SPECIAL REPORT: INTELLECTUAL PROPERTY

Data stored in cloud not guaranteed to remain private

Commentary by Alfred J. Saikali

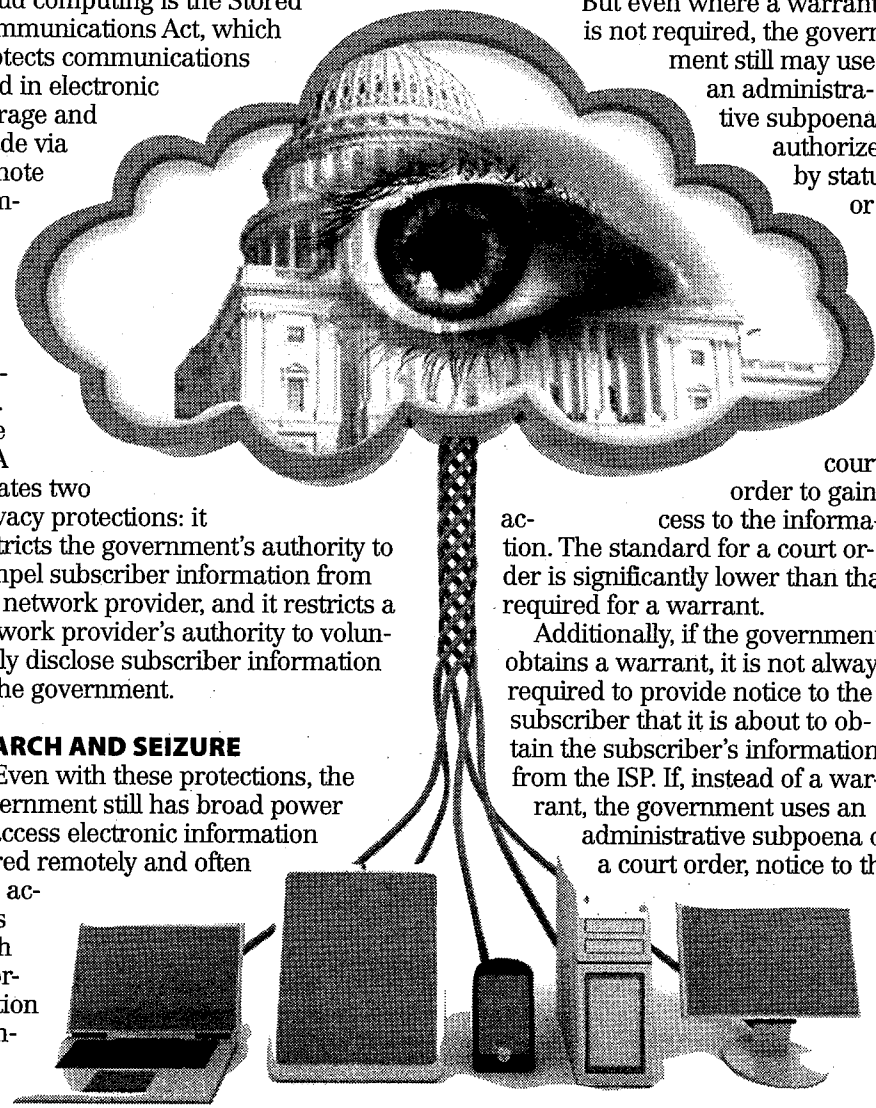

Saikali

Did you know that the government may — and often does — obtain data from Internet service providers without notice to the ISP's subscribers? In the second half of last year, the U.S. government made 4,601 requests for user data from Google.

While businesses and individuals are increasingly storing data in the cloud due to its efficiency and lower costs, the use of this promising technology may be frustrated if the government is able to easily obtain access — as it has in the past with email — to the much wider range of information available from cloud-computing providers.

Cloud computing can generally be thought of as an emerging architecture where data and applications exist in cyberspace and allow users to access them through any online device. In other words, instead of storing applications and data on a personal computer or company server, the applications are accessed online from any device with web access. Cloud-computing activities cover a wide breadth of activities, including e-mail, document applications such as word processing and spreadsheets, and file storage.

The Electronic Communications Privacy Act of 1986 is the primary statute regulating the government's right to access email from ISPs and information in the cloud. It was enacted 25 years ago and has not been revised significantly to reflect changes in technology. It governs the privacy rights of customers and subscribers of computer network service providers. The most relevant section of the law for cloud computing is the Stored Communications Act, which protects communications held in electronic storage and made via remote computing. The SCA creates two privacy protections: it restricts the government's authority to compel subscriber information from the network provider, and it restricts a network provider's authority to voluntarily disclose subscriber information to the government.



SEARCH AND SEIZURE

Even with these protections, the government still has broad power to access electronic information stored remotely and often can access such information without giving notice to the subscriber. Generally speaking, the government is less likely to need a warrant to access a subscriber's older electronic information that is stored remotely.

But even where a warrant is not required, the government still may use an administrative subpoena if authorized by statute or a court order to gain access to the information. The standard for a court order is significantly lower than that required for a warrant.

Additionally, if the government obtains a warrant, it is not always required to provide notice to the subscriber that it is about to obtain the subscriber's information from the ISP. If, instead of a warrant, the government uses an administrative subpoena or a court order, notice to the subscriber is required, but notice may be delayed for up to 90 days after the government has seized the data.

In short, the supposedly limited and specific circumstances for search and seizure of data without subscriber notice are not well-defined or understood, often as a result of the antiquated nature of the ECPA, and those circumstances often are interpreted differently by courts, interpreted broadly by police authorities and have been the subject of government abuse.

What does this mean for a company considering moving its proprietary and confidential data into the cloud? At a minimum, two conclusions should be drawn.

First, there currently is no assurance that communication through cloud computing is or will remain private.

Second, a company's options to prevent the government from gaining access to information stored in the cloud are limited, particularly if the company is not given prior notice. Because cloud computing involves a variety of information that typically has been stored only on personal and company servers, concerns about the government's encroachment on proprietary and confidential information are multiplied and have the potential of stifling advanced use of cloud computing unless changes are made to the ECPA.

Alfred J. Saikali is a partner with the law firm of Shook Hardy & Bacon. He specializes in information law and counsels clients on issues related to data security, data privacy, cloud computing and information management.