



Submission on review of the Copyright Act 1994: Issues Paper

Introduction

This submission is made by **Mega Limited** (New Zealand registered company no. 4136598). No part of this submission is private or confidential.

By way of background on Mega and its experience in dealing with infringement, copies of Mega's two most recent transparency reports, its Terms of Service and its Takedown Guidance policy are attached. From these, it can be seen that:

- Mega has 140 million registered users worldwide. They include businesses, professionals and private individuals. Since its establishment in 2013, users have uploaded over 56 billion files – including works of third parties that they do not hold the copyright or appropriate authorisation for. It is a common feature of cloud storage services to allow the sharing of user files, and Mega is no different: Users can establish folder shares with other Mega users or export URL links to files and folders. If a user makes a link public, e.g. by posting it to a forum, rights-holders who have good faith belief that the user data the link points to infringes on their rights can submit a takedown notice to Mega, which will be processed expeditiously. Mega user accounts are disabled (access barred and all existing links disabled) upon the receipt of the third takedown “strike”.
- From a level in 2013 of 0.02% of all files uploaded to an average now of around 0.0001% of all files, the percentage of infringing file/folder links notified to Mega is extremely small.
- Similarly, the number of users suspended after three or more copyright strikes has declined as a percentage of its overall user numbers.
- Very few copyright counter-notices (as that term is used in the DMCA) are issued despite Mega offering that facility (but note below at Question 62, Mega's concerns with counter-notices).
- Where Mega is notified of copyright infringement it takes down (disables access to) the file in question immediately (targeting takedown within 4 hours). If requested by law enforcement or third parties, the evidentiary material that Mega holds may be kept for release under a production order or civil process.
- Mega works closely with law enforcement in various jurisdictions and with rights-holder organisations to ensure that illegal content, including copyright infringing material, is promptly taken down.



Mega’s experience outlined above makes it uniquely placed to provide input on certain aspects of copyright law, as it impacts the operations of a cloud storage provider controlled from New Zealand and with 140 million registered users worldwide.

Mega has responded to the questions that are particularly relevant to its experience and operations using the original numbering from the issues paper. The fact that Mega has not responded to other questions raised in the issues paper does not imply any acceptance or rejection of, or any particular view on, those questions. Mega has views on other aspects of copyright law and reserves the right to comment further on those aspects in due course as the current review of the Act proceeds.

Responses to Issues Paper questions

19	What problems (or benefits) are there with communication works as a category of copyright work? What alternatives (if any) should be considered?
	<p><i>The current Copyright Act is ambiguous as to the legal impact of the way an infringing work is transported. It could be argued that section 131 does not apply to infringement by communicating a work, which would lead to the paradox that e.g. the operators of a website who actively obtain, curate and offer for download infringing works could not be criminally prosecuted in New Zealand.</i></p> <p><i>This is an issue that has been raised in the Dotcom proceeding (the most recent substantive decision of which was that of the Court of Appeal in Ortmann et al v United States of America [2018] NZCA 233 [5 July 2018]) (the case as it has progressed through the various courts is referred to in this submission as the “Dotcom Proceeding”). The Dotcom Proceeding has now moved to the Supreme Court, so this issue may be considered there (Mega understands the Supreme Court hearing is set down for June 2019).</i></p>
20	What are the problems (or benefits) with using ‘object’ in the Copyright Act? What changes (if any) should be considered?
	<p><i>Mega’s entire business is focussed on the storage and communication of digital files. It makes no sense in Mega’s view for the parallel importation provisions and the criminal provisions to refer to “objects” rather than works since this creates uncertainty as to whether digital files are covered by those provisions. In the Dotcom Proceeding, the High Court held that digital files are not objects, while the Court of Appeal came to the opposite conclusion. It is Mega’s position that it should not be relevant whether a person committed copyright infringement by uploading a protected work without claim of right to a cloud storage provider and disseminating the link or by copying the same work to a USB thumb drive and sending it by post.</i></p> <p><i>Mega often assists law enforcement consistent with its Takedown Guidance Policy (including with respect to copyright works) and faces uncertainty whether a request in relation to a digital file falls within section 131 and may therefore be treated as a potentially criminal matter. This has flow-on effects when considering whether release of personal information is justified under one of the exceptions to the privacy principles in the Privacy Act 1993, where it is alleged that disclosure is required for the purposes of a criminal matter.</i></p>



21	Do you have any concerns about the implications of the Supreme Court's decision in Dixon v R? Please explain.
	<i>Mega agrees with the finding of the Supreme Court. All files a user uploads to a cloud storage service certainly remain his or her property.</i>
22	What are the problems (or benefits) with how the Copyright Act applies to user-generated content? What changes (if any) should be considered?
	<i>User-generated content is content where the uploader and the copyright holder are the same person. Its dissemination by the creator/uploader therefore does not constitute infringing activity. However, user-generated content often contains snippets of copyrighted works that the uploader does not have authorisation to distribute, e.g. in the context of movie reviews and parodies. In contrast to the US DMCA, the NZ Copyright Act does not contain a fair use exception, so these are currently not legal in NZ.</i>
59	What are problems (or benefits) with the ISP definition? What changes, if any should be considered?
	<i>Mega has not experienced any difficulties with the definition.</i>
61	Do the safe harbour provisions in the Copyright Act affect the commercial relationship between online platforms and copyright owners? Please be specific about who is, and how they are, affected.
	<i>Provided that the online platform acts swiftly in response to allegations of copyright infringement, it is Mega's view that the safe harbours appropriately balance the interests of the platform, rights-holders and users. As noted above, the rate of complaints and takedowns reported to Mega has reduced significantly over the 6+ years it has been in operation. Mega's operations in this regard have been favourably received by international rights-holder organisations and law enforcement.</i>
62	What other problems (or benefits) are there with the safe harbour regime for internet service providers? What changes, if any, should be considered?
	<i>There are three issues Mega would call out here:</i> <i>1. Crimes Act vs Copyright Act</i> ----- <i>The decision in the Dotcom Proceeding is of concern in that it seems to allow an "end run" around the careful balance of interests established in the Copyright Act under the offence and safe harbour provisions. Specifically, if a rights-holder is able to argue that all that is needed is criminality under the Crimes Act and that the safe harbours do not apply in that circumstance, the protection the safe harbour provisions was intended to afford becomes illusory.</i> <i>It should be made clear that the offence provisions in the Copyright Act are a code and supersede the Crimes Act provisions.</i> <i>It seems to Mega that this was Parliament's intention when one looks at the safe harbour regime recently enacted in sections 24 and 25 of the Harmful Digital</i>



Communications Act 2015 (HDCA). In particular, section 24(4) of the HDCA provides that the HDCA safe harbour does not apply to certain other specified statutory regimes, including copyright, but otherwise applies to any other content hosted by an online content host. It does this because Parliament was aware that the Copyright Act had its own safe harbours, and therefore it would be confusing and create potential inconsistencies for there to be two safe harbour regimes with different tests and processes dealing with copyright material. So, Parliament's intention was clear – to ensure that an online content host is protected from all liability for user uploaded content, under the safe harbour in the HDCA, or, for copyright material, under the safe harbours in the Copyright Act, subject to the online content host complying with the terms of those safe harbours.

It is Mega's view that if Parliament intended the safe harbours in the Copyright Act to not apply where an action is brought under the Crimes Act, it would not have excepted the Copyright Act from the safe harbour coverage in the HDCA. The manner in which the court in the Dotcom Proceeding has created a lacuna in the comprehensive safe harbour coverage for online content envisaged by sections 24 and 25 of the HDCA was not intended by Parliament and, in Mega's submission, should be remedied by making it clear that the Copyright Act offence provisions supersede the Crimes Act (i.e. the Copyright Act is a code in respect of copyright criminal causes of action) or, if that is not possible, the Copyright Act safe harbours should be explicitly extended to cover Crimes Act causes of action.

2. Section 92B "without more"

Section 92B is a very important safe harbour for general ISP activities. For example, it affords a safe harbour in respect of infringement of the communication right where none of the other safe harbours may do so.

The operative provision of section 92B, subsection 2, provides that where the user merely uses the services of the ISP to infringe copyright, without more being done by the ISP, the safe harbour will apply [Emphasis added]

The issue for Mega is – what do the words "without more" mean? In Mega's view, they are intended to connote the ISP knowingly participating in the infringement in some fashion and therefore losing its safe harbour, but this is very unclear. In the Dotcom Proceeding, the US has alleged that various activities often undertaken by an ISP, are evidence of knowing criminal infringement by the defendants in that case. The simple answer in Mega's submission is to remove those words and provide that the safe harbour is lost if an ISP "authorises" an infringement, as that term is used in section 16(1) (i) of the Act. This would then make section 92B(2) consistent with section 92B(3), which does refer to authorisation. This will add reasonable certainty given persuasive decisions on authorisation such as that in the iiNet case in Australia.

3. Notice requirements

The US DMCA is clear on what establishes knowledge of infringement that requires an online storage provider to take action to retain safe harbour protection: The receipt of a valid takedown notification complying with a number of formal and legal



	<p><i>requirements. This is a much more reliable basis than the vague NZ Copyright Act language of “knows or has reason to believe”, and s 92C should be changed to only require an ISP to take action in response to a valid notification, along with exact requirements – along the lines of the US DMCA §512(c)(3)(A).</i></p> <p>4. Counter-Notices</p> <p>-----</p> <p><i>Operating globally, Mega has chosen to allow counter-notices to be submitted consistent with the DMCA process. However, because sections 92C and 92D of the Copyright Act do not include a counter-notice process, there is uncertainty as to the safe harbour under s92C where Mega reinstates material or re-establishes a user’s access where they have filed a successful counter-notice that ultimately turns out to be invalid. In that circumstance it could be argued that Mega had knowledge under section 92C, has not taken the infringing content down or disabled access, and has therefore lost its safe harbour. Mega would argue that it no longer has a reason to believe that the material is infringing under section 92C when it puts it back in response to a valid counter-notice but it would prefer this issue to be tidied up by introducing a formal counter-notice procedure in the Act.</i></p>
86	Should ISPs be required to assist copyright owners enforce their rights? Why / why not?
	<p><i>As Mega has shown, it is fully prepared to assist rights-holders and does not charge for this service. However, where any court action is taken (for example injunctions if these are found available under ss92B et al), then the costs of those injunctions should be borne by the applicant. Mega is not intentionally deriving any benefit from storing infringing content and is active in taking it down when notified and in discouraging its upload in the first place (through clear wording in its policies). Conversely, it is the rights-holder which derives benefit from the exploitation of its works and from any successful infringement action.</i></p> <p><i>Assistance beyond a streamlined notice-and-takedown process, such as automated fingerprinting to identify known copyrighted works (as implemented by YouTube’s “ContentID”) is not technically feasible for a general cloud storage service that allows users to store any type of data (which is different from YouTube, which requires the uploaded material to be in a valid video format for playback), as such technology would be trivially circumvented by users obfuscating or encrypting the infringing file. European lawmakers will soon find out that Article 13 cannot ever be enforced for this very basic reason.</i></p>
87	Who should be required to pay ISPs’ costs if they assist copyright owners to take action to prevent online infringements?
	See above.

Stephen Hall
 Executive Chairman
 5th April 2019



Takedown Guidance

Guidance on Requesting User Information or "Takedown" of User Data

Overview

Mega is 'The Privacy Company' and values the privacy of the users of its services. The company is committed to maintaining industry-leading levels of security and confidentiality of user information and data. However, privacy is not an absolute right and is subject to limitations.

This guidance describes how Mega will look to achieve that balance and, in particular, the approach it will generally take to requests in criminal and civil actions against or involving its users. This guidance is aimed at providing transparency to everyone interested in Mega's services and consistency in actions.

THIS GUIDANCE IS PROVIDED FOR ASSISTANCE ONLY. IT DOES NOT CREATE ANY LEGALLY BINDING OBLIGATIONS ON THE PART OF MEGA AND MEGA BEARS NO LIABILITY WHATSOEVER FOR COMPLYING OR NOT COMPLYING WITH IT, AS IT SEES FIT, AT ANY TIME. ALL LIMITATIONS AND EXCLUSIONS OF LIABILITY SET OUT IN MEGA'S [TERMS OF SERVICE](#) APPLY EQUALLY TO THIS GUIDANCE.

Mega reserves the right, unless required otherwise by applicable law, to provide differing levels and categories of information in response to different requests. Persons making a request should first check with Mega what information will be available, particularly before applying for a criminal law production order or using civil law procedures to obtain user information or data.

Mega may amend, replace or withdraw this guidance temporarily or permanently from time to time as it sees fit. Mega will generally try to give advance notice if possible, before changes to this guidance come into effect.

Guiding Principles

The fundamental privacy-protective design of Mega's services underlies Mega's approach to law enforcement and takedown requests. This includes user control over the encryption/decryption keys as well as the extent and manner to which their files/folders are shared. In considering any request for user data, user information or action involving a Mega user, Mega starts from the position that user data and information is private.

This guidance will be publicly available, including by publication on Mega's website. Mega may also periodically publish a summary of requests received and actions taken under this guidance.

Separate guidance provisions will apply to Emergency Response, Objectionable Material, and allegations of Copyright or Other Intellectual Property Infringing Material. These are dealt with separately below.

Even if the decryption key is provided to staff or otherwise publicly available, Mega generally will not view, or attempt to view, files against which action is requested but it reserves the right to do so where the file has been decrypted if it considers necessary or appropriate. Mega is not obliged to take action unless required to do so by applicable law but any action will be undertaken objectively, based only on the information provided by third parties, this guidance, its [Terms of Service](#) and its [Privacy & Data Policy](#). Where there is any inconsistency between those Mega documents, the Terms of Service prevail.

Mega will promptly inform the user of any action taken where practicable provided it considers it appropriate or is required to do so by applicable law and provided it is not legally prevented from doing so by a court or other authority with appropriate jurisdiction.

Applicable law under this guidance is New Zealand law. However, Mega may, if it chooses to do so, without being obliged to do so, and without submitting itself to any other jurisdiction's law or courts or tribunals, consider requests made by and assist non-New Zealand law enforcement authorities and civil claimants in whole or in part. It may decline to do so for any reason or no reason while being guided by the Principles detailed above.

General Guidance

The provisions in this section apply to all criminal law enforcement and civil information and takedown requests other than those for Emergency Response, alleged Child Exploitation Material, alleged Copyright Infringing Material or alleged Other Intellectual Property Infringing Material (for which, see below).

Other than as set out below in those specific situations, Mega will generally only take action when required to do so by applicable law or a court or law enforcement authority with appropriate jurisdiction, although it reserves the right to do so at any time and for any reason or no reason, as set out in its [Terms of Service](#). For criminal matters, this generally means a 'production order' as per Subpart 2 of Part 3 of the [Search and Surveillance Act 2012](#) is required rather than simply a formal or informal request for information and/or action. For civil matters, this generally means a court non-party discovery order or, if that is not available, a witness summons, subpoena or agreed affidavit or statement of facts. Persons making civil requests should strictly comply with the New Zealand District Court or High Court Rules.

The information to be provided or action to be taken by Mega shall be as specified in the relevant law or order, subject to Mega being technically able to provide that information or take that action. As noted above, persons making criminal or civil information requests should contact Mega first to see what information may be able to be provided.

Emergency Response

This is defined as a situation where, in the expert judgement of a senior officer of the New Zealand Police or similar law enforcement officer or authority acceptable to Mega, Mega has written assurance that the person making the request has valid reasons to believe that disclosure or action is necessary to prevent or lessen a serious threat (as defined in section 2(1) of the [Privacy Act 1993](#)) to

- public health or public safety;
- the life or health of an individual or individuals;

and where the person giving such assurance confirms in writing that the threat is of such urgency that there is not time to obtain a production order or other court order.

If satisfied as to the above, Mega may, in its discretion, accept a request in such situations in good faith. In doing so, Mega will be relying on the assurances given by the person making such request and will look to them and their organisation to cover any costs, damages, penalties, compensation or other liability should that assurance turn out to be incorrect or wrongly given for any reason.

The information to be provided or action to be taken by Mega shall be as specified by, and agreed with, the appropriately designated officer.

Mega will provide the New Zealand Police and other agencies approved by Mega with the mobile phone number and email address of contact person(s) who will act on behalf of Mega in an emergency response situation.

Objectionable Material - Child Exploitation Material, Violent Extremism, Bestiality, Zoophilia, Gore, Malware, Hacked/Stolen Data, Passwords

Mega does not condone, authorise, support or facilitate the storage or sharing of Child Exploitation Material (**CEM**), also known as Child Sexual Abuse Material (**CSAM**) or other objectionable material as defined in section 3 of the [Films, Videos, and Publications Classification Act 1993](#) or other internet-harming material. Mega will take down or disable access to such material, close the user's account and provide account details and other data to the appropriate authorities as it sees fit.

Allegations of Copyright Infringement ("notice and takedown")

Users are warned in Mega's [Terms of Service](#) and when using the service that they must comply with all laws including copyright and other intellectual property laws. This includes, but is not limited to, a warning when generating a link for sharing files/folders in the File Manager.

Mega will publish on its website the information to be provided and statements to be made by copyright owners or their duly authorised agents/representatives, to notify Mega of an alleged copyright infringement.

All copyright infringement "takedown" notices should be made via the [specific webform](https://mega.nz/copyright) at <https://mega.nz/copyright> published on Mega's website or by email to copyright@mega.nz with all the information specified in clause 19 of the [Terms of Service](#).

The notice provider of alleged copyright infringement shall be given the option of requesting either removal of link(s) to an allegedly infringing file or removal of all file(s) relating to a specific link/URL.

For file links, the submitter is able to choose one of three options:

1. Disable the reported link - the file will remain in the user's account;
2. Disable all links pointing to the same byte sequence - the file will remain in the user's account;
3. Disable all links and remove all files from all accounts referencing the same byte sequence - there is no user permitted to store this under any circumstance worldwide.

Folder links often refer to a large number of files, of which only some are claimed to be infringing. If the submitter doesn't provide identification of the individual copyrighted works and files within the folder that are claimed to have been infringed, MEGA disables the reported link consistent with option (1) above. Rights-holders submit type (3) takedown requests for specific files within a folder after obtaining the handles for specific files within a folder (*select file(s) and use the right-click Get link(s) function*).

Mega will act on copyright infringement "takedown" notices in accordance with its [Terms of Service](#).

Allegations of Other Intellectual Property Infringement ("notice and takedown")

Mega will act in response to allegations of other forms of intellectual property infringement (e.g. trade mark infringement) in broadly similar fashion as for copyright infringement, reserving to itself the same discretions, rights and protections.

"Takedown" Notices of alleged intellectual property infringement other than copyright infringement, setting out full details similar to those required for copyright infringement "takedown" notices, should be sent to ip@mega.nz

Civil Court Action for Alleged Copyright or Other Intellectual Property Infringement

Where a third party initiates court action against a Mega user for alleged copyright or intellectual property infringement and wishes to access information held by Mega for that purpose, the

General Guidance above applies, i.e. this generally means a non-party discovery order or, if that is not available, a witness summons, subpoena or agreed affidavit or statement of facts. Persons making civil requests should strictly comply with the New Zealand District Court or High Court Rules.

Last updated 15 November 2018, effective 17 December 2018.



MEGA LIMITED TERMS OF SERVICE (“TERMS”)

Scope of these terms	1-4
Your data	5-9
Your obligations	10-12
What you can't do	13-14
Our IP	15-16
Your IP	17
Copyright Infringement Notices	18-20
Copyright Counter-Notices	21-28
Other Infringement Notices	29-30
Suspension and Termination	30-33
Export Control	34
Severability and Waiver	35
Force Majeure	36
Disclaimers	37-44
LIMITATION OF LIABILITY AND INDEMNITY BY YOU	45-48
Disputes and Choice of Law	49-50
Refunds	51
Recurring Paid Subscriptions	52
Cancellation of Recurring Paid Subscriptions	53
Information and Privacy	54-55
Notices	56
Rights to Third Parties	57
Entire Agreement	58

Scope of these terms

1. Welcome to Mega. Mega Limited ("Mega", "we", "us") provides cloud storage and communication services with user-controlled encryption. We provide services ourselves and via our [related or affiliated entities, payment processors and resellers](#) who act on our behalf, at our website at <https://mega.nz>, subdomains and related sites ("website"), using our mobile apps ("mobile apps"), and our application programming interface ("API"). Using Mega, you and other users can encrypt your files and data by way of user-controlled encryption ("UCE"), upload, access, store, manage, share, communicate, download and decrypt files, information, material, text chats, voice chats, video chats and other data (all of which we call "data" in these terms) and give access to that data to others (all together, "services" and each, a "service"). If you have questions about how to use our services or the great things you can do with Mega, check our [Help Centre](#) or, if you can't find the answer there, check our [contacts](#) page for details of who to contact.
2. These terms are binding and apply to any use of the services, website and our mobile apps by you and anyone who you allow to access your data or our services. By using our services, the website or our mobile apps, you and they irrevocably agree to these terms. If you do not like these terms or don't want to be bound, you can't use our services, the website or our mobile apps. In particular, OUR SERVICES ARE PROVIDED SUBJECT TO CERTAIN DISCLAIMERS BY US AND UNDERTAKINGS BY YOU, INCLUDING AN INDEMNITY FROM YOU IF YOU BREACH THESE TERMS – see clauses 37-48. NEW ZEALAND LAW AND ARBITRATION OF ANY DISPUTES APPLIES EXCLUSIVELY – see clauses 49 and 50.
3. We can change these terms at any time by providing you at least 30 days' prior notice of the change, whether via our website, via our mobile apps, by sending you an email or via any messaging service we provide. Your continued use after that notice means that you agree to the changed terms. If you have paid for a subscription that is due to expire after that 30 day notice period and you do not wish to continue to use our services under the new terms, you may terminate your subscription before the new terms come into force. We will then (but not otherwise) refund the unexpired portion of your subscription payment within 30 days and close your account. For more information about refunds, recurring paid subscriptions and their termination, see clauses 55-57.
4. If you comply with these terms, then we grant you a non-exclusive, non-transferable, worldwide licence to access and use our services via the website, our mobile apps and our API if applicable, in accordance with these terms and any plan you have subscribed for.

Your data

5. If you allow others to access your data (e.g. by giving them a link to, and a key to decrypt, that data), in addition to them accepting these terms, you are responsible for their actions and omissions while they are using our services and you agree to fully indemnify us for any claim, loss, damage, fine, costs (including our legal fees) and other liability if they breach any of these terms. This is particularly the case where you are the administrator of a business account (see clauses 51-54 below).
6. UCE is fundamental to our services. This means that you, not us, have encrypted control of who has access to your data. You should keep your password and Recovery Key safe and confidential. You must not share your password with anyone else and should not release encryption keys to anyone else

unless you wish them to have access to your data. **If you lose or misplace your password, you will lose access to your data.** Encryption won't help though if someone has full access to your system or device. We strongly urge you to use best practices for ensuring the safety and security of your system and devices (e.g. via unique passwords, security upgrades, firewall protection, anti-virus software, securing and encrypting your devices). Mega will never send you emails asking for your password or suggesting that you click a link to login to your account, so do not be fooled by any such email since it will not be from us.

7. You must maintain copies of all data stored by you on our services. We do not make any guarantees that there will be no loss of data or the services will be bug free. You should download all data prior to termination of services.
8. Our service may automatically (without us viewing the file content) delete a file you upload, store, access or share where it determines that the file is an exact duplicate of a file already on our service (a process usually referred to as deduplication). In that case, the original file will be accessed by you and any other user and that file will be retained as long as any user has a right to access it under these terms. Any right of deletion that you exercise will not apply to a deduplicated file that is associated with another user.
9. We will store your data on our service subject to these terms and any plan you subscribe to. If you choose to stop using our services, you must download your data first because after that we may, if we wish, delete it.

If we suspend or terminate our services to you because you have breached these terms, or someone you have given access to has breached these terms, during the term of that suspension we may, if we wish, delete your data immediately or deny you access to your data but keep it for evidential purposes. See also clauses 51-54 below which set out details of what happens to users within a business account when the business account is suspended or terminated.

In circumstances where we cease providing our services for other reasons, we will, if we consider it appropriate, it is reasonably practicable and we are not prevented by law or likely to incur any liability in doing so, give you 30 days' notice to retrieve your data.

Your obligations

10. Once you have subscribed to a plan for our services (with payment having been made via the website, one of our mobile apps or one of our [related or affiliated entities, payment processors and resellers](#)), you need to pay the fees (if any) for that plan (and any other taxes or duties). No matter which reseller or related or affiliated entity of Mega you make payment to, your contract for services is with Mega Limited and is governed exclusively by these terms and our policies referenced in these terms. We can also change the fees for our services (other than those you have already contracted and paid for) at any time if we give you notice. In the absence of manifest error or other lawful error, you can't withhold payment or claim any set-off without getting our written agreement.
11. If at any time you do not make a payment to us when you are supposed to (including on termination), we can (and this doesn't affect any other rights we may have against you):

- 11.1. suspend or terminate your use of the service and/or;
 - 11.2. make you pay, on demand, default interest on any amount you owe us at 10% per annum calculated on a daily basis, from the date when payment was due until the date when payment is actually made by you. You will also need to pay all expenses and costs (including our full legal costs) in connection with us trying to recover any unpaid amount from you.
12. You must:
- 12.1. where you have subscribed for a service, always give us and keep up to date, your correct contact and any billing details and those of any users within a business account;
 - 12.2. comply with these terms and any other agreements you have with us and ensure that users within a business account, of which you are administrator, do likewise;
 - 12.3. comply with all applicable laws, regulations and rules when using the website, our services and with respect to any data you upload, access or share using our services and ensure that users within a business account, of which you are administrator, do likewise.

What you can't do

13. You can't, and will ensure that no users within a business account, of which you are administrator:
- 13.1. assign or transfer any rights you have under these terms to any other person (including by sharing your password with someone else) without our prior written consent;
 - 13.2. do anything that would damage, disrupt or place an unreasonable burden on our website or service or anyone else's use of our website, our mobile apps or a service including but not limited to denial of service attacks or similar;
 - 13.3. infringe anyone else's intellectual property (including but not limited to copyright) or other rights in any data;
 - 13.4. resell or otherwise supply our services to anyone else without our prior written consent;
 - 13.5. open multiple free accounts;
 - 13.6. use our website, mobile apps, API, or any service, including, without limitation, any communication tools available through the website, our mobile apps, or our API, or any forum, chat facility or message centre that we provide:
 - 13.6.1. to store, use, download, upload, share, access, transmit, or otherwise make available, data in violation of any law in any country (including to breach copyright or other intellectual property rights held by us or anyone else);
 - 13.6.2. to send unwelcome communications of any kind (including but not limited to unlawful unsolicited commercial communications) to anyone (e.g. spam or chain letters);
 - 13.6.3. to abuse, defame, threaten, stalk or harass anyone, or to harm them as defined in the Harmful Digital Communications Act 2015 (NZ) or any similar law in any jurisdiction;

- 13.6.4. to store, use, download, upload, share, access, transmit, or otherwise make available, unsuitable, offensive, obscene or discriminatory information of any kind;
 - 13.6.5. to run any network scanning software, spiders, spyware, robots, open relay software or similar software;
 - 13.6.6. to upload anything or otherwise introduce any spyware, viruses, worms, trojan horses, time bombs or bots or any other damaging items which could interfere with our, or anyone else's, network, device or computer system;
 - 13.6.7. to use any software or device which may hinder the services (like mail bombs, war dialing, automated multiple pinging etc.);
 - 13.6.8. to attempt to gain unauthorised access to any services other than those to which you have been given express permission to access; or
 - 13.6.9. to impersonate anyone or to try to trick or defraud anyone for any reason (e.g. by claiming to be someone you are not).
14. If you register with us, you will need to use a password in conjunction with your specific account email address. You need to make sure your password is secure, not used by you on other sites and confidential. Make sure you tell us straight away if you think or know someone else has used your password or there has been any other security breach. We will hold you responsible for anything done using your account and password. **MAKE YOUR PASSWORD A STRONG ONE AND KEEP IT SECURE.** We are not responsible if someone else gains access to your computer or other device and/or your Mega password and/or encryption keys for any files.

Intellectual Property

Our IP

15. You are not allowed to, and you can't let anyone else (including in particular any user within a business account of which you are administrator), use, copy, alter, distribute, display, licence, modify or reproduce, reverse assemble, reverse compile, communicate, share, transmit or otherwise make available, (whether digitally, electronically, by linking, or in hard copy or by any means whatsoever), any of our code, content, copyright materials, intellectual property or other rights without getting our permission in writing, other than in order to use our services as intended or as allowed under any open source licences under which we use intellectual property provided by others. The open source code that we use, where we obtained it, and licences for that code, are all referenced on our website and via our mobile apps.
16. Without limiting any other provision of these terms, you are only permitted to directly and specifically use the API if you register at the developer registration page and agree that you may only publish or make available your application after we have approved it pursuant to our application approval process and licence agreement available on request at api@mega.nz

Your IP

17. You own, or undertake that you are authorised to use, any intellectual property in any data you store on, use, download, upload, share, access, transmit or otherwise make available to or from, our systems or using our services. You grant us a worldwide, royalty-free licence to use, store, back-up, copy, transmit, distribute, communicate, modify and otherwise make available, your data, solely for the purposes of enabling you and those you give access to, to use our services and for any other purpose related to provision of the services to you and them.

Copyright Infringement Notices

18. We respect the copyright of others and require that users of our services comply with copyright laws. You are strictly prohibited from using our services to infringe copyright. You may not upload, download, store, share, access, display, stream, distribute, e-mail, link to, communicate, transmit, or otherwise make available any files, data, or content that infringes any copyright or other proprietary rights of any person or entity.
19. We will respond to notices of alleged copyright infringement that comply with applicable law and are properly provided to us. If you believe that your content has been copied or used in a way that constitutes copyright infringement, please provide us with the following information:
 - i. a physical or electronic signature of the copyright owner or a person authorised to act on their behalf;
 - ii. identification of the copyrighted work claimed to have been infringed;
 - iii. identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit us to locate the material including the exact URL link (with decryption key) to that material on Mega;
 - iv. your contact information, including your address, telephone number, and an email address; a statement by you that you have a good faith belief that use of the material in the manner complained of is not authorised by the copyright owner, its agent, or the law; and
 - v. a statement that the information in the notification is accurate, and, under penalty of perjury (unless applicable law says otherwise), that you are authorised to act on behalf of the copyright owner.
20. We reserve the right to remove data alleged to be infringing without prior notice, at our sole discretion, and without liability to you. In appropriate circumstances, we will also terminate your account if we consider you to be a repeat infringer. Details of our designated copyright agent for notice of alleged copyright infringement are on our [contacts](#) page.

Copyright Counter-Notices

21. We process all takedown notices based on good faith acceptance of the representations from the party submitting the takedown notice. We do not review the material before processing the takedown notice.
22. You may file a counter-notice if you believe that access to a file you have uploaded has been wrongly disabled because it was the subject of an incorrect takedown notice. You should only do so if you are confident that no other party owns copyright in the material, or you have rights to store the material and, if you are sharing it, that you have the right to do so.
23. Please understand that:
 - 23.1. When we receive your counter-notice, we pass it, including your address and other contact information, to the party who issued the original takedown notice. By submitting your counter-notice you authorise us to do so.
 - 23.2. Filing a counter-notification may lead to legal proceedings between you and the complaining party.
 - 23.3. There may be adverse legal consequences in New Zealand and/or your jurisdiction if you make a false or bad faith allegation by using this process.
 - 23.4. If, when using this counter-notice process, you make a false or bad faith allegation or otherwise breach these terms or any of our policies and that causes us any loss, costs (including legal costs), damages or other liability, we reserve the right to claim for and recover from you that loss, those costs (including full legal costs on a solicitor-client basis), damages and other liability, by deduction from any balance in our account and/or by proceedings in New Zealand and/or the jurisdiction of the address in your counter-notice.
 - 23.5. We provide this counter-notice process voluntarily for the purposes of all applicable copyright takedown and counter-notice regimes in New Zealand and other jurisdictions, but, in doing so, we do not submit to any jurisdiction, law, tribunal or court other than those of New Zealand, as set out in these terms. We may amend, suspend or withdraw this counter-notice process at any time, provided that any counter-notices in train at that time shall continue to be processed.
24. By filing a counter-notice, you are deemed to have accepted the above terms. If you do not accept the above terms, do not file a counter-notice.
25. To file a counter-notice with us, you must provide a written communication at <https://mega.nz/copyright> or by email to copyright@mega.nz that includes substantially the following:
 - 25.1. Identification of the specific URL(s) of material that has been removed or to which access has been disabled.
 - 25.2. Your full name, address, telephone number, email address and the username of your Mega account.
 - 25.3. The statement: "I have a good faith belief that the material was removed or disabled as a result of a mistake or misidentification of the material to be removed or disabled."

- 25.4. The reasons for that good faith belief, sufficient to explain the mistake or misidentification to the person who filed the original takedown notice.
 - 25.5. The statement "I will accept service of proceedings in New Zealand or in the jurisdiction where my address in this counter-notice is located, from the person who provided Mega Limited with the original copyright takedown notice or an agent of such person."
 - 25.6. Signature. A scanned physical signature or usual signoff in an email or using our webform will be accepted.
 - 25.7. You may also provide comments.
26. We will only accept a counter-notification directly from the user from whose account a folder or file has been disabled. Counter-notifications must be submitted from the email address associated with the Mega account.
 27. If we do not receive any further communication from or on behalf of the person who originally submitted the takedown notice, or any communication we do receive does not in our sole opinion adequately justify the original takedown notice, we may, but shall not be obliged to, reinstate the material in approximately 10-14 days provided we have no reason to believe that the material infringes copyright.
 28. Nothing in this counter-notice section prejudices our right to remove or disable access to any material at any time, for any reason or no reason.

Other Infringement Notices

29. If you consider there has been some other infringement or breach of law, or of these terms, and wish to file a complaint, contact us at the relevant address on our [contacts](#) page. We will generally require the same amount of detail as set out above for copyright infringement notices. See also our [Takedown Guidance Policy](#).

Suspension and Termination

30. You can terminate your access to our services at any time by following the 'Cancel your account' link in the Account section of the website or the Settings section of our mobile apps. However, we will not provide any part-refund for any allowance not used on any subscription you may have, other than under clause 3 above. If you are a business account administrator you may also terminate access to any user within the business account.
31. We can immediately suspend or terminate your, and that of other users within a business account, access, to the website and our services without notice to you:
 - 31.1. if you or they breach any of these terms or any other agreement you or they have with us;
 - 31.2. at any time if you are not a registered user;

- 31.3. if you are using a free account and that account has been inactive for over 3 months or we have been unable to contact you using the email address in your account details.
32. We may also terminate or suspend our services or any part of our services, for all users or for groups of users, without notice, at any time, for any reason or no reason.
33. All charges outstanding on your account must be paid at termination.

Export Control

34. You may not use, export, re-export, import, or transfer any software or code supplied as part of your use of our services: (a) into any United States or New Zealand embargoed countries; or (b) to anyone listed as a specifically prohibited recipient by the United States Government or the New Zealand Government. By using the website and our services, you represent and warrant that you are not located in any such country or on any such list. You also will not use the website or our services for any purpose prohibited by United States, New Zealand or any other law, including, without limitation, the development, design, manufacture or production of missiles, nuclear, chemical or biological weapons.

Severability and Waiver

35. If any provision of these terms is held to be invalid or unenforceable, the remaining provisions will remain in full force and effect. If we do not enforce any right or provision of these terms or if we in any instance grant any concession or indulgence, that will not be deemed a waiver of such right or provision or obligate us to grant any concession or indulgence to anyone else.

Force Majeure

36. We will not be liable by reason of any failure or delay in the performance of our obligations because of events beyond our reasonable control, which may include, without limitation, denial-of-service attacks, strikes, shortages, riots, insurrection, fires, flood, storm, explosions, acts of God, war, terrorism, governmental action, labour conditions, earthquakes, material shortages, extraordinary internet congestion or extraordinary connectivity issues or failure of a third party host, (each a "Force Majeure Event"). Upon the occurrence of a Force Majeure Event, we will be excused from any further performance of the obligations which are affected by that Force Majeure Event for so long as the event continues.

DISCLAIMERS

37. WE DON'T GIVE YOU ANY WARRANTY OR UNDERTAKING ABOUT THE SERVICES OR THE WEBSITE WHICH ARE PROVIDED "AS IS". TO AVOID DOUBT, ALL IMPLIED CONDITIONS OR WARRANTIES ARE EXCLUDED

AS MUCH AS IS PERMITTED BY LAW, INCLUDING (WITHOUT LIMITATION) WARRANTIES OF MERCHANTABILITY, FITNESS FOR PURPOSE, SAFETY, RELIABILITY, DURABILITY, TITLE AND NON-INFRINGEMENT.

38. We will try to give you access to our website and our mobile apps all the time, but we do not make any promises or provide you with a warranty that our website or the services will be without any faults, bugs or interruptions.
39. Whilst we intend that the services should be available 24 hours a day, seven days a week, it is possible that on occasions the website or services may be unavailable to permit maintenance or other development activity to take place or be periodically interrupted for reasons outside our control.
40. Information on our website will change regularly. We will try to keep our website up to date and correct, but again, we do not make any promises or guarantees about the accuracy of the information on our website.
41. We do not warrant that the services will meet your requirements or that they will be suitable for any particular purpose.
42. You are the controller in respect of some data Mega holds about you and Mega is the processor, for General Data Protection Regulation (“GDPR”) purposes. Mega is the controller in respect of some other data. See our [Privacy & Data Policy](#) for more details. These terms, our [Privacy & Data Policy](#) and our [Takedown Guidance Policy](#) are the contract between us that governs our processing of that data. It is your sole responsibility to determine that the services meet the needs of you, your business or otherwise and are suitable for the purposes for which they are used.
43. We also aren't legally responsible for:
 - 43.1. any corruption or loss of data or other content which you or anyone else may experience after using our website or our mobile apps, or any problems you may have when you view or navigate our website or use any of our mobile apps;
 - 43.2. devices or equipment that we do not own or have not given you;
 - 43.3. any loss or damage if you do not follow our reasonable instructions, these terms, our [Privacy & Data Policy](#) and our [Takedown Guidance Policy](#);
 - 43.4. any actions or non-actions of other people which disrupt access to our website, our mobile apps, or our API, including the
 - 43.4.1. content and nature of any data that you upload, access or share;
 - 43.4.2. content of ads appearing on our website or our mobile apps (including links to advertisers' own websites) as the advertisers are responsible for the ads and we don't endorse the advertisers' products;
 - 43.4.3. content of other people's websites even if a link to their website is included on our website or our mobile apps.
44. You warrant that if you are accessing and using the services for the purposes of a business then, to the maximum extent permitted by law, any statutory consumer guarantees or legislation intended to

protect non-business consumers in any jurisdiction (such as the Consumer Guarantees Act 1993 in New Zealand) do not apply to the supply of the services, the website, our mobile apps or these terms.

LIMITATION OF LIABILITY AND INDEMNITY BY YOU

45. TO THE MAXIMUM EXTENT PERMITTED BY LAW, WE (THIS INCLUDES OUR EMPLOYEES, OFFICERS, AGENTS AND AUTHORISED RESELLERS) ARE NOT LIABLE WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), EQUITY OR ON ANY OTHER GROUNDS TO YOU OR ANYONE ELSE FOR ANY DIRECT, INDIRECT OR CONSEQUENTIAL DAMAGE, LOSS, COST OR EXPENSE, DAMAGE TO PROPERTY, INJURY TO PERSONS, LOSS OF PROFITS, LOSS OF DATA OR REVENUE, LOSS OF USE, LOST BUSINESS OR MISSED OPPORTUNITIES, WASTED EXPENDITURE OR SAVINGS WHICH YOU MIGHT HAVE HAD, DENIAL OF SERVICE OR ACCESS TO OUR WEBSITE, OUR MOBILE APPS OR OUR API, OCCURRING DIRECTLY OR INDIRECTLY FROM THE USE OR ABILITY OR INABILITY TO USE, OR RELIANCE ON, OUR WEBSITE, OUR MOBILE APPS OR OUR API, OR THE SERVICES, AND BASED ON ANY TYPE OF LIABILITY INCLUDING BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), STATUTORY OR PRODUCT LIABILITY, OR OTHERWISE.
46. YOU SHALL INDEMNIFY US AGAINST ALL CLAIMS, COSTS (INCLUDING ALL OUR LEGAL COSTS), EXPENSES, DEMANDS OR LIABILITY, DAMAGES AND LOSSES WHETHER DIRECT, INDIRECT, CONSEQUENTIAL, OR OTHERWISE, AND WHETHER ARISING IN CONTRACT, TORT (INCLUDING IN EACH CASE NEGLIGENCE), OR EQUITY OR OTHERWISE, ARISING DIRECTLY OR INDIRECTLY FROM BREACH BY YOU OR ANYONE YOU GIVE ACCESS TO YOUR DATA, OF ANY OF THESE TERMS OR ANY POLICY REFERENCED IN THESE TERMS.
47. IF YOU ARE NOT SATISFIED WITH THE SERVICES, THEN YOUR SOLE AND EXCLUSIVE REMEDY IS TO TERMINATE YOUR USE OF OUR SERVICES AND THE CONTRACT YOU HAVE WITH US.
48. DESPITE THE ABOVE, IF ANY COURT OR OTHER COMPETENT AUTHORITY HOLDS US (THIS INCLUDES OUR OFFICERS, STAFF AND AGENTS) LIABLE FOR ANY MATTER RELATED TO THESE TERMS OR OUR SERVICES, OUR TOTAL COMBINED LIABILITY WILL BE LIMITED TO THE MOST RECENT SUBSCRIPTION AMOUNT YOU HAVE PAID TO US.

Disputes and Choice of Law

49. Any and all disputes arising out of this agreement, its termination, or our relationship with you shall be determined by binding arbitration under the Arbitration Act 1996 in Auckland, New Zealand, by one arbitrator who shall be a lawyer knowledgeable in relevant technology matters appointed by the President for the time being of the Arbitrators and Mediators Institute of New Zealand Incorporated (AMINZ) on a request by either you or us. The following terms apply to the arbitration in addition to those implied by New Zealand law:

49.1. Notice must be given to apply for any interim measure in the arbitration proceeding;

- 49.2. The arbitration proceeding will commence when a request is made to AMINZ to appoint an arbitrator;
 - 49.3. The arbitration shall be in English. The Arbitrator shall permit the parties and witnesses to appear by videoconference that we will organise and pay for;
 - 49.4. We will pay the arbitrator's fees and expenses unless the arbitrator determines that you should meet some or all of those fees and expenses because your dispute is frivolous or vexatious.
50. The relationship we have with you under these terms and their interpretation and construction together with any dispute, suspension or termination arising out of or in connection with them, is governed exclusively by New Zealand law. Mega does not submit to any other jurisdiction other than New Zealand and New Zealand law. You and we submit to the exclusive jurisdiction of the New Zealand arbitral tribunals (and courts for the purposes of the enforcement of any arbitral award or appeal on question of law). The parties agree to enforcement of the arbitral award and orders and any judgement in New Zealand and in any other country.

Business Accounts

51. For business accounts, the administrator of that account can see and deal with the files and data associated with all users within that account (including any data and any personal information). In addition:
- 51.1. if the business account is suspended or terminated, the action will affect the data and personal information of every user within that account;
 - 51.2. the administrator of the business account will be able to see and deal with, change or delete the files and data associated with every user within that account (including any of data and personal information);
 - 51.3. the administrator of the business account will be able to terminate any user's account within the business account, restrict or disable usage of the account, change any user's password and otherwise deny access to the account and all data and personal information and such users will then lose access to all their data and all personal information associated their account.
52. We will charge the credit card associated with the business account with the applicable fees per user (for a minimum of three users) at the monthly billing date, on a recurring basis.
53. Where a business account recurring payment fails for any reason, after 30 days we may suspend the account and all users within that account until payment is made. If no payment is made within a reasonable period of time, we will be entitled to terminate the business account and all users within that account, in which case all data and personal information associated with those users and the account will be subject to deletion in accordance with these terms.
54. Since business accounts and the users within them are entitled to unlimited storage, they are subject to a fair use policy as follows:
- 54.1. Business accounts are only to be used for business purposes;
 - 54.2. Business accounts are intended for multiple users and are not to be held or used by one person;

- 54.3. Each user must comply with these terms. Any breach of these terms by one user will be treated as a breach of these terms in respect of the whole account;
- 54.4. Mega will not be liable to any business account user should the actions of another user within the account, including the administrator of the business account, cause any loss or damage to another user within the business account (including by way of deletion, amendment, sharing or any other dealing with data or personal information);
- 54.5. Each user's use of the business service must be fair, reasonable and not excessive, as reasonably determined by us by reference to average and/or estimated typical per business user usage of the business service. We will consider usage to be excessive and unreasonable where it materially exceeds the average and/or estimated use patterns over any day, week or month (or other period of time as determined by us) ("excessive usage"). If we identify excessive usage or consider that usage patterns on any business account indicate that any of the usage is not for business purposes we may suspend, and after 30 days' notice terminate, any or all of the users or the whole business account, in which case data and personal information associated with those users and the account will be subject to deletion in accordance with these terms. Examples of such unreasonable usage patterns also include: making non-business data publicly available, adding users who do not appear to Mega to be associated with the business, and uploading or sharing files from non-business related third party sites.

Refunds

55. Unless otherwise provided by New Zealand law or by a particular service offer, all purchases are final and non-refundable. If you believe that Mega has charged you in error, you must contact us within 90 days of such charge. No refunds will be given for any charges more than 90 days old. We reserve the right to issue refunds or credits at our sole discretion. If we issue a refund or credit, we are under no obligation to issue the same or similar refund in the future. This refund policy does not affect any statutory rights that may apply. If you have made a payment by mistake and have not used the subscription plan services, you must contact support@mega.nz within 24 hours. This will be acknowledged promptly and answered within 7 days.

Recurring Paid Subscriptions

56. Recurring subscriptions will renew indefinitely, either monthly or annually, based upon your chosen subscription period, unless the subscription is cancelled prior to a renewal date. For recurring subscriptions established via mobile apps using in-app-purchase platforms, you should refer to your app store account for details of the dates and terms of the subscription. Any other recurring subscription will renew on the same day of month as it was established, except in cases where the day is not available due to a short month, in which case the renewal date will be moved to the first day of the following month.

Cancellation of Recurring Paid Subscriptions

57. Recurring subscriptions established through the mobile app using in-app-purchase platforms should be cancelled through the relevant app store account directly. Any other recurring subscription should be cancelled by navigating to <https://mega.nz/account> in your browser and selecting the option to cancel your subscription. Any payments processed after an effective subscription cancellation will be promptly refunded by us. If you cancel a paid subscription, but you maintain your Mega account as a free account, access to your account may be restricted or blocked if the level of use is above the limits applying to free accounts at that time.

Information and Privacy

58. We reserve the right to disclose data and other information as required by law or any competent authority. Our approach is referenced in our [Privacy & Data Policy](#) and [Takedown Guidance Policy](#), both of which are subject to these terms.
59. You and anyone else you give access to are also bound by our [Privacy & Data Policy](#) and [Takedown Guidance Policy](#).
By accepting these terms, you also accept our [Privacy & Data Policy](#) and [Takedown Guidance Policy](#).

Notices

60. You can contact us by sending an email to support@mega.nz. If we need to contact you or provide you with notice we will email you at the email address you have recorded in your account details and such notices will be valid and deemed to be received by you whether or not you are using that address. We may also send notices via any chat facility or internal messaging system we may provide.

Rights to Third Parties

61. Mega Limited employees, officers, agents, related companies and affiliates together with authorised suppliers of services to and authorised resellers of, our services, are entitled to the benefit of all indemnities and other provisions of these terms which are for the benefit of Mega in these terms.

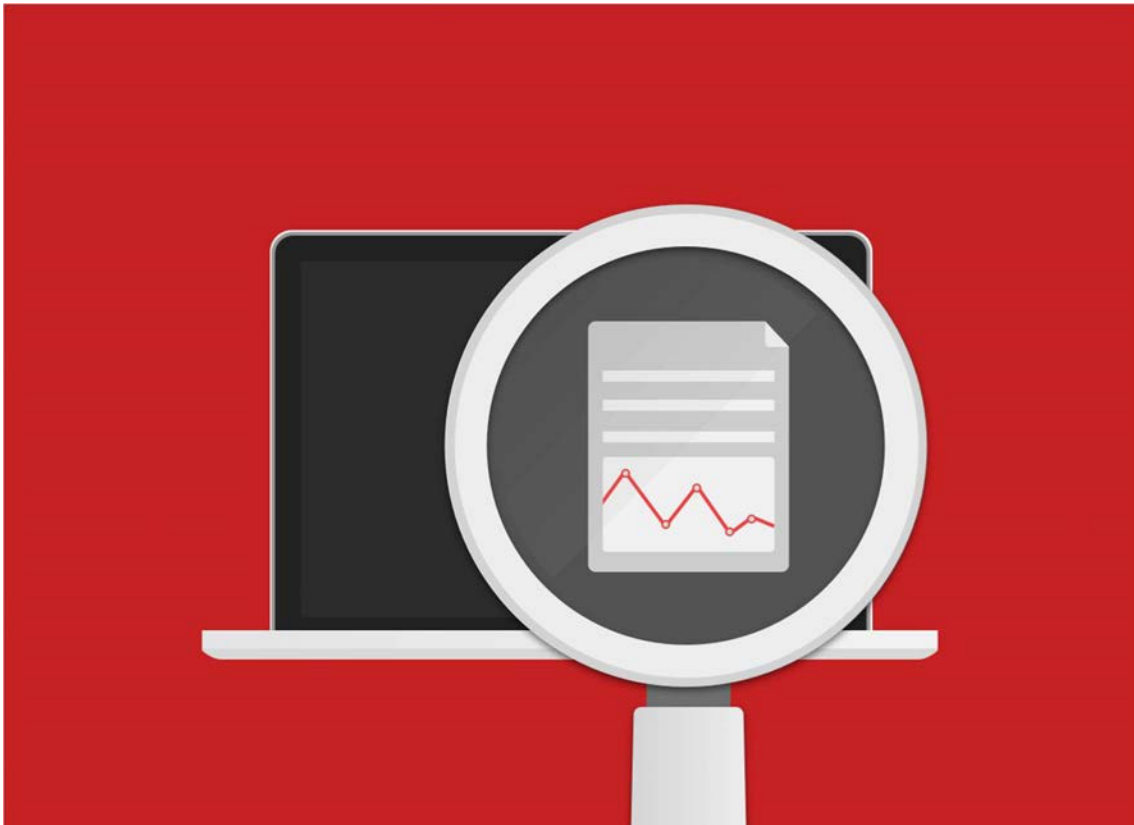
Entire Agreement

62. These terms, our [Privacy & Data Policy](#), and [Takedown Guidance Policy](#), the terms of any plan you purchase and any other terms and policies expressly referenced in these terms, together constitute the entire agreement between us relating to your use of the website, our mobile apps, our API and our services. From the date they come into force, in respect of any use of any of our services after that, they supersede and replace any prior agreement, arrangement or understanding between you and us



regarding the use of our services. No agreement, arrangement or understanding alleged to be made between us, or representation alleged to be made, by us or on our behalf, to you, if inconsistent with these terms, shall be valid unless agreed to in writing by an executive officer of Mega Limited.

Last updated 15 November 2018, effective 17 December 2018.



Mega Transparency Report

September 2017

Requests for Removal of Content and for User Information

Report Issued November 2017



Introduction

This is the third transparency report published by Mega since it commenced operations in January 2013. In accordance with its transparency policy, Mega periodically publishes statistics on takedown requests, subscriber information disclosure and related issues.

Regulatory Background

Mega was designed, and is operated, to ensure that it achieves the highest levels of compliance with regulatory requirements.

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, 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 they 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 access to the offending files disabled.

New Zealand's Copyright Act process provides Mega with a safe harbour, shielding Mega from liability for the material that its users upload and share using Mega's services. Although not technically bound by US or EU law, Mega also complies with the conditions for safe harbour under the US Digital Millennium Copyright Act (**DMCA**) process and the European Union Directive 2000/31/EC. Mega does so 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 takedown notices continues to be very small, indicative of a user base which appreciates the speed and flexibility of Mega's system for legitimate business and personal use.

The safe harbours in various jurisdictions require material to be removed or links disabled expeditiously. Some cloud storage 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.

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 requirements¹.

¹ <https://mega.nz/#terms>



Mega has very clear Terms of Service that have to be acknowledged by every new user before their account activation can be completed. Those terms make it very clear (e.g. in clauses 17-20) that Mega won't tolerate infringement or any other illegal activity.

However it is logistically impossible for any cloud storage service (or indeed any other service provider in the Internet chain, such as the computer supplier, ISP, browser supplier etc), to review all uploaded content due to the number of files that are uploaded each second. Mega's current rate is more than 40 million files per day or 500 per second. The infeasibility of checking uploads has been recognised in numerous court cases, even prior to enactment of the DMCA.

Even if content could be reviewed, it is not possible to determine whether it is infringing or not. Owners of many copyrighted materials provide the user with a licence to make a backup copy, so uploading it to a cloud storage service would not be infringing.

Other similar cloud storage services don't make any positive (but almost certainly futile) attempt to assess the copyright status of uploaded materials.

Requests for Removal of Content

Mega accepts takedown notices via a dedicated web page² or by email to takedowns@mega.nz

Requests are processed within a few hours, without reviewing their validity³.

The submitter is able to choose one of three options:

1. Disable the reported link - *the file will remain in the user's account;*
2. Disable all links pointing to the same byte sequence - *the file will remain in the user's account;*
3. Disable all links and remove all files from all accounts referencing the same byte sequence - *there is no user permitted to store this under any circumstance worldwide.*

Mega receives counter-notices from some users who dispute the validity of a takedown. These counter-notices are processed consistent with the safe harbour requirements. Our experience is that most of the counter-notices are genuine and appropriate, due to content owners and agents trawling the Internet using robots which generate incorrect notices on behalf of copyright owners and due to the failure of owners/agents to review the specific link content.

The number of unique takedown requests submitted represents a very small and declining percentage of the total number of files stored on Mega. In Q3 2017, the files taken down represented 0.0002% of the 36 billion files stored on Mega servers.

<https://mega.nz/#takedown>

<https://mega.nz/#copyright>

² <https://mega.nz/#copyrightnotice>

³ It is impossible to review the validity as the file contents are user-encrypted, unless the user has published or provided the encryption key.



		Total Takedown Requests	Taken Down Files / Total Files	Total Files (Billion)
2013	Q1	51,857	0.0192%	0.2
	Q2	53,772	0.0151%	0.3
	Q3	91,493	0.0142%	0.4
	Q4	117,546	0.0135%	0.6
2014	Q1	91,106	0.0063%	1.1
	Q2	102,798	0.0042%	1.8
	Q3	111,220	0.0028%	2.5
	Q4	404,965	0.0043%	3.6
2015	Q1	134,982	0.0021%	5.0
	Q2	84,210	0.0013%	6.6
	Q3	68,064	0.0008%	8.9
	Q4	57,108	0.0005%	11.9
2016	Q1	74,955	0.0005%	15.0
	Q2	110,878	0.0006%	18.2
	Q3	82,917	0.0004%	21.8
	Q4	85,605	0.0003%	25.8
2017	Q1	91,110	0.0003%	29.3
	Q2	90,156	0.0003%	32.5
	Q3	68,547	0.0002%	35.7

It should be noted that within these takedown statistics, there are a significant number of incorrect takedown notices that do not relate to infringing material.

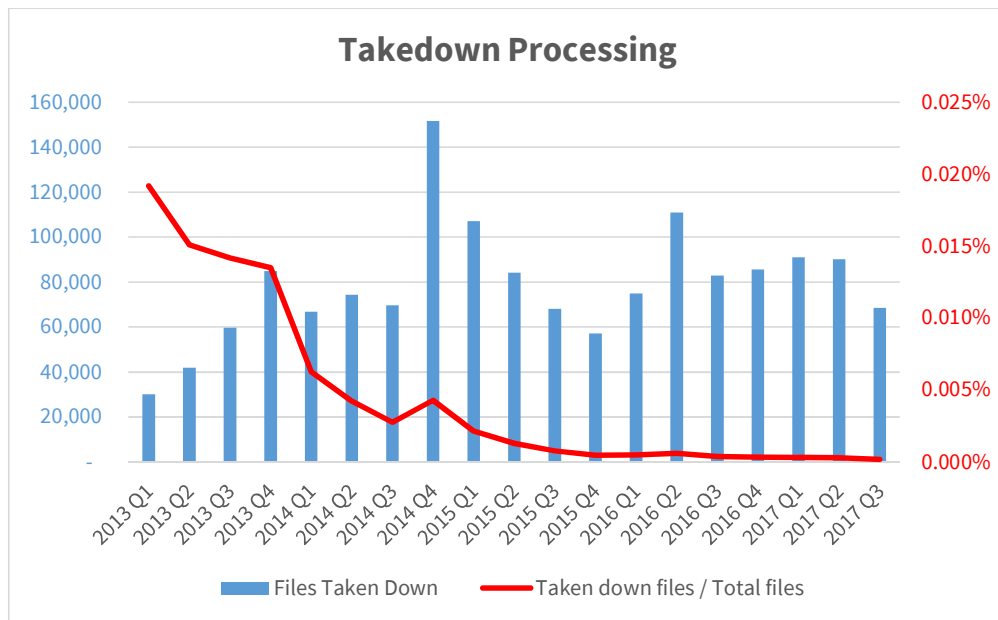


Figure 1 Requests for file takedowns show a continuing decline as a % of files stored



Repeat Infringers

Mega suspends the account of any user with 3 takedown actions. In some cases, the account can be reinstated where it is proved to be the subject of invalid takedown notices, but most suspended accounts are terminated. Up to 30 September 2017, Mega had suspended 70,000 users for repeated infringement. The data below shows that the suspensions are declining as a % of the number of registered users.

Year	Quarter	Number of Suspended Users	% of Registered Users
2013	Q1	1,137	0.043%
	Q2	2,336	0.067%
	Q3	3,305	0.073%
	Q4	7,821	0.131%
2014	Q1	5,719	0.074%
	Q2	2,965	0.030%
	Q3	2,017	0.016%
	Q4	2,722	0.018%
2015	Q1	2,376	0.014%
	Q2	1,523	0.007%
	Q3	1,285	0.005%
	Q4	*2,241	0.007%
2016	Q1	2,027	0.005%
	Q2	3,193	0.007%
	Q3	2,086	0.004%
	Q4	2,371	0.004%
2017	Q1	3,562	0.005%
	Q2	5,615	0.007%
	Q3	8,127	0.009%

*Plus 7,245 suspended due to the retroactive change to suspension after 3 strikes (previously after 5 strikes).

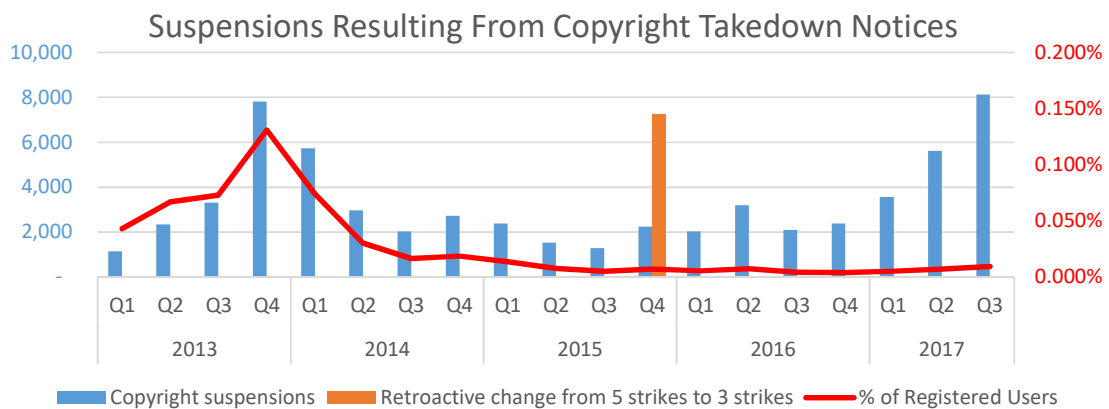


Figure 2 Suspensions continue to be a very low % of registered users.



Court Orders / Warrants etc

During the 2016-2017 year, Mega has disclosed information about 34 user accounts which are alleged to be involved in criminal activity overseas after being served a legal order from a NZ authority.

Objectionable (Illegal) Content

MEGA has zero tolerance for users sharing Child Sexual Abuse Material (CSAM). Any reports of illegal obscene content result in immediate deactivation of the file links, closure of the user's account and provision of the details to the New Zealand Government Authorities for investigation and prosecution.

Requests for Personal Information

Mega is 'The Privacy Company' and values the privacy of the users of its services. The company is committed to maintaining industry-leading levels of security and confidentiality of user information and data. However, privacy is not an absolute right and is subject to limitations. We take all requests for the disclosure of user information seriously. In considering any request for user data, user information, or action involving a Mega user, Mega starts from the position that user data and information is private.

Unless an Emergency Response is required, or disclosure is necessary to assess or gather evidence in relation to an active or proposed investigation involving child exploitation material, Mega will generally only provide user details when required to do so by New Zealand law, or by a New Zealand court or law enforcement authority with appropriate jurisdiction. Mega may consider requests made by non-New Zealand law enforcement authorities and civil claimants.

Mega defines Emergency Response as a situation where, in the expert judgement of a senior officer of the New Zealand Police or similar law enforcement officer or authority acceptable to Mega, Mega has written assurance that the person making the request has valid reasons to believe that disclosure or action is necessary to prevent or lessen an imminent and serious threat (as defined in section 2(1) of the Privacy Act 1993) to public health or public safety, the life or health of an individual or individuals and where the person giving such assurance confirms in writing that the threat is of such imminence that there is not time to obtain a production order or other court order.

If satisfied as to the above, Mega may in its discretion accept a request in such situations in good faith.

When we receive a request, we make sure it is legitimate and we provide advance notice to the affected user unless prohibited by a court order or where we decide delayed notice is appropriate, based on criteria described in our privacy policy.

All files stored on Mega are encrypted prior to being uploaded to our system and therefore we do not and cannot access that content unless we are provided with the decryption key. Mega does have access to registration information and IP addresses used to access our services.



The chart below shows the number of requests that were manually processed.

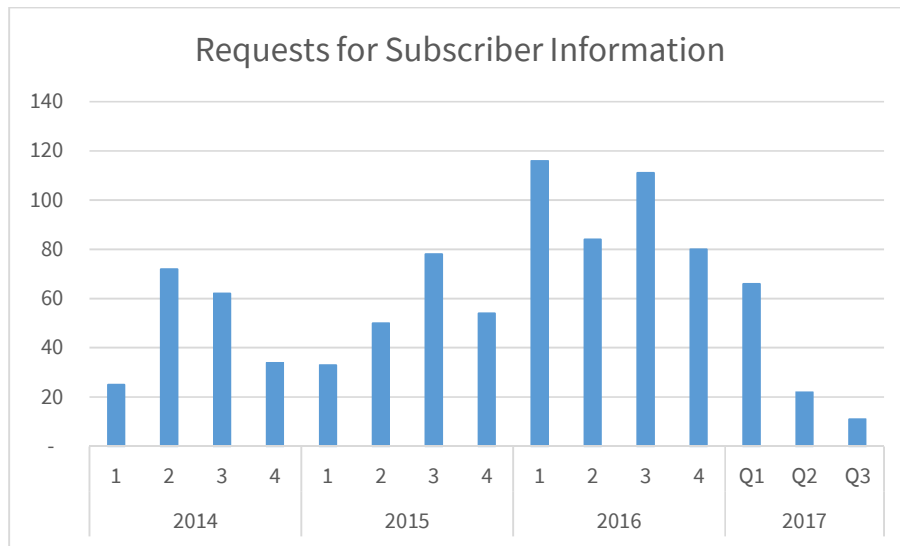


Figure 3 Requests for Subscriber Information have reduced due to automated transfers for CSAM

To assist the authorities with a backlog of CSAM cases, an automated tool was developed to directly provide the New Zealand Authorities with subscriber information for cases involving CSAM. The number of cases processed is shown below:

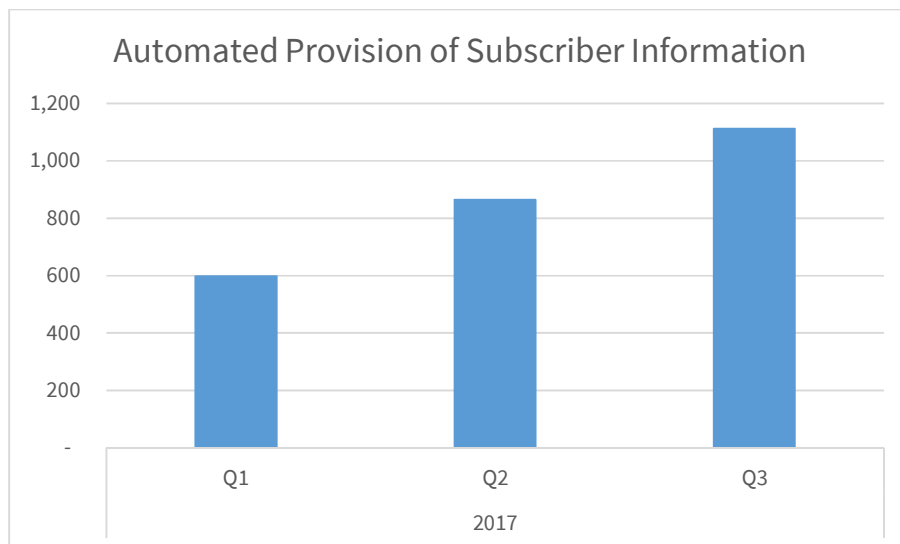
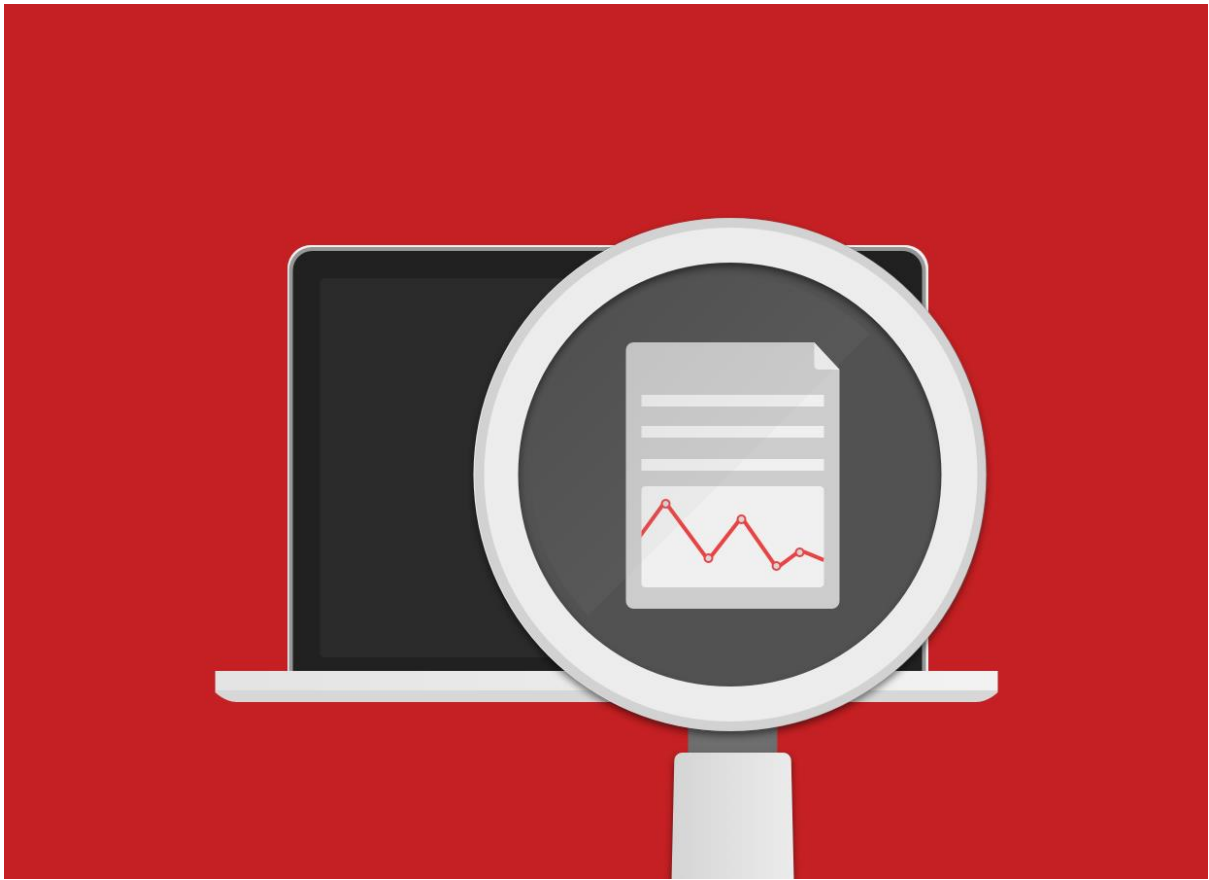


Figure 4 Automated transfers of subscriber information for CSAM cases



Mega Transparency Report

September 2018

Requests for Removal of Content and for User Information



Introduction

This is the fourth transparency report published by Mega since it commenced operations in January 2013. In accordance with its Privacy & Data Policy, Mega periodically publishes statistics on takedown requests, subscriber information disclosure and related issues.

Regulatory Background

Mega was designed, and is operated, to ensure that it achieves the highest levels of compliance with regulatory requirements.

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, 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 they reach Mega. However, if a user voluntarily shares a link to a file or folder that they have stored (with its decryption key), then anyone with that link can decrypt and view the folder/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 access to the offending files disabled.

New Zealand's Copyright Act process provides Mega with a safe harbour, shielding Mega from liability for the material that its users upload and share using Mega's services. Although not technically bound by US or EU law, Mega also complies with the conditions for safe harbour under the US Digital Millennium Copyright Act (**DMCA**) process and the European Union Directive 2000/31/EC. Mega does so by allowing any person to submit a notice that their copyright material is being incorrectly shared through the Mega platform. 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 takedown notices continues to be very small, indicative of a user base which appreciates the speed and flexibility of Mega's system for legitimate business and personal use.

The safe harbours in various jurisdictions require material to be removed or links disabled expeditiously. Some cloud storage providers target takedown within 24 hours. Mega targets takedown within a maximum of 4 hours, with takedowns usually being actioned much quicker than the 4 hour target.

When designing and implementing its takedown 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 requirements¹.

¹ <https://mega.nz/terms>
<https://mega.nz/takedown>
<https://mega.nz/copyright>



Mega has very clear Terms of Service that have to be acknowledged by every new user before their account activation can be completed. Those Terms make it very clear (e.g. in clauses 17-20) that Mega won't tolerate infringement or any other illegal activity.

However it is impossible for Mega to review content being uploaded by users as it is encrypted at the user's device before it is uploaded to Mega.

It is also logistically impossible for any cloud storage service (or indeed any other service provider in the Internet chain, such as the ISP, browser supplier etc), to review all uploaded content due to the number of files that are uploaded each second. Users upload approximately 40 million files per day or 500 per second. The infeasibility of checking uploads has been recognised in numerous court cases, even prior to enactment of the DMCA.

Even if content could be reviewed, it is not possible to determine whether it is infringing or not. Owners of many copyrighted materials provide the user with a licence to make a backup copy, so uploading it to a cloud storage service would not be infringing.

Other similar cloud storage services don't make any positive (but almost certainly futile) attempt to assess the copyright status of uploaded materials.

Requests for Removal of Content

Mega accepts takedown notices via a dedicated web page² or by email to takedowns@mega.nz

Requests are processed within a few hours, without reviewing their validity³.

For file links, the submitter is able to choose one of three options:

1. Disable the reported link - *the file will remain in the user's account;*
2. Disable all links pointing to the same byte sequence - *the file will remain in the user's account;*
3. Disable all links and remove all files from all accounts referencing the same byte sequence - *there is no user permitted to store this under any circumstance worldwide.*

Folder links often refer to a large number of files, of which only some are claimed to be infringing. If the submitter doesn't provide identification of the individual copyrighted works and files within the folder that are claimed to have been infringed, MEGA disables the reported link consistent with option (1) above.

Mega receives counter-notices from some users who dispute the validity of a takedown. These counter-notices are processed consistent with the safe harbour requirements. Our experience is that most of the counter-notices are genuine and appropriate, due to content owners and agents trawling the Internet using robots which generate incorrect notices on behalf of copyright owners and due to the failure of owners/agents to review the specific link content.

² <https://mega.nz/copyrightnotice>

³ It is impossible to review the validity as the file contents are user-encrypted, unless the user has published or provided the encryption key.



The number of unique takedown requests submitted represents a very small and declining percentage of the total number of files stored on Mega. In Q3 2018, the files taken down represented 0.0001% of the 49 billion files stored on Mega servers.

		Total Takedown Requests	Taken Down Files / Total Files	Total Files (Billion)
2013	Q1	51,857	0.0192%	0.2
	Q2	53,772	0.0151%	0.3
	Q3	91,493	0.0142%	0.4
	Q4	117,546	0.0135%	0.6
2014	Q1	91,106	0.0063%	1.1
	Q2	102,798	0.0042%	1.8
	Q3	111,220	0.0028%	2.5
	Q4	404,965	0.0043%	3.6
2015	Q1	134,982	0.0021%	5.0
	Q2	84,210	0.0013%	6.6
	Q3	68,064	0.0008%	8.9
	Q4	57,108	0.0005%	11.9
2016	Q1	74,955	0.0005%	15.0
	Q2	110,878	0.0006%	18.2
	Q3	82,917	0.0004%	21.8
	Q4	85,605	0.0003%	25.8
2017	Q1	91,110	0.0003%	29.3
	Q2	90,156	0.0003%	32.5
	Q3	68,547	0.0002%	35.7
	Q4	67,881	0.0002%	39.1
2018	Q1	56,179	0.0001%	42.5
	Q2	59,661	0.0001%	45.8
	Q3	51,048	0.0001%	49.2

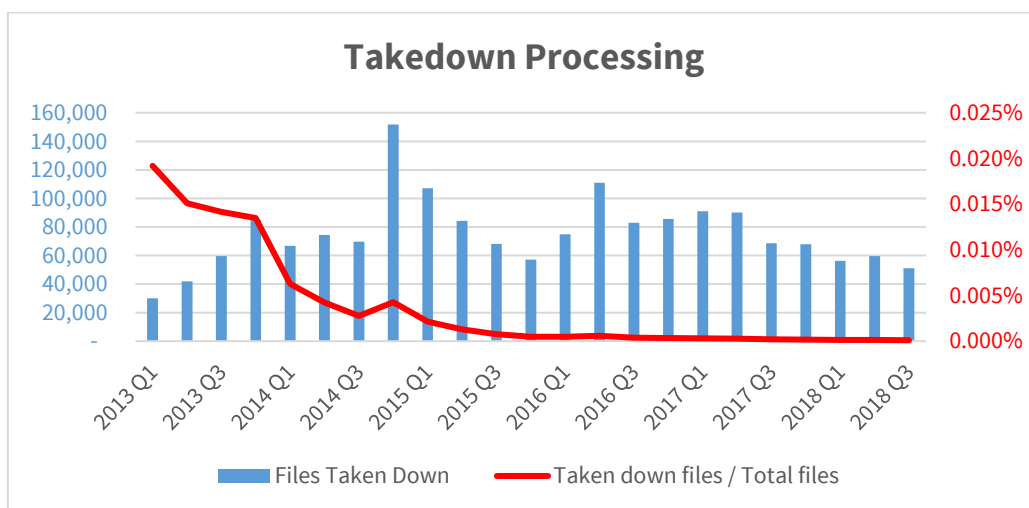


Figure 1 Requests for file takedowns show a continuing decline as a % of files stored



Repeat Infringers

Mega suspends the account of any user with 3 copyright takedown strikes. In some cases, the account can be reinstated where it is proved to be the subject of invalid takedown notices, but most suspended accounts are terminated. Up to 30 September 2018, Mega had suspended 78,000 users for repeated infringement. The data below shows that the suspensions are declining in absolute number and as a % of the number of registered users.

Year	Quarter	Number of Suspended Users	% of Registered Users
2013	Q1	1,137	0.043%
	Q2	2,336	0.067%
	Q3	3,305	0.073%
	Q4	7,821	0.131%
2014	Q1	5,719	0.074%
	Q2	2,965	0.030%
	Q3	2,017	0.016%
	Q4	2,722	0.018%
2015	Q1	2,376	0.014%
	Q2	1,523	0.007%
	Q3	1,285	0.005%
	Q4	*2,241	0.007%
2016	Q1	2,027	0.005%
	Q2	3,193	0.007%
	Q3	2,086	0.004%
	Q4	2,371	0.004%
2017	Q1	3,562	0.005%
	Q2	5,615	0.007%
	Q3	8,127	0.009%
	Q4	2,251	0.002%
2018	Q1	1,980	0.002%
	Q2	1,947	0.002%
	Q3	1,880	0.002%

*Plus 7,245 suspended due to the retroactive change to suspension after 3 strikes (previously after 5 strikes).

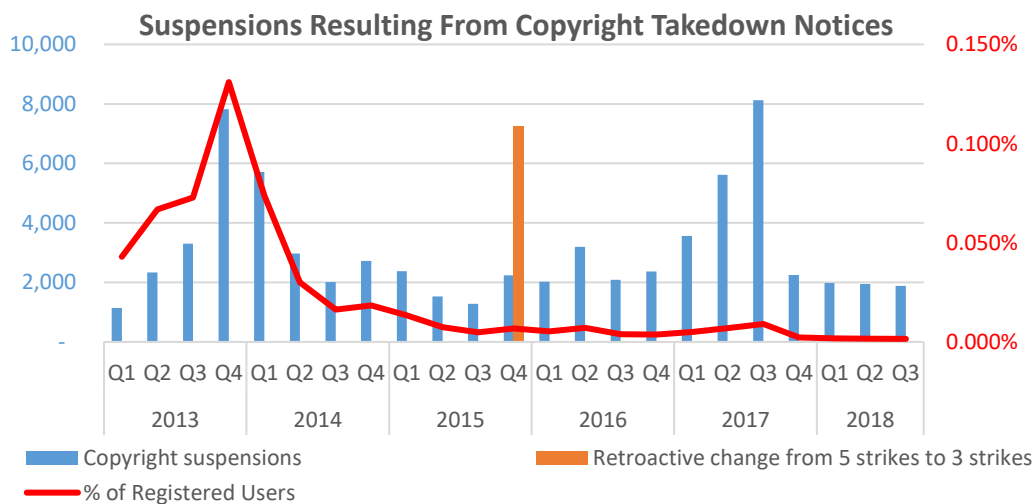


Figure 2 Copyright Suspensions continue to be a very low % of registered users.



Objectionable (Illegal) Content

- Child Exploitation Material, Violent Extremism, Bestiality, Zoophilia, Gore, Malware, Hacked/Stolen Data, Passwords

Mega does not condone, authorise, support or facilitate the storage or sharing of Child Exploitation Material (**CEM**), also known as Child Sexual Abuse Material (**CSAM**) or other objectionable material as defined in section 3 of the New Zealand Films, Videos, and Publications Classification Act 1993 or other internet-harming material. Mega has zero tolerance for users sharing such material. Any reports of such content result in immediate deactivation of the folder/file links, closure of the user's account and provision of the details to the New Zealand Government Authorities for investigation and prosecution.

As at September 2018 Mega had closed 66,000 accounts for sharing such content.

Court Orders / Warrants etc

During the 2017-2018 year, Mega was served 6 legal orders from NZ authorities and then disclosed account information for 171 user accounts which are alleged to be involved in criminal activity overseas.

Other Requests for Personal Information

Mega is 'The Privacy Company' and values the privacy of the users of its services. The company is committed to maintaining industry-leading levels of security and confidentiality of user information and data. However, privacy is not an absolute right and is subject to limitations. We take all requests for the disclosure of user information seriously. In considering any request for user data, user information, or action involving a Mega user, Mega starts from the position that user data and information is private.

Unless an Emergency Response is required, or disclosure is necessary to assess or gather evidence in relation to an active or proposed investigation involving child exploitation material or violent extremism, Mega will generally only provide user details when required to do so by New Zealand law, or by a New Zealand court or law enforcement authority with appropriate jurisdiction. Mega may consider requests made by non-New Zealand law enforcement authorities and civil claimants.

Mega defines Emergency Response as a situation where, in the expert judgement of a senior officer of the New Zealand Police or similar law enforcement officer or authority acceptable to Mega, Mega has written assurance that the person making the request has valid reasons to believe that disclosure or action is necessary to prevent or lessen a serious threat (as defined in section 2(1) of the Privacy Act 1993) to public health or public safety or the life or health of an individual or individuals, and where the person giving such assurance confirms in writing that the threat is of such urgency that there is not time to obtain a production order or other court order.

If satisfied as to the above, Mega may, in its discretion, accept a request in such situations in good faith.



When we receive a request, we make sure it is legitimate and we provide advance notice to the affected user unless prohibited by a court order or where we decide delayed notice is appropriate, based on criteria described in our Privacy & Data Policy.

All files stored on Mega are encrypted prior to being uploaded to our system and therefore we do not and cannot access that content unless we are provided with the decryption key. Mega does have access to registration information and IP addresses used to access our services.

The chart below shows the number of requests for subscriber information that were manually processed.

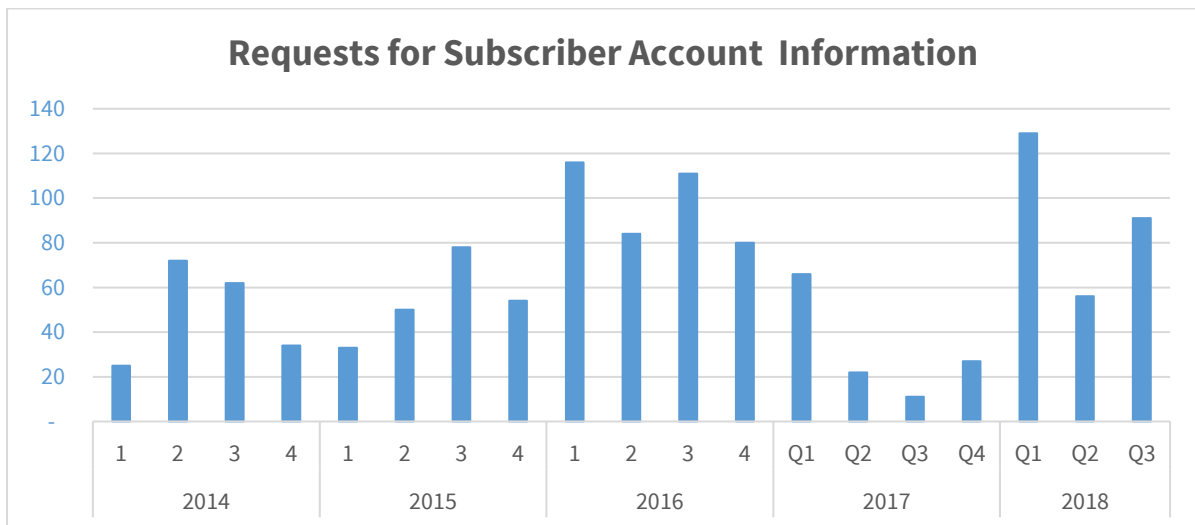


Figure 3 Requests for Subscriber Information – violent extremism and CSAM

To assist the authorities with a backlog of CSAM cases, an automated tool was developed to directly provide the New Zealand Authorities with subscriber account information for cases involving CSAM. The number of cases processed is shown below:

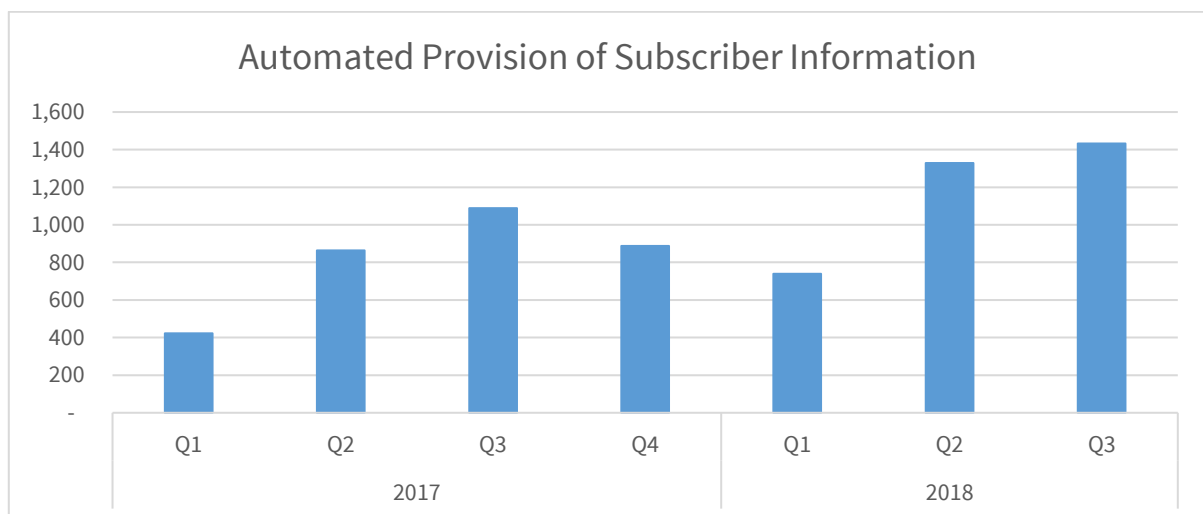


Figure 4 Automated transfers of subscriber account information for CSAM cases



GDPR

The General Data Protection Regulation in Europe came into force in May 2018. Mega didn't need to make any substantial disclosure or make changes to its operations as privacy has been at the core of Mega's operations since it commenced in 2013.

In 2013 MEGA pioneered user-controlled end-to-end encryption through a web browser. It provides the same zero-knowledge security for its cloud storage and chat, whether through a web browser, mobile app, sync app or command line tool. MEGA, The Privacy Company, provides Privacy by Design.

As all files uploaded to MEGA are fully encrypted, their contents can't be read or accessed in any manner by MEGA. Files can only be decrypted by the original uploader through a logged-in account, or by other parties who have been provided with file/folder keys generated by the account user.

Mega stores very limited Personal Data, such as the user's email address and limited activity detail relating to account access, file uploads, shares, chats etc. In May 2018 we introduced a feature to allow users to download Personal Data relating to their account. There were 212 downloads in Q2 and 275 downloads in Q3 2018.

Personal data is retained indefinitely while the user's account is open. After account closure, MEGA will retain all account information as long as there is any law enforcement request pending but otherwise for 12 months after account closure as users sometimes request that an account be re-activated. After 12 months, identifying information such as email and IP addresses will be anonymised (except that email address records will be retained for reference by the user's contacts or where the user has participated in chats with other MEGA users) but other related database records may be retained.

After user deletion of a file all deleted files will be made inaccessible, marked for deletion and deleted fully when the next appropriate file deletion purging process is run.

After account closure all stored files will be marked for deletion and deleted fully when the next appropriate file deletion purging process is run.

MEGA doesn't share data with any other party other than with competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences and as specified in the Privacy and Data Policy clause 13.

Mega Limited, as controller, is represented in Europe by

Mega Europe sarl
4 Rue Graham Bell
L-3235 Bettembourg
Luxembourg
gdpr@mega.nz



The Lead Data Protection Supervisory Authority is the Luxembourg National Commission for Data Protection. This is the appropriate authority for accepting GDPR complaints about MEGA.

NATIONAL COMMISSION FOR DATA PROTECTION

1, avenue du Rock'n'Roll

L-4361 Esch-sur-Alzette

Luxembourg

<https://cnpd.public.lu>
