



## Telecommunications Carriers' Forum

### Submission on the Copyright (Infringing File Sharing) Amendment Bill

*(This is a public version of this submission. There is no private version)*

<b>Version Number and Status:</b>	Final v2.2
<b>Version Date:</b>	<b>11 June 2010</b>

© 2010 The Telecommunications Carriers' Forum Inc. All rights reserved. Copyright in the material contained in this document belongs to the Telecommunications Carriers' Forum Inc. No part of the material may be reproduced, distributed or published for any purpose and by any means, including electronic, photocopying, recording or otherwise, without the Telecommunications Carriers' Forum Inc written consent.

# Submission by the Telecommunications Carriers' Forum on the Copyright (Infringing File Sharing) Amendment Bill

## CONTENTS

Introduction .....	3
Fact Scenario under the Bill .....	4
Background .....	4
<i>Issue 1 – Transition Period</i> .....	5
Step 1: Notices are sent to ISP; ISP matches to IP addresses.....	5
<i>Issue 2 – Inability to process notices</i> .....	6
Step 2: ISP sends out detection notices .....	6
<i>Issue 3 – Format of notices</i> .....	6
<i>Issue 4 – Overlap with section 92E (caching safe harbour)</i> .....	7
<i>Issue 5 – Overlap with sections 92C and 92D (storage safe harbour)</i> .....	7
<i>Issue 6 – Notice fees</i> .....	8
Step 3: ISP logs actions .....	8
<i>Issue 7 – Record retention</i> .....	9
Step 4: Account holder challenge.....	9
<i>Issue 8 – ISP definition</i> .....	9
<i>Issue 9 – ISP action on challenge</i> .....	10
<i>Issue 10 – Form of challenge notice</i> .....	10
Step 5: Copyright Owner consideration of challenge .....	10
<i>Issue 11 – Acceptance of challenge</i> .....	11
Step 6: Warning and enforcement notices .....	11
<i>Issue 12 – Definition of copyright owner</i> .....	12
Step 7 – Further challenges by account holder.....	12
Step 8 – Application to Copyright Tribunal .....	12
Step 9 - Copyright Tribunal hearing.....	12
<i>Issue 13 – ISP involvement in proceedings</i> .....	12
<i>Issue 14 – Strict liability/Vicarious liability</i> .....	13
Step 10 – Application for Account Holder identity .....	14
Step 11 – Enforcement in the District Court .....	14
<i>Issue 15 – Internet Account</i> .....	14
<i>Issue 16 – Termination</i> .....	15
<i>Issue 17 – Public disclosure</i> .....	15
Concluding comments.....	15

# Submission by the Telecommunications Carriers' Forum on the Copyright (Infringing File Sharing) Amendment Bill

## Introduction

1. This submission is made by the Telecommunications Carriers' Forum (**TCF**). TCF members provide more than 90% of the internet connections in New Zealand. Our members are BayCity Communications, CallPlus, Compass Communications, FX Networks, Kordia, Telecom New Zealand, TelstraClear, TrustPower, Vector Communications, Vodafone, Woosh and WorldxChange.
2. The TCF appreciates the opportunity to comment on the Bill and would like to appear before the Select Committee in support of its submission.
3. We have been integrally involved in this issue from the outset. To recap:
  - 3.1 With other ICT industry groups, we campaigned to have section 92A reviewed;
  - 3.2 But, once section 92A was passed, TCF members spent significant time and money attempting to develop a code of practice. In doing so, the TCF adopted a co-operative approach with all stakeholders, including major rights holder groups, and continues to maintain a working relationship with them;
  - 3.3 A concrete example of this co-operative approach was in the joint submission by TCF members and rights holder groups on the regulations promulgated under section 92D of the Copyright Act 1994; possibly the first time ISPs and rights holder groups have made such a joint submission anywhere in the World;
  - 3.4 We have consulted with officials and made submissions on the proposals which have lead to this Bill. In particular we refer to our submission made on 7 August 2009;<sup>1</sup>
  - 3.5 The TCF is also consulting with officials and has made a submission on ACTA since there is a direct correlation between some proposals put forward there and aspects of the regime proposed in the Bill. Similarly, the TCF expects to assist officials in their consideration of any digital copyright aspects of the Trans Pacific Partnership Agreement, currently proposed to be expanded to include the US, Australia, Peru and Vietnam.<sup>2</sup>
4. The reasons for that level of involvement include:
  - 4.1 ISPs are naturally concerned that their customers are treated fairly. This was a particular driver for much of the draft TCF code;
  - 4.2 ISPs' own businesses are dependent on copyright protection. They are also increasingly partnering in revenue sharing arrangements with content providers in the music, film and software industries and so are open to reasonable steps to protect that revenue stream;
  - 4.3 Conversely, large scale p2p infringers can be a drain on an ISP's available bandwidth, particularly at certain times of the day. In certain circumstances, this can adversely impact other ISP customers' access and speed of connection, which, in turn could potentially result in customers moving elsewhere;

---

<sup>1</sup> A copy of that submission is on the TCF site here - <http://www.tcf.org.nz/library/0185572e-89e7-4adc-a053-ae7eb1c40e30.cmr>

<sup>2</sup> <http://www.mfat.govt.nz/Trade-and-Economic-Relations/Trade-Agreements/Trans-Pacific/index.php>

- 4.4 Of the three stakeholders involved in graduated response processes (of which the Bill is an example) – account holders/users; copyright owners and ISPs – ISPs face the most significant workload in both set-up and continuing operation. Further, if termination is left as remedy, individual ISPs potentially face a significant adverse impact. That is because infringers will simply move to another ISP.
5. In this submission, we are pleased to continue this involvement. As with previous submissions, our focus is mainly on issues of direct relevance to ISPs in the operation of their businesses. We are however aware of and support some of the positions taken in more general submissions made by others. Therefore, the fact that we do not comment in this submission on a particular aspect of the regime should not necessarily be taken as support for it.
6. The Bill is a significant improvement on the uncertain position that was created under section 92A. We are pleased that many of the issues that we have raised in the past have been taken account of.
7. The TCF's view remains however that a notice and notice system would achieve much of the benefit that is hoped for in the proposed regime but at substantially less cost. We are strengthened in this view when we see:
- 7.1 The UK has pulled back from a 3 strikes termination regime and held at notice and notice in its recently passed Digital Economy Act;<sup>3</sup>
- 7.2 Canada has just proposed a notice and notice system in its C-32 Bill,<sup>4</sup> replacing the informal notice and notice system which has been operating successfully in Canada for some time.<sup>5</sup>
8. If we are to proceed with a full graduated response regime instead of notice and notice, as can be seen in the Bill, significant complexity is introduced and that comes at a cost. The intersection of copyright with the digital environment in which ISPs are integrally involved is not simple and presents challenges for all stakeholders. Since it is ISPs who will face any process issues with this regime, it is therefore useful to look at how it might actually operate if the Bill were to be passed in its current form and use that analysis to suggest any areas for change.<sup>6</sup>

## **Fact Scenario under the Bill**

### ***Background***

9. FlyNet is a mid sized New Zealand ISP. It has 20 staff, including 5 call centre/frontline support staff. Because it caters for high use customers in the media industry who are often accessing overseas content, FlyNet operates an industry standard caching solution, which stores regularly accessed material automatically in its own separate IP addressed server. When customers seek that material, instead of having to obtain it from overseas, FlyNet's cache server takes over and delivers it from here in New Zealand – a far more efficient system. FlyNet also provides a low cost introductory website creation/web hosting service for any of its customers that wish to use it.
10. Among FlyNet's many customers is an educational business, Ontap, which operates a distributed teaching model for the tourism and hospitality industry. Its 5 teachers and 45 students are able to log securely onto its systems from

---

<sup>3</sup> Details of how UK's notice and notice system is proposed to work can be found in Ofcom's draft code <http://www.ofcom.org.uk/consult/condocs/copyright-infringement/condoc.pdf>

<sup>4</sup> <http://www.scribd.com/doc/32401372/Copyright-Bill-C32>

<sup>5</sup> <http://www.cbc.ca/consumer/story/2007/02/14/software-warnings.html>

<sup>6</sup> Names and references used in these fact scenarios are fictional. Any resemblance to actual persons or entities is unintended and coincidental.

anywhere via a browser interface and, among other things, conduct realtime lessons and discussions over Ontap's network. They can also use Ontap's system to swap materials amongst each other and to download and upload material from and to the wider internet. Ontap staff and students use the p2p protocol to distribute large video files since they have found this the most efficient way of doing so.

11. FlyNet has allocated a fixed IP address to Ontap as part of a bundled business account which includes all voice, data and mobile phone access. The contract between FlyNet and Ontap has a three year term and includes routers, VoIP phones and mobile handsets for head office staff (free to Ontap as long as it remains exclusive to FlyNet for the three year term). There is also a termination fee payable by Ontap should the contract be terminated for any reason other than FlyNet default.
12. Meanwhile, NetFish, which acts as an agent for various intellectual property owners, has indicated that the major film, television and gaming software owners that it acts for are concerned at the damage being done to their businesses by infringing file sharers and wish to take advantage of the Bill.
13. Imagine it is 3 months since the Bill was passed into law and the regime has now become operative.
14. FlyNet has not had time and probably could not afford to automate its systems to cater for the regime. Its director and 5 call centre/support staff have been to a half day workshop on the processes and it has set up a manual database to record notices etc.

**Issue 1 – Transition Period:** As we shall see, this regime will be labour intensive to operate manually. Therefore some ISPs, including the larger ones who are TCF members, may look to automate as much as they can. Automation will in itself be non-trivial, costly and not all parts of the process will be able to be automated.

Any system implementation of this nature (both in terms of automation and in terms of staff recruitment and training) is unlikely to be able to be designed, introduced, tested and then made live within such a short period as 3 months. A period of between 6 and 12 months would typically be required.

### **Step 1: Notices are sent to ISP; ISP matches to IP addresses**

15. FlyNet receives 1,000 detection notices from NetFish within the first month of the regime becoming operative, and a smattering from other copyright owners. While NetFish does accompany each notice with the requisite fee, on checking the first batch of notices from NetFish and others, FlyNet's staff discover various problems. These include:
  - 15.1 Some seem to have been meant for another ISP since they are for IP addresses that FlyNet does not control. Conversely, one of the IP addresses is actually for FlyNet's own cache.
  - 15.2 When they match to an IP address some are for customers who are no longer with FlyNet.
  - 15.3 For one, the timestamp given must be incorrect because the IP number given in the notice was not in fact allocated to anyone at the time. FlyNet assumes this is because the time clock on the computer used to detect the alleged infringement is set at a different time to that on FlyNet's systems.
  - 15.4 Many of the notices seem to be about infringements that occurred over a week before the date FlyNet received the notification.

- 15.5 As FlyNet advises NetFish, it simply does not have the resources to deal with this volume of notices and so it has not actually processed some of them yet. NetFish's response is that FlyNet is therefore also liable for the infringements since it has lost its safe harbour by not complying with the regime. NetFish refers to section 92B(2A).
16. FlyNet staff discard the notices that they are incapable of actioning. For the overload, FlyNet realises that it is not expected to check the notices it receives comply with the Bill, it is just a conduit. However, even then, it does not have the resources to match this number of incoming notices to its IP address logs and then send out detection notices within the one week timeframe.

**Issue 2 – Inability to process notices:** Section 122C(2) of the Bill does provide some exceptions to an ISP's obligation to send out detection notices within a week of receipt. However, further exceptions are required where, through no fault of the ISP, it is unable to comply or, through sheer volume, it is incapable of complying within the one week timeframe.

It is important this is made explicit since an ISP's protection from infringement liability may depend on it.

Note also that section 92B(2A) needs to make it clear that if an exception in section 122C(2) applies and, as a result, the ISP need not take any further action, it will be considered to have complied with the entire regime and will therefore be protected from liability.

### **Step 2: ISP sends out detection notices**

17. Since NetFish's notices have a serious tone, FlyNet is concerned that sending them to its customers will generate unwarranted concern in some cases and cause complaints. It considers it reasonable to provide guidance and a fair explanation of the issues to its customers. It therefore elects to send its own detection notices.

**Issue 3 – Format of notices:** For all infringement notices (detection, warning and enforcement), it will be important for industry standard formats to be available for use by ISPs if they wish. These should be developed and major aspects at least mandated by regulations. The focus of all notices should be educational although with increasing warning through the warning notice and enforcement stages.

Standardisation and anticipation of customer questions and concerns will also assist to reduce costs. It will allow ISPs, if they wish, to create webforms where relevant information can be entered directly into the ISP's system by the copyright owner.

Note that the recently released UK Digital Economy Act Initial Obligations Code has more specific details of what notices should contain (including details of any agent authority to issue the notice) plus example notices attached. Ofcom also suggests ISP notice standardisation.<sup>7</sup>

18. As mentioned above, one of the notices FlyNet has received from a copyright owner refers to the IP address of FlyNet's own cache. FlyNet's operation of the cache complies with section 92E of the Act but it is now unsure whether it must comply with this new regime as well in order to retain its safe harbour. To

<sup>7</sup> <http://www.ofcom.org.uk/consult/condocs/copyright-infringement/condoc.pdf>

comply, it would have to send itself notices, which seems a complete waste of time.

**Issue 4 – Overlap with section 92E (caching safe harbour):** An ISP should not be required to forward notices or otherwise take any steps under this new regime where the IP address identified in a copyright owner’s notice is that of the ISP’s cache, provided that the ISP complies with section 92E. Section 122C(2) will require amendment as indicated under Issue 2 above. Section 92B(2A) will require amendment to add reference to section 92E.

19. FlyNet has also received notices alleging infringing material is being made available for download from one of its customer’s sites it hosts. Its initial reaction was this was only relevant to its notice and takedown procedure under sections 92C and 92D of the Act. However, on closer examination of the definition of file sharing in the Bill and the notice content requirements, it finds, to its concern, that this is also covered by the new regime.
20. It is therefore unsure again whether it must comply with the new regime, comply with sections 92C and 92D, or both. On the one hand it risks losing its safe harbour if it does not comply with both; but on the other the regimes are inconsistent and do not make any sense when worked together. Complying with both will also place further pressure on its already overstretched resources.

**Issue 5 - Overlap with sections 92C and 92D (storage safe harbour):** The definition of file sharing in section 122A of the Bill is far wider than what would normally be thought of as sharing. It does cover downloading by itself and therefore means that the new regime overlaps the notice and takedown/storage safe harbour regime in section 92C and 92D. Again, since ISP liability is dependant on this, clarity is required.

There would appear to be three options:

- Make the two regimes consistent. It is now obvious that the lack of due process in sections 92C and 92D is out of step with the account holder protections built into this new regime. This needs to be addressed quickly since evidence now suggests that infringers are shifting from p2p to other services. The TCF understands that there is a commitment to look at this in conjunction with other parts of section 92B-92E in the near future.
- Confine the definition of file sharing strictly to p2p type activities where material is downloaded and made available for upload at the same time.
- Add another exception to section 122C(2) and amend section 92B(2A) in the same way as has been suggested for section 92E under Issue 4 above.

21. Many of FlyNet’s customers do not have fixed IP addresses allocated to them. FlyNet’s system dynamically assigns an IP address whenever they log on. When they log out, that same IP address may then be allocated to someone else or it may be unallocated awaiting greater customer volume/demand. FlyNet recognises that this is going to be an issue for account holders and copyright owners to provide evidence on to the Tribunal or Court if necessary. As noted above, it has received notices relating to IP addresses, which, according to its records, were not even in use at the times set out in those notices.
22. This raises an even greater issue. If the detection method used by the copyright owner is based on a time clock which is different to FlyNet’s (even by just seconds) then potentially all of that copyright owner’s notices to FlyNet will refer to the wrong account holder, where dynamically assigned IP addresses are

involved. For example, FlyNet's records show that John was using IP address 198.9.188.567 from 10.30pm for just under 10 minutes (according to FlyNet's time clock, from 22:23:57 until 22:33:46). Immediately afterwards, Sally logged on and was dynamically assigned the same IP address. But, the detection service that NetFish uses has a time clock that is 46 seconds ahead of FlyNet's. If NetFish's notice alleges that an illegal download started at 22:33:10, then FlyNet will match that to John, when, had NetFish's time clock been set to the same time as FlyNet's, it should have been matched to Sally (since 22:33:10 on NetFish's system is 22:33:56 on FlyNet's).

23. Ontap however has been allocated a fixed IP address by FlyNet. Of the notices FlyNet receives, two from NetFish relate to Ontap's fixed IP address. FlyNet therefore sends a detection notice to Ontap's head office for one of them (it treats the second notice as being within the on-notice period for that copyright owner under section 122C(3)(b), so a detection notice is not required for that).
24. Coincidentally, it has received two other notices from two other copyright owners, which also match to Ontap's IP address. The first one is accompanied by the requisite notice fee so FlyNet sends Ontap another detection notice in respect of that copyright owner. The second notice is from a copyright owner in the US that FlyNet has never heard of. It is not accompanied by any payment but in its covering email, the copyright owner says it will pay FlyNet on receipt of its invoice. FlyNet is concerned that it may action the notice but then find it difficult to recover payment. It will obviously not be economic to take debt collection action to recover a notice fee from a US non-payer.

**Issue 6 – Notice fees:** As the TCF has previously submitted, notice fees must be sufficient to recompense ISPs for the cost of setting up this regime and for its ongoing operation. Otherwise, effectively, ISPs and their customers are subsidising copyright owners' enforcement of private property rights. We are not aware of a private business such as an ISP being expected to subsidise another business in this manner in any other industry in New Zealand.<sup>8</sup> These costs are not trivial but are difficult to predict since they depend on both the final form of the regime and on the volume of notices. That volume influences an ISP's decision as to whether it decides to automate (and incur capex cost at the outset) or deal with notices manually (in which case its opex costs will likely be higher than an ISP which automates). TCF members are currently assessing likely ranges for discussion with officials in due course.

If capex and opex costs are covered, TCF members may be comfortable with fees being regulated in some fashion (subject to inflation based annual adjustment), but with flexibility to agree arrangements for payment etc with copyright owners or their agents on a case by case basis. Different ISPs may want to charge more or less depending on their cost structures and methods of handling notices and the inevitable customer questions which will arise. Regulations under section 122R should provide this flexibility.

However, whatever is provided, it must be made clear in section 122(2)(e) that an ISP need not action a copyright owner's notice unless payment has been received or the ISP has expressly agreed with the copyright owner in question to accept payment later.

### **Step 3: ISP logs actions**

---

<sup>8</sup> TCF members reject the argument often made that they are profiting from infringing file sharing because this adds to their traffic volumes. In fact, such users often cause bandwidth clogging, which impacts on other customers. Those customers could potentially leave or may complain, either of which costs the ISP. They are also more likely to be a credit risk and to churn from one ISP to another, all of which undermines any profit element on what is already a very low margin business.

25. Disk storage is a cost to FlyNet's business so it only keeps information if it is necessary (primarily for billing purposes) and only for as long as it needs to. It is aware of the need under this regime to keep, for the 40 day period specified in section 122Q(2), IP address allocation records enabling it to determine which of its customers was using which IP address at which time.
26. It is also aware of the need to keep the information specified in section 122Q(2), logged both against copyright owners and against customers.
27. However, it, along with other ISPs, has received a letter from NetFish indicating that ISPs are required to keep details of all internet use including any details of content, type of traffic, length of time spent online etc under section 122Q(1) and that they must be prepared to provide that evidence to the Tribunal or Court on request. It would be uneconomic for FlyNet to keep that level of information and it has concerns that retention of information which is irrelevant to this regime would put it in breach of the Privacy Act.

**Issue 7 – Record retention:** The record retention obligation in section 122Q(1) should be confined to information necessary for the ISP to match an IP address and time of use specified in a copyright owner notice to one of its customers. There must be no implication that it is required to keep actual content or other use information. If a copyright owner wishes that sort of invasive evidence collection to take place then it should seek an appropriate Court order, just as Court orders are required for interception by law enforcement agencies.

#### **Step 4: Account holder challenge**

28. Ontap is surprised to receive the notices. It has no idea and no way of checking whether any of its students may have been sharing infringing material over its network and it would be too costly (and almost impossible technically) to implement any solution to check this. It is however comfortable, from its review of individual PC logs and discussions with staff, that none of its head office staff have been sharing the information in question.
29. It is also aware that 5 of its students in a hostel in Dunedin have had problems with their wifi since, over the period in question, a significant amount of spam has originated from them, which has been found to be a result of a security breach.
30. Finally, it's lawyer advises that in fact it may well be an ISP itself and that FlyNet's forwarding of the details of the notice from the copyright owners may well trigger an obligation for Ontap itself to comply with the regime as an ISP, or else face liability for the actions of all those using its network. This is problematic for Ontap, since, as noted above, it does not have any way of checking who was using its network to file share at any particular time.

**Issue 8 – ISP definition:** Whilst the definition of ISP in section 122A of the Bill has been confined compared to that which applies to sections 92B-92E of the Act, it still captures businesses which are not traditional ISPs. Since the focus of detection is on IP addresses, allocation of an IP address should be an additional factor defining an ISP. We note this is consistent with Ofcom's proposed ISP definition in the draft UK code referred to above at Issue 3.

It will be confusing to have two definitions of ISP side by side in the Act. We are aware that InternetNZ has suggested "IPA Provider", which is a logical name.

31. Ontap therefore sends a challenge notice back to FlyNet in respect of both detection notices it has received.
32. FlyNet is unsure whether it is meant to send the challenge notice to the copyright owners since it seems to be envisaged under section 122G(3) that it could make a decision to accept the challenge itself in certain circumstances. Ontap is one of FlyNet's major customers and it would be prepared to accept its argument that the problem has been caused by a security breach. However, when NetFish calls to enquire what has happened to its notices, on being told that FlyNet intends to accept the challenge, NetFish again threatens that if FlyNet does so, it will be liable when infringement is later found.

**Issue 9 – ISP action on challenge:** TCF members do not want to have to decide on the validity of a challenge, even if the challenge is made on the basis of a security issue. The rights affected are those of the copyright owner so it is for it to decide. Further, any decision making process such as this will not be able to be automated and therefore will require manual intervention at a reasonably high level, meaning more cost. Section 122G(3) should be altered to delete the words:

*...if the challenge raises an issue that should be addressed by the copyright owner rather than the ISP*

Similarly, sections 122G(4), 122H(1) and 122J(4) need to remove reference to the ISP considering or accepting a challenge without recourse to a copyright owner.

Once the copyright owner has considered the challenge, it will only be able to communicate its decision to the account holder via the ISP, since it will not have the account holder's identity or contact details at this stage. Section 122G(4) needs to be changed to reflect this.

33. FlyNet therefore decides it will simply send the challenge to NetFish and the other copyright owner for whom it has sent Ontap a detection notice. However, it is unsure how to deal with the fact that the challenge notice covers two different copyright owners. It sees also that the challenge notice is a little short on detail.

**Issue 10 – Form of challenge notice:** Anything which can remove ambiguity and streamline this regime, whilst protecting participants' rights, should be done. Detail of infringement notice content is given in the Bill and TCF members would like to see default standard forms for those notices set out in regulation. Similarly, details of what is expected in challenge notices should be provided. In fact, this is probably more important than for infringement notices, since account holders may need more guidance on these issues than copyright owners, who will often be acted for by agents with copyright law expertise.

For ISPs, having standardised forms will reduce questions and therefore cost.

TCF members do not however consider that the challenge notice should be accompanied by payment of a notice fee since this could have a *chilling effect* where an account holder has to respond to a number of notices it considers invalid (say, in a security breach situation). It would also be impractical and unfair for ISPs to collect fees from account holders in these circumstances.

### **Step 5: Copyright Owner consideration of challenge**

34. As expected, NetFish responds immediately to FlyNet, rejecting Ontap's challenge. Although NetFish is not in fact the copyright owner (NetFish is an agent for the owner), FlyNet assumes that NetFish's consideration and rejection complies with provisions which seem to require the copyright owner to take

action (e.g. section 122G(5) which says *If the **copyright owner responds** ...* [emphasis added]). FlyNet therefore passes that response on to Ontap under section 122G(5). As required, FlyNet logs these activities.

35. However, the other copyright owner whose detection notice has been challenged does not respond at all. FlyNet therefore logs the challenge as having been accepted with respect to that detection notice (under section 122H(1)) but is unsure what this means with respect to any further notices it might receive from that copyright owner.

**Issue 11 – Acceptance of challenge:** Under section 122H(2)(a) if a challenge is accepted (or deemed to be accepted because the copyright owner has not responded within the three week timeframe), all subsequent detection notices are cancelled.

It is unclear whether this relates just to detection notices that have been sent by the ISP to the account holder at that time or to all subsequent detection notices. We assume the former but this should be made clear. We are also uncertain what purpose is served by cancelling subsequent detection notices.

It is also unclear whether the references to copyright owner in sections 122G(4) and 122G(5) are intended to also include a copyright owner's agent. If they do not then it appears it is only a copyright owner and not an agent who can deal with a challenge notice. If they do however refer to an agent as well, then does this mean that all that agent's detection notices (for multiple copyright owners) are cancelled under section 122H(2)(a)?

#### **Step 6: Warning and enforcement notices**

36. Over the next few months FlyNet continues to receive a large number of notices compared to other ISPs. Many of these are from the same people, but, as FlyNet soon realises, with NetFish's notices for example, that does not mean that they are for the same copyright owner.
37. This adds complication and further manual review of the notices. FlyNet staff cannot just log each notice against a database based on sender. They must log against the copyright owner and this requires a more detailed review of the notice itself. At times, again, it is unable due to sheer volume, to process all notices within the week required.
38. Further, FlyNet discovers that apart from ensuring it gets paid per notice, it must also check both the timing of the infringement itself and the date of the notice to make sure that it does not fall within a quarantine period or an on-notice period, in addition to checking whether the notice is with respect to a copyright owner on behalf of which a detection or warning notice has previously been sent.
39. Here FlyNet becomes confused whether those periods apply just to NetFish and so it can treat all its notices as if they were from one copyright owner or whether it should treat NetFish's notices differently depending on which copyright owner it is representing in that notice. This has a major impact since if all NetFish's notices were aggregated, many could simply be logged but not actioned because they would be within on-notice periods. If not, then, by FlyNet's calculations, in month two, it sends two more detection notices and two warning notices to Ontap. In month three, it sends 2 more detection notices (for different copyright owners again), a warning notice and two enforcement notices.

40. **Issue 12 – Definition of copyright owner:** This overlap between a copyright owner and any agent who might send notices and act on its behalf is present in various places in the Bill (e.g. see para 34 above). It would be useful to clarify that any action may be taken by an agent on behalf of a copyright owner but shall only affect that particular copyright owner even where the agent acts for other copyright owners.

Alternatively, if it is intended that an agent might act as an aggregation mechanism, so that all notices issued by that agent, for different copyright owners, are aggregated and dealt with as if they were for one copyright owner, then that needs to be clarified by defining the copyright owner to include any agent (or contractor) who is authorised to send a notice on behalf of a copyright owner, or simply by referring to the sender of a notice as the copyright owner – this would make things simpler for ISPs. Of course in either case, the claim to ownership of the material in question must be substantiated by reference to the actual copyright owner under the Act.

Confused by receiving detection notices, warning notices and enforcement notices at the same time. It still considers that the problem is security related but, even if it is not, it has done all it can to make it clear to users of its network that infringement will not be tolerated (and has added a term to its acceptable use policies to make it clear that infringement can result in suspension or expulsion from its courses). It does not feel comfortable talking to NetFish and so the brunt of its confusion (and increasing anger) is felt by FlyNet's support staff.

#### **Step 7 – Further challenges by account holder**

41. Ontap challenges every notice therefore requiring FlyNet to continue to pass challenges and rejections backwards and forwards between Ontap and NetFish.

#### **Step 8 – Application to Copyright Tribunal**

42. NetFish considers that it is entitled and required to act independently for each copyright owner. Therefore, immediately on being informed by FlyNet that one of its customers has had two enforcement notices sent, following its rejection of the challenges to those notices, it makes two applications to the Copyright Tribunal under section 122J.
43. A week or so later, FlyNet receives two orders of the Copyright Tribunal under section 122J(3). Each order requires delivery to the Tribunal of name and contact details of the account holder (Ontap in both cases) and copies of all notices held on FlyNet's system with respect to each copyright owner.
44. NetFish also applies to the Tribunal to have FlyNet itself joined to the proceeding since it suggests that FlyNet has effectively authorised the infringements. FlyNet rejects this. It is unclear what NetFish is seeking to achieve other than putting public pressure on FlyNet but the Tribunal decides to accept submissions as to why FlyNet should be joined. Ultimately, the Tribunal decides that it can think of no reason why an ISP who has complied with the procedure need be joined and therefore declines NetFish's application, but not before FlyNet has had to spend time and money on legal advice.

#### **Step 9 – Copyright Tribunal hearing**

45. Ontap requests a hearing under section 122L rather than the matter being dealt with on the papers. It also requests that FlyNet appear in support as a witness.

**Issue 13 – ISP involvement in proceedings:** Provided an ISP has complied with its obligations under the regime, it should not be able to be joined to the

proceeding before the Tribunal. If the copyright owner wishes to allege that the ISP is somehow liable (e.g. because it has somehow authorised the infringing) it should issue a proceeding in the Court under the Act, not under this regime. We have no doubt that the Tribunal could deal with this issue itself but clarity in the Act will prevent such applications being made in the first place.

There should therefore be a specific limit put on the Tribunal's discretion in section 122K(1) preventing the ISP from being joined.

There is no adverse impact of such a restriction in terms of any evidence that might be required from an ISP since, by section 122M, standard witness summons and related provisions already in the Act (sections 216-218) are imported.

46. Ultimately, Ontap is ordered by the Tribunal to pay reparation to each copyright owner in the two proceedings. This is despite the Tribunal accepting that none of Ontap's head office staff had been involved in the infringement, that Ontap had no idea who had infringed, that Ontap had no general legal responsibility for the actions of any of the users of its network other than its staff and that Ontap had done everything it could in the circumstances to prevent infringement.

**Issue 14 – Strict liability/Vicarious liability:** This issue does not impact directly on ISPs. However, it is sufficiently important in its impact on ISP customers that we should comment. It seems to TCF members unfair that a business such as Ontap in this example, should be liable for copyright infringement when it has no knowledge of, or real ability to prevent, infringement but has done everything reasonably possible in the circumstances to discourage it.

This regime should be focussed on a better way of enforcing copyright under existing principles and should not create new forms of liability. Under the Act as it stands, Ontap would not be liable for infringement (since it has not engaged in infringement itself and has not engaged in any prohibited authorisation of infringement for the purposes of section 16(1)(i) of the Act).<sup>9</sup> However, it appears that it will be made vicariously and strictly liable under this regime. If vicarious liability is to attach, then in, the TCF's view, it should only do so on normal principles where the account holder has:

- An express legal relationship with the person for whom it is to be held responsible;
- The legal and factual ability, via that relationship, to control the actions of the person for whom it is to be held responsible.

It should also have a defence if it has done everything it is reasonably able to in the circumstances to prevent infringement and has not authorised that infringement.

Otherwise, TCF members' customers will be held liable where they would not have been before. In the face of that potential liability, the only option for persons who are considering providing network access to others will be to do so under very limited circumstances. It is hard to see how anyone would provide public access terminals at libraries, schools or universities, open wifi in towns and cities, free wifi at cafés or hotels or even invite anyone to use one's own network, unless they are an employee (where vicarious liability is an accepted principle).<sup>10</sup>

<sup>9</sup> The recent iiNet case in Australia provides useful guidance as to what constitutes authorisation in this context. *Roadshow Films Pty Ltd v iiNet Limited (includes summary) (No. 3)* [2010] FCA 24 (4 February 2010).

<sup>10</sup> We note in this regard that the Ofcom draft code referred to above at footnote 2 indicates that persons providing network access need to consider how to exercise such control as is necessary to prevent infringement, but it does not make any suggestion as to how this is possible (in TCF

### **Step 10 – Application for Account Holder identity**

47. At the same time it initiates proceedings in the Copyright Tribunal, NetFish makes an application to the District Court under section 122P to obtain the account holder's details. FlyNet then receives a Court order requiring it to disclose Ontap's identity.<sup>11</sup>

### **Step 11 – Enforcement in the District Court**

48. Once it has the account holder's details, NetFish initiates proceedings in the District Court under section 122O. FlyNet personnel are required to provide evidence.
49. Initial skirmishes tend to suggest that the Court has difficulty seeing how Ontap can be held liable for actions outside its control, despite the Copyright Tribunal's finding. FlyNet also provides evidence that it will suffer financial loss by virtue of any termination because it has provided equipment to Ontap on the basis that it will remain with it for the remaining 18 months of its term. A 6 month termination would effectively wipe out revenue which pays for that equipment. It is unclear what if any account the Court would take of this point.
50. Conversely, Ontap submits that it will be very seriously affected by termination including because it will be required to pay an early termination fee to FlyNet. Again, it is unclear whether the Court is required to take this into account. It is also unclear whether the Court could require that its entire account with FlyNet be terminated, which would leave it with no voice communication either. With its voice, data and mobile access terminated, it would effectively be out of business.

**Issue 15 – Internet Account:** TCF members and other ISPs in New Zealand are also telecommunication companies. Some bundle fixed line voice, mobile and internet data services together on the one plan. If termination is to remain as a remedy, then it must be made clear that it is only an internet data account that may be terminated. To address this, the definition of account needs to be added to refer to the IP address. It could therefore read:

**account** means an IP address based connection allocated to a user by an ISP (other than an account of that ISP itself).

(The words in brackets also address, in part, the overlap with section 92E (caching) referred to at para 18 above).

We note however that even this definition will come under increasing pressure as more and more services shift to IP based delivery. If an increasing number of people rely on IP based connections for all their voice, mobile and data, then it is difficult to see how termination can be sustained as a remedy.

51. Ultimately however, in the face of NetFish's claim for a 6 month termination of internet access under section 122O(1), the matter is settled for an undisclosed sum because of the uncertainty as to whether that penalty might be awarded and the severe impact if it were to be awarded.

---

members' view, because, in many circumstances, such control is not possible, or if it is, it would be uneconomic).

<sup>11</sup> The TCF is pleased to see the requirement in section 122P(2) that account holder ID information is only to be used for the purposes of any action under section 122O. This is important to ISPs interacting on a commercial basis with copyright owner groups (as it is for the account holder themselves).

**Issue 16 - Termination:** The TCF has consistently argued that termination is an unworkable and disproportionate remedy. We continue to hold that view. If termination is to remain, it needs to be made clear in section 122O that it is only the account with the ISP which has actioned the infringement notices that is affected. Any adverse impact on the ISP should also be taken into account and, if necessary, compensated.

52. In December 2011, as required by section 122Q(4) of the Bill, FlyNet publishes a report confirming its compliance with section 122Q. It is unsure what exactly it is meant to publish however. As other ISPs publish their reports what does become clear is that FlyNet has been targeted with notices by copyright owners including, in particular, NetFish. However, the figures also show that it is well down the list of ISPs whose customers have had fines awarded or been suspended.

**Issue 17 - Public disclosure:** If the intention is to gauge how the regime is working (we cannot see what other purposes is served), then:

- Copyright owners who use the system should also be required to publish statistics at the same time as ISPs. Since some copyright owners will be overseas based, this should be confirmed by them as part of their notices to ISPs;
- Details should be provided in the Bill or in regulations as to what level of detail is required to be published by both ISPs and copyright owners.

### Concluding comments

53. As the above shows, the regime proposed is complex and will be costly for ISPs to both implement and operate. It is however a vast improvement on the current section 92A.
54. As the TCF has previously submitted, it would be preferable for New Zealand not to take this step but instead to do what the UK and Canada have done and implement a notice and notice system (although without UK's threat of an internet black list).
55. This could be effected by finishing the regime at the detection notice stage. Surveys and experiences in Canada and other countries indicate that around 70% of account holders would cease infringing on receipt of a notice alone, without any sanction being threatened.
56. If that approach was adopted and studies then showed that New Zealand's rate of copyright infringement was not decreasing, the remainder of the Bill could be introduced. Again, this is consistent with the approach being taken in the UK in its Digital Economy Act 2010 (under which the Ofcom code is proposed).
57. If, despite that request, the balance of the regime is to be implemented then we would like to see two things:
- 57.1 A proper recognition of set-up and operational costs factored into the per notice fee payable by copyright owners;
- 57.2 Changes made to the regime to address the issues set out in this submission.
58. To the extent that those issues are to be addressed by regulation, we welcome officials' confirmation that those regulations will be consulted on. However, it should be noted that for ISPs, regulations detailing day to day operation of the regime are likely to be critically important to ISP set-up. Hence, any delay in

regulations beyond the passing of the legislation itself must be factored into the transition period.

59. In the meantime, we thank you again for the opportunity to make this submission and look forward to talking with Select Committee members at the Committee hearing stage.

*For information on any aspect of this submission, please contact:*

David Stone  
Chief Executive Officer  
Telecommunications Carriers' Forum

PO Box 302469  
North Harbour  
Auckland

[David.stone@tcf.org.nz](mailto:David.stone@tcf.org.nz)  
Mobile +64 21 937 879