MEGA

10 **February** 2015

# **Encryption & Anonymity** in digital communications

2015 **HRC**

# Contents

# Introduction

Following a public request for information by David Kaye for a report on the use of encryption and anonymity in digital communications, Mega would like to submit the information in this paper to provide a basic outline of what Mega is, how we operate, and how we comply with national laws, regulations and policies while providing individuals with uncompromised end-to-end encryption tools to enable them to protect their privacy.

Mega is a strong proponent of Privacy and upholding the Universal Declaration of Human Rights.

# The Privacy Company

When we launched MEGA early 2013, global mass surveillance by rogue governments under the pretext of fighting terrorism was still a wild conjecture and its proponents were often touted as conspiracy theorists. Edward Snowden's revelations 137 days later fundamentally changed public attitudes and it became excruciatingly clear that security by policy ("we have access to your data, but we promise to keep it confidential and not misuse it") had not been good enough. Anything short of security by design ("we cannot gain access to your data without you being able to find out"), for which strong end-to-end encryption is an essential prerequisite, now seems grossly insufficient.

MEGA was architected around the simple fact that cryptography, for it to be accepted and used, must not interfere with usability. MEGA is fully accessible without prior software installs and remains the only cloud storage provider with browser-based high-performance end-to-end encryption. The only visible signs of the crypto layer operating under MEGA's hood are the entropy collection during signup, the lack of a password reset feature and the novel (and browser-specific) ways file transfers are conducted. Today, millions of business and personal users rely on MEGA to securely and reliably store and serve petabytes of data and we believe that this success is the result of MEGA's low barrier to entry to a more secure cloud.

Mega also provides a secure, end-user controlled end-to-end encrypted voice and video conferencing service – MEGAChat. In the future Mega will provide other tools to ensure online privacy such as email and backup.

Although Mega provides strong privacy tools, it does not provide anonymity.

# Regulatory Compliance

Mega's service is governed by New Zealand law and users submit exclusively to New Zealand arbitral dispute resolution. Mega has sought extensive legal advice on its service by lawyers in New Zealand and various other jurisdictions, including the United States, to minimise the risk of non-compliance with regulatory requirements in the main jurisdictions in which it operates.

Mega maintains market leading processes for dealing with users who upload and share copyright infringing material or breach any other legal requirements. Mega cannot view or determine the contents of files stored in the Mega system as files are encrypted by users before the files reach Mega.

However, if a user voluntarily shares a link to a file they have stored (with its decryption key), then anyone with that link can decrypt and view the file contents. Mega's terms of service provide that copyright holders who become aware of public links to their copyright material can contact Mega to have the offending files removed from Mega's system.

The USA Digital Millennium Copyright Act (DMCA) process, the European Union Directive 2000/31/EC and New Zealand's Copyright Act process provide Mega with a safe harbour, shielding Mega from liability for the material that its users upload and share using Mega's services. Mega complies with the conditions on which that safe harbour is made available by allowing any person to submit a notice that their copyright material is being incorrectly shared through the Mega service. When Mega receives such notices it promptly removes or disables access to the offending file or files, depending on the type of request, consistent with the Terms of Service agreed to by every registered user. The number of files which have been subject to such take down notices continues to be very small, indicative of a user base which appreciates the speed and flexibility of Mega's system for fully legal business and personal use.

The DMCA requires links to be taken down expeditiously. Most cloud providers target takedown within 24 hours. Mega targets takedown within a maximum of 4 hours, with takedowns frequently being actioned much quicker than the 4 hour target. Mega plans to implement a public "Takedown Transparency Report" on its takedown statistics so that interested parties can see clearly that Mega is a totally compliant service.

In implementing its takedown notice policy and processes, Mega initiated discussions with New Zealand law enforcement authorities. Mega has adopted policies and processes which it has been advised are consistent with their requirements.[1]

The current safe harbours that apply to Mega under New Zealand law for user uploaded defamatory material under the Defamation Act 1992, for objectionable material under the Films, Videos, and Publications Classification Act 1993, for copyright infringing material under the Copyright Act 1994 and generally in respect of other illegal material under laws relating to aiding and abetting are complex and all differ from each other in certain respects. In general terms Mega will not be liable for user content unless it knows about it and fails to take appropriate action.

# Takedown System

Mega accepts takedown notices via a dedicated web page[2] or by email to takedown@mega.co.nz

They are processed within a few hours without reviewing their validity.

The submitter is able to choose

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

[1] https://mega.nz/#terms https://mega.nz/#takedown https://mega.nz/#copyright
[2] https://mega.nz/#copyrightnotice

# Mega Product Description

Mega provides encrypted, cloud based services that enable private, secure online storage, communication and collaboration for businesses and individuals. Mega provides browser-based User Controlled Encryption (UCE), which provides automatic encryption for all data transferred to and stored on Mega's cloud service. UCE means that only the user controls the encryption key. This provides a level of privacy and security that is unparalleled among mainstream cloud storage solutions and allows Mega to position itself as "The Privacy Company".

The Mega service was launched on 20 January 2013. Mega currently has over 15.5 million registered users as at the end of January 2015, and has added on average nearly 35,000 new registered users per day during January 2015. Users have stored more than 4 billion encrypted files in the Mega cloud and have been uploading on average over 15 million files per day during January 2015.

Many cloud users have assumed that the digital information they store in the cloud is private. However recent revelations of hacking and intrusion into our digital lives have highlighted that this is simply not the case. This is an increasing problem for many ordinary people and businesses who want to use the cloud without having their personal and business privacy invaded.

Mega helps address this by providing users with simple, fast, encrypted cloud based services that enable private, online communication and collaboration for businesses and individuals.

Mega considers that its cloud storage service provides much greater privacy protections for users than other major cloud storage solutions currently available in the market because of Mega’s unique and simple user-controlled encryption process.

Encryption has been available for many years but has not been easily accessible by ordinary users because it has been highly technical, difficult to implement, has required the installation of additional software and has required significant computer processing overhead.

Some cloud storage providers will encrypt data once it has been received from the user but the provider then holds the encryption key for all of the data stored on their service. This means that the cloud storage provider has full access to all users' data. This weakness could easily be utilised by government agencies, hackers or commercial interests to gain access to users’ data.

Mega's system is different. Mega has developed a system of encryption which runs in the user's browser and automatically encrypts the data locally on the user’s device before it is transferred to and stored on Mega's cloud service. This encryption process does not require installation of any software application or require any user involvement and it has virtually imperceptible impact on computer processing performance. This encryption is done automatically on the user's device (computer, tablet or phone), and only the user has the encryption key for the data. Mega calls this "User Controlled Encryption" or "UCE". Mega 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.

Mega considers that its key difference arises from offering simple, UCE which allows users greater privacy protections than other cloud storage solutions without adversely affecting the user experience.

The Mega encrypted cloud storage product has been designed from the ground up using the most modern internet technologies, in particular HTML5. This allows all of the encryption to be undertaken automatically within the browser without requiring any action by the user and makes the encryption unnoticeable by the user so it does not detract from the user experience. Users interact with Mega simply and easily and enjoy a modern, fast service.

The desktop browser product is complemented by a Windows sync tool that automatically replicates selected desktop folders and files with the same folder structure in the cloud. OS X and Linux versions were released during 2014. Android, iOS and Blackberry apps allow users to easily access their cloud files on mobile devices. The Windows Phone app, and multiple programming language bindings were released January 2015.

Mega, quite some time ago, has announced additional privacy products for consumers and businesses, such as MegaChat – video, audio conferencing and encrypted email. MegaChat has now been released and email is in the design stages. Encrypted cloud storage was the first, but not singular, product Mega released to the market. Mega is more than an encrypted cloud storage provider, Mega is building a privacy-based ecosystem to protect the privacy of customer's digital information and ensure collaboration remains private.

Mega receives many complimentary comments from satisfied users who appreciate the speed and functionality of the Mega service. Business users have commented to our support staff that they use the Mega service because

- It provides a secure private transfer and storage service;
- The transfers are much quicker than competitors who use older technologies;
- Mega supports long file/folder names, deep folder structures.

Users we are aware of include businesses in the biotechnology, media and design industries who frequently generate very large files that need to be transferred internationally and are easily handled by the Mega system.

Mega often has requests from users surrounding particular use cases for large files. We know for instance (because our users have told us) that types of usage include:

1. Sharing of recorded and annotated Computer Game tournaments (original non-breaching content). There is a very large amount of this;
2. Backups & restoration of computer systems for home and business;
3. Academic content such as recorded lectures, notes etc. shared with students;
4. Backup of medical records, such as test results, PET, CAT, MRI scans, for sharing with consultants globally in a private and secure manner;
5. Distribution of open source software releases;
6. Distribution of digital catalogues of goods, such as jewellery;
7. Judicial officers and Judges sharing court and other legal documents;
8. Large genomic data files being stored and accessed by researchers worldwide;
9. Independent filmmakers using Mega to distribute their works;
10. Independent music artists using Mega to distribute their works.

Third party developers are using the SDK to build new vertical applications such as smartphone backup and restore, storage and secure publication of Web sites.

# Deduplication

A recent report prepared by the Spanish National Cybersecurity Institute[3] compares Mega and Dropbox (and concludes a very favourable view of Mega). They review deduplication and conclude that Mega carries out client side single-user deduplication at a file level and server side cross-user deduplication of encrypted files.

However as an upload is encrypted by a key that is unique to that user, identical files uploaded by several users will not be identical once they are encrypted so they will appear to be different files to Mega.

The more relevant aspects of this matter are discussed in the 'takedown' section above.

# Sharing

Mega does not log the number of links generated by any user or utilised against particular files. Even if it did do so, the information would not provide any indication of non-compliant use as we are aware of users who generate significant link generation and sharing through entirely compliant use.

# Encryption

Mega provides user controlled encryption to meet the growing demand for privacy, by individuals, businesses and governments, not to facilitate breach of copyright, as demonstrated by Mega's rigorous terms of service and takedown processes.
Encryption has been publicly available for over 30 years and is entirely legal. Indeed it underpins the global banking industry and many other aspects of modern life.

# Conclusion

MEGA provides robust cloud storage with convenient and powerful always-on privacy. MEGA believes in your right to privacy and provides you with the technology tools to protect it. We call it User Controlled Encryption, or UCE, and it happens automatically.

All files stored on MEGA are encrypted. All data transfers from and to MEGA are encrypted. And while most cloud storage providers can and do claim the same, MEGA is different – unlike the industry norm where the cloud storage provider holds the decryption key, with MEGA, you control the encryption,

[3] https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/incibe_security_storage_dropbox_mega.pdf

you hold the keys, and you decide who you grant or deny access to your files, without requiring any risky software installs. It's all happening in your web browser!

The MEGA cloud is just the beginning. In the future, MEGA will provide UCE in your browser for a wide range of applications without the need to install anything. Our technology will protect your emails, calls, chats and video streams.

MEGA provides tools that make private and confidential online communication easy to use and is a strong proponent of privacy.

*"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*[4]

[4] Universal Declaration of Human Rights