


- **EPIC Alleges Google Is Helping U.S. Government Conduct Constitutionally Illegal Warrantless Searches**

 Man looks at tablet through magnifying glass showing how Google may be helping U.S. government to conduct warrantless searches

[Data Privacy Insights](#)

# EPIC Alleges Google May Be Helping U.S. Government Conduct Warrantless Searches

 [Nicole Lindsey](#)

One of the core underpinnings of U.S. society is that all individuals are protected from unlawful search and seizure of their private property. This concept is enshrined in the Fourth Amendment to the U.S. Constitution, which specifically requires law enforcement officials to obtain a warrant from a court in order to conduct a search of any private property. For that reason, it's especially troubling that Silicon Valley search giant Google may be involved in helping law enforcement officials evade this responsibility. In fact, according to the Electronic Privacy Information Center (EPIC), Google is actually helping the U.S. government conduct warrantless searches.

## **Warrantless searches and the U.S. constitution**

In an amicus brief filed with the United States Supreme Court, EPIC suggested that Google might be actively helping law enforcement officials bypass the Fourth Amendment in order to conduct warrantless searches. From a civil liberties perspective, Google's involvement is worrisome because it means that the right to avoid a "digital search" of one's property is being violated. One would never allow a "physical search" of one's property without a warrant, so why should a digital search by Google be allowed?

In terms of a real world example, we've all seen the Hollywood movies where police officers show up at the door of a suspected criminal, show them a piece of paper signifying that a U.S. court has signed off on a search warrant of the premises, and then proceed to scour the property for illegal or stolen possessions. In the movies, it's only the "dirty cops" who carry out warrantless searches.

But what happens in the digital realm? According to EPIC, law enforcement officials are using Google as a convenient end around the Fourth Amendment in order to carry out warrantless searches. If, for example, police officials would like to examine the digital files of certain suspects, they can simply turn to Google, which will do all the searching for them - and without the time, expense or hassle of getting a warrant for this search. For police departments, warrantless searches of digital material would be one way to make their criminal investigations much easier.

# Searching digital images without warrants

This concern about warrantless searches is more than just theoretical posturing – it is based on a specific case involving Google scanning images in billions of users’ files in order to help track down images of missing children as reported by the National Center for Missing and Exploited Children (NCMEC). If Google finds evidence of those images in user files, then it can contact law enforcement officials with information about the individual, even if there are no exigent circumstances. All of this, of course, is happening without the knowledge of the user and without the execution of any kind of search warrant.

At issue here is the exact process being used by Google to carry out these warrantless searches. Originally, the plan was for the NCMEC to give a database of image hashes (and not actual images) so that Google can hunt for identical image hashes elsewhere on the web. What’s unique about an image hash is that it is essentially a completely unique “fingerprint” of an image. (It’s a long alphanumeric string of characters that describe the content in the image) Thus, just as two people can’t have the same exact fingerprints, two images can’t have the same image hashes. So if Google finds a “match” of an image hash, that’s very strong evidence of two identical images – similar to what would happen if a police officer found your fingerprints at the scene of a crime.

Related Posts

[New Senate Bill Targets Dark Patterns Used by Big Tech Giants](#)

Apr 25, 2019

## [In the United States, Net Neutrality Makes a Comeback](#)

Apr 22, 2019

## [A Majority of Americans Still Have No Idea of How to Respond to a Data Breach](#)

Apr 19, 2019

But here's the thing – Google has developed a new proprietary algorithm that goes one step further on the path to warrantless searches. Instead of using image hash matching, this algorithm actively scans files to see if it can find a certain image. This is where things get a little fuzzy because nobody really knows how the algorithm works, and Google has not made it publicly available. You can think of it as a form of facial recognition technology that makes it possible to spot a face in the crowd. And, in this case, the “face in the crowd” is a missing or exploited child.

## **Negative implications of online warrantless searches**

However, it's easy to see how this technology could be used inappropriately. Or, even more worrisome, it could produce a so-called "false positive." In this case, a false positive would be a "match" that really isn't a match. Say, for example, you happen to have a child who looks a lot like a missing child in the NCMEC database – if Google identifies the image of your child as a match, you might be put into a very difficult situation. Imagine a police officer showing up at your door, demanding to conduct a search of your home to find a missing child.

That's why a civil liberties group like EPIC is getting involved in a Supreme Court case. As EPIC sees it, the potential for things to go horribly wrong far outweigh the possible good things that might happen. And, in a worst-case scenario, such technology from Google could be used for things like checking for religious views, political affiliations, and even the presence of "banned books" on your hard drive.

# China, the modern surveillance state, and warrantless searches

Think this is just a conspiracy theory? Well, Google has been involved with the Project Dragonfly search project in China, where the company is helping the Chinese government identify “sensitive” material on the Internet that Chinese officials don’t want showing up in search results. Thus, Google is developing technology that can identify content that might anger Chinese censors – and that involves doing things like searching for certain images or certain language used by political dissidents.

The solution, says EPIC, is “algorithmic transparency.” And that’s especially the case for any software solution that interacts with the criminal justice system. As technology like artificial intelligence (AI) becomes more and more prevalent, the ultimate fear is that all-knowing AI algorithm will use data gathered by digital bots to convict innocent individuals of crimes they never committed.

The good news, at least for now, is that the U.S. Supreme Court seems to be aware of the issues caused by a new era of digital surveillance. In a recent case, *Carpenter vs. U.S.*, the Supreme Court ruled that law enforcement officials needed to get a warrant before obtaining records from a cell phone provider. Failure to do so would violate the Fourth Amendment.

Clearly, in the digital age, the Fourth Amendment needs special care and protection. It’s just simply too easy to use automated surveillance these days. Searching digital content is easy, cheap and far too convenient. The ability to do so, when placed in the

wrong hands, could have very negative consequences for privacy and civil liberties.