

The Cloud is Just Someone Else's Computer

When you upload something to "the cloud," that just means it's on someone else's computer. Why does this matter?

Sometimes, people think this is how "the cloud" works. But it's more complicated than that.

Rather than connecting straight to some sort of special digital filing cabinet in the sky, cloud storage is actually a network of computers, usually in the form of servers that store your data and allow you to access it as digital files from outside locations such as a phone, tablet, laptop, or other internet-connected device.

Though it's a little more complicated, the "cloud" actually looks more like this.

All sorts of devices connect to "the cloud," including Internet of things (IOT) devices, such as Internet-enabled speakers, TV's, and thermostats that can be controlled through an Internet connection.

These cloud storage servers can be public, private, or a combination of the two, with pros and cons for each type. When choosing what services to use, it's helpful to know how data is being stored via cloud servers so you can make informed decisions about your own data based on your unique situation and threat model. For instance,

- How is the data [encrypted](#), if it is encrypted? With some services, the cloud storage provider may have access to your data, which means it may be possible for a government to access it.
- Can you easily and quickly delete your data from the servers? Are backups maintained (even temporarily)?
- Is two-factor authentication required for you to access your storage devices?

Alternative options to using cloud storage, which may or may not work for you, can be found in our Surveillance Self-Defense guide to "[Keeping Your Data Safe](#)."