



## **SUBMISSION**

by

**EMPLOYERS AND MANUFACTURERS'  
ASSOCIATION (N) INC.**

**Submission to  
Ministry for Economic Development**

**On**

**Section 92A Review Policy Proposal  
Document**

Prepared on 16 July 2009

## 1. BACKGROUND

This submission is made by the Employers and Manufacturers Association (Northern) Inc. (EMA).

The EMA is made up of some 8500 member business units covering the New Zealand region north of Taupo. This membership includes approximately 1500 manufacturers ranging from large to SME.

Within our membership there are a significant number of companies and organisations involved in the manufacture, importation, supply, distribution and retail of most product types and the provision of services in a wide range of service sectors including governmental, contractual, tourism, IT, banking, insurance and business advisors.

As an organisation the EMA supports international best practice to be followed and compliance costs are fully addressed in any legislation or regulation.

As the leading voice of business in the upper North Island we actively participate in both the submission process and any development of regulatory proposals that may impact on our membership such as those discussed within these proposals

## 2. CONTACT

For further contact in relation to this submission:

Garth Wyllie  
Executive Officer  
Employers and Manufacturers (N)  
Private Bag 92-066  
Auckland

Telephone: 09-3670913  
Direct: 09-3670935  
Mobile: 021-649900  
E-mail: [garth.wyllie@.co.nz](mailto:garth.wyllie@.co.nz)  
Web: [www.ema.co.nz](http://www.ema.co.nz)

## **SUMMARY STATEMENT**

The EMA is concerned that the application of section 92A will have undue impacts on business if applied and therefore does not support it in the current form or with the proposed structure for dealing with Right Holder complaints.

We believe the law as proposed is unworkable and in many instances may be unenforceable. The potential impacts on business have not been addressed should this proposal go ahead and we would expect that much clearer definition of its application to the businesses who rely in internet access for the continuation of the business and how any penalties might be applied to business is needed. The wider impacts of any enforcement as proposed in this review have not been addressed and we have attempted to outline where these exist.

The EMA has expressed in this submission a wide range of concerns that need to be addressed relating to the impact of employees use, contractor use and client use on the risk to businesses. These must be addressed.

The EMA believes that most business is not a high part of the risk profile for downloading of most RH work and while some responsibility must remain it should be reflective of both the risk and nature of business use of internet access in terms of application of any penalties. We accept that deliberate activity by a business to misuse commercially protected works must be deterred through appropriate enforcement action.

The EMA believes there are more appropriate mechanisms to address the issue of illegal downloading of copyright works and that these should be explored before proceeding with the implementation of this law.

## **SUBMISSION DETAIL**

We do not support the imposition of Section 92A and while recognising that the rights holders should be protected where possible we believe that enforcement by this method will be unwieldy and compliance cost heavy.

The only country to have applied a similar application of this law is France and this has not been well accepted even in that country. We believe that alternatives should be sought to section 92A that do not impose potential compliance costs on business but target offenders appropriately with the necessary penalties for deterrence.

Such alternatives may include blocking of file sharing sites or filtering to prevent such sites from being downloaded from. This is similar we believe to the application of Child Porn filtering

We would note that while severe penalties are being offered for downloading of works, no such actions is being contemplated for counterfeit products including movies and music cd's imported for personal use by consumers. Perhaps if both such products were being seized and the importing person was warned that they could not fly again if they were caught again, this section of the act would be in context of overall enforcement.

While this example may seem extreme we believe that the issue must be firstly seen in its wider context and secondly addressed with appropriate mechanisms to reduce or remove widespread abuse of copyright through targeting the source and not the effect.

We have responded to the questions raised in the discussion paper directly later in this paper however we also have some areas of particular concern that are not addressed in the paper and do not appear to have been addressed in considerations of this section of the law.

## **SPECIFIC CONCERNS**

While the paper does comment on the fact that a business may be impacted where multiple users of the connection exist we do not believe this area has been addressed adequately.

Of particular concern are the responsibilities of the subscriber business for actions by employees, contractors, other users of the businesses ISP Connection and including businesses or entities who provide guest services.

We also question the enforceability of any decision to terminate individuals within this process and raise questions about the implications of such actions on commercial agreements.

### **Employees Use of Internet**

There is an assumption that businesses can and will have in place software to prevent downloading of “works” which by definition is extremely wide and therefore extremely difficult to enforce without complex network management software.

In larger businesses this may be possible where perhaps dedicated IT staff serving the business exist. However given that most business are SME’s employing less than 5 staff this is not reasonable as a cost to impose on the business.

We believe that at most when an infringement notice is lodged against a business that is not related to systematic and deliberate involvement by the business itself, that the business should be able to respond by outlining what measures it is putting in place to prevent future re-occurrences which in the case of small businesses may be applying a use policy for internet access by staff.

The compliance cost potential of this section of law on SME’s is out of proportion to the risks to the RH’s and we believe there needs to be a fair recognition of this within the processes when the breach has occurred within a business rather than within an individual connection.

We believe that the actions of an individual employee should not be able to place the entire business in jeopardy through the businesses internet access being terminated even where the business has taken reasonable actions to try and prevent re-occurrence of breaches of the RH’s IP.

### **Contractors Use of Internet**

Many business use contractors to provide services such as IT maintenance and therefore access to systems is wide. The business may not be aware that any abuse is occurring

until it receives a notice and then it will need to identify that the breach is occurring through a contractor over an employee. Such action is difficult and particularly where multiple contractors are involved or individuals of the contracting service are changing frequently. Potentially breaches could involve multiple individual contractors and yet under this system the business will be held accountable for what essentially is out of their control.

We find this situation entirely unacceptable and again demonstrates, that a one size fits all approach, will place undue risk and compliance costs on businesses when they are clearly not the primary target.

### **Guest or other Use of Internet Access**

Some businesses provide guest access for visitors which may now be in jeopardy. Others provide access as part of their services to their clients.

For example Internet Café's, Hotels with Broadband access, schools and educational facilities and those providing Free Wi-fi access such as Libraries or local government free broadband access. All of these providers will now be forced to ensure they have filtering and blocking of downloading from known web sites and Peer to Peer file sharing web sites to try and avoid exposure to both notices of infringement and further action if users of their services breach the legislation.

Even with good blocking in place, new file sharing occurs regularly on the net and new software becomes available to get around such blocking/filtering meaning that these types of businesses will be extremely exposed under this law.

To see a hotel or a University for example, have its broadband connections terminated because its clients or students have abused the connection and using new file sharing software download RH's IP Works is an example of a perverse outcome of this law. More perverse would see such establishments cease to offer the service to prevent this action and consequently set back the take up of broadband use.

We believe that some forms of exemptions should have existed within the law or provisions to accept that such businesses or organisations have limited ability to prevent illegal activity but should be seen to take "reasonable proactive steps" to prevent it.

### **Perverse Outcomes of Enforcement of Termination on Business**

The action of termination is the extreme element in terms of the actions possible by the Copyright Tribunal however with such actions we believe that considerations must be given to perverse outcomes.

These include:

- termination of staff/redundancy,
- loss of business,
- inability to transact e-commerce,
- inability to transact Efpos,
- Internet Protocol phone systems made redundant or reluctance to move to this technology
- remote workers or branches using Internet Protocol phone connection unable to operate, receivership of businesses unable to continue trading
- contractual obligations relating to terms with an ISP will not be able to be met causing breach of contract litigation potential

Most businesses cannot operate without some form of internet access so the impact for a business from this action has far greater impacts than the same action against an individual in a domestic situation

### **Enforceability of Law**

While we are deeply concerned about the impacts of this law we also see a serious question on just how enforceable the law will be on the target individuals who are the culprits that the RH's which to stop.

Given our record of enforcement of traffic fines and the ability to actually get such fines paid, we question how well this will work without literally using bailiff actions to cease the offending persons hardware in lieu of the fines.

In the case of termination of an ISP connection we believe this is a joke given the availability of prepay broadband (Whoosh and Vodafone), the ability to switch to another ISP (unless some form of register is created and the individual does not use a false name) and the ability to use free Wi-fi where it exists to continue their activities.

In the case of prepay broadband if one connection is terminated then the individual just needs to go out and purchase another connection without giving details of who they are.

We would question how the ISP can provide any details or even contact the prepay person to issue an infringement notice to without this detail and yet there is no detail on requiring the capture of this data or how they would be able to deal with existing Prepay users who have not supplied this data.

For the ISP to simply cut off the Prepay access without due notice or process exposes them to risk under the Fair Trading Act in that they would have no legal right to do so and it may then be held that their transaction of selling the Prepay was False or Misleading Representations (s13) or Misleading Conduct in Relation to Services/goods (s10 & s11) or Demanding or Accepting Payment without intending to supply (s21)

The existence of a category of internet access without an ability for the ISP to know the subscriber details places the ISP in a position where they cannot action infringement notices for RH's in those circumstances and will need to be addressed.

Equally if a person requests a mobile or transportable broadband connection (prepay or otherwise) and does not supply the correct details to the ISP, the ISP cannot action infringement notices in accordance with the Phase 1 outline. (It is reasonable to assume that a person organising a wired connection will need to give more details and therefore be more traceable)

### **Contract Law Implications**

In many cases both business and individuals sign up to ISP connections through a term contract. For the immediate period no ISP will have this issue outlined in their contracts and hence termination may actually breach contract law through no fault of the ISP.

We would also question the impact in terms of fairness if this is not spelled out in headlines within any contract for internet connection in that in most cases neither the individual nor a business actually signs an agreement to obtain internet service and is reliant on the terms and conditions being available.

If an ISP signs up a new or renews an existing broadband subscriber without making it clear ahead of signing up that this law will still require them to pay if disconnected under the legislation, then the consumer may choose to exercise their rights under the Consumer Guarantees Act and potentially the ISP may also be misleading the consumer about the nature of the agreement under the Fair Trading Act if they were then to terminate or disconnect the consumer.

We believe that clarity is required to remove any such risk to ISP's if this law is to proceed and that the current law does not remove that risk to ISP's.

The issue of early termination fees being charged by some ISP's would also raise concerns as this would appear to apply additional penalty not necessarily considered by the Copyright Tribunal.

A business for example being disconnected from both its broadband and its data card mobile accesses might face fees for each one amounting in the hundreds of dollars each and if that also extended to areas such as Blackberry service potentially even more in a medium size business.

By example the EMA has an internet broadband Fibre optic connection, 2 DSL connections, and some 10 Data cards plus around 20 Blackberry connections. The cost of early termination fees to the EMA would around \$7000 in addition to the loss of ability to operate.

It is therefore essential that the impact on businesses needs to be addressed to prevent contractual issues occurring should this law proceed.

### **Enforcement on Businesses**

In a business situation many businesses will have more than one Broadband connection. Does termination apply to them all? If it does then this may be unfair as it might only be a single staff member using a data card to breach Act. To then apply this termination to the balance of the business including other data cards and/or hard wired connections would appear to be excessive in such circumstances.

To extend this further to multiple locations if the business has a single ISP for all would equally be unfair and does nothing but penalise the business for the actions of a single individual

The timing of infringement notices going to businesses is also an area that raises concerns where it is possible that the 30 days could have elapsed by the time the business receives the notice, gets it to the correct person to take action and then goes through the IT process of identifying the individual who may be offending. At which time a cease and desist notice may have also sent. This automatically places the business in high risk of the RH then pursuing to Phases 2 and 3 which will cost the business in terms of time.

### **Cost of Compliance to Business**

This law if implemented imposes a range of compliance costs to business that while difficult to quantify can be identified.

We see these as:

- Changes to employment terms to ensure action is possible under employment agreements

- Establishing policies and processes to deal with potential breaches and rules on what is acceptable for download and what is not.
- Establishing processes to deal with infringement notices
- Purchase and/or installation/configuration of software to block or filter out access to File sharing web sites and use of Peer to Peer software
- Allocation of staff time to these processes and to dealing with notices should they occur
- Cost of time involved in identifying individuals should a breach occur either in terms of staff or contractors time/cost
- Cost of responding to notices when they are received

## **QUESTION RESPONSES**

### **Introductory Question Responses**

1. We do not believe all issues have been addressed in this paper and question whether this will provide a fair or workable process for copyright infringements.
2. In principle the proposals are in the right direction however the issues raised in our concerns section of this submission need to be addressed.

### **Phase 1 Question Responses**

1. Yes this is, providing a workable solutions to our concerns are addressed
2. No but potential abuses by the RH may need to be monitored for
3. 9 Months should be adequate given that the life cycle of most downloaded material such as Games, movies or music has a 6 week to 3 months window and repeat offending will be known in a very short space of time by the RH
4. Yes but evidence needs to be held of this before any action can be taken and in line with a single work. There should not be any less level of evidence just because multiple works are involved.
5. This may be difficult to enforce and given ISP's will have at least a postal address for the subscriber this should not be necessary.
6. Yes as per point 2 of this set of responses such abuses need to be monitored for
7. No other than our concerns are raised separately being addressed.

### **Phase 2 Question Responses**

1. Yes
2. No
3. Yes but only if all the RH's have collectively lodged notices or the notices have been lodged through a representative agent organisation for all of the RH's such as an Association or patent attorney authorised to act for all RH's named. Some rules around this need to be clear as to who and when this can apply.
4. No other than our concerns raised separately being addressed.

### **Phase 3 – Question Responses**

1. Yes this is a good option to keep costs down however mediation only works if both parties are prepared to compromise and there is nothing stopping the RH refusing

to accept offers by the subscriber that might in most views be reasonable in order to force a Copyright Tribunal to hear the case. Some mechanism needs to be in place to address where a RH consistently fails to settle in order to push the case to the Copyright Tribunal.

2. Online is an option and may be more efficient depending on the subscriber
3. Yes
4. No question for this number
5. The option of warnings only through to termination may be viable but we believe that our concerns on this law need to be addressed in this regard
6. 12 months for an individual however for a business such length could be seriously damaging to the extent of putting the business “out of business” so we believe that unless the business itself is involved in the systematic breaches of the IP of RH’s then disconnection not an option that should be permitted
7. Yes there should be appeal to both the Copyright Tribunal and the High Court as options.
8. If there is a breach of IP found in the favour of the RH’s then costs may be awarded against the Subscriber in serious or systematic cases but otherwise costs should lie where they fall.
9. No other than our concerns raised separately being addressed.