How Google Threatens Your Children

Source: Mercola

by Dr. Joseph Mercola

August 6, 2019

STORY AT-A-GLANCE

- More than half of American K-12 schools use Chromebooks and Google apps, allowing Google to build brand loyalty from an early age
- Google's primary business is tracking, compiling, storing and selling personal data. By capturing children at an early age, it will be able to build the most comprehensive personality profiles of the population ever conceived
- By the time these children have grown into adulthood, every single preference, thought, belief and proclivity will be known about them, which will make them extremely vulnerable to manipulation
- Google allows hundreds of third-party software developers to access the emails of Gmail users, and they're not just using software to scan for keywords. In some cases, employees are actually reading the emails
- By default, Google Chrome allows any and all tracker cookies to follow your every move online

Google is without a doubt the largest and clearest monopoly on the planet. It dominates online searches and advertising, which in and of itself leads to automatic bias. As noted by Google's founders Sergey Brin and Lawrence Page in their 1998 paper, "The Anatomy of a Large-Scale Hypertextual Web Search Engine," "... [W]e expect that advertising funded search engines will be inherently biased towards the advertisers and away from the needs of consumers."

Google has also infiltrated many other areas of our day-to-day lives, having acquired dozens of other companies you might not realize belong to Google or its parent company, Alphabet.

Among the most well-known are YouTube, the largest video platform on the web, and Android, one of the most popular operating systems worldwide. <u>Google</u> also has significant influence over urban development, <u>health care</u> and childhood education.

Google has become ubiquitous in American classrooms

Google's influence over young children has been a concern for years. As noted in a 2014 article in the International Business Times, "How Google Took Over the American Classroom and Is Creating a Gmail generation":

"Google apps, services and increasingly, Chromebooks, have become ubiquitous in the American classroom and it's not hard to understand why: they require no expensive hardware, they never need to be updated, and they're free, an important consideration for cash-strapped districts ...

South Carolina's Richland School District 2 boasts 22,000 Chromebooks, which covers a student populace nearing 27,000, who also use Google Apps.

That makes for a sizeable student population that will become accustomed to utilizing Google services ... 'Education is at the core of Google's mission — to remove the four walls of the classroom and make the world's information accessible to all students,' a Google spokeswoman said."

Google will know everything about your child

However, for all its conveniences, Google poses a very real threat to all these children. As noted in a 2017 article in The New York Times — which details the strategic moves that allowed Google to take over the American classroom — "schools may be giving Google more than they are getting: generations of future customers."

In 2012, less than 1% of the tablets and laptops used in the U.S. school system were Google Chromebooks. By 2015, more than half the devices sold to K-12 schools were Chromebooks, equipped with a free suite of Google apps and education-specific programs.

When you consider Google's primary business is tracking, compiling, storing and selling personal data, by capturing children at an early age, it will be able to build the most comprehensive personality profiles of the population ever conceived — and there's no opt-out feature for this data gathering. As reported by The Washington Post in 2015:

"... [I]n a filing with the Federal Trade Commission, the Electronic Frontier Foundation (EFF) argued Google is tracking nearly everything students are doing when they are signed into their Google accounts and, in some cases, using that information to build profiles and serve them targeted ads in certain Google programs."

By the time these children have grown into adulthood, every single preference, thought, belief and proclivity will be known about them, which will make them extremely vulnerable to manipulation, not only through targeted advertising but also through what might be called customized censorship or targeted social engineering — in essence, the strategy of tailoring the

information any given individual can see in order to shape and mold their prejudices and ideas. The Washington Post writes:

"Google makes \$30 per device by selling management services for the millions of Chromebooks that ship to schools. But by habituating students to its offerings at a young age, Google obtains something much more valuable.

Every year, several million American students graduate from high school. And not only does Google make it easy for those who have school Google accounts to upload their trove of school Gmail, Docs and other files to regular Google consumer accounts — but schools encourage them to do so …

That doesn't sit well with some parents. They warn that Google could profit by using personal details from their children's school email to build more powerful marketing profiles of them as young adults ...

Unlike Apple or Microsoft, which make money primarily by selling devices or software services, Google derives most of its revenue from online advertising — much of it targeted through sophisticated use of people's data ...

'Unless we know what is collected, why it is collected, how it is used and a review of it is possible, we can never understand with certainty how this information could be used to help or hurt a kid,' said Bill Fitzgerald of Common Sense Media, a children's advocacy group, who vets the security and privacy of classroom apps."

Google teaches children to trust the least trustworthy

While most adults are now at least somewhat aware that Google

is spying on their every move and selling their personal data, children are simply too young to understand the long-term ramifications of this pervasive data gathering. (To get an idea of the kind of information tracked and stored, see "What Kind of Information Does Google and Facebook Have on You?")

Children are extremely vulnerable to influence of all kinds, and Google is taking full advantage of this. As pointed out by a Berkeley, California, teacher in a May 2018 article in The Outline:

"The video game Interland is part of Google's 'Be Internet Awesome' curriculum aimed at 'helping kids be safe, confident explorers of the online world' ... The game's release was met with positive reviews that completely miss the point ...

Interland sells to kids the message that Google is a trustworthy arbiter of online safety and privacy. And Interland is only one of many ways this message has become increasingly embedded in K-12 school classrooms ...

Beyond datamining, some parents and privacy advocates have expressed concern that even when kids are explicitly taught how to safeguard their personal information online, school-mandated Chromebooks and Google accounts implicitly train kids to accept surveillance and hand over personal information ...

Be Internet Awesome implicitly signals to students that Google is synonymous with privacy and safety. By focusing solely on personal choices, the program suggests that the power to protect personal information lies entirely within one's own hands and locates responsibility for doing so with the individual.

There's nothing wrong with telling students not to send money to someone claiming to be a Nigerian prince but for most people, most of the time, there is greater danger in all the usual and perfectly legal ways of persuading us to part with our money ...

[J]ust as the greater threat to our privacy, as anyone compromised in the Experian hack can tell you, comes not from, or not only from, crappy passwords but from numerous ways we are tracked without our permission or knowledge."

Google and third parties have access to your Gmail

One particularly offensive invasion of privacy is Google's snooping into Gmail emails. According to a July 2018 Wall Street Journal report, Google allows hundreds of third-party software developers to access the emails of Gmail users, and they're not necessarily just using software to scan for keywords. In some cases, employees are actually going in and reading the emails.

"One of those companies is Return Path Inc., which collects data for marketers by scanning the inboxes of more than two million people who have signed up for one of the free apps in Return Path's partner network using a Gmail, Microsoft Corp. or Yahoo email address," The Wall Street Journal writes.

"Computers normally do the scanning, analyzing about 100 million emails a day. At one point about two years ago, Return Path employees read about 8,000 unredacted emails to help train the company's software, people familiar with the episode say.

In another case, employees of Edison Software, another Gmail developer that makes a mobile app for reading and organizing email, personally reviewed the emails of hundreds of users to build a new feature, says Mikael Berner, the company's CEO.

Letting employees read user emails has become 'common practice' for companies that collect this type of data, says Thede Loder, the former chief technology officer at

eDataSource Inc. ... Neither Return Path nor Edison asked users specifically whether it could read their emails. Both companies say the practice is covered by their user agreement ...

Neither Return Path nor Edison mentions the possibility of humans viewing users' emails in their privacy policies. Mr. Berner says he believes Edison's privacy policy covers this practice by telling users the company collects and stores personal messages to improve its artificial-intelligence algorithms."

According to The Wall Street Journal, Gmail has 1.4 billion users worldwide — "more users than the next 25 largest email providers combined." While Google claims to have stopped scanning Gmail emails for the purpose of creating targeted advertising after being slapped with a class-action lawsuit in 2017, accusing the company of illegal wiretapping, it seems quite clear privacy is not a guarantee when using Gmail for your personal or business correspondence.

Making matters worse, while Google's developer agreement does not allow third-parties to store, make permanent copies of, or expose a user's private data, Google doesn't emphasize enforcement of those policies, developers told The Wall Street Journal.

Is Google developing dossiers on children? You bet

Getting back to your children, is Google developing personality dossiers on them? According to a 2017 report by the Electronic Frontier Foundation, a nonprofit focused on "defending civil liberties in the digital world," the answer is yes. As reported in its executive summary:

"Throughout EFF's investigation over the past two years, we have found that educational technology services often collect

far more information on kids than is necessary and store this information indefinitely.

This privacy-implicating information goes beyond personally identifying information (PII) like name and date of birth, and can include browsing history, search terms, location data, contact lists, and behavioral information.

Some programs upload this student data to the cloud automatically and by default. All of this often happens without the awareness or consent of students and their families.

In short, technology providers are spying on students — and school districts, which often provide inadequate privacy policies or no privacy policy at all, are unwittingly helping them do it."

Your child's school may be spying on your home life too

PJ Media reports there have also been incidents where school employees have remotely accessed students' computers while in their homes. This surprising trend was revealed by the ACLU in the summer of 2017. In a June 15 article on UCLA.org, Marcela Betancur writes:

"Most Rhode Island school districts participate in '1-1' programs — in which third parties provide free laptop devices to students for the school year ... We recently found out that most of the state's participating schools give themselves the ability to remotely spy on their students through these loaned devices.

We published our findings early this month in a report titled 'High School Non-Confidential: How School-Loaned Computers May Be Peering Into Your Home' ... The report found that more than 60 percent of Rhode Island school districts today

participate in the 1-1 program.

It also discovered that a majority of those districts allow school officials or administrators to remotely access the device — while a student is at home, without their knowledge, and without any suspicion of misconduct.

We know from an outrageous Pennsylvania case, in which school administrators were found to have activated webcams to spy on students in their homes, that this obvious privacy concern is not hypothetical. Yet only six districts specifically stated in their policies that they would not remotely access the webcams or microphones of devices distributed through the programs."

When it comes to potential privacy invasions by your child's school, you'll need to address such concerns with school administrators. There are, however, some ways to limit the amount of information Google can gather on your child. In its January 23, 2018, issue under "How to keep Google From Spying on Your Kid's Chromebook," Laptop Magazine provides detailed instructions on which settings to check or uncheck to minimize the data flow.

Google Chrome is an open-door invitation for spying

If you value your privacy at all you will want to STOP USING CHROME immediately. I installed the <u>Brave</u> browser earlier this year and it already has blocked one quarter million ads and 34,000 trackers.

In a June 21, 2019, article, Washington Post technology columnist Geoffrey Fowler highlights the problems with Google Chrome specifically, noting that in one weeklong web surfing experiment, Chrome "ushered more than 11,000 tracker cookies into our browser," and that "Seen from the inside, [Google's] Chrome browser looks a lot like surveillance software."

The experiment led Fowler to switch to Mozilla's Firefox browser, in which privacy protection is the default. In Fowler's weeklong test, Firefox automatically blocked 11,189 tracker requests — cookies that companies and data tracking firms use to gather information about the websites you visit in order to build your personality profile.

Surprisingly, Fowler discovered tracking cookies from websites "you would think would be private," such as Aetna and the Federal Student Aid department. Both "surreptitiously told the data giants every time I pulled up the insurance and loan service's log-in pages," Fowler writes.

He also discovered that Chrome automatically logs you in whenever you use Gmail, thereby allowing Google to track your activity and collect information for personalized ads without your knowledge (since you didn't specifically log in). When doing an online search using Chrome on your Android cellphone, it also shares your location with Google, even if you've turned off location sharing.

"At a minimum, Web snooping can be annoying. Cookies are how a pair of pants you look at in one site end up following you around in ads elsewhere. More fundamentally, your Web history — like the color of your underpants — ain't nobody's business but your own. Letting anyone collect that data leaves it ripe for abuse by bullies, spies and hackers," Fowler writes, adding:

"There are ways to defang Chrome, which is much more complicated than just using 'Incognito Mode.' But it's much easier to switch to a browser not owned by an advertising company ... I've chosen Firefox, which works across phones, tablets, PCs and Macs. Apple's Safari is also a good option on Macs, iPhones and iPads, and the niche Brave browser goes even further in trying to jam the ad-tech industry."

Google plan: Dictate outcome of 2020 presidential election

Google (or more accurately, Alphabet, the rebranded parent company that houses all of the various divisions) has become a gigantic octopus-like super entity, the tentacles of which reach into government, food production, health care, education, military applications and the creation of AIs that may run more or less independently.

A key component of many of these enterprises is data — your personal usage data; the tracking of every webpage you've ever visited and every single thought you've ever written on a Google-enabled device, along with geo tracking your every move.

Ultimately, what can be done with that kind of information, besides personalized advertising? How might it be used in combination with military AI-equipped robots? How might it be used to influence your health care decisions? How might it be used to influence your lifestyle decisions?

How might (or is) it used to shape politics and society at large? As reported June 24, 2019, by Project Veritas, undercover footage shows Google executive Jen Gennai making statements that raise strong suspicions about the company's intent to manipulate the 2020 U.S. presidential elections. The video caught the attention of U.S. Rep. Louie Gohmert, R-Texas, who issued a statement:

"This video shows Google's biases are now a threat to a free and fair election, all while they hide behind the immunity given by Congress years ago when they were supposed to be a simple 'town square' where everyone's voice could be heard without biased results.

In fact, Google references a significant role they see themselves fulfilling in the 2020 elections. This discovery should set off alarm bells throughout the country. It is no secret that Google has a political agenda. Multiple brave tech insiders have stepped forward and exposed Google's censorship of content and specialized algorithms.

This media giant's 'social justice narrative' should distress all Americans who value a free and open society. Google should not be deciding whether content is important or trivial and they most assuredly should not be meddling in our election process. They need their immunity stripped and to be properly pursued by class action lawsuits by those they have knowingly harmed."

As discussed in "Google Buries Mercola in Their Latest Search Engine Update" Part 1 and Part 2, the holistic health community as a whole has most definitely been harmed by Google's censorship and search algorithms, but we're likely just the beginning. Given time, there's no doubt in my mind the online censorship will spread across all fields of endeavor, eliminating views deemed to be in opposition to its goals and financial aims.

It's time to dethrone Google

Today, being a conscious consumer includes making wise, informed decisions about technology. Anyone who has spent even a small amount of time pondering the ramifications of Google's ever-growing monopoly over our day-to-day lives is likely to shudder at the possibilities, and agree that we cannot allow this to continue. To be part of the solution, I encourage you to take the following actions:

Boycott Google by avoiding any and all Google products:

- Stop using Google search engines. Alternatives include DuckDuckGo and Startpage
- Uninstall Google Chrome and use <u>Brave</u> or <u>Opera</u>
 <u>browser</u> instead, available for all computers and mobile

devices. From a security perspective, Opera is far superior to Chrome and offers a free VPN service (virtual private network) to further preserve your privacy

- If you have a Gmail account, try a non-Google email service such as ProtonMail, an encrypted email service based in Switzerland
- Stop using Google docs. Digital Trends has published an article suggesting a number of alternatives
- If you're a high school student, do not convert the Google accounts you created as a student into personal accounts
- Sign the <u>"Don't be evil" petition</u> created by Citizens Against Monopoly

https://youtu.be/LT4x90BMcjA

Χ