

Following is the ISPANZ Submission on the draft Code of Practice for S92A.

- This is a poorly written law - We respectfully urge the government to delay the implementation and review the law and seek a first principles review of the Copyright Act. We commend the TCF in developing a code in trying to make that law fit.
- We respect the creative sectors need to make a buck, and recognise a healthy creative sector is good for ISP's - we want a nation of not just net consumers, but also net providers. An even mix of content and 'eyeballs' if you will. Many ISPANZ members believe a healthy local creative sector is crucial/critical to improving the economics of delivering high performance 'broadband' to all in this country.
- We have grave concerns around the disruptive impact of this on us as ISPs and particularly on our business customers, at a time when we should be focusing on building the digital economy, not tearing it down.
- We may not catch the worst offenders - we're very very concerned about the arms race (trust networks, private trackers, blocklists, encryption etc) making this whole thing futile. No one knows what percentage of the market are prepared to enter the 'arms race'. This is a danger for all of us. We have one chance to get this right. Lets not try and use the excellent work of the TCF to try and make a poorly formed law fit. Lets actually get it right.
- We have reservations about the on going accuracy on the integrity of the detection systems, and demand a extremely thorough 3rd party (an agreed organisation within NZ) audit of the system. The system should be audited on a regular basis. That audit should generate a metric around 'confidence level' of the audited system - or at least an estimate of the number of false positives. A condition of a pre approved rights holder status should include a mandatory 3rd party audit. The confidence level of a system (at a level to be agreed) is a criteria to being pre approved. Should the 'confidence level' fall below a threshold, the rights holder would be removed from the pre-approved register. The audit should also check to see if the detection process/system breaches copyright and licensing of 3rd parties.
- We have very serious concerns for the business community (or certain ISP's) to be able to resolve down to employee/end user level without rightsholders identifying the monitoring IP addresses and protocol (the NAT problem) as part of the accusation. Unless rightsholders agree to do this, we see no technical means available to resolve the accusation with the end user. This presumes businesses invest in NAT session storage and datamining capability at their cost. We estimate the cost of storing information to be serious if the business community is serious about compliance. Consider this (estimates based on a limited data):
 - We assume NZ Business policy is to present a written warning to an employee if it is certain that employee has infringed.
 - We assume that NZ business trusts an accusation as acceptable.

- We estimate that in excess of 90% of NZ Businesses use Network Address Translation (NAT), as a means of connecting its employees to the NZ business supplied internet connection.
 - NAT Sessions occur at a rate in a business of a frequency between approximately 3.5 - 4.5 translations per second per Mbps of use on average.
 - Occupied Disk space is in the order of approximately 300 Bytes per Translation.
 - Expected Storage time is approximately 6 weeks (4 weeks based on CoP notification time, 2 weeks for margin of error)
 - Alternatively if a single business has an average of 4Mbps/8 hour 5 day work week, for 6 weeks, the resultant storage requirements is 4GB.
 - Alternatively if the combined Internet load of NZ Business is 1Gbps, then the resultant stored data that needs to managed by NZ business is around 1000 Terabytes of data.
 - We ask the Government if it wishes NZ Business to be strictly compliant with the law and bear the costs collectively of storing 1000 Terabytes of data that it can query should a S92A accusation be made. NZ Business will need to query that data in order to resolve/confirm which employee MAY have broken that law. Even then, we are assuming the accusation process is flawless if we are to be sure they are not breaching employment law.
 - This does not consider the compliance costs of business purchasing hardware that supports the recording of NAT sessions.
 - We suggest that the compliance costs of NZ business collectively storing 1000 TB of data and managing it, is considerable, if NZ business does not want to risk breaching employment law.
- We insist on a regular (monthly) report from Rights holders that lists ISP by accusation count. Should that show that an ISP is getting accusation notices that is disproportionate to it's market share (give or take an agreed percentage), then that ISP should have the right to enter into the agreed disputes process for all future accusations until the disproportionality of accusations is resolved.
- We note that we should be vary wary about developing law and codes of practice which alienate a certain technology. Peer to Peer Technology (Bittorrent etc) is used in many ways. For example, CNN recently broadcast the Barrack Obama inauguration on the internet via p2p technology. Clearly we are in developing times. Rightsholders need to provide very detailed information in terms of an accusation to ensure we are dealing with the use of a technology rather than the technology itself.
 - We will reserve serious doubts over the proposed disputes process until we are confident of the on going 'confidence level' of the detection system of a pre approved rights holder.
 - The arbitrator in a dispute must be independent of the accused and accuser. We reject Rightsholders being in the position of Accuser and Judge and Jury.

- We implore on rightsholders to come up with a viable legal alternative in the digital age - before S92A is actioned.

Regards

Jamie Baddeley
President
ISPANZ.