recommence collecting student personal information, including the websites the student has visited, passwords the student uses, and webpages the student has bookmarked. In other words, Google's design choice permits school administrators to enable impermissible collection of student data, *even if some parents make an informed choice to turn it off*, thereby placing Chrome for Education outside the bounds of the Student Privacy Pledge.

The Chrome for Education administrative settings can also be configured to allow third-party websites to track student users' physical location. This is discussed separately below in section 2 because it constitutes sharing rather than collecting student personal information - a distinct violation of the Student Privacy Pledge.

The Chrome for Work and Education Help website explains that the above-mentioned features are "cloud-managed," meaning that the administrator-controlled collecting and sharing of student personal student information will apply on any device a user logs in to with her

[32] CHROME FOR WORK AND EDUCATION HELP, MANAGE USERS, SET CHROME POLICIES FOR USERS, https://support.google.com/chrome/a/answer/2657289?hl=en (last visited Nov. 4, 2015).

student account: the administrator-chosen policies "*apply even if a user signs in to a personal or public device*" (emphasis added):[33]



This article is for Chrome for Work and Education administrators only.

In your Admin console, you can configure policies for your organization's users that apply each time someone uses their Google Apps account on a Chrome device, an Android device, or the Chrome browser. These policies are cloud-managed, so they apply even if a user signs in to a personal or public device. They *do not* apply to users in Guest mode or users signed in with a Google account outside your organization (such as their personal Google Account).

This means that if a student left her Google for Education Chromebook at school but signed in to her student account on her parents' home computer (using the Chrome browser) to complete a homework assignment, her web browsing history and passwords could be collected by Google and her location could be shared with websites she visits.

Additionally, in Google Apps for Education, school administrators can control which Google services students can access, including those services outside the core Google Apps for Education suite.[34] Thus, should students navigate to any of these additional Google sites, Google can collect student personal data and use it for the company's own purposes, including serving targeted advertisements to students within these non-Education Google apps, in violation of the Student Privacy Pledge as discussed above in Claim A.[35]

2. Google Shares Student Personal Information Through Changeable Administrative Settings in Chrome

Aside from collecting, maintaining, and using student personal information, the administrative settings Chrome for Education allow school administrators to permit student personal information to be *shared* with third-party websites, in further violation of the Student Privacy Pledge.

In the same settings page where administrators can choose whether Google can collect a user's passwords or browsing history, school administrators can also choose whether "websites are allowed to track the user's [here, students'] physical location."[36]

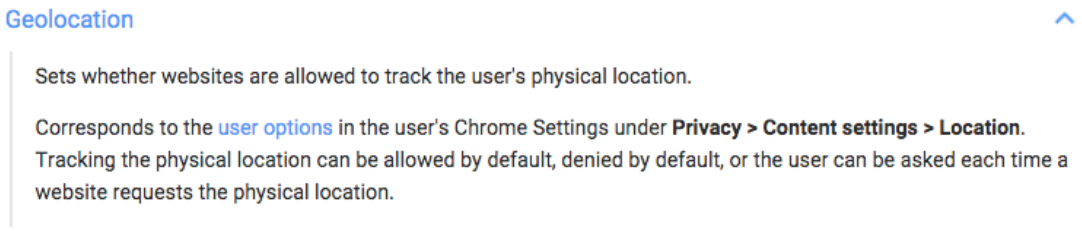
---

[33] CHROME FOR WORK AND EDUCATION HELP, MANAGE USERS, SET CHROME POLICIES FOR USERS.

[34] Google Apps for Administrator Help, Control who can access Google services, https://support.google.com/a/answer/182442 (last visited Dec. 1, 2015).

[35] In addition to being able to turn "services on/off", school administrators can also control "service-specific settings." Google Apps for Education Administrator Help, Admin Console Feature Map, https://support.google.com/a/answer/3035631?hl=en&ref_topic=3113051 (last visited Dec. 1, 2015).

[36] CHROME FOR WORK AND EDUCATION HELP, MANAGE USERS, SET CHROME POLICIES FOR USERS.



Sharing a student's physical location with third parties is unquestionably sharing personal information beyond what is needed for educational purposes. This is especially so as people increasingly use mobile devices to access the Internet because a greater amount of location information is produced by the typical Internet user of today than yesterday, due to mobile technology.[37]

V. GROUNDS FOR RELIEF

A. Google's Violation of the Student Privacy Pledge is an Unfair or Deceptive Act or Practice Under § 5 of the FTCA

Section 5 of the Federal Trade Commission Act provides that "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[38] When the Commission has reason to believe that any person has used or is using unfair or deceptive practices in or affecting commerce, it shall issue a complaint against such person in an administrative proceeding, if it believes such a proceeding to be in the public interest.[39]

In light of its signature to the Student Privacy Pledge, Google's collection, maintenance, and use of student browsing habits and other information constitutes an "unfair or deceptive act or practice." Furthermore, the ability of Google for Education administrators to enable the sharing of student users' locations constitutes an additional violation of the Student Privacy Pledge and thus a distinct unfair or deceptive act.

1. Unfairness

For the reasons stated above, Google's actions constitute an unfair practice under the FTCA. A practice will be deemed unfair and illegal under the FTCA if it (1) causes or is likely to cause substantial injury to consumers; (2) cannot be reasonably avoided by consumers; and (3) is not outweighed by any countervailing benefits to consumers or competition that the practice produces.[40]

---

[37] *Report: 60 Percent Of Internet Access Is Mostly Mobile*, Marketing Land (Feb. 19, 2014), http://marketingland.com/outside-us-60-percent-Internet-access-mostly-mobile-74498 (last visited Nov. 9, 2015).
[38] Federal Trade Commission Act § 5, 15 U.S.C. § 45(a)(1) (2006).
[39] *Id.* § 45(b).
[40] 15 U.S.C. § 45(n) (2006); FTC Policy Statement on Unfairness (1983), *appended to International Harvester Co.*, 104 F.T.C. 949, 1070 (1984), *available at* https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

Google has substantially injured students and their parents by promising not to collect, maintain, use, or share student personal information that is not necessary for educational purposes, and then in fact collecting student browsing history, passwords, and additional information, using the information it collects for its own purposes, and sharing geolocation information about students, all unrelated to any educational purpose.

Google's violations of the Student Privacy Pledge cannot be reasonably avoided by students and their parents. Google collects student personal information when students are logged in to their Google for Education accounts. And even if Chrome Sync can be turned off at the device (Chromebook) level, it and other settings are controllable by school administrators, enabling Google's collection and sharing of personal student information.

Lastly, Google's collection and sharing of personal student information in violation of the Student Privacy Pledge does not enable Google to provide a benefit to users that outweighs the unfair act. Google already does not create advertising profiles to monetize personal student information like it does for its standard free Gmail services, so stopping future collection would not necessitate a significant price increase for schools that currently partner with Google for Education or those that want to in the future.

2. Deceptive Practices

Google has also committed deceptive acts or practices by publically signing onto the Student Privacy Pledge, promoting its signatory status on its website, and then not adhering to the commitments outlined in the Pledge.

The *FTC Policy Statement on Deception* provides that the Commission will find deception if there is a representation, omission, or practice that is likely to mislead the consumer acting reasonably under the circumstances, to the consumer's detriment.[41] Google's representation that it complies with the commitments stipulated in the Student Privacy Pledge is a representation likely to mislead a reasonably acting consumer.

B. The Federal Trade Commission Has Acted Against Similar Violations in the Recent Past

The FTC on numerous occasions in recent years has sanctioned companies for violating promises or representations made to consumers related to protecting their privacy (including sanctioning Google in 2011 and collecting a record settlement):

- Google agreed to pay a $22.5 million civil penalty to settle Federal Trade Commission charges that it misrepresented to users of Apple Inc.'s Safari Internet browser that it would not place tracking "cookies" or serve targeted ads to those users, violating an earlier privacy settlement between the company and the FTC.[42]

---

[41] FTC Policy Statement on Unfairness (1983), *appended to International Harvester Co.*, 104 F.T.C. 949, 1070 (1984), *available at* https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

[42] *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, FEDERAL TRADE COMMISSION (Nov. 29, 2011),

- The Federal Trade Commission sent a letter to a court overseeing bankruptcy proceedings of education technology company ConnectEdu, raising concerns about the proposed sale of the company's assets, which include student information; in its privacy policy ConnectEdu promised consumers that prior to any sale of the company, they would be notified and have the ability to delete their personally identifiable data, however these notice provisions do not apply in a sale of the company resulting from bankruptcy proceedings.[43]

- Facebook settled Federal Trade Commission charges that it deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public.[44]

- Thirteen companies have agreed to settle Federal Trade Commission charges that they misled consumers by claiming they were certified members of the U.S.-EU or U.S.-Swiss Safe Harbor Frameworks when their certifications had lapsed or the companies had never applied for membership in the program at all.[45]

- A company that markets video cameras designed to allow consumers to monitor their homes remotely and that claimed in numerous product descriptions that they were "secure" settled Federal Trade Commission charges that its lax security practices exposed the private lives of hundreds of consumers to public viewing on the Internet.[46]

- The Federal Trade Commission approved a final order resolving the Commission's complaint against Nomi Technologies for misleading consumers about the available choices to opt-out of the company's mobile device tracking program. Nomi misled consumers with promises that it would provide an in-store mechanism for consumers to opt out of tracking and that consumers would be informed when locations were using

---

https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented (last visited Nov. 6, 2015).

[43] *FTC Seeks Protection for Students' Personal Information in Education Technology Company ConnectEdu's Bankruptcy Proceeding*, FEDERAL TRADE COMMISSION (May 23, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/ftc-seeks-protection-students-personal-information-education (last visited Nov. 6, 2015).

[44] *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*, FEDERAL TRADE COMMISSION (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep (last visited Nov. 6, 2015).

[45] *Thirteen Companies Agree to Settle FTC Charges They Falsely Claimed To Comply With International Safe Harbor Framework*, FEDERAL TRADE COMMISSION (Aug. 17, 2015), https://www.ftc.gov/news-events/press-releases/2015/08/thirteen-companies-agree-settle-ftc-charges-they-falsely-claimed (last visited Nov. 6, 2015).

[46] *Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy*, FEDERAL TRADE COMMISSION (Sep. 4, 2013), https://www.ftc.gov/news-events/press-releases/2013/09/marketer-Internet-connected-home-security-video-cameras-settles (last visited Nov. 6, 2015).

Nomi's tracking services, yet the FTC's complain alleged these promises were false.[47]

- The Federal Trade Commission approved a final order settling charges that Snapchat deceived consumers with promises about the disappearing nature of messages sent through the service as well as the amount of personal data the app collected and the security measures taken to protect that data from misuse and unauthorized disclosure.[48]

- An Atlanta-based health billing company and its former CEO settled Federal Trade Commission charges they misled thousands of consumers who signed up for an online billing portal by failing to adequately inform them that the company would seek highly detailed medical information from pharmacies, medical labs and insurance companies.[49]

VI. Request for Injunction and Other Relief

EFF respectfully requests that the FTC investigate Google's unfair or deceptive acts or practices pursuant to its investigative powers in 15 U.S.C. §§ 46, 49, 57b-1 & 16 C.F.R. §§ 2.1 and 2.2.

EFF respectfully requests that, upon finding the unfair or deceptive acts or practices discussed above, the FTC serve upon Google a complaint stating its charges and containing notice of a hearing pursuant to 15 U.S.C. § 45.

Finally, 15 U.S.C. § 53 authorizes the FTC to seek, and the district courts to grant, preliminary and permanent injunctions against acts or practices that violate any of the laws enforced by the Commission if the Commission determines that such injunctive relief "would be to the interest of the public."[50] Based on Google's unfair or deceptive acts or practices, EFF asks the Commission to:

- Order Google to destroy ALL personal student information collected by Google, without student or parent authorization, that is not necessary for educational purposes associated with ALL Google for Education student accounts (browsing history, passwords, tabs, bookmarks, etc.);

- Order Google to, prior to destroying any personal student information not necessary for educational purposes, provide all student account holders and, as is reasonably feasible, all parents, notice of Google's previous collection and use of

[47] *FTC Approves Final Order In Nomi Technologies Case*, FEDERAL TRADE COMMISSION (Sep. 3, 2015), https://www.ftc.gov/news-events/press-releases/2015/09/ftc-approves-final-order-nomi-technologies-case (last visited Nov. 6, 2015).
[48] *FTC Approves Final Order Settling Charges Against Snapchat*, FEDERAL TRADE COMMISSION (Dec. 31, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-approves-final-order-settling-charges-against-snapchat (last visited Nov. 6, 2015).
[49] *Medical Billing Provider and its Former CEO Settle FTC Charges That They Misled Consumers About Collection of Personal Health Data*, FEDERAL TRADE COMMISSION (Dec. 3, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/medical-billing-provider-its-former-ceo-settle-ftc-charges-they (last visited Nov. 6, 2015).
[50] 15 U.S.C.A. § 53.

student personal information in violation of the Student Privacy Pledge;

- Enjoin Google from collecting, maintaining, using, or sharing any personal student information not necessary for educational purposes (including in aggregated or anonymized form), without student or parent authorization, as long as it remains a signatory to the Student Privacy Pledge; and

- Provide such other relief as the Commission finds necessary and appropriate.

OR

- Order Google to withdraw from the Student Privacy Pledge; and

- Provide such other relief as the Commission finds necessary and appropriate.

Respectfully submitted,

/s/ Nathan D. Cardozo

Nathan D. Cardozo
Staff Attorney

Sophia S. Cope
Staff Attorney

Electronic Frontier Foundation[51]
815 Eddy St
San Francisco, CA 94109
Phone: (415) 436 9333
nate@eff.org

DATE: December 1, 2015

[51] EFF would like to thank our legal intern, Michael Godbe, for his outstanding work researching and drafting this complaint.