Free speech is fleeting, this content will disappear in: 0 Hours : 14 Minutes : 31 Seconds Learn More

Court Says Google Analytics Is Illegal

Analysis by Dr. Joseph Mercola Fact Checked

May 18, 2022

Download PDF

Previous Next

STORY AT-A-GLANCE

- Google's history of collecting personal data and manipulating your behavior extends to the Analytics program website owners use to evaluate the actions of people who visit their sites. A French agency says Google Analytics breaches GDPR rules based on a 2020 court case
- European Union citizens and residents have the right to refuse to have online data collected, sold or distributed. Weeks before the French action, Austrian authorities also found Analytics violates GDPR rules
- After years of research, Robert Epstein, a Harvard trained psychologist, found Google uses manipulative and deceptive practices that can sway your perceptions and behaviors, which is not limited to buying practices but also influences presidential elections
- Surveillance data are helping to feed China's social credit system that has enslaved a country's citizens so they are unable to go to school, ride the train, buy groceries or get a good job unless their social credit score meets the government standard

Google has a long history of collecting your personal data and using it to manipulate your behavior. A regulatory agency in France is the latest to find the data collected by Google Analytics breaches European privacy laws.[1]

Google has also been busy in the U.S. during the pandemic, in one instance partnering with Apple to create a smartphone app called MassNotify.[2]

This is used to track and trace people and then advertise the user's COVID-19 status to others. Despite the intent to advertise user COVID status to others, the MassNotify website says the tool was developed "with a focus on privacy."[3] Yet the app was also downloaded to Android phones without consent.

Early in 2022, four attorneys general filed four separate lawsuits against Google for deceptive practices in collecting location data from the public.[4] The suits allege that Google continues to track location data even after people turn off the location tracking app on their smartphone. Karl A. Racine is the attorney general for the District of Columbia and one of the attorneys general who filed a lawsuit against Google. He said in a statement:[5]

> *"Google falsely led consumers to believe that changing their account and device settings would allow customers to protect their privacy and control what personal data the company could access. The truth is that contrary to Google's representations it continues to systematically surveil customers and profit from customer data."*

The action taken by France's National Commission for Informatics and Liberties (CNIL) is based on a July 2020 case from the Court of Justice in the European Union (EU), which affects data transfer outside the EU.[6]

EU and 3 U.S. States Have Rules That Govern Internet Traffic

The 2020 Court of Justice case was based on violations of the EU's General Data Protection Regulation (GDPR). This law was effective May 25, 2018, and is one of the toughest privacy and security laws that govern websites. The law imposes obligations on websites that target or collect data from EU citizens or residents. It does not make the distinction where the website originates.

In other words, if your website collects data or does business with any EU citizen or resident, no matter where your business is located, the GDPR rule may apply to you.[7] The second part that applies to Google Analytics covers when the website tracks cookies or the IP addresses of EU citizens or residents.[8]

The data collection is classified as "monitoring behavior."[9] The GDPR allows monitoring activity to happen but only when there is transparency and the user understands the data are collected and has the option of opting out, which is designed to protect personal data regardless of where it's collected, used or stored.

In the U.S., three states now have consumer data privacy laws similar to the GDPR. These states are California, Colorado and Virginia. They have many provisions in common with the GDPR, "such as the right to access and delete personal information and to opt-out of the sale of personal information."[10]

France Is the Latest to Say Google Analytics Is Illegal

The July 2020 court case on which this new ruling is based, was won by Max Schrems, the lawyer who sued Facebook for privacy violations against EU citizens and won.[11] It has become known as the "Schrems II" judgment,[12] and happened just weeks after Austrian data protection authorities also ruled that Google Analytics violates the GDPR.[13]

The Austrian ruling found that IP addresses and personal identifiers in cookie data could be combined to identify visitors, which is in essence surveillance. To reach the ruling the regulator looked at a variety of measures that Google said it used to protect data in the U.S.

However, they did not find there were enough safeguards to block intelligence services to meet GDPR standards. TechCrunch published part of the decision from a machine translation of the German text:[14]

> *"US intelligence services use certain online identifiers (such as the IP address or unique identification numbers) as a starting point for the surveillance of individuals. In particular, it cannot be excluded that these intelligence services have already collected information with the help of which the data transmitted here can be traced back to the person of the complainant."*

The CNIL works with private and public organizations to ensure compliance with the law.[15] A single website was called out for noncompliance with the GDPR, stating it breached Article 44 since data from Google Analytics are transferred to the U.S.[16]

CNIL gave the website operator one month to comply with removing Google Analytics from their website. The ruling is one of 101 complaints that were filed in August 2020 following the successful court case in July 2020. In a press release, CNIL wrote:[17]

> *"[A]lthough Google has adopted additional measures to regulate data transfers in the context of the Google Analytics functionality, these are not sufficient to exclude the accessibility of this data for U.S. intelligence services. There is therefore a risk for French*

website users who use this service and whose data is exported."

As AppleInsider[18] points out, Google support pages also acknowledge that Google Analytics is not compliant with "the European Economic Area's General Data Protection Regulation (GDPR), or California's California Consumer Privacy Act (CCPA), or other similar regulations."[19]

According to TechCrunch,[20] CNIL left the door open for website owners to use Google Analytics when substantial changes are made to ensure the anonymity of statistical data being collected and transferred to the U.S.

However, the Austrian decision took a broader interpretation of personal data and found that the IP address may be enough when combined with other smaller bits of data already held by Google to identify a site user. Under the current conditions, Google Analytics is noncompliant with the GDPR, which has clear implications for any website using tools that transfer data to the U.S. without measures to ensure anonymity of the data.

While the CNIL began the process with one website, the joint efforts by EU regulators suggest that it will have ramifications across the EU. TechCrunch later learned from the regulator in France that Facebook Connect "has also been the subject of complaints to the CNIL, which are currently being investigated."[21]

Google Shifts Perception and Behavior Without Your Knowledge

The objection against Google data collection through their Analytics program is the opportunity it gives the behemoth to collect your personal data and use artificial intelligence to make decisions about your actions. This then leads to greater manipulation of your opinions and behaviors.

Robert Epstein is a Harvard-trained psychologist whom I interviewed in early 2020.[22] For the last decade he has helped expose the manipulative and deceptive practices Google uses against you. Through his research that began in 2013, he discovered that biased search results can influence public opinion and sway undecided voters.

These biased search results are produced by recognizing your previous behavior online and gently swaying your opinion. Epstein found that the strength of that influence was shocking and that Google can block website access on browsers other than their own. These findings were published in U.S. News & World Report in 2016.[23] The power the search engine pose threatens society in three specific ways, which Epstein discussed during our interview:

1. Google is a surveillance agency with significant powers which are spread across its properties including Google Docs, Google Drive, YouTube and Google Wallet.

2. Google can restrict or block (censor) access to websites across the internet. They can even block access to entire countries or the internet as a whole. The most significant issue with this type of censorship is that you don't know what you don't know. When information is removed from search engines, you don't know it exists and you don't go looking for it elsewhere.

3. The company has the power to manipulate public opinion by presenting specific content to the user and through search ranking. Epstein explains:[24]

   > *"To me, that's the scariest area because as it turns out that Google is shaping the opinions and the thinking and the beliefs and the attitudes and the purchases and the votes of billions of people around the world without anyone knowing that they're doing so … without leaving a paper trail for authorities to trace.*
   >
   > *They're using new techniques of manipulation that have never existed before in human history and they are for the most part, subliminal … I've stumbled onto a whole set of techniques that Google has developed that work extremely well … these are invisible effects, so they're subliminal in that sense, but they don't produce tiny shifts.*
   >
   > *They produce enormous shifts in people's thinking, very rapidly. Some of the*

techniques I've discovered are among the largest behavioral effects ever discovered in the behavioral sciences."

How Google Can Influence Elections and Society

During the interview,[25,26] Epstein described his controlled, randomized, double-blind and counterbalanced experiments that revealed the number of ways that Google can shift public perception. The first effect he discovered was something called search engine manipulation effect (SEME). The aim of the experiment was to see if results biased toward a particular political candidate could shift a user's opinions and leanings.

He predicted a voting shift preference of 2% to 3%. What he got was a shift of 48%, which he initially thought was an error. In the early experiments, they used undecided voters from the U.S. and a real election for the prime minister of Australia in 2010. In other words, they used real candidates with a real election and real search results.

During a second experiment, they found a 63% shift in voter preference when they hid the bias in the search results. A large-scale investigation showed the few who noticed the bias in their search results were not protected from the effect. In fact, it shifted them further toward the bias rather than away from it.

In the months leading up to the 2016 presidential election, he engaged 95 field agents whose identities they kept secret and equipped them with passive software that allowed them to look over the shoulders of people as they did election-related searches. They found there was pro-Clinton bias in the top 10 search positions on the first page of Google, but not on Bing or Yahoo.

This showed a significant pro-Clinton bias on Google. From this data, he was able to calculate how many votes could have been shifted with that level of bias by using data collected since 2013. At a bare minimum, he believes 2.6 million undecided voters could have been shifted to Hillary Clinton and as many as 10.4 million possible on the high end.

Google Surveillance Helps Feed China's Social Credit System

Google surveillance information goes beyond manipulating your behavior through searches to supporting social credit systems being developed around the world. China's social credit system has been in effect since 2018. The system awards and subtracts points for certain types of behavior in their citizens. This video shows only a small extent to which this social system controls the lives of citizens in China.

The small part shown in the video is extensive. The process was conceived in 2014 and rolled out in 2018. By 2020, in the middle of the pandemic, China's established digital infrastructure could track and trace its citizens as it related to their health status, social media posting, contributions to charities, volunteer actions, shopping patterns, decisions and more.

Like your credit score, a person's social credit score can go up and down. It is integral to your ability to do anything in public, including buying groceries, riding on public transportation or going to public events. Bad behavior can also be punished by slowing your internet speed, banning your children from certain schools or getting higher education, or being barred from certain types of employment.

Central to the process is public shaming. According to a report in Blaze Media as the social credit system was rolled out, "China says that it is trying to "purify" society by rewarding the trustworthy and punishing those it deems as untrustworthy."[27]

The actions against citizens through the social credit score system are based on surveillance data that Google makes accessible to countries interested in this kind of Orwellian surveillance scheme. It is the largest monopoly the world has ever seen that siphons data deep into your everyday life and collects data on nearly every move you make and conversation you have.

Your movements can be tracked online, even when you don't think you're using their products. Google Analytics program is just one method they use to track everything you do on any website that has their free product installed. Although these services are presented to users as free, they are actually a tightly integrated package of surveillance tools and Google is making money by selling your data and serving you ads to manipulate and direct your behavior.

A 2015 Wired article[28] revealed some of the details of how Google's online empire is built, noting "One of the company's cluster switches provides about 40 terabits per second of bandwidth — the equivalent of 40 million home internet connections," and "Google now sends more information between its data centers than it trades with the internet as a whole."

Say Goodbye to Google

To make inroads to protect your privacy, you simply must avoid Google products, as they account for the greatest personal data leaks in your life. Mercola.com is Google-free. We do not use Google Analytics, Google ads or Google search for internal searches. To protect your privacy, be sure to ditch or replace:

- **Gmail —** Every email you write is permanently stored.[29] It becomes part of your profile and is used to build a digital model, which allows them to make predictions about your thinking, wants and desires. Many other older email systems such as AOL and Yahoo are also used as surveillance platforms. ProtonMail.com, which uses end-to-end encryption, is a great alternative and the basic account is free.
- **Google's Chrome browser —** Everything you do is surveilled, including keystrokes and web pages visit.[30] Brave is a possible alternative that is faster than Chrome and suppresses ads. It's based on Chromium, the same software code that Chrome is based on, so you can easily transfer your extensions, favorites and bookmarks.
- **Google search engine —** This applies to any extension of Google, such as Bing, Yahoo and iPhone's personal assistant Siri, which draws search results from Google. Alternative search engines include SwissCows and Qwant. Avoid StartPage, as it was recently bought by an aggressive online marketing company[31] which, like Google, depends on surveillance.
- **Android cell phones —** These run on a Google-owned operating system,[32] and can track you even when you're not connected to the internet, whether you have geo-tracking enabled or not.
- **Google Home devices —** These devices record everything that occurs in your home or office.

This includes speech and sounds such as brushing your teeth and boiling water. Even when they appear to be inactive, they are sending information back to Google. Android phones are also always listening and recording,[33] as are Google's home thermostat Nest[34] and Amazon's Echo and Alexa.[35]

+ Sources and References

TODAY'S FREE ARTICLES

1 New Food System Will Stop at Nothing to Control You

2 The Cognitive Costs of Virtual Communication

3 Don't Underestimate Your Need for This Critical Nutrient

Show Comments (20)

Post your comment

Join the World's #1 Natural Health Newsletter for FREE!
Latest Trustworthy News from Dr. Mercola — delivered straight to your inbox!

Enter your email address

Subscribe Now!

Telegram Gab Gettr MeWe Snapchat Tiktok BitChute Rumble

Mercola proudly supports these charities and organizations. View All

INSIDE MERCOLA.COM

About Dr. Mercola
Health Articles
Podcast
Special Reports
En Espanol
Mercola Social Responsibility

HELP

Contact Us
Media Inquiries
Mercola Community FAQ

Disclaimer: The entire contents of this website are based upon the opinions of Dr. Mercola, unless otherwise noted. Individual articles are based upon the opinions of the respective author, who retains copyright as marked. The information on this website is not intended to replace a one-on-one relationship with a qualified health care professional and is not intended as medical advice. It is intended as a sharing of knowledge and information from the research and experience of Dr. Mercola and his community. Dr. Mercola encourages you to make your own health care decisions based upon your research and in partnership with a qualified health care professional. If you are pregnant, nursing, taking medication, or have a medical condition, consult your health care professional before using products based on this content.

If you want to use an article on your site please click here. This content may be copied in full, with copyright, contact, creation and information intact, without specific permission, when used only in a not-for-profit format. If any other use is desired, permission in writing from Dr. Mercola is required.

Terms & Conditions • Updated Privacy Policy
© 1997-2022 Dr. Joseph Mercola. All Rights Reserved.

TRUSTe

BREAKING NEWS

EMAIL
ARTICLE

PREVIOUS ARTICLE

NEXT

ARTICLE