Alphabet-Google & the Military 5G Network

by <u>Dr.Joseph Mercola</u> April 18, 2018 <u>Source</u>

Story at-a-glance

- Google and Facebook are two of the largest and clearest monopolies in the world and, between them, the harvesting of your personal information goes far beyond what most people realize is even possible
- Ninety-eight percent of Facebook's revenue comes from advertising, totaling \$39.9 billion last year alone. The more personal information you share, the greater Facebook's profit stream
- Cambridge Analytica is accused of creating a system to profile individual U.S. voters using "improperly gleaned" data from 87 million Facebook users to target them with personalized political ads during the presidential campaign
- Google is not only the largest monopoly in the world, it's also the world's greatest artificial intelligence (AI) company, which facilitates the company's ability to sort through all your data with deep learning algorithms to detect patterns that can be exploited for profit
- The data harvesting going on between Facebook and Google is enormous. A summary of the kind of information these two corporations collect, track and store on each and every single user is included

Google and Facebook are two of the largest and clearest monopolies in the world, and between them, the harvesting of your personal information goes far beyond what most people realize was even possible.

I have recently removed Google Search from this website and replaced with a search engine without the privacy concerns, but has similar capabilities. The search bar at the top of the website is the most used and essential feature for you to research the many thousands of pages I've published over the last 20 years.

Google catches every single thing you do online if you're using a Google-based feature, and Facebook has a record of everything you've ever said or "liked." All of this data is being used to build very powerful personality profiles that are sold for profit and used in a variety of different ways.

As previously reported by Gawker:

"Every word of every email sent through Gmail and every click made on a Chrome browser is watched by the company. 'We don't need you to type at all,' [Google co-founder Eric] Schmidt once said. 'We know where you are. We know where you've been. We can more or less know what you're thinking about.'"

Facebook Sells Your User Data, and It Can Be Used Against You

According to CNN Money, 2 98 percent of Facebook's revenue comes

from advertising, totaling \$39.9 billion last year alone. The company is now facing a firestorm after The New York Times and British media outlets reported Cambridge Analytica used "improperly gleaned" data from 87 million Facebook users to influence American voters.³

This is not the first time political parties have utilized facebook data without your knowledge, and it won't be the last. Political parties will continue to fight about who used what data to manipulate voters in the least worst way. What is important to understand is that you and your network of friends are being heavily watched and this data is sold with the intent to manipulate your actions.

This manipulation is not just about politics, it's making YOU the product. The intimate details about you, your family and friends are being sold because it is valuable to entities that want to influence you.

In the video above, Cambridge Analytica data scientist Christopher Wylie, who blew the whistle on his employer, revealing the company built "a system that could profile individual U.S. voters in order to target them with personalized political advertisements" during the presidential campaign. As noted by CNN:

"If the Cambridge Analytica scandal leads to tougher data protection regulations — as some policymakers are demanding — or puts people off sharing as much about themselves online, that could hurt Facebook's revenue, and that of all social media platforms."

It's important to realize that Google is also the world's greatest artificial intelligence (AI) company, having purchased Deep Mind for \$400 million several years ago. Deep Mind now employs over 700 AI researchers, the largest collection anywhere in the world.

They are responsible for defeating the human Go champion in 2017, which far exceeds the complexity of defeating a human chess champion. With this level of AI, it is not hard for them to sort through all your data with their deep learning algorithms to detect patterns that can be exploited for profit.

What Kind of Data Does Facebook and Google Really Have on You?

In a March 30 article for The Guardian, Dylan Curran takes a deep dive into the data harvesting going on between Facebook and Google, and for anyone concerned about their privacy, the results are disconcerting to say the least. Here's a summary list of the kind of information these two corporations collect, track and store on each and every single user:

Extremely detailed location tracking

If you have a Google-enabled device on your person that has location tracking turned on, it will store the exact details of where you are at any given moment, and this data accumulates from the first day you started using Google on the device. To review the details of your own data, see this

<u>Google Maps Timeline</u> link.

Complete search histories on all devices

Google keeps tabs on everything you've ever searched for, on any device, including search histories you've deleted from an individual device. To check your own search data, see

Google's MyActivity page. 6

Personalized advertisement profile

Based on your data profile — location, gender, age, work and private interests, relationship status, income, health concerns, future plans and so on — Google creates personalized advertisements that might interest you. Have you ever done a search for a particular product or service and suddenly found yourself flooded with ads for that precise thing? That's your data profile at work. To see your personalized ad profile, see Google's Ads Settings.²

App usage

Do you use apps and extensions? If so, Google knows which ones you're using, how often, when, where and with whom you're interacting when you do. To see your app usage data, check out Google's Security Permission Settings.⁸

YouTube history

Much can be gleaned from the types of videos you're interested in, and Google keeps tabs on every single one you've ever searched for, watched and commented on. To review your own data, see your <u>Youtube Feed History page</u>.⁹

Facebook interactions

Like Google, Facebook records, tracks and stores every single thing you do on Facebook: Every post, comment, "like," private message and file ever sent and received, contacts, friends lists, login locations, stickers and more. Even the recurrent use of certain words is noted and can become valuable currency for advertisers.

When Curran downloaded all of the information Facebook has stored on him, he ended up with a 600MG file, or roughly 400,000 word documents. For individuals who start using Facebook at a young age, the lifetime data harvest could be inconceivably large. To view and download your Facebook data,

see <u>Facebook's Download Your Info</u> page. 10

Clandestine microphone access

Disturbingly, both Facebook and Google have the ability to access your microphone without your knowledge. If you suddenly find yourself on the receiving end of ads for products or services you just spoke about out loud, chances are one or more apps are linked into your microphone and are eavesdropping. Below is a video by Safer Tech describing how to disable the microphone on your device to prevent Facebook

and Google apps from listening in. 11

Clandestine webcam access

Your built-in webcam on your phone, tablet, laptop or computer can also be accessed by various apps. To learn more about app permissions, see "How to Master Your App Permissions So You Don't Get Hacked — The Full Guide," by

Heimdal Security. 12

As noted in this article, "For a long time, app permissions were something the regular PC user had no idea about. When installing new software on a computer, we were never asked if application X could access our web camera, our list of contacts, etc. ... App permissions may seem like a nuisance, but the better you know how they work, the safer you can keep your data."

Event tracking

By tracking your Google calendar entries, combined with your location data, Google knows what events you've attended, when and for how long.

Your fitness routine

If you use Google Fit, all the details about your fitness routine and workouts, down to how many steps you've taken on any given day, are recorded and stored.

A lifetime of photographic evidence

Twenty years ago, photos were a private matter, reminisced over in photo albums and displayed around the home. Today, people's lives are on public display online, and Google captures it all. When combined with facial recognition software and other technological identification applications, including metadata detailing the time and place of each snap, your photos are a treasure trove of private information.

A lifetime of emails

Google also has every single email you've ever sent, received and deleted.

Deleted files and information

You probably delete files and information every now and then for the sake of safety, right? You might decide to delete that list of passwords from your phone, for example, in case you lose it or it gets hacked. Well, Google still has all of that information.

As noted by Curran, showing a screen shot of his downloaded Google data, "This is my Google Drive, which includes files I explicitly deleted, including my resume, my monthly budget and all the code, files and websites I've ever made, and even my PGP private key, which I deleted, that I use to encrypt emails."

If you've done it or researched it, Google and Facebook have a record of it

Like Facebook, Google allows you to download a copy of the data they have stored on you. Curran's personal data cache from Google was 5.5GB big, equal to about 3 million word documents. Essentially, your Google account contains a detailed diary of everything you've ever done or planned to do, and where you were when you did it. To download your own

Google cache, see <u>Google's Takeout page</u>. 13

How Is Your Personal Information Being Used?

Google has "your bookmarks, emails, contacts, your Google Drive files ... your YouTube videos, the photos you've taken on your phone, the businesses you've bought from, the products you've bought through Google … data from your calendar, your Google Hangout sessions, your location history, the music you listen to, the Google books you've purchased, the Google groups you're in, the websites you've created, the phones you've owned, the pages you've shared, how many steps you walk in a day," Curran writes, noting his own data cache included: 14

"... every Google Ad I've ever viewed or clicked on, every app I've ever launched or used and when I did it, every website I've ever visited and what time I did it at, and every app I've ever installed or searched for.

They also have every image I've ever searched for and saved, every location I've ever searched for or clicked on, every news article I've ever searched for or read, and every single Google search I've made since 2009. And then finally, every YouTube video I've ever searched for or viewed, since 2008.

This information has millions of nefarious uses. You say you're not a terrorist. Then how come you were Googling Isis? ... Manage to gain access to someone's Google account? Perfect, you have a chronological diary of everything that person has done for the last 10 years."

Indeed, the 2013 article, "What Surveillance Valley Knows About You," is an eye-opening read that may be well worth your time, describing just how grossly invasive this data collection and distribution is, and how dangerous it can be if you end up on certain lists. Unfortunately, many still fail to see the problem Google presents.

Its services are useful and practical, making life easier in many ways, and more fun in others. That's the bait, and many

have swallowed it hook, line and sinker, not giving any thought to the ultimate price paid for such conveniences, or simply underestimating the threat that all of this personal data collection poses. If you fall into this category, I ask you to give this issue some serious thought, because monopolies threaten our very way of life, and in more ways than one.

Employees Uneasy About Militarization of Google

Google's data harvesting is particularly concerning in light of its military connections, ¹⁶ and the fact the company has repeatedly been caught infringing on privacy rights and misrepresenting the type and amount of data it collects and shares on its users. Make no mistake about it: Capturing user data is Google's primary business. ¹⁷ The fact that it provides practical services while doing so only serves as a convenient distraction from the fact that privacy violations are taking place.

Earlier this month, more than 3,100 Google employees signed a letter to CEO Sundar Pichai, urging him not to go ahead with plans to provide AI technology to the Pentagon's drone program, known as Project Maven. As reported by Fox News, "Google's AI contribution could ... improve the system's ability [to] analyze video and potentially be used to identify targets and civilians." The letter also urges Pichai to establish a corporate policy that disallows it from participating in "warfare technology."

Email correspondence obtained via freedom of information act requests also reveal Google has maintained an intimate relationship with the National Security Agency (NSA) for a

number of years. In 2014, Al Jazeera¹⁹ published correspondence between NSA director general Keith Alexander and Google executives Sergey Brin and Eric Schmidt. At the time, former NSA contractor Edward Snowden had gone public about the NSA's ability to spy on civilians.

In a 60 Minutes special, NSA cyberdefense chief Debora Plunkett claimed the agency had thwarted a plot by the Chinese to capitalize on a technical vulnerability in the basic input/output system (BIOS) of computers sold to the U.S. System BIOS refers to the firmware that initializes hardware activation when you start up your computer, and provides runtime services for the operating system and various programs. Plunkett claimed the NSA worked with computer manufacturers to fix the vulnerability.

However, according to Al Jazeera, the NSA did "exactly what Plunkett accused a nation-state of doing during her interview," namely inserting back doors into BIOS, thereby gaining access to the raw data of any given computer. According to a 2013 article by Spiegel Online, an internal NSA catalog reveals the agency in fact has back door access for a number of different end-user devices.²⁰

The Making of an Orwellian State

Some experts believe the plan to combine Alphabet-Google's data harvesting with a military <u>5G network</u> is a very bad idea. "What could possibly go wrong with a nationalized, dual-use, military-civilian, secure 5G wireless network to centralize all military and civilian U.S. transportation traffic control and management with Alphabet-Google as the only commercial wireless ISP 'financing/anchor tenant?' Way too much," Scott Cleland, former White House deputy coordinator for international communications and information policy, writes on

his blog.²¹

"... National Security Council Staff apparently have a network vision for a secure 5G wireless network for the U.S. military, that is ultimately capable of C3I (command, control, communications, and intelligence) of the 'total situational-awareness,' necessary for the 21st century, 'Internet of the Battlefield' of integrated, autonomous warfare of vehicles, drones and robots ...

Who could compete with a new government-sanctioned, Alphabet-Google, 'information transportation superhighway' monopoly? Who's going to watch these watchers? And what are the incorruptible proposed checks and balances to prevent the near absolute power of a 'Google-GoverNet' from becoming a modern Orwellian Big Brother Inc.? ...

Consumer networks are the primary security vulnerability for national security networks. Alphabet-Google has well-documented hostility to cybersecurity, privacy, and accountability to government. Comingling Google's unmatched civilian surveillance database with military C3I artificial intelligence capabilities on the same network is a recipe for abuse of power ... And Alphabet-Google warrants antitrust scrutiny and prosecution, not antitrust absolution."

Protect Your Privacy by Avoiding Google and Facebook

Indeed, Alphabet, the rebranded parent company of Google and its many divisions, has turned into an octopus-like super entity with tentacles reaching 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 incredibly

detailed personal usage data.

Ultimately, your user data and personal details can be used for everything from creating personalized advertising to AI-equipped robotic warfare applications. As noted in previous articles, Google's involvement in education and health care also has far-reaching ramifications, and in these settings your personal data could potentially be used to influence not only your personal lifestyle decisions but also to shape society at large.

Today, being a conscious consumer includes making wise, informed decisions about technology, and two of the greatest personal data leaks in your life are Google and Facebook. Here's a summary of action steps you can take right now, starting today, to protect your privacy. For more information, see Goopocalypse.com's boycott Google page.

- 1. Sign the <u>"Don't be evil" petition</u> aimed at Google, created by Citizens Against Monopoly
- 2. Avoid any and all Google products:
- a. Stop using Google search engines. So far, one of the best alternatives I've found is $\frac{DuckDuckGo^{22}}{DuckDuckGo^{22}}$
- a. Uninstall Google Chrome and use the <u>Opera browser</u> instead, available for all computers and mobile devices.²³ From a security perspective, Opera is far superior to Chrome and offers a free VPN service (virtual private network) to further preserve your privacy
- b. If you have a Gmail account, close it and open an account with a non-Google affiliated email service such as ProtonMail, ²⁴ and encrypted email service based in Switzerland
- c. Stop using Google docs. Digital Trends has published an article suggesting a number of alternatives²⁵

- d. If you're a high school student, do not convert the Google accounts you created as a student into personal accounts
- 3. <u>Minimize your use of Facebook</u>, and be mindful of what you post, click, and comment on while there