

MEGA LIMITED

**ANALYSIS OF THE EVIDENCE RELATING TO ALLEGATIONS IN A
NETNAMES REPORT ON CYBERLOCKERS**

**A REPORT ON MEGA'S BUSINESS PRACTICES AND LEGAL &
REGULATORY COMPLIANCE POLICIES**

CONTENTS

	Page
A. INTRODUCTION _____	2
i. Purpose of this report.....	2
ii. A summary of our findings.....	3
B. MEGA: AN OVERVIEW _____	6
C. LEGITIMATE CLOUD-STORAGE SERVICES VS. CYBERLOCKERS _____	8
i. Legitimate cloud storage providers.....	8
ii. How does a cyberlocker differ from such providers?.....	9
D. ANALYSIS OF CHARACTERISTICS IDENTIFIED IN THE NETNAMES REPORT __	11
1. STORING AND SHARING CONTENT	11
i. Sharing content.....	11
ii. Additional services designed to support the storage of data.....	13
iii. Additional products.....	15
iv. Analysis of files held by Mega – types of content stored	15
2. BUSINESS MODELS OPERATED BY PLATFORMS	18
i. Basic and premium accounts.....	18
ii. Advertising.....	22
iii. Affiliate programme.....	23
3. COMPLIANCE WITH REGULATORY REGIMES	24
i. Legal requirements upon Mega as a platform operator.....	25
ii. Notice and takedown policies	27
iii. Takedown statistics.....	30
iv. Third-party linking sites	33
E. SUMMARY AND CONCLUSIONS _____	35
ANNEX A _____	37
ANNEX B _____	40
ANNEX C _____	41

A. INTRODUCTION

Mega is a cloud hosting and storage provider which provides encrypted, cloud-based file-sharing and collaboration services to millions of businesses and individuals. Mega is different from many other major cloud storage providers as it utilizes browser-based 'User Controlled Encryption', which automatically encrypts all data before it is transferred to and stored on Mega's cloud service. This means that only the user controls the encryption key (to which Mega has no access), providing a high level of privacy and security to its users. It is for this reason that Mega is able to position itself as "The Privacy Company."

Olswang LLP is an international law firm based in London with offices around Europe and in Singapore, and is renowned for its deep industry expertise in technology, media and telecoms. Olswang regularly advises on anti-piracy matters and recently supported the Intellectual Property Adviser to the British Prime Minister in drafting a set of recommendations for the Secretary of State to fight online piracy. It also supports high profile clients in their fight against piracy, and in particular has advised the former UK Film Council on the creation of findanyfilm.com (now run by the British Film Institute), a site for consumers to find any film and learn where it can be watched, acquired or downloaded legally.

Olswang's market-leading media litigation practice is widely recognised as one of the leading defamation practices in the UK and for a number of years has been consistently ranked in the top tiers of all major legal directories.

i. Purpose of this report

In September 2014 the UK-based online brand management agency NetNames published a report into cyberlockers that was commissioned by the Digital Citizens Alliance, a US-based internet campaign group backed by the Motion Picture Association of America. The report, entitled *"Behind the Cyberlocker Door: A report on how shadowy cyberlocker businesses use credit card companies to make millions"* accuses Mega of being a "cyberlocker" and profiting from "content theft".

The term cyberlocker has become a pejorative term used to describe a platform designed specifically to enable the mass infringement of copyright and to share illegal content. Cyberlockers pose a substantial threat to rights holders, particularly the film industry which claims to be significantly adversely affected by content theft through the use of cyberlocker sites. In 2010 the COO of Paramount Pictures, Frederick Huntsberry described cyberlockers as the "*preferred method by which consumers are enjoying pirated content*".¹

The NetNames report claims Mega is one of a number of cyberlocker platforms specifically established for the sharing of infringing content and makes a number of allegations against Mega

¹ <https://journals.dartmouth.edu/cgi-bin/WebObjects/Journals.woa/xmlpage/4/article/426>

concerning its business model and the extent to which it complies with relevant legal and regulatory requirements.

The NetNames report has been extremely damaging to Mega. Most notably, it has been relied upon by United States Senator Patrick Leahy to apply pressure to major payment providers and credit card companies to withdraw their services from those identified in the NetNames report.²

Olswang has been commissioned by Mega to analyse the NetNames report and carry out a forensic analysis of the evidence and data upon which the NetNames allegations have been made, in order to establish whether there is any factual basis for these allegations. This report sets out our conclusions and analysis.

Grant Thornton New Zealand Limited were retained by Olswang to provide independent assurance on the data relied upon in this report. The data analysis relied upon in this report was either tested, validated or re-performed by Grant Thornton.

ii. A summary of our findings

In summary, Olswang has concluded that the allegations in the NetNames report are highly defamatory of Mega and appear to have no factual basis whatsoever. The NetNames report contains numerous factual inaccuracies and methodological errors and draws conclusions that are entirely wrong. In fact, Mega cannot be said to share a single one of the cyberlocker characteristics specified in the NetNames report. For instance:

- **There is no evidence that the bulk of files stored on Mega are infringing:** The NetNames report states that the *"overwhelming bulk of files found on cyberlockers are infringing,"* whilst *"searches by NetNames for infringing materials stored on legitimate cloud services found negligible amounts of content."* Analysis of the size of files uploaded to the Mega platform over a recent typical 24-hour period showed that just 2% were larger than 20MB. This demonstrates that the overwhelming majority of files uploaded to Mega are significantly too small to be likely to be infringing video files. Since infringing video files are alleged by NetNames to be the most significant source of cyberlocker traffic (and therefore profit), it follows that Mega is not a haven for such infringement.
- **Mega's target audience is entirely different from that of a cyberlocker:** Mega's services and platform features demonstrate that they are principally targeted towards 'primary' users, who use the Mega platform to upload and store content for personal use, rather than 'secondary' users who would merely use the Mega platform as a source from which to download files. This is entirely contrary to the NetNames description of how cyberlockers function; namely by encouraging secondary users to pay to download material.

² See <http://www.leahy.senate.gov/download/binder1>

- **Mega provides services that would be of no benefit to a cyberlocker:** The emphasis on primary users is reflected by the fact that Mega provides sophisticated encryption technology, that it includes browser extensions, provides desktop and mobile apps to allow users to sync across different devices and mobile platforms, provides a Software Development Kit (SDK) and that its affiliate program is only targeted towards software developers. None of these core features of the Mega platform would have any application to secondary users solely interested in downloading content, towards whom the platform would be targeted if it were a cyberlocker.
- **Mega's platform is not attractive for users who wish to distribute content to a mass audience:** One of Mega's key selling points is its User Controlled Encryption. In order to share files on the platform, a user must share the decryption key. That choice must be made consciously by the user sharing the key or including it in a shareable link. In addition, the system is designed so that one party cannot "reshare" a link that has been shared with them. This is quite different from other forums where material that is downloaded will automatically be available for upload by others, for instance in a peer-to-peer sharing swarm. If a user's aim is to share infringing content, it would not make sense for them to choose an encryption-based privacy platform that requires additional steps to be taken to share content. This provides an additional barrier to the ability to share content widely and indiscriminately.
- **Mega's business model is entirely different from those used by cyberlockers:** The NetNames report describes the cyberlocker business model as the service of advertising and charging users for access to enhanced download features, such as the ability to conduct faster and multiple downloads. In contrast, (i) Mega does not currently host any advertising on its platforms, and (ii) its primary revenue stream is through premium accounts which offer signed-up users additional storage and services. Rather than enhancing the ability to just download content, Mega's services enhance the user's ability to store content, e.g. by providing extra storage. Mega's business model is therefore identical to most other major cloud storage providers such as Box, Apple iCloud, Microsoft OneDrive, Dropbox and Google Drive.
- **Mega complies with the law:** Mega operates robust compliance and takedown procedures in accordance with local and international laws. Again, this is entirely at odds with what would be expected of a cyberlocker that was designed specifically to support mass copyright infringement.

In coming to these conclusions, Olswang has also identified a number of aspects in which the NetNames report's methodology, in particular as to the content of the files stored on Mega, is wholly inadequate.

By way of example:

- **The analysed file sample is too small and unrepresentative:** In preparing the report NetNames only analysed a tiny fraction of the total files stored on Mega in their effort to determine the proportion of total files that are likely to be infringing. The sample was

unrepresentative as it only looked at publicly available files and it entirely disregarded the vast majority of files stored on Mega, which are encrypted and not publicly shared.

- **The analysis of the files itself is unreliable:** Furthermore, although the NetNames report makes claims as to numbers of infringing files, no analysis was undertaken of the content of the files themselves. The NetNames report only looked at filenames. Clearly this does not provide an accurate basis on which to determine the contents of a particular file, as file descriptions vary hugely between users and may bear little to no relation to the contents of the file.

Not only do we consider there to be no basis to conclude that Mega is a cyberlocker, we also consider that the conclusions drawn in the NetNames report are inherently unreliable and fundamentally flawed. Full details of these methodological flaws are set out in the body of the report below.

In order to assist Mega's customers and industry partners, this report sets out in detail Olswang's analysis of the NetNames report and the reasons why Mega should not be considered a cyberlocker, as well as a summary of the extensive measures that Mega takes to maintain robust legal and regulatory compliance policies and procedures.

B. MEGA: AN OVERVIEW

Mega provides encrypted, cloud-based storage services to both individual and business users. Whilst the service shares a number of similarities with various other well-known cloud storage platforms such as Box, Dropbox, Google Drive, Microsoft OneDrive and Apple iCloud, Mega differs by providing automatic user controlled encryption. This means that when users upload files to their Mega cloud (or save them locally to a folder that is automatically synced to their Mega cloud account), the files are automatically encrypted locally on the user's device (computer, tablet or phone) before being uploaded, and only the user controls access to the encryption key for the data.

This so-called 'User Controlled Encryption' (UCE) means that Mega itself does not know the content of any files uploaded to its system and cannot review that content unless a user voluntarily discloses the decryption key for that content, allowing the content to be decrypted by whoever has that key. In the wake of recent scandals into hacking and intrusions into digital lives, this addresses a real need for businesses and individuals to have a fast, encrypted, cloud-based service that enables private, online communication and collaboration.

The Mega service was launched on 20 January 2013. As at the end of April 2015, Mega had over 18 million registered users and is adding on average around 30,000 new registered users per day. Since the service launched on 20 January 2013 users have stored more than 5.5 billion encrypted files in the Mega cloud, and the total number of files uploaded per day averages over 17 million.

Mega Corporate Structure and Board

Mega Limited is a private limited company registered in New Zealand with company number 4136598. It is privately owned by 17 local and international investors. Details of its ownership and structure are publicly available on the New Zealand Government's Companies Register.³ On 24 March 2014, it announced plans to be listed on the New Zealand Stock Exchange (NZSX) through a reverse listing into TRS Investments Limited, a company currently listed on the NZSX. In May 2015 this proposal lapsed but it is still intended that the company will list on a recognized stock exchange in 2015.

At present, Mega has a board of three directors but has undertaken a search for suitably qualified and experienced directors to be appointed. Mega has an independent CEO, technical team and Board who are focused on listing the company and meeting the relevant regulatory requirements.

Current directors are:

- Stephen Hall (Chairman);

³ See <http://www.business.govt.nz/companies/app/ui/pages/companies/4136598>. Details of the ownership and control of the corporate shareholders of Mega can also be obtained from the same site.

- Brian Clarkson; and
- Zhaowu Shen.

Proposed new appointments for independent directors are:

- Andrew Simmonds. Mr Simmonds is Managing Partner of Simmonds Stewart, a boutique corporate and commercial law firm for technology companies and investors which he co-founded in 2006. He has extensive experience advising on international technology related transactions.
- Glen Chean. Mr Chean is the New Zealand Marketing Director for Huawei, a world-leading provider of telecommunications infrastructure, services and devices. He has over fourteen years' experience in the NZ consumer electronics industry, having held positions with a number of leading consumer electronics companies including Sony, Samsung and LG.

Further details of the current directors and senior management are provided in **Annex A**.

As is apparent, the directors of the company are individuals with a wealth of experience in the growth and development of successful companies within the technology market.

C. LEGITIMATE CLOUD-STORAGE SERVICES VS. CYBERLOCKERS

Cloud storage services are used widely by both individuals and businesses to back-up, store and share content online in a controlled fashion. Cloud storage is increasingly being used by businesses as it provides a cheap, easy-to-use way to store large volumes of data securely and the services require very little up-front or long-term end user investment.

In 2013 the number of cloud-based online service users was estimated at 2.4 billion and this number is projected to increase to 3.6 billion by 2018.⁴ In 2014, an average of 21% of European Union citizens used a cloud storage system to store files and 15% to share files.⁵

i. Legitimate cloud storage providers

Like many other well-known legitimate cloud storage providers such as Box, Dropbox, Google Drive, Microsoft OneDrive and Apple iCloud, Mega provides users with a personal cloud-based online 'drive' to which they can upload and store content.

By storing content in the cloud in this way, users may access that content from any location that has internet access. This has a number of benefits, including:

- greatly increased flexibility over the content itself, with the ability to access it from anywhere;
- the ability to access and share content over multiple devices such as a desktop computer, tablet and/or smartphone;
- a safe and secure means of backing-up content remotely to guard against data loss;
- the ability for users to securely share content and collaborate with others by providing them with access to certain files, folders or online workspaces rather than having multiple copies of those files, folders or workspaces sent backwards and forwards between individuals;
- the ability to store and share much larger files than would be possible with email;
- the ability to integrate deep folder structures and organise a large number of files with ease from a single online location; and
- seamless integration with devices through browser extensions and mobile apps.

⁴ <http://www.statista.com/statistics/321215/global-consumer-cloud-computing-users/>

⁵ INCIBE (Spanish National Cybersecurity Institute) report, *Security in cloud storage services: Analysis of Dropbox and Mega*

ii. **How does a cyberlocker differ from such providers?**


In contrast to legitimate cloud storage services, the term "cyberlocker" is used pejoratively to describe a platform that has been intentionally designed to support, encourage and promote the mass sharing of files (primarily copyright infringing files) among strangers with no regulation or controls, in order to profit from that infringement through advertising and the sale of additional features.

The NetNames report's definition of cyberlockers is:

"Online services that are intentionally architected to support the massive distribution of files among strangers on a worldwide and unrestricted scale, while carefully limiting their own knowledge of which files are being distributed. The link to a user's file stored on a cyberlocker can be posted to any location for any user to access: cyberlockers generally place no limits on who can download or stream a file."

The term cyberlocker is commonly used to refer to platforms that encourage the illegal and/or unauthorised sharing of copyrighted video files in particular, and indeed this is very much the focus of the NetNames report.

David Price, who when the NetNames report was released was the Director of Piracy Analysis of NetNames, gave a presentation on the findings of the NetNames report at the Information Technology & Innovation Foundation in Washington DC on 18 September 2014.⁶ The presentation included the following slide summarising NetNames' definition of a cyberlocker by reference to the differences between how a cyberlocker and a cloud storage service operate:

DEFINING CYBERLOCKERS		
	CYBERLOCKERS	CLOUD STORAGE SERVICE
Online storage of user-uploaded content	Yes	Yes
Unrestricted and unlimited distribution	Yes	No
Rewards users for wide distribution	Yes	No
Bandwidth limits	No	Yes
Repeat infringer policies	No	Yes
Personal file synchronisation	No	Yes
Majority of content infringing	Yes	No
Who is the client?		
	Cyberlockers	Cloud storage services
	The downloader who	The uploader who
	views advertising	pays for storage space
	pays for a premium account	pays for synchronisation
		

⁶ <http://www.itif.org/events/stealing-profit-close-look-revenue-online-piracy-websites>

Our report demonstrates that Mega firmly identifies with each of the characteristics associated with a cloud storage service and has none of the characteristics exclusive to a cyberlocker as identified by NetNames. The only possible conclusion that can be drawn from the facts is that Mega is not a "cyberlocker" according to NetNames' own definition of this term.

The remainder of this report contains an analysis of each of the alleged "cyberlocker" characteristics in the NetNames report and whether they apply to Mega.

D. ANALYSIS OF CHARACTERISTICS IDENTIFIED IN THE NETNAMES REPORT

From our analysis of the NetNames report and how it relates to Mega, we consider that the key factors in distinguishing between cyberlockers and legitimate cloud storage providers fall broadly under the following headings:

- Storing and sharing content
- Business models operated by platforms
- Compliance with regulatory regimes

In determining whether Mega can be considered a cyberlocker according to the NetNames definition above, we have analysed in detail these aspects of the Mega platform to determine which, if any, demonstrate the qualities typically associated with cyberlockers.

1. STORING AND SHARING CONTENT

i. Sharing content

The key characteristic that NetNames uses to identify a cyberlocker is the extent to which the platform has been designed to support and encourage the sharing of files on a massive scale. Indeed, the NetNames definition of cyberlockers describes them as "*online services that are intentionally architected to support the massive distribution of files among strangers on a worldwide and unrestricted scale.*" (emphasis added)

In common with all other major legitimate cloud storage providers (such as Dropbox, Apple iCloud, Box, Microsoft OneDrive and Google Drive) a feature of Mega's platform is that it provides users with a limited number of ways to share content that is stored in their cloud.

To share content stored on Mega, users can share any folder within their cloud drive with others who also have a Mega account. Alternatively, users can generate a link to any of their files or folders and export the link, making it accessible to someone without a Mega account. The decryption key can be shared with the link or can be sent separately, perhaps using a different method of communication to ensure that the confidentiality created by the encryption is maintained. This feature might be used by a business user to ensure that the confidentiality of their business information is maintained. Users can give three access levels to those that they share folders with: read-only access, read/write access (files can be added, but not deleted), and full access (files can be added and deleted).

It is therefore the user who is responsible for deciding to whom they wish to grant or deny access to their data. Mega itself does not have access to any decryption keys that have not been made

available to it by the user, and is unable to view what each user stores without the user providing the encryption key to do this.⁷

These sharing mechanisms are extremely similar to those provided by other legitimate cloud storage services and do not make Mega any more attractive for those wishing to upload infringing content and share it with large numbers of users than any other legitimate provider. By way of comparison, the following well-known cloud storage providers also provide the ability to share content in a limited manner:

- On Google Drive, a user may also share a file by generating a link. That link can then be shared via email, Google+, Facebook, Twitter or other communication methods. As with Mega, a user can decide whether that link should be available for anyone with access to the link or should be restricted to specific persons. They can also choose whether those to whom the link is shared can view, comment or edit the content of the link. Users also have the ability to give access to files on Google Drive by making them attachments to emails. Mega does not operate an email service and does not offer this option.
- On Box, a free user may share a file by sharing it via a link, emailing it or embedding it. If the user decides to share the file via a link, they may choose to create a public link or create a link within the folder to be shared with others who have been granted access to that folder. If they create a public link, they can specify whether it is downloadable or read only. Only users with a premium account can password protect their links. This is a premium feature which is unavailable on free personal accounts, so only premium users are able to add this level of protection to their content.⁸

The distinction between Mega and other legitimate cloud storage providers is the encryption technology which provides all users (regardless of whether premium account holders or not) with exclusive control of the decryption key necessary to access their content. Indeed, the inherent design of the Mega platform, the central feature of which is UCE to encrypt files to ensure privacy and security for its users, is in fact entirely at odds with NetNames's description of a cyberlocker designed to encourage the wide-scale sharing of files. It is therefore plain that the Mega service has not been "*intentionally architected to support the massive distribution of files among strangers*".

The NetNames report goes on to state that "*Most [legitimate] cloud storage services [...] allow their clients to share files with others who also have a reason to access the file*" (emphasis added). We assume that what NetNames means by this is that legitimate cloud storage services systems are targeted at users who wish to share with other specific users for a specific common purpose (e.g. collaborating on a book, negotiating a legal agreement, or sharing family

⁷ However, Mega does have certain information about the type of files stored, including their size, please see page 15 below.

⁸ <https://support.box.com/hc/en-us/articles/200519848-Can-I-password-protect-my-shared-links->

photographs), rather than simply making a file available indiscriminately to anyone. This is a characteristic that Mega shares with those legitimate cloud services. Furthermore, the fact that all content on Mega is encrypted using UCE before being uploaded clearly makes it less likely that files will be shared indiscriminately.

ii. **Additional services designed to support the storage of data**

A further feature that NetNames characterises as an important indicator of cyberlockers is that they are targeted primarily at the many users who pay to download content (i.e. secondary users), whether per file or via a subscription, rather than those who upload content to the platform.

In contrast, many of the key features and benefits of the Mega platform have been designed solely with the primary user (i.e. the uploader) in mind. The most significant of these are (i) Mega's use of UCE technology; (ii) the ability for users to synchronise files across devices; and (iii) the provision of additional browser extensions and mobile apps to make the uploading of and access to files by the user more seamless. We deal with each of these in turn below.

User Controlled Encryption technology

Despite the many benefits of traditional cloud storage, some of the most commonly-cited weaknesses of these services are privacy and security.⁹ By uploading personal content to remote servers and through channels over which the user has no control, the risk of that data becoming compromised is likely to be significantly increased.

Mega's platform has been designed from the ground up with this in mind, to provide users with complete privacy over their data both when data is being transferred and when it is being stored in the cloud. Commonly if a user wanted to achieve that level of encryption security it would have to use two services: one to encrypt the data before transfer; and one to store the data. Mega rolls both into one platform.

As stated above, Mega uses UCE for the private and secure online storage and communication of data for both businesses and individuals. Mega considers this to be a unique selling point in the cloud storage market.¹⁰ Traditionally, encryption has been complicated to implement and requires the installation of additional software by users. By contrast, Mega's browser-based encryption does not require the installation of additional software. It has been designed around modern HTML5 internet technology and runs automatically in the user's browser.

⁹ <http://www.techradar.com/news/internet/data-privacy-how-safe-is-your-data-in-the-cloud--1170332>; <http://www.out-law.com/en/articles/2015/march/security-and-privacy-issues-main-barrier-to-government-cloud-deployment-in-eu/>

¹⁰ Mega is aware of other commercial providers that offer UCE (such as Wuala, Spideroak, Tresorit, Peerio, Stackfield etc) but believes the user experience is not as simple as with Mega.

From the perspective of considering whether or not Mega is a cyberlocker, this is striking for three reasons:

- Firstly, the primary benefit of this feature, the private and secure transmission and storage of content, is targeted towards the primary user and does not encourage the indiscriminate sharing of content favoured by cyberlockers.
- Secondly, the technology required to provide UCE is extremely complex and requires a considerable amount of investment in developer time to implement. A cyberlocker designed to support the wide-scale, indiscriminate sharing of files would have absolutely no use for such technology and there would therefore be no incentive to invest in implementing it.
- Thirdly, the NetNames report alleges that cyberlockers often spread malware and viruses, for example, because they require download of additional software or carry advertising that encourages such download. However, the browser-based encryption used by Mega significantly minimizes the risk from malware and infection as it does not require the installation of additional application software by the user and Mega does not host advertising. In addition, the Mega code checks and certifies each piece of application code that is downloaded and run in the user's browser.

File synchronization and mobile use

Another characteristic associated with the NetNames definition of a cyberlocker is that contrary to legitimate cloud service providers, cyberlockers do not support mobile use or allow file synchronization between a user's devices¹¹. This is because their services are targeted towards secondary users who download content rather than primary users who principally store and access content for their own purposes, often across different devices.

Similar to other legitimate cloud storage providers such as Microsoft OneDrive, Apple iCloud, Google Drive, Box and Dropbox, Mega has developed and provides file synchronization for both computers (Windows, OS X and Linux) and mobile (Android, iOS, Blackberry and Windows Phone) devices. Its 'sync' product replicates selected desktop folders and files with the same folder structure in the cloud. Its mobile applications allow users to sync media to the cloud from a smartphone or tablet and are available to download from all major app marketplaces.¹² We understand that cumulatively, these mobile applications provided by Mega have been downloaded onto more than six million unique devices¹³.

¹¹ See for example page 5 of the NetNames report.

¹² See for example <https://itunes.apple.com/nz/app/mega/id706857885?mt=8> and <https://play.google.com/store/apps/details?id=nz.mega.android&hl=en>

¹³ Device installs as at 30 April 2015: Android: 3.52m, Apple iOS: 2.76m, Windows Phone: 140,449

The fact that Mega is accessed by mobile app by a large number of its users suggests that it is not being used by them to download or share infringing video content, which would typically involve files that are too large for most handsets to capably handle. We would instead expect that this would be carried out by users from desktop or laptop computers, which have both much more capacity for storing large files and are better equipped for consuming content directly from the device due to their larger displays.

Furthermore, file synchronization has little to no benefit to secondary users only using the Mega service either as a platform to download files or to those who wish to use the platform to widely share infringing content with others. There would be no financial incentive for a platform targeted towards such users to invest in and implement this functionality. However, Mega's file synchronization capacity appears to have been simply ignored by NetNames in its report.

iii. Additional products

Mega has stated that its overall aim is to protect the privacy of customers' digital information through the development of products relying on UCE. These products require significant investment and expertise. It has recently released a beta version of MegaChat, a service designed for primary users to make encrypted audio and video calls. We also understand that it is currently developing a service for encrypted text messages and plans to develop encrypted email.

It would not be part of a cyberlocker's business model for it to consider investing in and developing such products since they do not support the indiscriminate mass sharing of infringing material, identified by NetNames to be their central means of making profits.

iv. Analysis of files held by Mega – types of content stored

Furthermore, analysis of the files presently stored on Mega's servers does not suggest that the bulk of files are likely to be infringing video files, as implied by the NetNames report.

Given that the files stored on the Mega platform are encrypted, there is no way to analyse all files stored or to view and identify those that are likely to be infringing (in particular, video files). Even if this were technically or logistically possible, it would be difficult to determine the percentage of such files which constitute potentially infringing material. For example, in many jurisdictions the law allows a user to upload a copy of a CD or DVD that they already own for personal use or backup, so the mere presence of a large media file (such as a video) on the Mega platform would not necessarily be evidence of a copyright infringement.

Analysis of the size of files uploaded to Mega over a recent typical 24-hour period, showed that of the approximately 21.4 million files uploaded that day, **98%** were less than 20MB in size.¹⁴ Files

¹⁴ Analysis shows that the 24-hour sample period falls within the usual pattern of the volume of data uploaded to Mega on a daily basis over the past eight months.

of this size are unlikely to be infringing video content. By way of illustration, a two-hour standard-definition movie is about 1.5 GB in size, and a two-hour high-definition movie is about 4 GB in size.¹⁵

The various privacy features built into the Mega platform therefore mean that it is only possible to make general conclusions about the overall nature of the content stored. On the assumption that the file types most easily identifiable as potentially infringing will be video files (and indeed this appears to be the focus of the NetNames report), it appears that these could only constitute a very small proportion of the total files held on Mega's servers.

On the basis of all the above evidence in this section, the much more reasonable conclusion is that Mega principally is being used by users to store images and documents for personal and/or business use and not to store or share any video content, let alone infringing video content.

Flawed methodology of NetNames report

The NetNames report purports to analyse the content held on Mega's servers. However, the methodology used in carrying out this analysis is fundamentally flawed.

The methodology used by NetNames involved analysing the titles of "a random sample of 500 files" identified through third-party search engines by conducting searches based on "agnostic and unbiased" search terms. From these search results alone, the researchers decided the "likely copyrighted status" of each of the 500 files based on whether the name of the file was classified by them as being "commercially available". An inference was then drawn that files with names that were classified as "commercially available" were infringing content.

The precise methodology used is described in the NetNames report as follows:¹⁶

"During April and May 2014, NetNames' Discovery Engine technology – an automated internet search, retrieval and categorization system – was used to crawl the internet looking for links to files held on the thirty cyberlockers analyzed in this research. Crawling began at major search engines such as Google and used all two letter or longer words from the Dale/Chall simple word list as initial 'seeds'. Each of those words were sent to search engines in combination with the names of the direct download cyberlockers included in the research. For instance, some sample search terms were 'afternoon 4shared', 'aunt depositfiles' and 'ache sockshare'. This helped ensure that the searches performed were agnostic and unbiased towards any particular type of content.

Each page returned to the Discovery Engine was automatically examined for any links that may be available for any of the thirty cyberlockers. Each link was then automatically

¹⁵ <https://support.apple.com/en-us/HT204370>

¹⁶ See pages 41-42 of the NetNames report.

followed to the cyberlocker and the filenames of the content located on the cyberlocker was recorded. Files were not downloaded or further analyzed. For each cyberlocker, a random sample of 500 files in total was classified on the basis of the filename. Each of the 500 files was then analyzed for likely copyrighted status (except for those files which could not be identified and files that were identified as pornography)."

On this basis, NetNames concluded that, of the 500 publicly shared files stored on Mega that were analysed, 407 *"were commercially available and believed to be infringing"*.

This methodology is fundamentally flawed for a number of reasons:

- Firstly, the analysed sample of 500 files was taken from files which have been shared publicly by Mega users online. As explained above, UCE automatically encrypts users' files stored on the Mega platform and the overwhelming majority of Mega users do not make their files publicly available in this way. The sample of files analysed is therefore not representative of the vast majority of encrypted files stored on the site. It is likely that those who wish to share infringing content with a wide audience would do so by making files publicly available. On the same basis, it would therefore be reasonable to conclude that the publicly available files selected by NetNames are more likely to be infringing than the majority of the encrypted files. In other words, the sample is inherently biased towards finding infringing content.
- Secondly, the number of files analysed was extremely small when compared with the overall number of files on the server. In September 2014, when the NetNames report was published, Mega had approximately 2.5 billion files stored on its servers. This means that the sample of files analysed represents just 0.00002% of the total number of overall files.
- The conclusion that files were *"commercially available and believed to be infringing"*, was drawn purely on the basis of the name of each file. The NetNames report makes clear that the actual files identified *"were not downloaded or further analyzed"*.
- The report does not give any explanation for when a title is deemed to be *"commercially available"*, or what this is intended to mean. The inference that anything with a *"commercially available"* title is automatically infringing is incorrect and heavily biased towards an effort to identify potentially infringing content rather than an objective analysis of a random sample of content.

Furthermore, a number of key points from NetNames' methodology were left entirely unexplained, for instance the actual key words used for the Mega searches, how many links were generated from the Dale/Chall word list for Mega and how NetNames treated any dead or invalid links (which could distort the statistics).

From this analysis, it is plain that the conclusion drawn in the NetNames report that 81.4% of the material stored in Mega is *"commercially available and believed to be infringing"* content is wholly unsupported. No analysis has been conducted by NetNames as to the actual content of the files

identified and in any event the content that has been identified is from an extremely small sample size that is biased towards infringing content.

It is of course the case that all cloud storage providers are likely to have a certain number of users who share content in a manner that is infringing. It is for this reason that legitimate providers operate notice and takedown policies and benefit from intermediary liability safe harbour regimes in respect of content uploaded by their users of which they are unaware (see Section 3 below). It is therefore possible that certain of the publicly shared content identified by NetNames in the sample taken is infringing; in this sense, Mega is no different from other legitimate providers who have no control over what users upload. Like those other providers, Mega operates stringent notice and takedown procedures for the removal of such content.

However we do not consider it possible on the basis of the above to conclude that the amount of infringing content on Mega is proportionately any higher than any other legitimate provider.

2. BUSINESS MODELS OPERATED BY PLATFORMS

The NetNames report describes the cyberlocker business model as "*designed around content theft*" and alleges that cyberlockers make millions of pounds in annual revenue "*by operating as hubs for the for-profit distribution of infringing digital copyrighted content.*" It alleges that this model is based on attracting customers who desire to download and share popular, infringing content, and to that end, "*cyberlockers generally pay or provide incentives to those who distribute popular infringing content and discourage the use of their services for reliable data storage.*"

On this basis, Olswang again concludes that Mega's business model is entirely at odds with NetNames' own description of those used by cyberlockers. We set out our findings in further detail below.

i. Basic and premium accounts

Firstly, the NetNames report sets out the typical revenue sources and outgoing costs of the "*cyberlocker business model*" as follows:

- Primary sources of revenue:
 - Payments for premium accounts
 - Advertising
- Primary costs/outgoings:
 - Incentive-based payments made to affiliates
 - Hosting costs
 - Staffing costs

Plainly, these factors are common to almost all cloud storage providers, whether "legitimate" or not. Payments for premium accounts are the principal revenue sources for most legitimate cloud storage providers. The "freemium" pricing strategy, by which a basic product or service is provided free of charge but money is charged for an enhanced product with additional "premium"

features and/or functionality, is a common business model for the provision of cloud-based storage and many other internet services.

As a preliminary point, therefore, it would be entirely insufficient to distinguish cyberlockers from legitimate cloud storage providers on the above analysis alone.

Whilst both cyberlockers and legitimate cloud storage providers offer basic and premium accounts to users, according to NetNames the key difference between them is that legitimate providers' plans are typically structured to provide enhanced services relevant to the user's ability to store content, whilst plans offered by cyberlockers are instead geared towards the user's ability to download content. For example, NetNames finds that Turbobit and Rapidgator's premium services offer increased download speeds for premium account holders.¹⁷

Mega, on the other hand, offers the same download speed to all of its users (regardless of whether a user is a premium account holder) and, as illustrated below, falls squarely within the first of these categories.

Comparison of cloud storage services

Provider / Plan	Storage	Bandwidth	Price
Mega	50 GB	10 GB/mth	Free
	200 GB	1 TB/mth	€4.99/mth
	500 GB	2 TB/mth	€9.99/mth
	2 TB	4 TB/mth	€19.99/mth
	4 TB	8 TB/mth	€29.99/mth
Google Drive ¹⁸	15GB	No limit unless Google deems use to be "egregious" ¹⁹	Free
	100GB		\$1.99/month
	1TB		\$9.99/month

¹⁷ Page 13 of the NetNames report and <http://turbobit.biz/>

¹⁸ <https://support.google.com/drive/answer/2375123?hl=en>

¹⁹ <https://productforums.google.com/forum/?hl=en#!category-topic/docs/sharing/Cvr2QPmmsds>

OLSWANG

	10TB 20TB 30TB		\$99.99/month \$199.99/month \$299.99/month
Dropbox ²⁰	2GB 1TB Business packages: 5 TB for 5 users	20GB/day (links only) ²¹ "about 200GB"/day (links only)	Free £7.99/month £11/user/month
Apple iCloud ²²	5GB 20GB 200GB 500GB 1TB	No publicly available information was found.	Free £0.79/month £2.99/month £6.99/month £14.99/month
Box ²³	10GB 100GB Unlimited	10GB/month for free accounts 1TB/month for paid accounts ²⁴	Free £7/month if individual; £3.50/month for business with 3-10 users Business use: £11/user/month for minimum of 3 users

²⁰ <https://www.dropbox.com/pro>; <https://www.dropbox.com/business/buy>

²¹ <https://www.dropbox.com/help/4204>

²² <https://support.apple.com/en-is/HT201238>

²³ https://www.box.com/en_GB/pricing/; <https://app.box.com/signup/personal>

²⁴ <https://support.box.com/hc/en-us/articles/202985243-How-Does-Box-Measure-Bandwidth-Usage->

Basic accounts

The NetNames report states that typically a direct download cyberlocker will offer "*a free basic restricted service to users. For instance, only one file is allowed to be downloaded at any one moment, files above a certain size cannot be downloaded, transfer speeds are capped, usually at around 100Kb/s; and users have to sit through a wait periods before a download can begin*". As identified above, this is therefore only relevant to the user's ability to download content.

By contrast, Mega's basic service offers 50GB of storage and the same download speed as its premium accounts (subject to a bandwidth limit of 10GB a month). Furthermore, Mega does not cap download speeds, limit the number of files or amount of data any user may download in any particular period, or impose waiting periods before a user may download content.²⁵ In this way, Mega's basic service is similar to those provided by many other major legitimate providers.

Mega's basic service therefore does not share any of the characteristics of a cyberlocker set out in the NetNames report.

Premium Accounts

As can be seen from the table above, Mega's premium packages also mirror those provided by other legitimate storage providers by offering users greater storage space and bandwidth, rather than increasing the extent to which users can download content. In this regard, the packages offered by Mega are clearly targeted towards primary users and are also very similar to those offered by other major storage providers.

It is clear from the above that both Mega's free and premium services are designed primarily for users interested in storing data rather downloading content from others.

Mega offers large volumes of cloud storage to its users (up to 4 TB). There are a number of legitimate reasons why users would require large volumes of cloud storage, such as:

- Sharing of recorded and annotated, Computer Game tournaments (original non-breaching content);
- Backups & restoration of computer systems for home and business;
- Storage of privileged legal material for sharing between lawyers and their clients;

²⁵ Mega has provisions to limit download speed but this is only done in circumstances where there is a high volume of traffic on the network and it is necessary to limit speed in order to regulate infrastructure capacity. This is therefore not used as a matter of course or as a typical 'feature' of free accounts.

- Academic content such as recorded lectures, notes etc. shared with students;
- Backup of medical records, such as tests results, PET, CAT, MRI scans, for sharing with consultants internationally in a secure manner;
- Distribution of digital catalogues of goods, such as jewellery;
- Large genomic data files being sorted and accessed by researchers.

This non-exhaustive list shows that there are a myriad of legitimate uses requiring large volumes of confidential, easily accessible cloud storage. Mega's service is ideal for these users, in particular because of the security provided by UCE.

Restriction of sharing and bandwidth

The NetNames report states that legitimate cloud storage providers "*limit the amount of sharing permitted*", citing the example of Dropbox which provides free users with 20GB of bandwidth per day, and Pro users with 200GB each day. In contrast, the NetNames report states that cyberlockers typically limit the speed at which downloads may be performed in order to encourage users to pay to upgrade to higher speeds.

As is demonstrated by the breakdown above, Mega operates a bandwidth limit in the same way as other legitimate storage providers and does not limit download speeds. The bandwidth allowance is intended to provide a better level of service for paying users than for free users who are subject to throttling if there is undue congestion on Mega's facilities. As the NetNames report notes, all users are offered the same speed of downloads, whether or not they are a premium user.

ii. Advertising

In addition to revenue from premium accounts, advertising is also identified in the NetNames report as another main source of revenue for cyberlockers.

The advertising described in the report is intrusive in nature and adversely affects the cyberlocker user's experience by featuring pop-up advertising or pop-under advertising which often activates when a user clicks on a page. Such advertising is therefore typically referred to as "spamvertising" due to its generally intrusive and insidious nature.

Many legitimate cloud storage providers also derive revenue from advertising featured on their platforms.²⁶ However by contrast, such advertising does not share the "spamvertising" characteristics described above.

²⁶ E.g. Google AdSense, which is a well known and extremely lucrative advertising platform that allows users to monetise their online content.

Mega uniquely differs from both cyberlockers and many other legitimate cloud providers in that in the two years of its existence, its business model has not depended on hosting advertising of any kind across any of its services.

The NetNames report acknowledges that Mega does not host advertising and is therefore an "exception" to the other 29 cyberlocker companies named. However it still categorises Mega as a cyberlocker despite it being clear that Mega's primary sources of revenue do not share any of the characteristics ascribed to cyberlockers. We therefore see no possible basis on which such a conclusion can be drawn.

iii. **Affiliate programme**

The NetNames report identifies one of the main costs for cyberlockers as money paid out to "affiliates" as part of an affiliate or rewards scheme. It describes affiliates as *"subscribers uploading the most widely distributed content or persuading the most users to sign up for premium accounts."* The report goes on to describe the provision of a rewards scheme as *"one of the points which distinguishes cvberlockers from legitimate cloud storage services"*.

Two types of affiliate scheme are identified in the NetNames report:

- where users are rewarded for introducing other users to the website who sign up for a premium account; or
- where users who upload content are rewarded on a pay-per-download model.

It is alleged in the NetNames report that the latter of these models encourages copyright infringement as users are incentivised to upload content that will be popular and downloaded by a number of other users, the inference being that popular content is likely to be exclusive, infringing content. The most obvious example of such content is pre-release full length movies (which we refer to above).

The terms of Mega's affiliate program are published on its website and can be found on the homepage dropdown menu, under the "Developers" tab.²⁷ That is because the program is targeted at software developers. Far from encouraging subscribers to upload content and incentivise the sharing of infringing material, the scheme is designed to reward developers who integrate their products with Mega's storage platform, thereby bringing more primary users to Mega. For instance, an ideal affiliate for Mega would be an app developer who developed their app using on Mega's software development kit for file storage (hence Mega provides full SDK terms and guidance on its site).²⁸ In this sense, Mega's affiliate program is very similar to

²⁷ <https://mega.co.nz/>

²⁸ <https://mega.co.nz/#sdk>

programs operated by other legitimate platforms. We note that Dropbox operates a developer program and that Box has a program for alliance, channel and development partners.

Mega's affiliate Terms of Service also require the affiliate to operate and maintain any affiliate site in accordance with all applicable laws and to warrant that it or its site shall not contain or promote materials that infringe or violate the copyright or other intellectual property rights of Mega, its affiliated entities or any third-parties.²⁹

The NetNames report estimates that Mega pays out \$66,789 per month to affiliates. The source of this figure is unexplained, and it is entirely false.

To date, Mega has not finalised any affiliate relationships and therefore has never paid any commission or retainer to any affiliate. However there are currently several affiliate partnerships under consideration with third-parties who are working to develop apps in which the Mega product may be utilised. By way of example, the projects include:

- Developing a means for users to use Mega as a private and secure storage for the backup and restoring of smartphone data;
- Developing a means for web designers to use Mega as a secure and safe storage for digital assets used in directly publishing websites from the cloud;
- Developing a way in which mobile phone operators may include Mega access in their base plan offerings; and
- Building a research collaboration system for confidential genomic data with very large files.

Unlike typical affiliate schemes operated by cyberlockers, the Mega program does not provide any incentive to the affiliate to upload content of any kind.

3. COMPLIANCE WITH REGULATORY REGIMES

Given that cyberlockers are allegedly designed to encourage mass infringement of copyright, it is perhaps unsurprising that a key feature of cyberlockers identified in the NetNames report is the lack of any robust compliance framework or adequate takedown and repeat infringer policies.

Olswang has closely reviewed the policies and practices that Mega has adopted to deal with copyright takedown requests and other legal requests, such as requests from law enforcement agencies, and has compared these with the equivalent policies adopted by other major cloud storage providers. We consider that these policies are robust, consistent with international best

²⁹ <https://mega.nz/#affiliateterms>

practice and provide an effective level of protection to rights holders where unlawful or infringing content is identified.

Not only do we therefore conclude that Mega cannot be considered a cyberlocker on this basis, but in a number of cases Mega in fact provides a more effective copyright takedown regime than a number of other major legitimate cloud providers.

Details of our findings are set out as follows.

i. Legal requirements upon Mega as a platform operator

As a first step, it may be of assistance to readers to set out the legal requirements with which Mega is obliged to comply in its capacity as a platform operator, in order to put the summary of its legal policies below into context.

Mega is based in New Zealand, registered with the New Zealand Registrar of Companies and governed by New Zealand law. Its Terms of Service provide that its users submit exclusively to New Zealand arbitral dispute resolution. However as a matter of practice, the copyright laws of New Zealand, Europe and the USA all provide online intermediaries with a safe harbour defence from liability for infringing content uploaded by their users where the intermediaries are unaware of that content.

New Zealand

Section 92B of the New Zealand Copyright Act 1994, as amended by the Copyright (New Technologies) Amendment Act 2008, makes clear that *"merely because"* a user may use the services of an internet service provider (which includes hosting providers such as Mega) to infringe copyright, the ISP itself:

- (a) *"does not infringe the copyright in the work;"*
- (b) *"must not be taken to have authorised [the user's] infringement of copyright in the work;"* and
- (c) subject to the ability to obtain injunctive relief, *"must not be subject to any civil remedy or criminal sanction".*³⁰

Similarly, section 92C of that Act provides that an ISP used to host an infringing work does not itself infringe copyright in the hosted work unless it *"knows or has reason to believe that the*

³⁰ Section 92B(2)(a)-(c) New Zealand Copyright Act 1994

*material infringes copyright in the work"*³¹ and *"does not, as soon as possible after becoming aware of the infringing material, delete the material or prevent access to it"*.³²

Sections 92B and C of New Zealand's Copyright Act are largely based on equivalent Australian legislation, which, in turn, was derived from Section 512 of the US Digital Millennium Copyright Act (the 'DMCA'), section 512(c) of which in particular provides a safe harbor for online storage providers.

New Zealand law also provides similar safe harbours for online service providers in respect of other illegal or infringing material where the provider has no knowledge of that material.³³

USA & Europe

Whilst Mega is governed by New Zealand law, US and European copyright laws also provide a similar safe harbour regime to intermediaries.

(a) USA

As noted above, section 512 of the DMCA provides that online storage providers will be immune from liability for copyright infringements carried out by their users on their platform where, in addition to complying with standard technical measures and removing repeat infringers, the provider:

"(A)

- (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;*
- (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or*
- (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;*

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

³¹ Section 92C(ii)(a)(i) New Zealand Copyright Act 1994

³² Section 92C(ii)(a)(ii) New Zealand Copyright Act 1994

³³ E.g. Section 21 New Zealand Defamation Act 1992 (defamatory material) and section 122(2) New Zealand Films, Videos, and Publications Classification Act 1993 (objectionable material)

*(C) upon notification of claimed infringement [...], responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity".*³⁴

Further, section 512(m) of the DMCA states that there is no general obligation to monitor activity occurring on its service or to "*affirmatively seek facts indicating infringing activity*" and this has been applied by the US courts.³⁵

More broadly, section 230 of the Communications Decency Act of 1996 (the 'CDA') provides neutral internet intermediaries with general immunity for liability for torts committed by users on their platform. Specifically, this states that: "*No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*".³⁶

(b) Europe

In Europe, an equivalent provision is set out in European Union Directive 2000/31/EC (the "E-Commerce Directive"), Article 14(1) of which provides that an "*information society service provider*" such as Mega is:

"not liable for the information stored at the request of a recipient of the service, on condition that:

(a) the provider does not have actual knowledge of illegal activity of information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."

The E-Commerce Directive has been implemented into the national law of all 28 EU Member States. Article 15 of the E-Commerce Directive also stipulates that there should be no obligation upon platform operators to actively monitor content on their platforms.

ii. Notice and takedown policies

Mega has a number of clear notice and takedown procedures in place which comply with the statutory provisions set out above and allow any person who identifies unlawful or infringing content on Mega's platform to inform Mega of the material in question and to request its removal.

³⁴ 17 U.S.C. § 512(c)

³⁵ For instance, see *Viacom International Inc. et al. v Youtube et al.*, 07 civ. 2103 (LLS) (S.D.N.Y Apr 12, 2013) and *Disney Enterprises, Inc. v Hotfile Corporation*, 11-20427 (S.DA.Fla. 2013)

³⁶ 47 U.S.C. § 230

In circumstances where Mega becomes aware of such unlawful or infringing material on receipt of such notices, it then takes steps to promptly remove or disable access to such content in accordance with the relevant law. These procedures are set out clearly on the Mega website and in its Terms of Service.³⁷

Submitting a copyright takedown request

Copyright holders who become aware of infringing material on the Mega platform can contact Mega via a dedicated copyright notice webpage to inform Mega of infringing content on its platform.

The user submitting the notification is able to choose from the following takedown options depending on the nature of the infringement:

- Disable one link per file – the file will remain in the user's account;
- Disable multiple URLs per file – the file will remain in the user's account; or
- Remove all underlying files of the supplied URL(s) – there is no user permitted to store this under any circumstance worldwide.

The reason for these distinctions is that Mega recognises, as do the laws in the jurisdictions noted above, that the same file stored on Mega may be legitimately stored by one user and in respect of another be infringing. The first user may be entitled to store it for personal use or backup whereas the second user may not be entitled to the file in the first place.

When Mega receives a takedown request on the basis of an alleged copyright infringement, its practice is to remove or disable access to the file or files within 4-8 hours and it typically does so in less than 4 hours. Mega does not have the ability to decrypt the material complained of and does not assess whether there has been a genuine copyright infringement; its policy is simply to remove the material in question when a complaint is received.

This policy is therefore fully compliant with the New Zealand Copyright Act 1994 and the equivalent intermediary liability regimes provided for in the US DMCA and European E-Commerce Directive.

These procedures are notable given that Mega itself cannot view or determine the contents of files stored in the Mega system, as files are encrypted by users before the files reach Mega. Unless a user has voluntarily shared a link to a file they have stored on an open basis (with its decryption key), Mega therefore has no way of knowing whether any particular content on the platform is unlawful or infringes third-party rights without being specifically informed of this. Mega nevertheless takes down any such material of which it is notified.

³⁷ See also Mega's Takedown Guidance <https://mega.co.nz/#takedown>

It is worth noting that in the Introduction on page 2 of the NetNames report, it states that cyberlockers are *"intentionally architected to support the massive distribution of files among strangers on a worldwide and unrestricted scale, while carefully limiting their own knowledge of which files are being distributed"* (emphasis added). In respect of Mega, it is therefore inferred that Mega offers this level of encryption purposely in order to allow Mega simply to deny all knowledge of any unlawful content on its site. The evidence does not support this assertion for the following reasons:

- Firstly, from a legal perspective the provision of encryption alone would not enable Mega to avoid all liability for infringing content hosted on its platform, in circumstances where it was made aware of such content and then failed to take steps to remove it. It is therefore not correct for the NetNames report to suggest that Mega can rely on encryption simply as a means to avoid legal liability for all infringing content in this way.
- To the extent that Mega receives takedown requests for encrypted content, it could refuse to respond to these requests and seek to rely on the applicable intermediary hosting defences set out above on the basis that it has no way of knowing whether the content complained of is unlawful or not. However, Mega does not distinguish between copyright takedown requests for content with or without the encryption key and responds to all valid takedown requests by removing the offending material. Such a response is entirely at odds with the expected behaviour of a cyberlocker.

The Mega Terms of Service

Mega's Terms of Service³⁸, which each user expressly agrees to by checking a box when they sign up to the service, make it clear that by using the service, users agree not to:

- *"infringe anyone else's intellectual property (including but not limited to copyright) or other rights in any material"; or*
- *"use our website or a service, including, without limitation, any communication tools available through the website, or any forum, chat room or message centre that we provide: to store, use, download, upload or otherwise transmit, data in violation of any law (including to breach copyright or other intellectual property held by us or anyone else)".*

Users must also agree that when using the service they will comply with all laws including copyright and other intellectual property laws. This includes, but is not limited to, the following banner-style warning when generating a link for sharing files/folders in the File Manager:

"Copyright Warning: MEGA respects the copyrights of others and requires that users of the MEGA cloud service comply with the laws of copyrights. You may not upload,

³⁸ <https://mega.co.nz/#terms>

download, store, share, display, stream, distribute, e-mail, link to, transmit, or otherwise make available any files, data, or content that infringes any copyright or any proprietary rights of any person or entity."

A screenshot of this warning as it appears onscreen is at Annex B. We note that many of the other legitimate cloud service providers do not provide such a warning to users when sharing content.

iii. Takedown statistics

Mega's preliminary statistics show that it receives a very low rate of takedown requests relative to the total number of files on its servers. The table below sets out the total number of takedown requests processed since commencement in Q1 2013, including but not limited to takedown requests for copyright purposes.

Period	No of Takedown Notices	No of Files Requested to be Taken Down	% of Stored Files
2013 Q1	4,034	51,857	0.033%
2013 Q2	7,500	53,772	0.019%
2013 Q3	9,072	101,339	0.024%
2013 Q4	9,774	111,162	0.018%
2014 Q1	9,673	91,597	0.009%
2014 Q2	11,471	105,422	0.006%
2014 Q3	13,145	108,890	0.004%
2014 Q4	9,941	402,152	0.011%
2015 Q1	11,225	131,377	0.003%

Note: These statistics include all notices received, even if incorrect, invalid or relating to files that have already been removed.

As explained above, requested takedowns are actioned by Mega without any analysis as to whether the files identified contain genuinely infringing material (which would be impossible to determine in the case of encrypted files with no encryption key). Mega expects that the number

of links that it has taken down is significantly overstated because of the number of false and repetitive reports submitted to Mega.

Comparison with cyberlockers named in the NetNames report

Google's transparency report provides statistics as to the number of DMCA takedown requests that it received to remove content from its search engine in relation to Mega's domain name. From Mega's inception on 30 January 2013 to 10 May 2015, Google has received 7,950 requests for the removal of a total of 48,615 URLs.³⁹ This is a very low percentage of the total number of files stored on Mega, 0.0009% of the 5.5 billion files.

The NetNames report identified Mega as one of 15 "direct download cyberlockers". Below is a table generated from Google transparency and Alexa global rank traffic data showing the number of URLs requested to be removed from the Google search results that Google received in the 12 months up to 29 April 2015 for the domains named as "direct download cyberlockers" in the NetNames report. The first column also shows the relative ranking of each domain with regard to the total number of URLs that Google has had to remove in that same period. The final column shows each domain's global popularity, calculated by Alexa.com using a combination of average daily visitors to the site and page views on the site over three months ending on 29 April 2015.

Rank order of specified domains ⁴⁰	Domain ⁴¹	Number of URLs requested to be removed from Google search results	Alexa global traffic rank ⁴²
1	rapidgator.net	7,901,196	707
2	uploaded.net	6,708,841	425
3	4shared.com	6,489,323	419
14	zippyshare.com	1,882,413	509
59	turbobit.net	997,877	1,314
60	bitshare.com	964,299	6,927

³⁹ <http://www.google.com/transparencyreport/removals/copyright/domains/mega.co.nz/>

⁴⁰ Ordered by number of URLs requested to be removed, as reported by Google for the 12 months to 29 April 2015.

⁴¹ Domains named as "direct download cyberlockers" in the NetNames report.

⁴² An estimate of the site's popularity, calculated by Alexa using a combination of average daily visitors to the site and pageviews on the site over the three months to 29 April 2015. The site with the highest combination of visitors and pageviews is ranked #1. [Taken from www.alexa.com on 30 April 2015]

82	freakshare.com	734,277	9,590
88	ryushare.com	708,991	8,627
91	letitbit.net	649,351	3,797
249	uptobox.com	292,196	1,539
534	1fichier.com	148,688	3,459
930	2shared.com	84,204	7,120
966	filenuke.com	76,961	4,361
1,211	depositfiles.com	51,039	3,525
1,777	mega.co.nz	26,059	485

The table demonstrates that Mega has high levels of user traffic compared to almost everyone in the table but that Google receives low numbers of requests for removals for URLs on the Mega domain from its search results. This distinguishes Mega from the other domains named as "direct download cyberlockers" in the NetNames report, and in particular, the table shows that in the 12 months to 29 April 2015, Google received a much higher level of URL removal requests for the domains with comparable user traffic to Mega. This is entirely consistent with our findings that Mega's platform, and UCE in particular, is targeted at primary users rather than indiscriminate widespread sharing which would result in more publicly searchable files and therefore more takedown notices to Google.

It should be noted that the number of takedown files is inflated as a result of robots who generate incorrect notices on behalf of copyright owners. For instance, in the first week of March 2015 Mega received a takedown request for "El Capital", a pdf document of the Spanish translation of Karl Marx's "Das Kapital" which is not in copyright. Mega assumes that this is likely to have occurred because a robot confused the file with the Manga Comic Strip also named "El Capital", which is still under copyright.⁴³

Repeat infringer policies

In addition to Mega's takedown process, it also operates a '5 strikes' policy for repeat infringers. This ensures that any user account that is the subject of five separate instances of takedown

⁴³ <http://www.casadellibro.com/libro-el-capital-manga/9788425431333/2110340>

action will have their account suspended.⁴⁴ At the time of writing 29,290 user accounts had been suspended by Mega for this reason, comprising less than 0.16% of total Mega users.

Law enforcement requests

Mega's compliance with regulatory regimes is not limited to copyright and it also complies with any requests made by law enforcement agencies in accordance with Mega's Privacy Policy, which specifies that:

"If we think it is necessary or we have to by law in any jurisdiction then we are entitled to give your information to the authorities. We reserve the right to assist any law enforcement agency with investigations, including and limited to by way of disclosure of information to them or their agents. We also reserve the right to comply with any legal processes, including but not limited to subpoenas, search warrants and court orders. We may disclose your information to enforce or apply our Terms or any other agreement we have with you; or to protect the rights, property, or safety of us or our other users or the operation of our services and the website."⁴⁵

Mega also discloses certain information to law enforcement agencies where required to do so under a court order.⁴⁶

It is clear that Mega would not have robust policies in place of the type described above if it were in fact a cyberlocker as described in the NetNames report and/or encouraged the mass infringement of copyright. As the above analysis demonstrates, Mega adopts similar policies as other major cloud storage providers.

In view of some public confusion between Mega Limited and a company called MegaUpload Limited, we have included at Annex C a note about the latter company.

iv. Third-party linking sites

Finally, the NetNames report states that *"direct download cyberlockers are intentionally designed to offer no search capability"*. Instead, the report alleges that users of cyberlockers locate links to infringing content via third-party *"link sites"* which collate and index content held elsewhere. It is alleged that users then access infringing material after browsing for titles to download through such third-party linking websites.

It is important to note that the lack of a search facility by itself clearly cannot prove anything, and it should not be a feature associated with the definition of a cyberlocker. Mega does not provide public search facilities as its service is intended for storing and sharing material for consumers

⁴⁴ All takedown requests received within a 24-hour period will count as one 'instance' of takedown action for these purposes.

⁴⁵ <https://mega.co.nz/#privacy>

⁴⁶ <https://mega.co.nz/#takedown>

and businesses, not for such content to be generally accessible to other users and/or the public. In this sense, Mega is no different to other major cloud storage providers such as DropBox and Google Drive which also do not have public search functions, for exactly the same reasons.

More generally, whilst Mega is aware that such third-party linking sites exist, these sites are not related to, affiliated with or controlled by Mega in any way. As set out in more detail above, Mega responds to takedown notices when it is made aware of copyright infringing or other unlawful material on its platform. Mega also takes steps to have content removed from the internet where it misrepresents a connection to Mega, for example on Facebook pages. However, in most cases Mega is simply not in a position to incur considerable legal costs by pursuing legal proceedings against such sites, many of which are not solely targeted towards Mega in any event.

Finally, it is also worth noting that these sites will only link to publicly available content on Mega. As stated above, this is an insignificant proportion of the overall files held on the website.

E. SUMMARY AND CONCLUSIONS

Having reviewed the NetNames report and undertaken analysis of Mega's service, Olswang has found no evidence to conclude that Mega can be considered a cyberlocker, or that it knowingly, willingly or even passively assists in or condones wide scale copyright or other infringement.

For the reasons set out above, all of Mega's characteristics are consistent with those of a legitimate cloud storage provider in the same way as Google Drive, Microsoft OneDrive, Apple iCloud, Dropbox and many other similar providers. We have not found any basis for the claim that it has been "*intentionally architected to support the massive distribution of files among strangers on a worldwide and unrestricted scale*".

Accordingly, Olswang does not consider Mega's inclusion in the NetNames report to have any factual basis whatsoever.

Our key findings in each area analysed are set out below:

Storing and Sharing

- Mega's platform is designed for personal and business users who wish to store and access their data remotely across different devices, as is the case with other legitimate storage providers.
- All files are encrypted and are not available to be accessed and/or downloaded unless specifically shared with others by the user who uploaded them.
- The automatic encryption utilised by Mega means that the platform is not attractive for users wishing to share content with large numbers of people, in particular as users have to take additional steps to share content with others.

Business Model

- Mega's business model is the same as other legitimate cloud storage providers: it operates a 'freemium' service where users pay for greater storage capacity and bandwidth, not greater download speeds.
- Mega's affiliate programme does not offer any "*rewards*" to users who share popular content, nor have we identified any other incentive for users to upload or share content of any kind.

Compliance with Regulatory Regimes

- Mega operates a robust notice and takedown policy which complies with international laws.

- As the majority of files stored on the platform are encrypted, Mega cannot assess the validity of each copyright takedown request it receives and its policy is simply to remove the material in question when a complaint is received.
- The number of takedown requests submitted to Google in respect of the Mega domain name is extremely small when compared to the cyberlockers identified in the NetNames report.

Legal summary

The allegations made in the NetNames report are seriously defamatory of Mega and for the reasons set out in this report, clearly have no basis in fact. The wide publication of the NetNames report and the defamatory allegations that it contains have already caused Mega considerable financial and reputational damage, and is likely to continue to do so if the allegations relating to Mega continue to be published.

Mega is in a position to commence legal proceedings for defamation against those responsible for the publication of the NetNames report, including but not limited to NetNames Limited and any directors, employees or individuals responsible for authoring, editing or publishing the NetNames report. No attempt was made to verify with Mega any of the factual allegations contained within the NetNames report, and NetNames refused to comply with a takedown request made by Mega in relation to the NetNames report. There is no legal justification for such disregard for the truth in relation to allegations which are seriously defamatory.

Olswang LLP

15 May 2015

ANNEX A

Mega Director and Management Biographies

Brian Clarkson BA, Dip Ed, Dip Ed Tech (Plymouth), Director

Mr Clarkson is a successful entrepreneur with 25 years' experience in starting, running, growing and selling small businesses profitably. His main experience is in technology businesses, and specifically in internet delivered training in international markets. Mr Clarkson was Chief Operating Officer of Mega until August 2014. Previously he was CEO of Instra Corporation, an international domain name registration business operating in Melbourne, Napier and Auckland. Mr Clarkson has broad experience in all areas of business, including Sales, Marketing, Finance and Accounting, Product Development, Brand Development and Administration, and has also held roles with the following enterprises:

- Clarkson Trading Pty Limited as owner, CEO and Director from 2009 to present;
- Clarkson Family Investments Pty Limited as part owner, CEO and Director from 1985-2011;
- Janet Clarkson (Medical) Pty Limited as part owner and Director from 1985 to 2009;
- DVP Media Pty Ltd as part owner, CEO and Director from 2001 to 2009 (when the business was sold to Jones & Bartlett in Boston MA, USA);
- Domain Directors Pty Limited (Instra) from 2010 to 2012 as CEO;
- QANTM Pty Limited as General Manager – Production from 1998 to 2000; and
- DVP Media Pty Limited as part owner, CEO and Director from 1993 to 1998.

Stephen Hall MCom (Hons) CA INFINZ(Cert) Director and Chief Compliance Officer

Mr Hall joined Mega as CFO in April 2013, shortly after it commenced operations, and was CEO from January to July 2014. He has held senior management positions in a number of industries in Australia and New Zealand, including listed public companies. Mr Hall has also held the following executive positions:

- Chief Executive – Genesis Research and Development Corporation Ltd 2004-2010
- Head of Corporate Services - Genesis Research and Development Corporation Ltd 2000-04;
- CFO / Company Secretary – St Lukes Group Limited (Listed NZX) (1998-2000);
- GM Finance & Admin / Company Secretary – Watercare Services Limited (1991-1998);
- Northern Region Manager – Smith & Smith Glass (1989-1991);
- Manager – Thorobred Yarns & Feltex Yarns (1984-1988);
- Financial Controller – Feltex Properties Group Limited (1984-1985);
- Finance Development Manager – Feltex NZ Limited (1981-1984); and
- Company Secretary / General Manager – Boart Australia Limited (1977-1981).

Zhaowu Shen – Director

After graduating from Xiamen University in China in 1984, Mr Shen held the position of Secretary for Fuzhou City Government Office in China from 1984 to 1992. After retiring from his secretary

position in 1992, Mr Shen established a State Owned Enterprise residential property development company and served as general manager. The company specialised in residential housing difficulties of urban residents to solve their residential problems. In 1995, the company restructured and was renamed as Fujian Kangtai Residential Property Development Co., Ltd, and Mr Shen discontinued managing the company further. That same year, Mr Shen founded the Fuzhou Contue Enterprise Group. He has served as both the CEO and major shareholder of Contue Enterprise Group. Currently the headquarters of Contue Enterprise Group are located in Shenzhen, China and it has over 30 subsidiary companies all over China, including the primary business of real estate development as well as associated industries of construction, hospitality, commercial, high-tech, property management and trade. As the major shareholder and CEO of Contue Enterprise Group from its establishment until present, Mr Shen has been influential in the business' significant growth and success.

Graham Gaylard NZCE BSc MBA - Chief Executive Officer

Mr Gaylard has 30 years' experience in the information technology sector. He was the co-founder and Chief Executive of NetValue Limited, a ten year old web, applications development and hosting company based in Hamilton, New Zealand. In 2009 Mr Gaylard founded Real Time Genomics Inc., a San Francisco based bioinformatics company. Mr Gaylard raised Silicon Valley venture capital funding from Catamount Ventures, Lightspeed Ventures as well as New Zealand venture capital from Evander Management. Prior to NetValue Mr Gaylard co-founded software company Computer Systems Engineering, and Wave Internet. In 2000, both CSE and Wave were sold to an American software technology firm. Mr Gaylard's positions ranged from Chief Architect through to Manager of Research and Development. Prior to this Mr Gaylard has held IT technical and management positions in NZ Dairy Group, (now Fonterra) as a systems engineer, and various roles with Telecom NZ (now Spark), including as a Senior Electrician, Electrical Engineering Associate and Applications Development Consultant. Passionate about technology based ventures and entrepreneurship, Mr Gaylard is currently the Chair of SODA Inc., a Waikato based incubator for start-ups and also guest lecturer at tertiary institutions. Mr Gaylard has also provided business consulting for technology based start-up companies as well as undertaking private angel investments.

Stuart Inglis BCMS (Hons), PGDMS, Ph.D - Chief Technology Officer

Mr Inglis is a professional computer scientist with over 30 years' programming experience and a passion for software innovation. He has a blend of technical excellence and software project management experience, with a background in algorithm design, intellectual property creation, high performance computation and low-level optimisation. He has expertise in software development, high reliability hosting, data analysis and complex solution development. His first commercial experience was the NZ director and R & D software developer for a New York company called Webmind. This was followed by founding a San Francisco data analysis company Reel Two Inc in 2001. The NZ subsidiary of Reel Two was sold to NetValue in 2007 where Mr Inglis became a shareholder and director. He joins Mega from his previous role as the CTO of Hamilton firm NetValue, which saw him lead the technical development of large projects and high-tech spin off companies including Real Time Genomics and SureChem. NetValue's subsidiary company Interspeed is a leader in high-reliability hosting. Mr Inglis has a huge

commitment to the community and along with his family place high value on sponsoring community based charities. He has been an early-stage shareholder in several NZ businesses and is actively involved in the angel investment community.

Greg Daniel B Com DipGrad CA - Chief Financial Officer

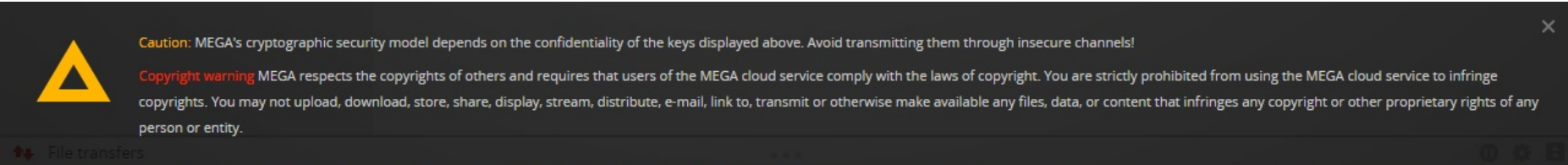
Mr Daniel is a Chartered Accountant with over 15 years of local and international business experience. Mr Daniel has held a range of executive roles in both private and publicly listed companies including a successful IT start-up based in Europe. Mr Daniel's previous executive roles include:

- Chief Financial Officer, Metro Office Fund Limited, Auckland;
- Financial Controller, Cristal Air International Limited (HRV), Auckland;
- Chief Financial Officer, Palmers Franchise Systems Limited and Sierra Coffee Company Limited, Auckland;
- Finance Manager, Azure Solutions Limited, London, United Kingdom;
- Financial Controller, Anite Calculus Limited, London, United Kingdom;
- Audit Senior, The National Audit Office, United Kingdom; and
- Audit Junior to Audit Senior, PKF Ross Melville Chartered Accountants, Auckland.

OLSWANG

ANNEX B

Figure 2:



MegaUpload Limited and Kim Dotcom

Kim Dotcom is a well-known software entrepreneur who was a director of the separate company MegaUpload Limited. MegaUpload operated from 2005 until January 2012, when it was shut down through court action initiated by the United States Department of Justice in relation to various allegations of copyright infringement. Proceedings are ongoing against MegaUpload, Kim Dotcom, and other persons associated with MegaUpload.

None of the ongoing proceedings relates to Mega Limited and Mega's platform operates entirely differently to MegaUpload – utilizing a different business model and different technology.

Mr Dotcom was briefly a director of Mega Limited at the time of its inception. Due to Mr Dotcom's high profile in the technology world, Mega Limited is often inaccurately described as "Kim Dotcom's Mega" in the media.

However, Mr Dotcom was only a director of Mega Limited from its inception in January 2013 to October 2013 when he left to develop his political and other business interests. He has not held any executive, non-executive, operational, managerial or governance role with the company since October 2013, nor has he been engaged in any consultancy or advisory capacity and he has not received any salary or remuneration from Mega.

Since stepping away from Mega Mr Dotcom has commented publicly on the business of Mega Limited through a variety of channels, including to the 460,000 followers of his Twitter account, which include many journalists from technology publications. However, Mr Dotcom does not represent the company and is not authorised to make any public statements on behalf of the company. Any public statements made by him are made purely in his personal capacity.