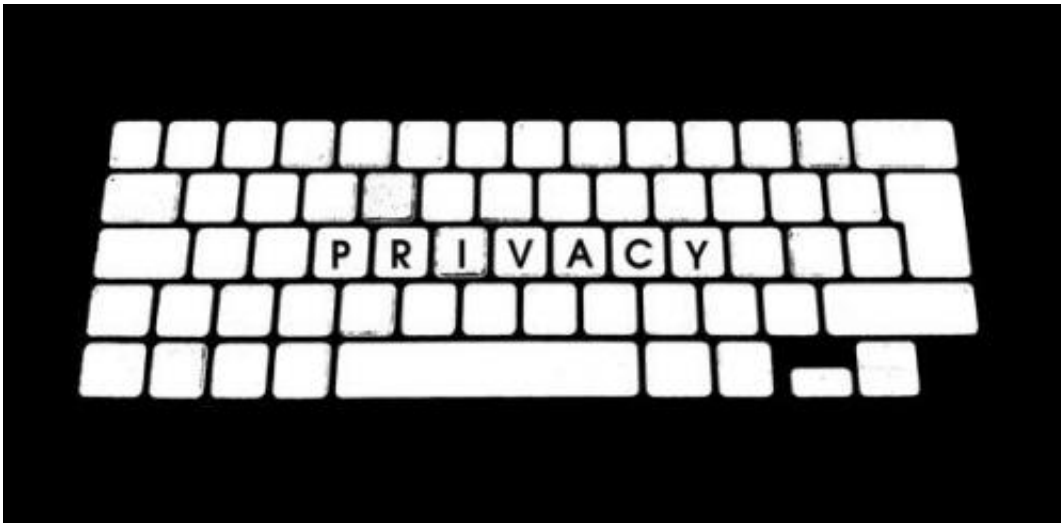# How can we protect our information in the era of cloud computing?

January 26 2015

Credit: g4ll4is

Private information would be much more secure if individuals moved away from cloud-based storage towards peer-to-peer systems, where data is stored in a variety of ways and across a variety of sites, argues a University of Cambridge researcher.

In an article published in the *Proceedings of the Royal Society A*, Professor Jon Crowcroft argues that by parcelling and spreading data across multiple sites, and weaving it together like a tapestry, not only would our information be safer, it would be quicker to access, and could potentially be stored at lower overall cost.

The internet is a vast, decentralised communications system, with minimal administrative or governmental oversight. However, we increasingly access our information through cloud-based services, such as Google Drive, iCloud and Dropbox, which are very large centralised storage and processing systems. Cloud-based services offer convenience to the user, as their data can be accessed from anywhere with an internet connection, but their centralised nature can make them vulnerable to attack, such as when personal photos of mostly young and female celebrities were leaked last summer after their iCloud accounts were hacked.

Storing information on the cloud makes it easily accessible to users, while removing the burden of managing it; and the cloud's highly centralised nature keeps costs low for the companies providing the storage. However, centralised systems can lack resilience, meaning that service can be lost when any one part of the network access path fails.

Centralised systems also give a specific point to attack for those who may want to access them illegally. Even if data is copied many times, if all the copies have the same flaw, they are all vulnerable. Just as a small gene pool places a population at risk from a change in the environment, such as a disease, the lack of variety in centralised storage systems places information at greater risk of theft.

The alternative is a decentralised system, also known as a peer-to-peer system, where resources from many potential locations in the network are mixed, rather than putting all one's eggs in one basket.

The strength of a peer-to-peer system is that its value grows as the number of users increases: all producers are also potential consumers, so each added node gives the new producer as many customers as are already on the network.

"Since all the members of a peer-to-peer network are giving as well as consuming resources, it quickly overtakes a centralised network in terms of its strength," said Crowcroft, of the University's Computer Laboratory.

The higher reliability and performance of fibre to the home, the availability of 4G networks, and IPv6 (Internet Protocol version 6) are all helping to make decentralised networks viable. In practice, a user would carry most of the data they need to access immediately with them on their mobile device, with their home computer acting as the 'master' point of contact.

"Essentially, data is encoded redundantly, but rather than making many copies, we weave a tapestry using the bits that represent data, so that threads making up particular pieces of information are repeated but meshed together with threads making up different pieces of information," said Crowcroft. "Then to dis-entangle a particular piece of information, we need to unpick several threads."

Varying the ways that our information is stored or distributed is normally done to protect against faults in the network, but it can also improve the privacy of our data. In a decentralised system where data is partitioned across several sites, any attacker attempting to access that data has a much more complex target – the attacker has to know where all bits of the information are, as opposed to using brute force at one point to access everything. "The more diversity we use in a peer-to-peer system, the closer we get to an ideal in terms of resilience and privacy," said Crowcroft.

A peer-to-peer system could also be built at a lower overall cost than a centralised system, argues Crowcroft, since no 'cache' is needed in order to store data near the user. To the end user, costs could be as low as a pound per month, or even free, much lower than monthly internet access

costs or mobile tariffs.

"We haven't seen massive take-up of decentralised networks yet, but perhaps that's just premature," said Crowcroft. "We've only had these massive centralised systems for about a decade, and like many other utilities, the internet will most likely move away from centralisation and towards decentralisation over time, especially as developments in technology make these systems attractive for customers."

More information: "On the duality of resilience and privacy." [DOI: 10.1098/rspa.2014.0862](#) . Published 21 January 2015

Provided by University of Cambridge

Citation: How can we protect our information in the era of cloud computing? (2015, January 26) retrieved 25 April 2024 from https://phys.org/news/2015-01-era-cloud.html