What Is The Cloud And Is It Safe?

February 12th, 2016

Why do we use the cloud?

There was a time we used to buy furniture to hold our media. CD racks, DVD racks, photo albums and filing cabinets filled our living rooms, guest room closets and wherever else we could pile them. Even in our cars, we would install massive CD changers to keep our music flowing or carry enormous books of CDs so we could have our tunes while on the open road. If you try to explain this to young people today, they'll look at you like you just described preparing your covered wagon rather than a mid-2000s Honda Civic. If you try to explain audio cassettes, they might just suspect you have a loose screw or two..

Today's media and data is so small, it might as well not even exist. Using the Apple Music and Spotify libraries as a guideline, every song that's ever been recorded and released would fit into flash storage drives the size of a 12-ounce can of Crystal Pepsi. Even as our data gets smaller, we make so much more of it that it can get out of hand – much like processor speed, the amount of information the world produces doubles every two years. Some of that information is pictures of kittens and makeup tutorials, but we also produce a lot of data that isn't nearly that important.

In such a data-driven world, we trust more and more of our lives to the cloud, and often it seems like blind faith. After all, what is the cloud? How much do you know about it? Are their laws governing the way people use it? Most importantly, have you taken enough steps to protect yourself when all of your information exists on what is, if we're really honest about it, not much more than a metaphor for the shared hallucination that is modern life?

Why should I start to care now?

This week, iPhone users started noticing problems with Safari. Initially attributed to an iOS update from earlier this month, it is now suspected to be a server-side problem stemming from Apple's cloud-based syncing with its Safari web browser. The issue doesn't affect security, but it demonstrates a critical problem with cloud-based computing, something all of the major tech companies are pushing us toward. And it's something where we have little control over our online security.

The cloud itself has insinuated itself in a variety of news stories in the last few years, from the theft of intimate photos belonging to Hollywood stars like Jennifer Lawrence to the operation for ending corruption in FIFA. Cloud storage is behind the surge in Amazon's stock valuation, because they are the largest provider of cloud storage to businesses, including Netflix, the largest private user of bandwidth on the planet. The cloud is the basis for Google's push into the laptop business via Chromebooks, and by extension, the efforts of a variety of organizations to get low-cost laptops in the hands of less-privileged kids. It's even changed Microsoft Office, probably the most ubiquitous piece of software in the world, by forcing Microsoft to create free versions of its Office suite and charge for excess storage of the files you create.

In other words, your investments, your data and the future of law enforcement may be intimately tied to cloud-based computing, and something as simple as a server-side bug can have an enormous ripple effect for millions of users. The issue won't be going away any time soon, as more people use the web more often on mobile devices, which will eclipse 50% of personal Internet usage in the next few years. These devices rely on storage in the cloud to compensate for smaller on-device storage capabilities and a lack of long-term storage peripherals.

What is the cloud?

The cloud is a series of servers which store data that can be accessed by users whenever it's needed. This frees up hard drive space while protecting us from data loss due to hardware failure, including a stolen laptop or dropping your phone into the pasta you're boiling on the stove. It's not magical, and your information doesn't live on the Internet in any particularly novel way. Instead of a home video being stored on your local storage, it is stored on someone else's storage, far away. These server farms are enormous undertakings, and if you're into mechanical processes and design, they're also beautiful and fascinating. For example, check out these pictures of Google's data centers: http://www.google.com/about/datacenters/

How much of my data is stored on the cloud?

The amount of your information stored on the cloud varies from person-to-person, but if you're reading this on a device that plugs into a wall at any point, you've got at least some data on the cloud. If you own an iPhone, your device backs up your photos, videos and music to the cloud, in addition to storing periodic backups of your phone. If you have a web-based email address, like one from Gmail, Yahoo! or AOL, your emails are backed up there as well. Depending upon which apps you use, your health details, dating history or even your exact current location could be on the cloud as well, possibly being shared with third parties.

Wait, who can see what?

For the time being, the government can probably see more of your data than you think. Exact details are fuzzy, and you can make your own moral judgments on homeland security, domestic spying and Edward Snowden. However, if you think the government doesn't want access, keep in mind that Apple is currently fighting both California and the United States federal government to keep a form of encryption on your data that it can't break. Apple no longer wants to surrender data to the government, so it has blinded itself from seeing large swaths of your data. The government is less happy about this, because that data might point to potential threats to homeland security. Again, this article isn't trying to make a moral or political claim. The point is that the government is a third party who wants the ability to look at your data, which represents another point of vulnerability to a malicious attack.

Outside of the government, a lot of the companies that maintain those expensive server farms pay for all of that technology by sharing some or all of your personal information with private businesses. You should already know that, of course. If a web service is free to you, then the company providing it makes its money some other way. If they're charging you, they still might make money by selling your data.

You'll never know, because you accepted the terms without reading them. Don't feel bad, though, we all do that. The iTunes end user license agreement (EULA) is over 20,000 words long, about four times as long as the Constitution of the United States. There are, however, some resources to help you. For a shortened and simplified version of various EULAs, try tosdr.org, which is a donations-based organization that explains what you're agreeing to and offers an add-on for your browser so it's only a click away.

Is my data safer when it's in my control?

That question is up for debate, but usually the answer is no. In most instances, end users are the most vulnerable point of attack for cyber scammers. However, when you have control of your data, you can work to make it safer. When you don't, you're trusting someone else with it. To put it another way, Apple Pay, Samsung Pay, and other tokenized payment plans are the safest way to make a purchase because they require your thumbprint, protects your data with single-use encryption that's worthless to a third party, and doesn't store your info in the cloud. Doing your best to emulate those services is a good idea.

So, what do I do to protect myself from the cloud?

The easiest solution is to spend some time and some money. Find a single site to store your files, whether it's with Google, Microsoft, Apple, or Dropbox. Read each of their EULAs and decide for yourself. Then pay them to get as much storage as you need, rather than spreading your files among various services in order to stay under the amount for free storage.

Next, go through and make a list of which sites and services have what information of yours. Determine your level of comfort. Delete what you can live without, move the rest to somewhere you feel safe. Clear out your email inbox whenever you can. Don't archive private data, like medical records or financial statements, with your email provider. Instead, save them locally on storage you have at home or work, which you can disconnect from the Internet. A 2-terabyte solid state removable storage drive is less than $100 and offers you great protection. As an added measure, back up your drive in a second location once a month, in case something happens to your house.

Finally, as you move forward, try to think critically about what you're telling people. If someone can make money off your information, they'll find a way to do so. The only way to protect your information and that of your family's is by being vigilant.

Sources:

https://tosdr.org/

http://www.slate.com/articles/technology/technology/2014/11/end_user_license_agreements_does_it_matter_that_we_don_t_read_the_fine_print.html

http://genius.com/Apple-itunes-terms-of-service-annotated

http://www.theguardian.com/media/pda/2010/aug/02/infographic-data-cloud

http://www.infostor.com/storage-management/worlds-data-doubling-every-two-years-.html