Who has your Cloud-Back?

Cloud computing security and legal issues have been in the news on a daily basis. How are industry, government, and individuals handling the risks?

For you late filers, the IRS (Internal Revenue Service—U.S. tax revenue collection agency) online system for filing taxes is broken. “On my way over here this morning, I was told a number of systems are down at the moment,” IRS Acting Commissioner David Kautter told lawmakers at an IRS oversight hearing Tuesday [17 April 2018]. “We are working to resolve the issue and taxpayers should continue to file as they normally would.” These systems are supported by cloud servers although the IRS appears need to update its technology.²,³

I normally file my taxes online. So how would I “normally” file now? Will the IRS give me an extension? Will I have to go back to paper but miss the deadline? Do I pay the penalty? Are there any protections for me?

Quick: Answer the above questions and don’t take longer than a few seconds to do so. If your data backup system, or worse yet, your primary application running in the cloud stopped working tomorrow, what would happen?

What if your social media profile or cloud-based contacts disappeared? Could you get a job? Contact people?

What if there was a search warrant out for your data in the cloud? Could legal authorities get that data?

This column will explore the recent news about the data we store in the cloud knowingly and unknowingly, and whether or not we own that data. Although regulations vary across jurisdictions and continue to evolve, it is universally believed that an individual’s data is a digital gold mine. How do we, as individuals, control our own individual pieces of data gold?

MOBILE APPLICATION DATA MINING

In the late nineties, I was taking a graduate class on internet programming using Perl and CGI. The professor asked us, “What if your spending patterns on the Web were used by a corporation to sell you things? Or by the government? Or by law enforcement? I personally didn’t care. I had nothing to hide. He warned me saying that may not always be the case. One of the students wrote on a chat board: “I guess that I must be a very dull person but I do not care who knows where I
am and what I am buying. What are these other people doing that is so nefarious? I've looked at some bikini clad women on the Internet now and then—so what. Get a life people!”

It turns out that way more data about way more things is being collected about us on our phones than we could have ever imagined. AppCensus is a website that provides privacy ratings for over 80,000 Android apps. Applications running on an Android device aren’t supposed to obtain the device’s unique code (referred to as an Android ID which identifies the phone’s hardware), because that could be used to track the phone’s entire workings for the life of the phone—and therefore the duration of your use of that phone. All your phone’s data, including your identity data, every time you did something on your phone when you were supposed to be doing something else, and much more, is being stored.

And it gets more disturbing. Serge Eglemen, the creator of AppCensus, says that 2,500 apps (half of what he tested) have sensitive data that could help to identify the users without permission, which violates the Children’s Online Privacy Protection Rule.

So what to do? You can start by studying your privacy settings on your Google Dashboard and be overwhelmed by all the data collected about you. Your trips, orders, searches, and photos you have taken. You can be befuddled by going into the Facebook settings for privacy. In addition, you can read in full the privacy statements of every application you install on your phone. And even then, because applications sometimes don’t follow their own policies, you still don’t truly know what will happen to your data.

With the Facebook fiasco of 87 million users data being leaked to Cambridge Analytica without permission, Mark Zuckerberg, the Facebook CEO, told the Senate that the company is going through “a broader philosophical shift in how we approach our responsibility as a company.” But several senators pointed out that Facebook is a monopoly and the alternatives are slim. A young adult I know deleted his Facebook account in high school only to realize in college that he couldn’t live without it. Study groups, sports, and social gatherings were all done through the site. And he went through a pariah stage when he started back up because he had no connections.

This digital gold mine is your life. These applications are mining everything about you and the only way to prevent it is to go back to using a landline phone and stop using the Internet. But times are changing.

CLOUD STORAGE LEGAL PROTECTIONS

In Zuckerberg’s remarks to the US Senate, he said that Facebook must give the user simple language regarding what his company does with their data and a way to permanently and quickly delete their personal data. In California, the state government is looking at creating an oversight organization that would require exactly this. Europe has already enacted this and I have noticed recently that groups I work with are scrambling to comply with the General Data Protection Regulation, which will go into effect in May. The law says:

- Users must give explicit consent for use of their personal data, and can withdraw that consent at any time.
- Companies must provide copies of data on demand.
- If that data is stolen, companies must notify victims within 72 hours.
- Violations can result in fines of as much as 4 percent of a company’s annual revenues, or 20 million euros — about $25 million USD.

American companies might follow the European standard because companies find it easier to maintain a single process for ensuring protections, rather than having various protections based on regions.

“If we’re going to see a move to do this kind of thing,” said Danny O’Brien, a privacy activist at the Electronic Frontier Foundation, “right now is that moment.”
The Government Wants Your Data

A case that has now reached the Supreme Court is about Microsoft Corporation and its refusal to comply with a warrant seeking data. The data happens to be stored in Ireland and Microsoft says that the data is under Irish law and not US law. The Clarifying Overseas Use of Data (CLOUD) Act will establish that US warrants cover data stored by US companies regardless of where the servers physically exist. At first, I thought that I didn’t really want the government to get at my data. But consider the problem of data localization.

Some countries get around having a law like the CLOUD Act by requiring that data about their citizens be stored only in their country. China is pushing for data to be stored at their government-run data centers so they get unhindered access to data. Information uploaded by Chinese iCloud customers is stored at a Chinese government-run data center located in China.

Your Data is Safe Up Here

If your storage on a cloud server became unavailable, do you have any rights or even any way to get it back? For now I’m keeping a local copy on a hard drive and a cloud-based copy of all of my important data. And I’m using multiple clouds. But even more reliable solutions may be on the way. One company is proposing what they say is a failsafe way to store data. Wasabi Technologies Inc. is working on data centers orbiting the earth called “Space Belt.” “It’s super, super secure,” Wasabi cofounder David Friend said. “To knock this thing out, you’d have to launch a bunch of satellite-killers.” The technology looks to be affordable and offers an alternative to traditional storage, although presumably, data access times might not be on par with terrestrial solutions.

CONCLUSION

The safety of our personal information and all that we do in the cloud is up for grabs and we need to take control. Personal persistence and better technology may be the answer. IEEE Cloud Computing magazine has many articles on security related issues including a recent article that examine breakthroughs in blockchain to make user data more secure. But government controls will also be necessary to make sure we are protected and elected officials are learning about the issue to make better laws. Our digital data is our essence, worth more than gold, and we need to protect ourselves.

REFERENCES


ABOUT THE AUTHOR

Christine Miyachi is a systems engineer at Xerox Corporation and holds several patents. She works on Xerox’s Extensible Interface Platform, which enables developers to create applications that work with Xerox devices by using standard web-based tools. Miyachi graduated from the University of Rochester with a BS in electrical engineering. She holds two MIT degrees: an MS in technology and policy/electrical engineering and computer science and an MS in System Design and Management. Contact her cmiyachi@alum.mit.edu.