Cloud Computing in the Wake of MegaUploads

Joelle Vincent considers the implications for cloud computing industry following the investigation and shutting down of online storage service provider, MegaUploads.

Cloud computing has been a buzz topic for a while, as companies seek the benefit of its scalability, availability and efficiency. We are now, however, starting to see some cautionary tales of its use. The much publicised recent shutdown of online storage service provider MegaUploads raises important issues to be considered by users of cloud computing. Time and resources need to be spent on due diligence to understand what services the cloud provider is offering and to ensure that the cloud provider is an appropriate and trustworthy supplier of those services.

MegaUploads users had access to their data cut off, regardless of whether or not it is suspected of being copyright infringing material.

Background

MegaUploads was a cloud storage solution business and, according to the United States government's indictment against it, at one time was estimated to be the thirteenth most frequently visited site in the world.[1] Its shutdown is one of the largest criminal copyright cases in history. The specific claims relate to conspiracy to commit racketeering, copyright infringement and money laundering, criminal copyright infringement by electronic means and by distributing a copyrighted work being prepared for commercial distribution, aiding and abetting criminal copyright infringement, fraud by wire and aiding and abetting fraud by wire.[2]

There is sufficient drama surrounding the case to ensure that the details of it have received much attention. MegaUploads founder Kim DotCom is a larger-than-life character: reportedly a German hacker millionaire who lives in the most expensive house in New Zealand and owns 18 luxury cars with numberplates like 'HACKER', 'GUILTY' and 'GOD'.[3] The alleged facts of his arrest have included that he hid in a safe room with a sawn-off shotgun while police cut their way through the metal door.[4] Kim DotCom has since been reported to have made accusations that he was beaten by police during the arrest and that once in prison was contacted by a person who, claiming to be a prosecutor, offered to guarantee his release for a fee.[5]

However, the issue for readers of this publication and concern for legitimate users of cloud services is that all MegaUploads users had access to their data cut off, regardless of whether or not it is suspected of being copyright infringing material.

The Incident

MegaUploads offered a digital locker storage service where users anonymously upload digital files to be accessed via URL by themselves or other users.

Significantly, the MegaUploads site was structured primarily as a temporary storage solution. Unless users paid a premium fee for permanent storage, material was retained for only three months from the time it was uploaded.

It is alleged in the Indictment that this means that the main purpose of MegaUploads was to enable illegal file-sharing of material such as films, music and software.[6] Evidence referred to in the Indictment suggests that this was in fact the MegaUploads business model.[7] The site offered financial incentives to users whose uploaded files are the most popular downloads: most commonly these would be pirated copies of unreleased or newly released films and television shows.

However, legitimate use of the site had also been made by many people, including to legally share copyright material, to backup data from computers and even as a primary storage solution.

It is not known to what degree, if at all, such legitimate users will ever be able regain access to their materials. In most cases access is time-sensitive and the damage will have already been done. Access will only be restored if the alleged infringers are found innocent and resolution of the case could take months.

It even appeared at one point that the data may be deleted in the interim. MegaUploads' data hosting service provider threatened to delete the data if it did not receive the ongoing payments it was owed by MegaUploads,. Payment appeared to be unlikely given the seizure of MegaUploads' directors' assets. The data hosting service provider has since released statements that there is no imminent data loss for MegaUploads users and that it will attempt

However, legitimate use of the site had also been made by many people, including to legally share copyright material, to backup data from computers and even as a primary storage solution.

1 Superseding Indictment filed by The United States in the United State District Court for the Eastern District of Virginia on 16 February 2012, paragraph 13.

2 Indictment, filed by The United States in the United State District Court for the Eastern District of Virginia, 5 January 2012; Superseding Indictment, filed by The United States in the United State District Court for the Eastern District of Virginia, 16 February 2012.

3 Amrutha Gayathri, 'Kim Dotcom: 10 Most Strange Facts About the MegaUploads Founder' 4 February 2012, *International Business Times*.

4 Above n4.

5 Greg Sandoval, 'Bail denied again for MegaUploads' Kim Dotcom', 3 February 2012, *CNET News*.

6 Superseding Indictment filed by The United States in the United State District Court for the Eastern District of Virginia on 16 February 2012, paragraph 2.

7 Superseding Indictment filed by The United States in the United State District Court for the Eastern District of Virginia on 16 February 2012, paragraph 5.

MegaUploads suggest that jurisdiction will not necessarily be a barrier to enforcement and that the inherently global nature of cloud computing may be reflected in its legal ramifications.

to assist legitimate users to regain access.[8] In the absence of direct contractual relationships with individual users, the data hosting service provider's desire and ability to fulfil this ambition remains to be seen.

Implications

While MegaUploads does involve some extreme circumstances, it is not difficult to imagine the same user access difficulties arising with less colourful cloud computing providers. In fact, many other consumer-oriented services have already responded by altering, relocating or shutting down altogether their file-sharing oriented storage solutions.

The occurrences in MegaUploads suggest that jurisdiction will not necessarily be a barrier to enforcement and that the inherently global nature of cloud computing may be reflected in its legal ramifications. The copyright holders who are losing the most to online piracy, and are therefore the most invested in actions such as this, are the United States entertainment industry major players. So, it is likely that any future actions of this scale in relation to illegal file sharing will follow a similar model of United States Government indictment, arrest and (as will be relevant in most cases) extradition. As we have seen, the United States Government may have the right to demand access to a cloud provider's system regardless of where it is hosted and actions by law enforcement agencies in other countries in relation to such an inherently global system as cloud computing can affect users in Australia.

Lessons Learnt

What has happened to MegaUploads and its directors and users certainly does not mean that businesses should avoid using cloud computing.

As such services become increasingly available and commonplace, MegaUploads is a timely reminder to apply caution about the choice and use of a cloud solution.

Businesses looking to take up cloud computing services can minimise the risks by taking certain precautions. For example interested business should:

- research and evaluate cloud service providers for trustworthiness – not just in relation to their stance on intellectual property rights but also with regard to potential bankruptcy, which could result in loss of access for users;
- make sure they use a business-focused cloud solution, as consumer-oriented services are more likely to be used by other users for copyright infringement and become the target of investigation by law enforcement agencies, resulting in interruption of services;
- consider using a private cloud model rather than publicly driven infrastructure;
- ensure adequate contractual protection of the service relationship (for example, review access service levels and credits where those levels are not met; review maintenance windows and ensure the provider steps up to compliance with laws in conducting the service);
- be wary of employees risking data loss by independently using consumer-oriented services to store corporate data and consider establishing employee policies regarding cloud storage; and
- ensure that data stored on the cloud is always readily available in back-up elsewhere and have a plan in place in case their cloud computing solution becomes suddenly unavailable.

Joelle Vincent is a third year lawyer at Allens Arthur Robinson, in the intellectual property practice group.

---

8 Carpathia Hosting's Updated Statement on Megaupload Servers and Customer Data (2012), viewed on 23 February 2012, http://www.carpathia.com/carpathia-hostings-updated-statement-on-megaupload-servers-and-customer-data; Megaretrieval (2012), viewed on 23 February 2012, http://www.megaretrieval.com/.