ROBIN SPRINGER

VOICE VALUE

Is Your Voice Data Safe in the Cloud?

Cloud-based files may have less legal protections than you think

Cloud computing is becoming more ubiquitous seemingly by the day. As these offerings proliferate, fewer local computing options are available. Users enjoy enhanced convenience, including a wide variety of applications, minimal upfront licensing costs, decreased investment for hardware, scalability, easy administration, and more flexible workflows.

Server-based dictation products enable users to dictate from multiple devices—whether a desktop computer, digital recorder, tablet, or cell phone—and have the information automatically synced among those devices. No more manually transferring voice files or updated voice commands between one's home, office, and mobile devices.

But users may not realize the privacy risks inherent in cloud computing.

"There are three main ways data can be compromised," says Jacob Hoffman-Andrews, senior staff technologist at the Electronic Frontier Foundation (EFF): (1) the government may send a legal request demanding the company turn over the data; (2) the account may get hacked by a third-party; or (3) the company holding the data could use it inappropriately or in ways the user didn't contemplate.

Government actors can range from the police to the NSA to civilians who work for the government, acquiring information on the government's behalf (say, a company that hosts user data on its server). These players would want the data in connection with criminal investigations. Currently, the Electronic Communications Privacy Act (ECPA) is the primary means to protect electronic data from government actors.

The problem is, the ECPA was written in 1986, long before cloud-based services were popular. An amendment that broadened the types of information protected by a wiretap statute, the ECPA was intended to prevent unauthorized government access to private electronic communications.

In decades past, most people stored data on their personal computers, in their own homes. They paid for internet usage by the minute, typically logging on to their ISPs just long enough to download the messages before logging off, and then managing their messages on their own close-to-the-ground physical PC. Messages were not stored indefinitely on a server somewhere in the ether, like they are today on services like Dropbox and Gmail.

If the government wanted this information, it had to produce a warrant based on probable cause—unless the information had been sitting on the server for 180 days. Then, the message was considered abandoned, and it was subject to a lower standard of protection: a subpoena.

Data on a user's personal computer, though, was subject to the warrant requirement. And that's where we remain today: If you have information on the hard drive of your laptop, the government needs a warrant before it can seize the data, but if it's on a third-party server for more than 180 days, all the government needs is a subpoena.

Privacy advocates believe the ECPA should be updated to reflect how people currently use technology, requiring a warrant for data requests regardless of where the data is stored.

Advocates think privacy law should be updated to reflect how people currently use technology.

California has made the progress that has not yet been seen on the national level. CalECPA, the state's version of the ECPA and a law championed by companies including Apple, was signed into law in October 2015; it requires the heightened warrant standard before government actors can seize user data.

"It's the responsibility of anyone who uses the cloud to read the company's terms of service and privacy policy," attorney Heather Antoine says. "They will explain what happens to your data."

But 91 percent of adults believe consumers have lost control over how personal information is collected and used by companies, and only 5 percent say they feel very secure sending private information via email, according to a 2014 Pew Research study.

In EFF's 2015 "Who's Got Your Back Report," the organization ranked 24 companies based on industry-accepted best practices, which include these three criteria: (1) requiring the government to obtain a warrant before providing the content of user communications; (2) publishing a transparency report of data regarding the number of times governments sought user data and how often the company provided the information to the government; and (3) publishing a law enforcement guide explaining how they respond to data demands from government.

Companies are also rated on whether they tell users about government data requests; publically disclose data retention policies, including how long they maintain data; and publically oppose backdoors, among other factors.

In a future column, I'll be talking with companies that host dictation services to see how our industry protects user data. Stay tuned. ☒

Robin Springer is an attorney and the president of Computer Talk, Inc. (www.comptalk.com), a consulting firm specializing in speech recognition and other hands-free technology services. She can be reached at (888) 999-9161 or contactus@comptalk.com.