Responsible Practices for Cloud Storage Services

Introduction

Cloud storage services have become an important feature of modern computing platforms, with increasing worldwide reliance upon mobile devices and location-independent enterprise computing. Cloud-based storage is becoming a necessary component of any mobile business or lifestyle. For example, there are significant security risks associated with local storage on computers, devices, or storage media that can be lost or stolen: a laptop or thumb drive left behind on a plane can expose its owner both to loss of all data or to persistent, undetectable attacks on the security of the data.

Workers who travel often prefer to rely on computers and devices available locally at their destinations without carrying their equipment and data with them. Employers may make select documents available to their employees via third-party services so that, in sensitive locations, the employees need not expose their network traffic to others. Publishers may to make their works widely available using cloud-based storage as an efficient and cost-effective alternative to direct hosting. Collaborators may share projects and large files with each other in a location where no single person controls the platform. There are countless other existing uses for cloud-based storage, and new uses are constantly evolving.

While cloud storage has been available for years, with a variety of well established and newer companies providing it, certain high-profile cases have put cloud storage in a spotlight. Some accuse customers of cloud storage services of misusing those services to carry out copyright infringing activities. Some cloud storage providers also stand accused of encouraging and exploiting those customers' abuses.

RapidShare has faced its own controversies, but for years now it has been working diligently on multiple fronts to distinguish itself as an important and responsible company in this growing industry.

Because any customer can misuse these services to engage in wrongful conduct, including copyright infringement, RapidShare, like other operators of such services, has a strong reputational interest in actively promoting legitimate uses, and discouraging illegitimate uses, balancing the needs for safe, reliable, and private storage and

communications with respect for intellectual property and the public interest in reasonable enforcement. For that purpose, RapidShare publishes this first industry manifesto of Responsible Practices for Cloud Storage Providers. It welcomes debate and further discussion that balances the legitimate expectations of all stakeholders, including copyright holders, service providers, customers, and the public.

1. It goes without saying that cloud storage services should take all steps necessary to qualify for the safe harbor for hosting services under the U.S. Digital Millennium Copyright Act. That safe harbor under American law sets standards for any company around the globe that wishes to access the American marketplace and provides protection for any such company against monetary awards and broad injunctions. Among those standards are:

a. Expeditious removal or disabling of access to allegedly infringing material or activity upon a properly formed notice.

b. Designation of an agent to receive notifications of claimed infringement, with an appropriate filing in the U.S. Copyright Office and notice clearly available on the service itself.

c. Publication and implementation of a policy calling for termination, in appropriate circumstances, of account holders or subscribers who are repeat infringers.

d. Expeditious removal or disabling of access to infringing material or activity when the provider gains knowledge of an infringement or facts or circumstances make the infringement apparent.

e. Accommodation of, and non-interference with, any industry-standard content protection technologies.

f. The strict avoidance of any direct financial benefit from infringing activity or infringing material.

g. The exercise of any right and ability to control infringement by users to bring about the cessation of such infringement.

2. Responsible cloud storage service providers will take a number of steps to go above and beyond safe harbor practices for the protection of copyright holders. They include:

a. No second-guessing or evaluating of claims made in properly formed takedown notices. The DMCA safe harbor allows the users themselves to defend their own conduct; the cloud storage service provider need not take on itself a role of judge. The service provider must step out of any dispute between a copyright claimant and an accused user, without taking anyone's side.

b. Protection against restoration of suppressed materials. Cloud storage service providers should make efforts to detect repeated efforts by users to store materials that the service provider previously deleted or disabled based on takedown notices, unless the users provided properly formed counter-notifications. This means that service providers must determine, to the extent technically feasible, unique signatures of disabled files and scan new files for identical signatures.

c. Attention to compromised or improperly disseminated user credentials. Cloud storage service providers should actively review major public

providers of access credentials of encrypted files and disable file access to those files where it appears that those credentials might be compromised or improperly published.

d. Rare compensation to customers based on download volume. Services should not provide compensation to users based on download volume unless the services have a good-faith belief that those users are properly using the storage platform to monetize dissemination of their own, or authorized, material. For example, some recording artists have adopted cloud storage services as a vehicle for monetizing their own works. This type of new business model deserves support while it does not justify giving malefactors a reward for their misbehavior. These monetization relationships should be custom designed and there should be individualized oversight of the enrollment process.

e. Termination upon substantial body of accusations without proof of infringement. Services should terminate account holders or subscribers not merely upon proof that they are infringers but when sufficient copyright holders have called their conduct into question. In such cases, services deserve an explanation from the users as to why the suspicions are unfounded.

f. Valid, current e-mail addresses of subscribers and account holders. Services should require valid e-mail addresses of subscribers and account holders in order for them to register new accounts. In the event a copyright holder seeks account holder information through valid legal procedures, the service should have access to valid e-mail address information to furnish in response, which may facilitate an inquiry to the e-mail service provider. The service should periodically test the validity of subscriber e-mail addresses and require updating of obsolete email addresses in its system.

g. Trained customer service personnel. Services should train their customer service personnel to avoid interactions with customers that appear to pertain to copyrighted material of others.

h. Default settings for stored files: only for private access of the customer. To the extent customers seek to expose files to others or to the public, they should have to override the default setting or provide access credentials to a trusted colleague.

i. Deletion. Customers should have the ability to delete their own files and access to their own files for their protection and for the avoidance of sharing.

3. Responsible cloud storage service providers should be readily accessible and complainant-friendly for both notifications and legal process. This includes the following:

a. Robust staffing of a well trained anti-abuse team to respond to notifications of claimed infringement. Service providers must deploy personnel sufficient to handle the volume of notifications that arrive, without persistent backlogs. Spikes in volume of notifications must lead to additional emergency staffing and overtime, subject only to employment law limitations on hours and working conditions.

b. Services should be amenability to service of process. Service providers should either reside in a country that belongs to the Hague Convention for the Service of Process Abroad or should voluntarily comply with requests to waive service

of process with respect to subpoenas for user information. They should also reside in a jurisdiction that shows respect for copyright law.

c. Collaboration to facilitate notification process. Where a copyright holder has developed a history of frequent or large-scale notices, the service provider should offer it an opportunity to collaborate with the service provider to build a notification tool to automate creation of DMCA-conforming notifications of claimed infringement in a way that will ease burdens on copyright holders and facilitate speedier handling of those notifications by the service provider.

d. Visible management. Service providers should make public the identities of the persons in its top executive ranks. Knowledgeable representatives of the company should be available for press, customer service, and sales inquiries.

e. Visible policies. Service providers should make clear their privacy policies and details about information that is available to them about their account holders or subscribers and other users.

f. Inspection as last resort. While cloud storage service customers normally have a right to expect privacy of their stored materials that they have not shared publicly, privacy policies should establish that service providers retain the right to inspect files of repeat accused infringers or accused violators of the service's terms of service who, after reasonable notice to them by the service provider, have made no good-faith counter notifications or efforts to justify their conduct as non-infringing or as not violating the service provider's terms of service. A service provider shall serve notice on the customer two weeks before any such inspection, at that customer's last known e-mail address, giving the customer sufficient time to oppose inspection or voluntarily to remove its materials from the service.