Telecommunications Carriers' Forum

Submission on section 216 of the Criminal Procedure (Reform and Modernisation) Bill

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

Version Number and Status:	Final v1.1
Version Date:	**11 February 2011**

Submission by the Telecommunications Carriers' Forum on section 216 of the Criminal Procedure (Reform and Modernisation) 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 2degrees, BayCity Communications, CallPlus, Compass Communications, Enable Networks, FX Networks, Kordia, Northpower, Telecom New Zealand, TeamTalk, 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. The TCF recognises the importance of name suppression orders in safeguarding the operation of the criminal justice system in New Zealand.

4. Our submission is confined to section 216 of the Bill, which would impose criminal liability on ISPs for failure to remove or disable access to name suppressed material.

Executive *Summary*

5. This is another example of ISPs being required to police the internet, not because they have any responsibility for the relevant content, but because they are presumed (incorrectly) to be capable of doing so. That ignores a number of fundamental issues:

    5.1 ISPs have no knowledge or control of the material which is published using their services.

    5.2 Therefore, ISPs do not possess the "guilty intent" which should be a pre-requisite to any liability.

    5.3 This regime appears to be based on the assumption that there is ISP liability for which a *safe harbour,* protecting the ISP from that liability, is required. Since ISPs are not publishers of name suppressed materials this is a false assumption.

    5.4 The risk and cost to New Zealand ISPs, as innocent third parties forced to undertake a quasi-regulatory role, needs to be balanced against the likely futility of suppressing information on a global internet, particularly given the information in question has already been "published" by a third party.

    5.5 There are no other similar ISP targeted regimes anywhere in the world as far as we are aware. This proposal is novel and untested.

6. No evidence has been provided that such an imposition on New Zealand ISPs is required given historical co-operation with legitimate law enforcement activities.

7. For these reasons, section 216 should be deleted.

8. If that is not accepted, the proposed regime should only apply to content on a website which is hosted in New Zealand, which content can, as a practical matter, be taken down. It should not apply to other forms of content, for example, email transmission, back ups, caches or file sharing which is not viewable in transmission and therefore is not published in the ordinary meaning of that word. This is because traditional ISPs do not, and cannot effectively, scrutinise general internet traffic, which would be necessary on a continuous basis if checking for name suppressed material being transmitted through their

systems. Unless limited as suggested, the broader regime would present insurmountable technical and legal problems.

9. It is inappropriate to attribute criminal (or civil) liability on the basis that anyone *has reason to believe* the material breaches the relevant suppression order or provision – it lacks the necessary legislative clarity and imposes liability where the person does not have the requisite intent. The regime needs to be based on **actual knowledge**.

10. We note that actual knowledge appears to have been intended by the Law Commission in its report which gave rise to section 216 and was accepted by Cabinet. The Law Commission has recently confirmed that, in its view, the *reason to believe* wording does not reflect Cabinet policy.

11. For these reasons we strongly suggest that this regime be divided into two parts:

    11.1 The current section 216 should be modified to apply to persons who exercise editorial control in the ordinary course over information accessible by a user over the internet (bloggers and website owners being an example). In this submission we refer to these parties as **content controllers**. Once notified of a breach of a name suppression order on their site, since they have the ability to exercise editorial control, liability for failure to take down the relevant content may be appropriate.

    11.2 "Traditional" ISPs who provide hosting services but who do not exercise editorial control in the ordinary course. In this submission we refer to these as **traditional ISPs**. If a content controller has failed to act once notified of a breach of a name suppression order on a site that the traditional ISP hosts on its servers, the traditional ISP could then be notified about the relevant content, and requested to act in the public interest by taking it down, where is practicable and not disproportionate in terms of interference with other legitimate material on the site. In that case a possible answer may be to have a Judge or Registrar consider that issue and make an appropriate order. If liability attaches, it is because the notice from the Court Registry has not been complied with, so the position should be the same as would apply if a telecommunication company failed to comply with an interception warrant.

12. This traditional ISP regime should therefore be implemented via an appropriate "notice and take down" regime – i.e. where an ISP is provided with a notice in a prescribed format by the Court Registry, advising the ISP that specified material it hosts on its servers at a certain location is in breach of a name suppression order or any of sections 205, 207 or 208 of the Bill. Such a regime is analogous to the system adhered to by telecommunications companies under the Telecommunications (Interception Capability) Act 2004, where assistance is provided to Police and other authorised surveillance agencies.

13. Also by analogy to the interception regime and the proposed copyright infringing file sharing regime, cost recovery should be included as an option to be introduced by regulation should that become necessary.

14. As with the interception regime, traditional ISPs should be given full statutory protection from liability if acting in good faith.

15. Further detail is provided below.

Detailed submission

ISP Intermediation

16. Because traditional ISPs provide the conduits through which internet content flows, they are being treated in this proposal as if they are somehow responsible for that content. That is factually and legally incorrect. Traditional ISPs have no involvement whatsoever with content in their general day to day operations. They do not have staff scrutinising the massive streams of data which move around and into and out of New Zealand. They are not publishers of the content – they do not even know what the content is.

17. Traditional ISPs are very different from media organisations, bloggers or other content controllers in this regard. Media organisations sell the news. There is a benefit to them in being the first to break a story and to report as many details as they can. Whether a name is suppressed is therefore directly relevant to them and, like bloggers and other website owners, they have direct control over whether identifying information is published or remains published. A traditional ISP's position on the other hand is more akin to Transit NZ as the provider of New Zealand's roads or a telco in respect of telephone conversations. No-one would suggest that Transit NZ could be criminally liable for activity on its roads or that the telco is liable for any illegal content in a telephone call – so too should traditional ISP liability be rejected in this instance.

18. However, ever since the advent of the Digital Millennium Copyright Act in the US (**DMCA**), on which section 92C of the Copyright Act, and now section 216 has been based, artificially created traditional ISP responsibility has been used to justify traditional ISP liability. It is wrong under the DMCA and it is wrong here. Just because traditional ISPs **can** intermediate with respect to content does not mean that they should and it certainly does not mean that they should be held liable if they do not.

19. Ironically, regimes such as this are referred to as *safe harbours* for traditional ISPs. This makes it seem as though traditional ISPs are being given some sort of benefit – protection from liability which would otherwise accrue. That is generally incorrect in the copyright arena and it is certainly incorrect here. Traditional ISPs are not involved in any decision to transmit or host name suppressed material. They have no knowledge of that material when it is transmitted or posted on the internet. In the criminal context they have no *mens rea* or "guilty intent".

20. Section 216, by stating that ISPs will not be liable for breaching a name suppression order if they do certain things, ignores this. It simply assumes that traditional ISPs should be liable and uses that as the stick to impose a responsibility for policing the internet. Effectively, this sets the traditional ISP up as policeman, prosecutor, judge and jury, having to:

    20.1 constantly be alive to name suppression issues;

    20.2 decide whether material is suppressed or not;

    20.3 if it is suppressed, decide how best to deal with that material (e.g. take a website down in whole or part, block access, delete the material from its servers or variations of the above), and

    20.4 take into account the rights of the customer both under its contract with the traditional ISP and under the Bill of Rights Act. If the traditional ISP, in attempting to comply with section 216, gets it wrong, then it can expect its customer to make a claim against it.

21. Traditional ISPs are not set up to perform this role (as much as they support appropriate name suppression in principle) – a role which is quasi-regulatory in nature, given that it is designed to promote the public interest by preventing general breaches of suppression orders.

22. Having researched the position, we are not aware of any other jurisdiction which seeks to make traditional ISPs liable for name suppressed material. In particular, in Australia, where the law in this area has been subject to recent review in both South Australia and New South Wales, there has been no suggestion that traditional ISPs should be involved in this way.

23. Similarly, the Law Commission's report, on which this proposal is based, contains no justification for the imposition of liability on traditional ISPs and, as far as we are aware, no TCF members were directly consulted by the Law Commission.

24. The other reason why ISP intermediation in this area is misguided is that it is likely to be ineffective. There are two reasons we say this:

    24.1 The internet is global and New Zealand law cannot operate extra territorially, so the proposed regime would not prevent overseas publication of the relevant information. This is exactly what happened in the *Lewis*[1] case, where Mr Lewis's name had been suppressed but turned up on overseas media sites, available for viewing in New Zealand, shortly after. As was noted in the *Cameron Slater (Whaleoil)* case[2], while unfortunate, there may be very little that can be done about this.

    24.2 Secondly, the Court of Appeal has recognised the futility of continued suppression once a name has already been published and become available via the internet. Since section 216 is predicated on the fact that a suppression order has already been breached by someone else placing the information on the internet, the Court of Appeal's conclusion is highly relevant:

> *The Court should be reluctant to leave an order in effect if it is already, or is likely to be ineffective, in practice because of actions which are not themselves in breach of the order*[3]

    As noted above, TCF members recognise the importance of name suppression and do not condone breach of suppression orders. What we are pointing out is that it is unfair to impose a statutory takedown regime and potential criminal (or civil) liability on New Zealand traditional ISPs in circumstances where the Court of Appeal has recognised the futility of continued suppression and, if asked, would in all likelihood not continue the suppression order itself.

25. **Our primary submission therefore is that section 216 should be deleted**.

26. If, despite this, third party responsibility for taking action in respect of suppressed material is to be mandated, there remain a number of issues with the proposal as presented.

Who is an ISP?

27. The definition of ISP is not strictly an issue for TCF members (who are clearly all ISPs under any definition). However, we note that it was generally accepted that the same definition of ISP when used in the Copyright Act caught just about anyone who provided any form of internet connectivity or service to

1 *Lewis v Wilson & Horton Limited* [2000] 3 NZLR 546.
2 *Police v Slater,* Unrep, DC AK, CRN 004028329-9833, 14 September 2010, per DCJ Harvey at paragraph [78].
3 *Television New Zealand Limited v R* [1996] 3 NZLR 393.

anyone else. This lead the Select Committee to recommend a significant narrowing of the definition of ISP for certain purposes in the Copyright Act, to exclude:

> *… universities, libraries, and businesses that provide Internet access but are not traditional ISPs*[4]

28. There is clearly a disconnect between the purpose in section 216(1)(a), which focuses only on storage by the ISP and the definition of ISP in section 216(5)(a) which retains the references to ISPs who transmit, route or provide connections. In our view the activities in section 216(5)(a) are not relevant to this issue and all that is needed is to cater for hosted material as covered in section 216(5)(b).

29. The danger in leaving section 216(5)(a) in place, even where the purpose is expressed to be storage, is that as information is transmitted over ISP systems and the internet in general, it is copied and therefore, arguably, **stored**, at least momentarily. That is why it is necessary to have an exception for transient reproduction under section 43A of the Copyright Act 1994, without which momentary copies made as information is transmitted over the internet, might be argued to infringe copyright. Obviously, those transient copies cannot be accessed by anyone in the ordinary course and therefore are not relevant to the issue of name suppression. So, to avoid any doubt on this issue, the superfluous definition in section 216(5)(a) should be deleted.

30. That does not solve all issues however. The definition in section 216(5)(b) is lifted directly from the Copyright Act 1994. One of the problems we foresee with that in the suppression context is that there may be multiple ISPs, even assuming that transmitting ISPs are not included.

31. This is easiest to see in a blog situation. Where a traditional ISP provides space on its servers for that blog, it is the blogger who exercises editorial control over comments and other contributions. However, it is possible to argue that both the traditional ISP and the blogger are hosts. There is no definition of that term.

32. In our view, the person primarily responsible for taking down the suppressed material in those circumstances should be the blogger. The same applies to any content controller. Only after that avenue has been used and failed, should the "traditional" ISP become involved. Its involvement should be recognised as being in a different category – the provision of assistance in the public interest, to prevent further dissemination of suppressed material.

33. We therefore suggest that the regime be divided into two parts:

    33.1 The current section 216 should be modified to apply to content controllers who exercise editorial control in the ordinary course over information able to be viewed by a user over the internet (bloggers and website owners being an example). Once notified of a breach of a name suppression order on their site, since they have the ability to exercise editorial control, liability for failure to take down may be appropriate.

    33.2 If the content controller fails to take prompt action, then the traditional ISP should be notified. Once notified of a breach of a name suppression order on a site that the traditional ISP hosts on its servers, it may or may not be technically possible for it to take down or disable access to that particular material without affecting large amounts of legitimate material. If access can be denied to the suppressed material itself then the

[4] Commentary to the Copyright (Infringing File Sharing) Amendment Bill under the heading *Internet Service Provider*, as reported back on 3 November 2011 - http://www.legislation.govt.nz/bill/government/2010/0119/latest/DLM3331800.html

traditional ISP would obviously do that. The question then remains what it is expected to do if that is not possible.

34. In either case however, there is a threshold issue in ensuring that either a content controller or a traditional ISP has sufficient information to act on.

How does the traditional ISP or content controller know?

35. *Reason to believe* is an objective "reasonableness" standard and is inappropriate. It is not used as a standard for criminal liability anywhere else in the Crimes Act 1961 and therefore will create uncertainty because there will be no precedent available to decide when a traditional ISP or content controller has *reason to believe*. Uncertainty is not desirable in a civil context such as copyright but it is plainly unacceptable in a criminal one. In this regard, we note the Law Commission report on which section 216 is based[5] has not been implemented accurately (despite the Cabinet paper[6] mistakenly asserting that it has). The recommended standard in the Law Commission report was **actual knowledge**:

> *Where an ISP … becomes aware that they are carrying or hosting information* ***that they know*** *is in breach of a suppression order ...* [emphasis added][7]

36. What appears to have happened is that the drafters of the Bill have seen "becoming aware" and "knowledge" as alternative tests rather than essential components of the one test. They have therefore assumed that section 92C of the Copyright Act (which carries the two as alternatives) reflects the policy agreed by Cabinet. That appears incorrect to us and is a very significant issue for traditional ISPs. At a workshop hosted by InternetNZ on 4 February 2011, Dr Warren Young of the Law Commission confirmed that a mistake appears to have been made in this regard.

37. Putting this issue in practical terms however, there are two separate but related problems for a traditional ISP or a content controller:

    37.1 First, how does the traditional ISP/content controller know that a name suppression order has been issued?

    37.2 Secondly, how does the traditional ISP/content controller know which part(s) of the material it is hosting is in breach of the suppression order?

Notification

38. The only way for ISPs and content controllers to **know** is if they are told of the name suppression order and of its contents. That would put them in a similar position to media organisations that are currently notified of suppression orders. It would be grossly unfair for traditional ISPs in particular to be subjected to greater risk of liability than publisher media organisations because they are not notified and have an objective standard imposed.

39. In fact, it is arguable that the combination of the *reason to believe* objective test and the fact that this regime is quasi-regulatory in nature, means that the offence would be treated as one of strict liability in certain circumstances (i.e., no intention to breach the suppression order would be required on the part of

---

5 *Suppressing Names and Evidence* NZLC 109, issued 22 October 2009 - http://www.lawcom.govt.nz/sites/default/files/publications/2009/11/Publication_149_453_R109.pdf

6 http://www.*justice*.govt.nz/policy/criminal-justice/copy_of_documents/Criminal-Procedure-Simplification-Project/Name Suppression Cab Paper.pdf

7 *Supra note* 1 at paragraph 7.26 Recommendation R26.

the traditional ISP)[8]. The current proposal distinguishes between knowledge (i.e. intent) and *reason to believe* (an objective test). Therefore, it can be argued that if it is reasonable to conclude that a traditional ISP **should** have been aware from surrounding facts that material should be suppressed, but does not suppress that material, then it is liable. Given that the traditional ISP has had no involvement in the decision to publish, imposing such a strict liability regime would be particularly unfair.

40. The Law Commission also recommended that *a national register of suppression orders should be advanced as a matter of high priority*[9]. With the breadth of the current definition of ISP, it is difficult to see how a register will work by itself[10]. A register is certainly a necessary ingredient but, as we note below at paragraphs 44 and 45, even this does not deal with all issues.

41. Note also that any notification regime must cater for the lifting and variation of suppression orders. Traditional ISPs have obligations to their customers under their service contracts and under the Bill of Rights Act if performing a quasi-regulatory role. Once a suppression order is lifted then the ISP will therefore need to respond to that, if it is able by unblocking access. It can only do so if it is notified.

42. Conversely, if there is no official notification process and the *reason to believe* standard remains, the regime will have a potential chilling effect on free speech. It could easily be used by a disgruntled accused whose name has not in fact been suppressed. If such a person were to falsely notify a traditional ISP or content controller, there would be no way for them to accurately check the falsity of that notification without a national register. Faced with the risk of liability if they do not comply with a valid notice and having no way to check, they would have little choice but to take the material down or disable access. This is exactly what has happened in the copyright context as documented on the www.chillingeffects.org website.

43. It would be a disappointing irony if measures designed to enhance open justice by restricting name suppression availability in fact had an opposite effect.

Knowledge of breach

44. While receiving official notification of a suppression order may be sufficient for a blogger or website owner to locate the relevant material, it is unlikely to be sufficient to allow a traditional ISP to do so. Since the traditional ISP has not made the conscious decision to publish the relevant material and has no editorial oversight (unlike a blogger or media organisation), the ISP will not know where the relevant material is located. For a large traditional ISP, even automating a keyword search of the massive amounts of material it hosts is unworkable and would constitute an unwarranted intrusion on the privacy of its customers. For a smaller traditional ISP, the cost and greater privacy intrusion of a manual search is even more onerous and unjustified.

45. There are also insurmountable technical issues:

    45.1 Keyword searches for names will inevitably throw up false positives. However, it may not be possible for the traditional ISP to determine what information is legitimate, and what is in breach of the suppression order. If it cannot easily make this determination, then it may, nonetheless, be

---

8 See the leading case of *Millar v Ministry of Transport* [1986] 1 NZLR 660 (CA), in which the Court of Appeal indicated that where there was specific reference in legislation, regulatory offences could be strict liability – i.e. no need for intent.

9 *Supra* note 5 at paragraph 6.65, Recommendation R24.

10 The *Law* Commission's *Issues Paper 13* issued in December 2008 raised this problem in paragraph 7.21 indicating a concern that wide access to a national register containing necessary details of the suppressed name might defeat the object of the suppression order in the first place.

forced to take down or disable access to material, meaning such material may be incorrectly subjected to this regime.

45.2 If the suppressed material is deliberately obscured or coded by the publisher, as it was in the Cameron Slater (Whaleoil blog) case[11], then a keyword search will be ineffective. There is no realistic way for a traditional ISP of any size to handle this issue, as any such review would have to be undertaken manually. However, that fact alone would arguably not protect a traditional ISP from having *reason to believe*. That uncertainty is inappropriate in a criminal context.

46. In case it should be argued that these problems are being exaggerated since section 216 simply replicates an internationally accepted notice and takedown regime, that should be rebutted. The *reason to believe* test is unique to New Zealand in section 92C of the Copyright Act. It does not reflect the **actual knowledge** requirements of the DMCA or its Australian equivalent for that matter. It is an inappropriate standard here as it is in section 92C.

Conclusions and Recommended Solutions

47. Given the legal and technical difficulties associated with the proposed s216 regime, and conversely, the futility that has been implicitly recognised by the Court of Appeal, our view is that section 216 should be deleted. Our view is strengthened by the fact that we have been unable to find any similar regime anywhere else in the world.

48. If, despite that, section 216 is to proceed, in our view, the only way for it to operate is to have a two tier system.

49. First, notice should be given to the content controller since it has the ability to exercise editorial control. If the content controller fails to exercise that control as soon as is practicable, then it should be liable as proposed in section 216.

50. If the content controller has failed to take down or disable access, the traditional ISP should be notified of the suppression order and location of the breach in question (URL, IP address or other location information).

51. If it is technically possible for the traditional ISP to take down the particular suppressed material or disable access to it, then it should do so as soon as practicable. However, if it is not possible for it to do so without disabling other non infringing parts of a site, then we question whether that is appropriate. TCF members support the intent of the Bill to prevent wider dissemination of suppressed material but it is hard to see how disabling access to large amounts of non-infringing material, in order to disable access to one suppressed name, is proportionate.

52. One possible way of dealing with this would be to have a Judge or Court Registrar issue an order having considered that issue of proportionality.

53. Traditional ISPs should not be liable in the same way as content hosts since they are innocent third parties who have no involvement in the site in question, no involvement in the publication of the suppressed material, no editorial control and are acting effectively in the public interest. If there is to be any liability it should be the same as that which telecommunication companies have if they fail to comply with an interception warrant.

[11] *Supra* note 2, as discussed at paragraphs [138]-[139] and [162]-[165].

54. Again, by analogy to the interception regime:

54.1 TCF members would like to see a regulation making power included in section 216 so that traditional ISP cost recovery can be added later should it be found that is necessary; and

54.2 Traditional ISPs should be given specific protection from liability where acting in good faith under this regime, should it be found that material was not in fact suppressed or had ceased to be suppressed (see section 20 of the Telecommunications (Interception Capability) Act 2004).

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

David Stone
CEO, Telecommunications Carriers' Forum
PO Box 302469
North Harbour
Auckland
+64 21 937 879