

Four Attorneys General Claim Google Secretly Tracked People

Analysis by [Dr. Joseph Mercola](#)

✓ Fact Checked

STORY AT-A-GLANCE

- › Four attorneys general have sued Google for its deceptive practices in collecting location data from the public
- › The separate lawsuits allege that Google continued to track location data of its users even after they had disabled location tracking
- › Google’s misleading claims to users regarding privacy protections available in their account settings have been ongoing since at least 2014
- › The attorney general for the District of Columbia launched an investigation into Google after a 2018 AP News report revealed Google was tracking people’s movements even when they’d opted out of such tracking
- › The suits allege that Google’s products are designed to pressure users to allow location tracking “inadvertently or out of frustration,” in violation of state consumer protection laws

If you’ve ever felt like Google’s watching you, it’s because they, quite literally, are. “The truth is that contrary to Google’s representations it continues to systematically surveil customers and profit from customer data,” Karl A. Racine, the attorney general for the District of Columbia, said in a statement.¹

He's among four attorneys general who have sued Google for its deceptive practices in collecting location data from the public. The separate lawsuits allege that Google continued to track location data of its users even after they had disabled location tracking.

"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," Racine said.²

Google's Been Secretly Tracking People Since at Least 2014

Racine initiated an investigation into Google after a 2018 AP News report revealed Google was tracking people's movements even when they'd opted out of such tracking.³ Google's misleading claims to users regarding privacy protections available in their account settings have been ongoing since at least 2014, Racine's investigation found.⁴

The AP investigation included a real-world example from privacy researcher Gunes Acar, whose location was tracked to dozens of locations over the course of several days, and the data saved to his Google account, even though he had turned "Location History" off on his cellphone.⁵

Location data collected by Google has been used in criminal cases in the past, including a warrant issued by police in Raleigh, North Carolina, to track down devices in the area of a murder.⁶ When you use an app like Google Maps, it will ask you to allow access to location, but it also tracks your location during use of apps that you might not expect. According to the AP investigation:⁷

"For example, Google stores a snapshot of where you are when you merely open its Maps app. Automatic daily weather updates on Android phones pinpoint roughly where you are. And some searches that have nothing to do with location, like "chocolate chip cookies," or "kids science kits," pinpoint your precise latitude and longitude – accurate to the square foot – and save it to your Google account.

The privacy issue affects some two billion users of devices that run Google's Android operating software and hundreds of millions of worldwide iPhone users who rely on Google for maps or search."

Tracking You Even When 'Location History' Is Off

At issue is the company's continued tracking of its users even when Location History is turned off. "If you're going to allow users to turn off something called 'Location History,' then all the places where you maintain location history should be turned off," Jonathan Mayer, a former chief technologist for the Federal Communications Commission's enforcement bureau, told the AP. "That seems like a pretty straightforward position to have."⁸

Indeed, it states on Google's Account Help webpage, "You can turn off Location History for your account at any time." Only lower down on the page does it explain, however, that location data may still be saved even if Location History is paused:⁹

"If you have other settings like Web & App Activity turned on and you pause Location History or delete location data from Location History, you may still have location data saved in your Google Account as part of your use of other Google sites, apps, and services.

For example, location data may be saved as part of activity on Search and Maps when your Web & App Activity setting is on, and included in your photos depending on your camera app settings."

Aside from hiding location tracking under settings users wouldn't expect, like Web & App Activity – which is turned on by default – Google is accused of collecting and storing location information via Google services, Wi-Fi data and marketing partners, again after device or account settings had been changed to stop location tracking.¹⁰

In addition to the District of Columbia, the attorneys general of Texas, Washington and Indiana have also filed lawsuits against Google for their deceptive data collection practices. The suits allege that Google also pressured users to use location tracking

more often because it claimed – falsely – that its products wouldn't function properly without it.¹¹

“Google has prioritized profits over people,” Todd Rokita, Indiana attorney general, told The New York Times. “It has prioritized financial earnings over following the law.”¹² Texas, meanwhile, has also filed an antitrust lawsuit against Google that alleges it has abused a monopoly over ad space auctions to marketers. The suit joins those from more than a dozen other states that claim Google has maintained and abused a monopoly over searches online.¹³

Google Is Even Tracking Children

Google has been called a dictator with unprecedented power because it relies on techniques of manipulation that have never existed before in human history, according to Robert Epstein, a Harvard trained psychologist who is now a senior research psychologist for the American Institute of Behavioral Research and Technology, where for the last decade he has helped expose Google's manipulative and deceptive practices.

They're not only a surveillance agency – think about products like Google Wallet, Google Docs, Google Drive and YouTube – but also a censoring agency with the ability to restrict or block access to websites across the internet, thus deciding what you can and cannot see.

Google has also infiltrated education with its Google classrooms, usage of which skyrocketed during the pandemic, but many aren't aware that even their children are being tracked. The attorney general of New Mexico filed a suit against Google for its educational tools in its classroom suite, helping to “break through the fog,” Harvard professor Shoshana Zuboff said:¹⁴

“[The suit is] identifying the huge amounts of data that they're taking about kids, how they track them across the internet are they integrate it with all the other

Google streams of information and have it as a foundation for tracking those children all the way through their adulthood.”

The suit was later dismissed, but the attorney general filed an appeal, maintaining that Google’s G-Suite for Education products “spy on New Mexico students’ online activities for its own commercial purposes, without notice to parents and without attempting to obtain parental consent.”¹⁵

Google Force Installed COVID-19 Tracking Apps

In another sign of Google’s dictatorial tendencies, it partnered with the Massachusetts Department of Public Health and Apple to create a smartphone app called MassNotify, which tracks and traces people, advising the users of others’ COVID-19 status.

While the tool claims to have been developed “with a focus on privacy,”¹⁶ the app suddenly appeared on Massachusetts residents’ Android phones out of nowhere, without consent. The feature must be enabled by the user for it to function, but it’s extremely disconcerting that the tool was automatically added to people’s cellphones, whether they intend to use it or not.

In China, COVID-19 tracking apps have been used as surveillance tools in collaboration with its social credit system, raising red flags that this force-installed app could be tracking residents’ movements and contacts without their knowledge and consent. The MassNotify app uses Google’s and Apple’s Bluetooth-based Exposure Notifications Express program.

The software framework was first released in April 2020,¹⁷ with the goal of allowing users who test positive for COVID-19 to report their results, which then sends out an alert to anyone whose phone crossed paths with the positive case and may have been exposed. The Exposure Notifications Express program acts as a blueprint from which states can implement their own tracking systems without having to develop their own individual apps.

While other states have required users to download an app to use the system, MassNotify was integrated directly into the operating system of Android phones.¹⁸ Such apps are based on technology developed by Apple and Google that was previously known as the “Privacy-Preserving Contact Tracing Project”¹⁹ and is now referred to as the Exposure Notifications API (application programming interface).

In a May 2020 Forbes article by Simon Chandler, he pointed out that while contact tracing apps “may be cryptographically secure,” they still “threaten our privacy in broader and more insidious ways,”²⁰ namely encouraging you to keep your cellphone with you at all times and tracking your whereabouts while you do, and further “normalizing” the constant use of technology to dictate your freedoms and behavior.

Using ‘Trickery for Profits’

The attorneys’ general lawsuits against Google are seeking fines and an end to Google’s use of “dark patterns” that influence users to give up more and more personal data in order for the company to increase its profits. The suits allege that Google’s products are designed to pressure users to allow location tracking “inadvertently or out of frustration,” in violation of state consumer protection laws.²¹

“Google uses tricks to continuously seek to track a user’s location,” Racine said. “This suit, by four attorneys general, on a bipartisan basis, is an overdue enforcement action against a flagrant violator of privacy and the laws of our states.” The more data that Google collects about individual users, the more advertising dollars it can generate. But, Racine noted, “The time of trickery for profits is over.”²²

In a similar lawsuit filed in 2020, Arizona attorney general Mark Brnovich also alleged that Google used deceptive practices to track its users’ locations. That suit stated:²³

“This case concerns Google’s widespread and systematic use of deceptive and unfair business practices to obtain information about the location of its users, including its users in Arizona, which Google then exploits to power its lucrative advertising business. Google makes it impractical if not impossible for users to

meaningfully opt-out of Google's collection of location information, should the users seek to do so."

Location data, meanwhile, can be used to reveal your gym memberships, health care visits, stores and restaurants you frequent or where you go to church. It may also be used to provide personalized ads on digital billboards as you pass by, and Google tracks and provides to its customers information about how well online ads work to drive people into brick-and-mortar stores.²⁴

In addition to disabling as many location tracking apps as possible, and deleting your location history from your Google accounts, you can avoid additional Google products – and the privacy invasions they entail – using the following tips:

- Stop using Google search engines. Alternatives include [DuckDuckGo](#) and [Startpage](#)
- Uninstall Google Chrome and use Brave or [Opera browser](#) 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 instead such as [ProtonMail](#), an encrypted email service based in Switzerland
- Stop using Google docs. Digital Trends has published an article suggesting a number of alternatives²⁵
- If you're a student, do not convert the Google accounts you created as a student into personal accounts

Sources and References

- ^{1, 2, 4, 10, 11, 12} [The New York Times January 24, 2022](#)
- ^{3, 5, 6, 7, 8} [AP News August 13, 2018](#)
- ⁹ [Google Account Help](#)
- ¹³ [The New York Times January 21, 2022](#)
- ¹⁴ [European Union, A Europe fit for the digital age](#)
- ¹⁵ [HuntonPrivacyBlog.com December 2, 2020](#)
- ¹⁶ [Mass.gov, Enable MassNotify on your smartphone](#)

- ¹⁷ [The Verge September 1, 2020](#)
- ¹⁸ [Boston Globe June 22, 2021](#)
- ¹⁹ [Apple.com, Privacy-Preserving Contact Tracing](#)
- ²⁰ [Forbes Coronavirus Contact Tracing Apps May 4, 2020](#)
- ^{21, 22} [The Washington Post January 24, 2022](#)
- ^{23, 24} [Consumer Reports May 28, 2020](#)
- ²⁵ [Digital Trends Best Google Docs Alternatives April 28, 2017](#)