Is Your Cloud Drive Really Private? Not According to Fine Print

Published: Friday, 15 Mar 2013 | 8:22 AM ET
By: Rosa Golijan, NBC News


Getty Images

If you upload a copy of a legally bought DVD to your cloud drive, could your provider label it as a copyright violation? What about a honeymoon photo set that includes one too many bikini shots — could an overzealous automated porn filter delete your pictures by mistake?

Some popular cloud storage providers sweep accounts looking for illegal data. Right now, the focus is on hunting for child pornography, but their terms of service allow for other kinds of files to be considered non grata as well.

"When users place their data with cloud computing services, they lose the ability to maintain complete control of that information," said Lillie Coney, associate director of the Electronic Privacy Information Center (EPIC).

The fight against child pornography

A Maryland man was charged earlier this month with possession of child pornography after authorities were tipped off by the National Center for Missing and Exploited Children (NCMEC). Police say Verizon Online found approximately 23 suspect images during a routine sweep of the man's cloud drive and alerted NCMEC, a non-profit established by Congress and primarily funded by the Justice Department.

While cloud storage providers are required by law to respond to known or suspected instances of child pornography, not all scan users' accounts looking for them.

Apple — which declined to comment — and Microsoft, along with Verizon Online, state in their user agreements that they reserve the right to actively search stored files.

Dropbox, Amazon and Google — the former two of which did not respond to requests for comment — take a more hands-off approach, according to their terms of service. They will investigate notifications of suspected illegal activity, but won't use automated pre-screening.

Is there a difference between services that actively police and those that don't? Coney says yes.

"One is treating data like it belongs to them and the other is following a due-process approach regulated by the courts or existing laws," she told NBC News.

No one argues against the virtues of stopping child pornography. But not all providers make it clear to customers where that fight ends and others — such as the hunt for pirated media files — begin. "There is a need to update (electronic privacy legislation) to help establish the boundaries for due process, police authority and the role of the courts," Coney said.

"If too many decisions are left to individual vendors or cloud service providers to decide, that may bring more harm than good."

How cloud storage is policed

The system that scans cloud drives for illegal images was created by Microsoft and Dartmouth College and donated to NCMEC. The organization creates signatures of the worst known images of child pornography, approximately 16,000 files at present. These file signatures are given to service providers who then try to match them to user files in order to prevent further distribution of the images themselves, a Microsoft spokesperson told NBC News. (Microsoft implemented image-matching technology in its own services, such as Bing and SkyDrive.)

The process is meant to "protect child victims from being revictimized by having images of their abuse circulated online," John Shehan, executive director of NCMEC's Exploited Children Division, told NBC News.

Marianne Grant, a senior vice president at the Motion Picture Association of America, said it was possible for services to use similar tools to filter for other sorts of content.

"There are two opportunities to look at content," when it's going into a cloud-storage account and when it's leaving, she said. "There is technology to do this," Grant added, pointing out that file signatures — unique hashes or fingerprints — could be used to confirm the nature of the files.

"It wouldn't necessarily be the (service provider), it could be the owner of a site or cloud service" that would use the scanning technology, she said, adding that third-party vendors are often used for this sort of filtering.

Microsoft and Verizon Online declined to comment on whether their automated scanning processes are used to catch content other than child pornography. (Apple declined to comment on its cloud storage policies for this article.)

Can there be real privacy in the cloud?

Disagreement among cloud storage providers on whether to scan or not illustrates a gray area

that may trip up privacy advocates and law enforcement professionals alike. EPIC's Coney said that the fine print just isn't enough.

"Terms of service should not be the standard for due process," Coney said. "Laws enforced by the courts should establish what is permissible and what is not.

"The increased use of cloud computing services will raise questions regarding Fourth Amendment protections for that information, property rights between content creators and content holders, and the ability to port data from one cloud service to another," she added.

In other words, even if you're happy with your cloud storage provider, pay attention to the files you're uploading, and keep a back-up of everything on a real hard drive at home.