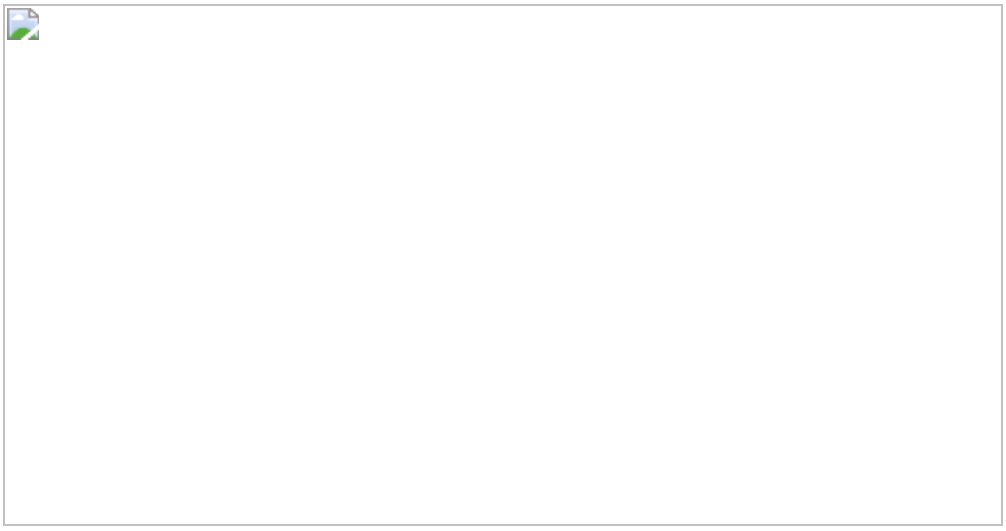
How Google Is Helping The US Government Violate Your Privacy

Profile picture for user Tyler Durden
by Tyler Durden

Authored by Derrick Broze via The Mind Unleashed blog,

A new court filing argues that Google is helping the U.S. government circumvent Fourth Amendment protections in order to conduct warrantless searches.



The Electronic Privacy Information Center (EPIC) has formally accused Google of scanning billions of personal files of users at the request of the U.S. government. EPIC recently filed a “friend of the court” brief alleging that Google is helping the U.S.

government conduct warrantless searches by scanning user files in search of potentially illegal content or evidence of crimes.

The brief came in response to United States v. Wilson, a case where Google scanned images of billions of users files in an attempt to track images of missing children reported by the National Center for Missing and Exploited Children (NCMEC). **After scanning the images contained within users files, Google contacts law enforcement to share information on individuals who may have images of missing children.** However, this entire process happens without permission from users or a warrant issued by a court. EPIC's brief argues that "*because neither Google nor the government explained how the image matching technique actually works or presented evidence establishing accuracy and reliability, the government's search was unreasonable*."

EPIC says this situation is allowing law enforcement to ignore Fourth Amendment protections against unreasonable search and seizure of property and conduct warrantless searches with help from Google.

> "*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*," *CPO Magazine* reports. "*For police departments, warrantless searches of digital material would be one way to make their criminal investigations much easier*."

The crux of this particular case revolves around a new Google algorithm that actively scans files to find a specific image using image matching. Previously, the NCMEC was supposed to provide Google with image hashes that are used to identify a unique image without showing the actual image. However, Google's new algorithm uses image matching instead of image hashing. **EPIC said the "*lower court made a key mistake*" by confusing file hashing with the more personal method of image matching.**

EPIC's concern centers around the ways such a technology could be used to target users for their religious views, political affiliations, or even for possessing banned content. For example, after the shooting in Christchurch, New Zealand, officials threatened jail time to any New Zealand citizen in possession of the shooter's livestream video. With Google's current policy, what's to stop New Zealand's law enforcement from asking Google to search user files for a copy of the banned "hate content"?

This type of arrangement allows the U.S. government to avoid going to a court to request a warrant and also sets a dangerous precedent for future invasions of privacy. The world's largest search engine company is facing increasing scrutiny as news of their failures to protect user information makes headlines around the world. For example, Google recently came under fire for choosing to build a censored version of their search engine for the Chinese government under the Dragonfly program.

If Google continues to make it clear to the world that they do not care about privacy or respecting users' rights, why are so many people still using the tool? The reality is that corporations

will continue to work with governments to erode privacy—and thus, freedom—as long as they know billions of people around the world will still use their services.

The answer?

Seek alternatives to Google's search engine and other services. Vote with your time and dollar by supporting companies that actually care about privacy—and say "goodbye" to Google.