Public Version

Copyright Act 1994

Issues Paper

Ministry of Business Innovation & Employment

5 April 2019

Summary

1. Thank you for the opportunity to submit on the Issues Paper. As an owner and distributor of copyrighted works, as well as New Zealand's largest internet service provider, Spark has a unique perspective on the challenges of applying our Copyright Act in a digital age and in online environments. We support a thorough review of the Act and look forward to the review providing more certainty in the regime for all parts of the copyright ecosystem.

2. Protection of copyright, and copyrighted works, is fundamental to the continued health and growth of New Zealand's creative industries. But online environments challenge many of the assumptions upon which our current Copyright Act was founded on. Controlling copyright infringement online is a fundamentally different challenge to controlling it in offline environments. As an internet access provider – a provider of the "pipes" that carry internet traffic – Spark recognises that, as a last resort where action against the source of the problem has been unsuccessful, we may have a role in assisting copyright holders in better protecting their copyrighted content against copyright infringement online.

3. But it is our long-held view that customers prefer to access legitimate content. The success of services like Netflix, Lightbox, Spotify etc demonstrate people are willing to pay for the right content, at the right price. This reinforces our belief that vibrant and accessible online markets, that provide lawful access to the content New Zealanders want to access, at prices that are affordable, is the most effective way of reducing online copyright infringement.

4. We acknowledge and accept that the proliferation of these models will not stop all online piracy. No solution to copyright infringement will ever be 100% successful online - this is an unavoidable feature of online environments where people will always find and publicise simple ways for people to circumvent network restrictions.

5. In this context – if we accept that legal business models for accessing online content will over time serve the needs of the large majority of New Zealanders, and if we accept that no scheme will be 100% perfect – we believe that any online copyright infringement enforcement mechanisms considered should:

    a. **Replace, not augment, the existing three-strike mechanism**. It is clear to us that rightsholders no longer see value in this mechanism, so if new mechanisms are to be added we recommend removing this unsuccessful mechanism from the Act.

    b. **Be proportionate**. Any new mechanism must be designed with recognition that it can only ever successfully target the uncommitted participants in copyright infringement. A large part of the rationale for any mechanism will undoubtedly be to dissuade everyday New Zealanders from inadvertent or unknowing copyright infringement. This means any such mechanism should be simple for consumers to understand, and simple for internet service providers to operate.

    c. **Place the costs for introducing and maintaining copyright-protecting mechanisms on the rightsholder(s) that request them**. They are the parties that will receive the benefits of those mechanisms so are the right parties to bear these costs.

6. The capabilities of ISPs who are merely connectivity providers should be distinguished from the business of online content hosting platforms such as websites, peer-to-peer sites or social media companies, for example, who intentionally provide a means for online content to be distributed to end-users. This latter group will always be able to take a more proactive and effective role in addressing copyright content on their platforms than the operators of the "pipes" that internet traffic travels over. These are very different types of businesses and

need to be considered separately from a policy perspective to avoid unintended consequences.

7. ISPs should only be required to support one type of action by rights holders to avoid duplicating cost and effort. If network blocking is to be introduced, this should see a consequential retiring of the three strikes peer to peer process.

8. ISPs actions to block in the aftermath of the events in Christchurch should be distinguished from site blocking to protect copyright interests as these actions were taken under extraordinary circumstances and for a very limited period of time. Our experience showed that site blocking proved to be a clumsy solution which can frustrate legitimate online activity, and ISPs should not be responsible for deciding what content is blocked.

9. ISPs should otherwise not be responsible for the decision to implement blocking and should only act as required by law. Likewise, they should not cover the costs of protecting third party interests.

Introduction

10. Spark is New Zealand's leading digital service company. Our goal is to help all of New Zealand win big in a digital world. Spark offers a range of products and services to consumers and business. These include voice, broadband and mobile services through our Spark, Skinny and Bigpipe brands, data and analytics through Qrious, business and cloud services through Revera and Digital Island, on demand TV and movies from Lightbox and a range of online sports (including the Rugby World Cup 2019) from Spark Sport.

11. Copyright legislation affects our business in different ways: As an internet access provider we rely on 'safe harbour' provisions as we do not have the technology to proactively monitor and evaluate data passed across our network by end users. At the other end of the spectrum we rely on copyright legislation to protect our investments in on demand TV and sport content.

12. There is no denying that technology has changed the environment in which copyright law must exist and it has introduced challenges that were not envisaged even a few years ago. The time is right to review copyright legislation and ensure it remains fit for purpose.

13. Above all, we need a copyright regime which provides certainty to all stakeholders, including rights holders, organisations and individuals. Without this we may end up depriving New Zealanders by disincentivising the creation and investment in new copyright material.

Issues

Definition of an Internet Service Provider (ISP)

14. As the issues paper notes, the definition of ISP in the Copyright Act is extremely broad. The implications of this broad definition is that it risks confusing and conflating issues that are specific to certain parts of the market. The result is that policy solutions which are appropriate to one part of the market may also be applied to other parts with negative consequences.

15. For example, an internet access provider only provides access to the internet and is focussed on connectivity for its customers. These providers are similar to the postal service in that they do not have the technical or operational capability to monitor the actual contents of the data packets (or the letters in a postal context) that traverse their networks for infringing content. If these providers take action to block content it is a blunt instrument, often inadvertently restricting legitimate use of the network. Where technologies like caching are used, these are

to improve the efficiency of the service as they act autonomously to improve performance for their customers, and they don't result in long term retention of the content in our network.

16. Content hosting may have slightly more control over content on their networks as they have a direct relationship with the organisation which uses their service. However, they too are unlikely to be able to proactively monitor activity on their servers and must reach out to the organisation responsible for the content itself if they are made aware that there is an issue.

17. At the other extreme are content providers such as social networks that have businesses and content platforms that are designed to facilitate, and monetise, the sharing of content and information between end-users. These companies are in a much better position to take a more proactive role in addressing copyright content on their platforms.

18. In fact, the objective of copyright legislation should always be to target any copyright infringement prevention mechanisms as close as possible to the source of the content. It is better to require the site owner to remove the content from the site itself rather than rely on crude blocking approaches to stop people reaching that site.

19. Each of these businesses have their own issues from a copyright perspective. The issues are different enough that they should be considered separately from a policy perspective to avoid unintended consequences of rules applying to one being applied to another. For example, a website owner is able to easily disable a live stream of copyrighted content whereas this is very difficult for an ISP to block. While a social media platform provider may be able to shut down a specific livestream being provided over its platform, without affecting the rest of its platform, an ISP can usually only block the entire platform or none of the platform.

20. To avoid over regulation and scope creep, definitions of services should reflect the different types of business so that the rules that apply to an internet access provider (for example) reflect the operational capabilities and limits of this type of provider, compared to a social media company.

21. For the rest of this document we use our preferred definition of ISP which is limited to those organisations which provide their end users with connectivity to the internet.

Internet Service Provider Liability

22. Safe harbours are essential for an ISP to do business. Purely from a practical point of view, ISPs cannot be held responsible for what their customers do online. This applies to copyright infringement as much as it does to other types of criminal activity. ISPs simply do not have the technical capability or resources to monitor everything their customers do, nor should ISPs be required to do so. The cost and disruption to do such monitoring would be prohibitive as well as undermining confidence in internet services.

23. Despite being a feature of all the main comparable jurisdictions, there is a suggestion noted in the issues document that safe harbour may reduce incentives on ISPs to help right holders stop piracy. This is incorrect. The bottom line is that ISPs cannot be expected to track all activities on the internet and make a decision on whether specific activities infringe copyright, nor do we have the capability.

Issues with the infringing file sharing regime

24. Spark complies with its obligations under the Act by having a three notice regime for infringement of copyright by individuals using peer-to-peer (P2P) file sharing technologies. While this process was initially used, it is no longer being actively used by rights holders.

25. We cannot comment on how effective the regime was at reducing copyright but we note the following:

    - The $25 fee was set to be reflective of ISP costs as the process to manage and coordinate notices across multiple time periods required ISPs to implement systems and processes. Cost recovery is an important policy principle.

    - We acknowledge there were some mistakes in the notices at the very early stages of implementation of the regime, but these were teething issues which were quickly addressed. Spark worked closely with the rights holders who were using the process to ensure the prescribed process was as efficient and effective as possible for all parties involved.

26. The arrival and popularity of legal content services in New Zealand has reduced the incentives on most individuals to obtain content illegally. Lightbox, Netflix, Neon, Spotify etc have meant that people can access quality content using user friendly services with none of the risks of downloading unknown files from dubious sources.

27. We are neutral on whether the three notice regime should remain, but note that it does create ongoing costs for our business as we need to maintain the system even if it isn't being actively used. It is inefficient to have multiple solutions to copyright issues. If site blocking is considered to be a more appropriate solution, then the three notice regime should be disestablished.

Site Blocking

28. It has been widely noted that a number of rights holders are interested in website blocking as a way to prevent access to content which they consider is breaching copyright. From a policy perspective, ISPs actions to block in the aftermath of the events in Christchurch should be distinguished from site blocking to protect copyright interests as these actions were taken under extraordinary circumstances and for a very limited period of time. However, from a technical perspective, our experience in blocking access to the Christchurch terrorist video was that blocking is a blunt instrument which can impact legitimate uses of sites.

29. Blocking can never be completely effective and no matter how complex the blocking solution is, it can always be circumvented. Not only that, but people will share details of how blocks can be avoided and even make simple solutions to help others access the content. VPNs are one way of avoiding network blocks and cannot be blocked themselves as VPNs have legitimate uses.

30. With this in mind, blocking should be seen as a signal to New Zealanders that the content being distributed on a particular site is inconsistent with New Zealand law. It should not be considered a way to prevent 100% of the offending activity, because for every technological blocking solution, there will inevitably be a technological way of avoiding that solution. This is important when considering the technology solutions that ISPs can use to do their blocking.

31. If site blocking is to be prescribed in legislation, then the following principles should apply

    - ISPs should be able to use blocking techniques which are appropriate to their network. The mechanism should be clear that DNS blocking is sufficient, and that ISPs do not need to block individual IP addresses. IP address blocking is an order of magnitude more complex for ISPs than DNS blocking

- There should be legal certainty around the regime with parties wishing to block sites required to get a formal website blocking injunction from a Court or independent authority
- The blocking should apply equally to all RSPs
- Only the Court or independent authority should be able to confirm and direct ISPs to block sites
- The blocking order should be prescriptive on the duration of the blocking, and what happens after that period (eg another order is needed to extend the blocking)
- There should be a clear process for how the sites can be removed from the blocked list if the offending content is removed, and how new sites with exactly the same content can be added to the list in an efficient and transparent way.
- RSP costs should be recovered from the party requesting the blocking where they face incremental costs as a result of the blocking injunction. The UK Cartier case sets out some clear principles for this.

32. For transparency, and to reinforce that accessing infringing content is wrong, ISPs should be obliged to provide a 'landing page' that people will see if they try to access blocked content. Without this, customers will think their internet connection is faulty and contact their ISP for support. This drives costs in to the ISP's business, is frustrating for customers and fails to deliver an advocacy message around access to copyright content, which is important from a wider education perspective. It is far more efficient to have a page which explains why the content is blocked and describes the process that the content owner, or a customer, can go through if they think the site is erroneously blocked.

The decision on whether content is infringing

33. The question on whether linking to infringing content is effectively 'authorising' the infringing is important for ISPs. If linking to content is considered an offence, then a website blocking injunction could be used to require ISPs to block such content.

34. There is an argument that if someone links to content which they know is infringing then they should be liable in some way for their actions in directing others to this content. Care is needed when reviewing this aspect of legislation as it may have implications for people who link to other types of content, such as material which has been classified as objectionable by the Chief Censor.

35. Copyright infringement is a legal question and is often unclear. More generally, the key issue from an ISP's perspective is that the decision of what content breaches copyright, and should potentially be blocked, is not left to the ISP to decide. ISPs do not have the resource or expertise to analyse content, nor should they become the defacto censors of the internet in New Zealand. If ISPs were responsible, they would risk challenges from a number of stakeholders if they blocked access to legitimate content or didn't blocking infringing content. Both have risks for ISPs. This situation would be further complicated if one ISP chose to block the content but another chose not to. Instead it should be for the court to decide whether content is infringing and not the ISP.

Blocking Live Streaming Content

36. Live streaming is different from website blocking in that it is very hard to block technically. It is also very labour intensive as it requires manual work in our network to block the streams. Also, as noted above, no approach is fool proof and all blocking can be bypassed with mainstream (and legitimate) technologies like VPNs.

37. ISPs cannot be made accountable for blocking live streams, and instead the platform hosting the live stream should be liable for the content and be required to take action to stop it. It is also worth noting that content owners can apply legitimate security techniques to protect their own streams and the onus for this should remain firmly on the copyright interested party.

Re-transmission and WiFi networks

38. The consultation document notes there are challenges around re-transmissions and Wifi networks. As a point of principle, legislation should be technology neutral as, from a policy point of view, the issues are the same whether the service is delivered over a fixed or wireless network. In practice, internet access may incorporate a range of different technologies (including fixed and wireless) and cross different networks. Just because the last connection to the customer is WiFi should not imply the service is retransmitted. The exact same situation would apply if the last connection to the customer is a physical wire.

Technological protection measures (TPMs)

39. We agree that copy protection TPMs are an important issue that should be considered as part of the review.

40. Access control TPMs should also be considered in the review as content is often licensed on a geographic basis and copyright holders need the ability to protect their rights.

Transient or incidental reproduction

41. There are questions about the role of caches in a network because they may not be considered an ‘integral and essential’ part of the technological process. This stems from the fact they are optional to install. However, where they are installed it is to improve the efficiency of traffic flows to customers and results in a better experience for both the customer and the site owner. Caching is automatic and usually the customer will be unaware they exist in the network.

42. Given caches benefit all parties and their operational is transparent to all parties, if seems counterintuitive to exclude these devices from safe harbour protections and therefore disincentive their use. This would result in slower website loading for consumers.

43. Caches should be treated the same way as the rest of an ISP’s network as their sole purpose is making more efficient use of connectivity.

Technological processes (cloud computing)

44. Cloud computer is ever more pervasive in both the consumer and business space. One way to consider the policy issues it creates is to separate the activity from the physical location of data.

45. For example, if someone stores an infringing file on their google drive or Dropbox folder it should not matter of where the file is physically located. The fact is that it is an infringing file controlled by an individual.

46. At the same time, we need to be careful in how cloud computing is regulated as this is an evolving global market and companies are making decisions on where in the world to locate their businesses internationally based on the regulatory environment.

Non-expressive use of copyright works (data mining and AI)

47. Data mining and AI introduce a number of interesting questions and we are keen to be involved in the discussion in this area.