Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

23 March 2015

Communications Alliance Ltd

By email: info@commsalliance.com.au

Submission to Communications Alliance re: Copyright Notice Scheme Industry Code

Contents

General comments

The Australian Privacy Foundation does not support the proposed Industry Code C653:2015 Copyright Notice Scheme (the Code). The Code has many serious problems including:

- With potential impact on all Australian Internet users, its characterisation as 'Industry' Code is flawed, its development excluded users as equal stakeholders and offered inadequate consultation, resulting in bias to interests of one industry group and against users and citizens
- It interferes with the privacy of individuals

- It exposes completely innocent account holders to potential litigation due to the actions of another person accessing their Internet connection
- It is inconsistent with the *Privacy Act* 1988 (Cth)
- There is no Privacy Impact Assessment or privacy oversight
- It does not contain adequate protections for individuals
- A lack of procedural fairness in the notice process
- The dispute resolution process does not meet dispute resolution standards in Australia
- The burden on copyright holders to adequately verify their claims, and commit to an appropriate and fair enforcement and litigation process, is manifestly inadequate.
- Copyright holders, particularly foreign movie rights holders, are the beneficiaries of the scheme, without having been obliged to offer their goods and services on fair non-discriminatory terms to Australian users, and contrary to the outcome of their failed *iiNet* litigation, yet the essential requirement that they and not consumers must bear the entire cost of this scheme is not covered in the Code.

The concerns listed above are serious and should mean the Code should not proceed. If the Code were to proceed it requires significant amendment with a more comprehensive consultation process.

Lack of adequate consultation process

This Code has the potential to affect the vast majority of Australians as so many Australians have an Internet connection. It adds to an inconsistent, confusing, user-hostile set of industry-centred codes affecting Australian Internet users.[1]

Its construction as an industry code is flawed, since it directly affects all Australian users of the Internet. Users, consumers and citizens are essential stakeholders, with a key interest in a balanced application of law to the digital environment and online economy to support the legitimate interests of all participants, but they have been sidelined.

An adequate consultation process is mandatory and this has not happened. We note that the Australian Privacy Foundation was not consulted at all in the development of this Code. Given the serious repercussions for the privacy of individuals who may face litigation following the introduction of this Code, a failure to seek the views of privacy advocates indicates a flawed process in the development of this Code.

We also contend that the consultation process following the release of this Code has been rushed and not widely publicised. The Australian Privacy Foundation was not alerted to this consultation and we found out about this consultation through an article in the news.

A consultation process that relies solely on all Australians reading every article in the news to find out about a potential significant change in their contract with their ISP is clearly inadequate.

We also understand that despite having been under negotiation for years since the failure of the rights-holders' *iiNet* litigation in the High Court (which decisively rejected the rights-holders' flawed interpretation of the current *Copyright Act* insisting "authorization liability" obliges ISPs to act on behalf of the rights-holders against the interests of their customers by breaching obligations of confidentiality, secrecy) for most of this period no consumer interests were involved. Grudgingly

[1] See *Drowning in Codes of Conduct: An analysis of codes of conduct applying to online activity in Australia*, Chris Connolly and D Vaile, Cyberspace Law and Policy Centre supported by auDA Foundation, launched on World Consumer Rights Day at ACCC-hosted national consumer forum in Melbourne, March 2012, http://cyberlawcentre.org/onlinecodes/report.pdf

tolerating a belated and limited involvement by ACCAN, not as an equal partner and without equal and equivalent participation by consumer interests, cannot remedy the unwillingness to engage with user and consumer stakeholders on transparent and equal terms.

Privacy

Individuals have an expectation of privacy, confidentiality and personal information security when contracting with an ISP, protected by the secrecy and confidentiality provisions of laws and contracts. Every individual wants to be able to use ISP services with trust and confidence that s/he is not being spied on, surveilled or harassed. This Code interferes with that expectation of privacy and undermines any trust and confidence individuals have with ISPs.

It does not appear to be accompanied by any structured effort to identify the risks and threats it poses to privacy and related interests (and potential for mitigation of these threats), such as a Privacy Impact Statement, and does not appear to recognise the serious nature of these threats. The potential for privacy impacts whether personal or in the form of massive data breach, or abuse of the proposed 'Metadata Retention' scheme sold as an answer to fears of terrorism, do not seem to have been contemplated and taken into consideration.

As stated below, a Privacy Impact Statement is required before this Code should proceed. This should be open and transparent, so all affected Australians can assess the risk to themselves.

Internet and the household - identifiability fail?

The account holder for an Internet connection often shares this connection with their family or household (and sometimes unwittingly with others). This is often now via wireless Wi-Fi and NAT technology, rather than older wired technologies. An account holder often has little or no effective control of the actual use of the Internet by other members of the household, their visitors, or others who may gain access to the Wi-Fi access point by authorised and unauthorised means.[2]

Weak passwords may be set and left for years, with increasingly long-range Wi-Fi points also broadcasting to the neighbourhood, accessible by Google's passing Streetview snooping operation from the roadway, and hackable by anyone within range.[3] IP addresses are automatically dynamically re-allocated by the access point, local IP allocation logs are often not kept or not easily accessible, and the translation of device MAC addresses to IPs a difficult task.[4]

The underlying problem is that the IP technical information generated by ISPs is increasingly not reliable to identify individuals. IP data will become even less reliable over time, as the 'Carrier Grade NAT' system for fast, dynamic reallocation, and simultaneous sharing of allocated IP

[2] It is increasingly well established that domestic Wi-Fi access points are a complex, bug-prone and very insecure form of access control, with recently revealed NSA- or GCHQ-instigated 'backdoors' potentially vulnerable to abuse by anyone, old firmware with inbuilt cryptographic flaws generally unpatched, a very low standard of password strength practiced by most users, and older models offering trivially easy to breach security controls. The problem is the de facto assumption that a skilled and diligent Unix system administrator/network technician will look after these complex devices. This was unrealistic by the mid-90s, but the flawed model remains profitable and may now be too expensive to fix.

[3] Given the recent failure of all relevant senior ministers to be able to properly explain what 'metadata' is, it would be instructive as a mental exercise to test each member of the current Cabinet as to their ability to reliably secure and forensically diagnose usage of their home Wi-Fi access point. If they can't all do it, arguably no-one else should be expected to, since the technical skills are rarely available or affordable.

[4] The limited retention issue also applies to ISPs, with 2 year 'Metadata Retention' for terror purposes the result. Will home users face a de facto home "metadata retention" scheme: with those without retained local metadata and able to prove who used a particular IP being denied the presumption of innocence?

addresses, moves from the mobile network to the terrestrial network to cope with IPv4 exhaustion in 2011. Under CG NAT, the same IP address is shared among many account holders at once.[5]

This Code has the strong potential for an account holder to be harassed, threatened and sued for conduct that is not their own. The account holder may simply be unable to identify the responsible person, and/or unable to stop the conduct. This is unjust, and inconsistent with the rule of law.

It also is based on assumptions that should perhaps be the subject of a test case, given the proponents' view of the "authorisation liability" principle in the Copyright Act was rejected in the High Court. The implicit assertion under the Code is that the account holder is subject to "authorisation liability" for any packets passing over their account. It is not clear that this would always be the case, or what it would be necessary for the account holder to do to discharge the obligation.

It is also well known that children are users of Internet, and could not reasonably be expected to understand the law and technical issues of copyright in Australia.[6]

It is arguable that other members of the household should reasonably be entitled to confidentiality in their internet use.

This Code has a strong potential to cause significant family stress with no access to advice or guidance on how to resolve the matter, and with limited technical capability to bring to bear on it.

Recommendations: **the Account holder should be able to challenge a notice on the basis that s/he is not responsible for the alleged conduct, and be given detailed technical guidance, and assistance if requested, at the expense of the rights holder, on how to resolve this issue, if that is possible.**

The common result that the Account holder will not be able to decisively identify the individual responsible must be accepted as an outcome. The onus must be on the accuser to establish the identity of the individual involved.

The reverse onus of proof, that the account holder must prove their innocence, should not be entrenched in the Code.

The *Privacy Act* and Privacy Impact Assessment

The Code clearly states that no personal information will be provided to a third party.

It is unclear whether the IP address or similar metadata is considered to be personal information. In the US, the definition of "PII" is much narrower than in Australia.

This does not mean the Code meets the requirements under the *Privacy Act*. It is noted that there is no report or comment publicly available from the Privacy Commissioner on this issue. There are

[5] See http://potaroo.net, August 2014 and May 2013 posts. Identification here requires the 30,000 samples per day per user, down to the millisecond level, envisaged by APNIC chief scientist Geoff Huston, and the capture of every destination server IP address as well as the client device IP. Query if this Code relies on implied access to the Metadata Retention honeypot being set up in the name of terror?

[6] Senior copyright lawyers have suggested to one of the authors that the incomprehensibility of the 2006 amendments to the *Copyright Act* to ordinary people is not a problem (they belatedly legalized certain Australian uses of iPods and PVRs, but not others, long after these were legal in the US). And the rights holders' apparent intention in this Code to disregard the unfavorable outcome of the *iiNet* case in the High Court also complicates how an ordinary person is supposed to understand the law: do they follow what the court says is the law (rendering this Code irrelevant), or what the industry says?

a number of issues with the Code that arise under the Australian Privacy Principles (APP) that have not been subject to any transparent and publicly available analysis.

APP 2 allows access to anonymity and pseudonymity. ISPs should now have processes in place for individuals to access anonymity and pseudonymity as there might be a demand for this given the proposed Code and the weakened approach to privacy of ISPs. The Code does not deal with this clear right.

APP 3.1 and 3.2 appear to be breached by the Code. The collection of information on websites visited is not reasonably necessary or in fact relevant to the role of the ISP. It is very likely that any discovery process by a copyright holder will seek to access the Internet records of the individual collected by the ISP.

It is not proposed to go through every APP here. However, the above analysis indicates that it is necessary for a full and open Privacy Impact Assessment to be performed before this Code can proceed, or be amended. The copyright holders need to pay for this assessment.

It should be conducted by an independent expert who is acceptable to a range of user and consumer interests, given the previous efforts to exclude these stakeholders from full engagement.

Recommendation: **the Code should not proceed until a comprehensive Privacy Impact Assessment is performed, by an independent expert acceptable to a range of user and consumer interests, involving proper consultation with affected stakeholders, and published**

Lack of adequate protections for individuals

The court system provides protections for individuals that require the plaintiff to discharge its burden of proof in civil cases.

The rights holders could commence litigation and use discovery processes to collect relevant information, if they can persuade a court of relevance and admissibility. They appear to prefer this Code scheme instead.

For the copyright holders to bypass the courts, apparently rely on obligations in contradiction to the outcome of *iiNet* in the High Court, and receive the benefit of this Code, the copyright holders must discharge a similar burden of proof.

The Code does not have sufficient detail about the audit process, the burden of proof and safeguards with error.

The audit systems do not appear to have any safeguards to ensure that accusations are not made when a "fair use" or fair dealing defence would usually be available. Nor does it adequately address the technical issues around identifiability, either under CGNAT or under home access points used by non-technically-trained individuals.

Section 3.3 needs to be rewritten to provide a positive obligation for the auditor to verify that the following requirements have been met:

- A process for establishing and verifying the technical information on which the notice is based, and identifying and resolving the fundamental problems of unreliable identification of users of devices
- A process for identifying fair use or fair dealing, and ensuring no notices are issued on that basis
- That a burden of proof has been developed and must be met and audited before any notification. The burden of proof needs to be developed and included in the Code

- The audit must be made public to ensure transparency
- Technical processes must be explained in sufficient detail to enable public scrutiny, or for the Account holder to seek conclusive further technical advice if they are uncertain as to the veracity of the claims
- The audit must ensure that any process does not include a process of breaching privacy in obtaining evidence

The Code also needs to make it explicit that Copyright holders have no access to metadata that an ISP may hold. This requirement is reflected in Recommendation 23 of the *Advisory Report on the Telecommunications (interception and Access) Amendment (Data Retention) Bill 2014* by the Parliamentary Joint Committee on Intelligence and Security.

Recommendations: **section 3.2 needs to be revised to ensure adequate protections for individuals including a transparent audit process, resolution of the unreliability of IP information for identifying individuals, accounting for fair use and fair dealing, respecting privacy, enabling review, and discharging a set burden of proof to avoid mistakes**

The Code should explicitly note that Copyright holders do not have access to metadata.

Procedural fairness

Procedural fairness is a key principle for our justice system in Australia. Procedural fairness must be a guiding principle for this Code. We contend that this Code does not meet the requirements of procedural fairness.

The first breach of procedural fairness is that the individual does not have the opportunity to dispute the first notice. If an individual believes the first notice is simply inaccurate, they should have the opportunity to dispute the notice immediately.

The individual should not have to wait for a third notice. This is simply unfair. It also wastes resources where there may have been an obvious mistake. The right to dispute an inaccurate assertion should never be delayed. This is an interference with access to justice. There is no doubt that the notices will be subject to discovery and the notices will be relied on as evidence.

Recommendation**: all notices are subject to challenge, including the first**

The second issue is that there does not seem to be an internal dispute resolution process available at all.

An individual must be able to engage with the ISP about the issue, and request information and documents about the full range of data and evidence held by the ISP (including information provided by the Copyright holder to the ISP). An individual must be able to see the full range evidence held against them, provided in a manner that facilitates them seeking further advice and assistance if necessary.

Recommendation: **the Code must require the availability of an IDR process including a specific section in the Code that gives the individual rights to request all relevant documents and information, including all information relied on by the rights holder, and all information or data from the ISP that could be relevant.**

Dispute resolution process

Many Codes affecting consumer use of the Internet in Australia defective in some respect (See Drowning in Codes, referred to above). We contend that the proposed dispute resolution process

under the Code does not meet the standards set out in *The Benchmarks for Industry based Customer Dispute Resolution Schemes* issued by the Government in 1997. The standards are available at **www.anzoa.com.au**.

ISPs are already part of a dispute resolution scheme that does meet these benchmarks being the Telecommunications Industry Ombudsman. It is completely unacceptable to set up a system that does not comply with the required standards and fails to use the system that is available.

The proposed Adjudication Panel has not been subject to any audit to ensure it meets the required standards. The detail in the Code is insufficient to verify compliance.

Charging for access interferes with access which is a clear standard. All approved dispute resolution schemes in Australia are free.

The copyright information panel does not include balanced representation of industry and consumers which again does not meet the required standards. There is a danger that panel members will be appointed who are sympathetic to rights holders or dependent on them (as is the case for many copyright litigators).

Recommendations: **the Telecommunications Industry Ombudsman must be the dispute resolution scheme used in the Code.**

Copyrights holders must pay the full costs of access to the scheme, and all ancillary costs of operation of this Code.

Any adjudication panel should be a mix of members nominated by rights holders and members nominated by consumer and Internet user stakeholders.

Copyright holders

This Code has been developed following demands by copyright holders. Copyright holders have always had access to court to enforce their rights. This Code significantly assists copyright holders in getting evidence for their case, and also in pressuring alleged responsible account holders to give in without independent external examination of claims by a court. It is appropriate that copyright holders pay for all the costs of this scheme including ISP costs, dispute resolution costs, auditing and a privacy impact assessment.

This is particularly appropriate in the current context, where the obvious alternatives suggested to rights holders, namely 'meeting the market' and providing all their available product on fair and non-discriminatory terms to Australians, had not been thoroughly pursued before this intrusive scheme developed in a non-consultative way. (There have been some minor, reluctant, piecemeal improvements, but not the dramatic industry-wide abandonment of the fundamental discriminations against Australian consumers over price, timing, back catalogue, sources, compatibility, monopolistic technological choices, range of options or refusal to supply that would be needed to drive a robust change in consumer perception and practices, and undermine the incentives to bypass the measures protecting the current discriminatory business models.)

In the interests of proportionality, if a party seeks to impose a privacy-intrusive scheme on others without pursuing all reasonable alternatives to support their interests, it is not reasonable to expect the others to pay for this voluntary choice.

Recommendation: **the copyright holders must pay for the costs related to this Code.**

Speculative invoicing

There is a real risk that the discovery information obtained by copyright holders will be used for speculative invoicing. This is an unfair process, and individuals should not be subject to this type of harassment.

Individuals should be able to access the TIO for dispute resolution if a speculative invoice is received to ensure that the claims are evidence based. Any invoices sent should include the details of how to dispute it.

***Recommendations*: The Code should specifically require an enforceable undertaking from all copyright holders or their agents participating in activities under the Code or using information from it that details appropriate conduct in enforcing their alleged rights against alleged infringers, or against others asserted to share the same IP address.**

This needs to be subject to further consultation. The absence of procedural protection against speculative or abusive tactics is a critical failure of the Code, and it alone should suffice to have the draft withdrawn prior to proper consultation.

Thank you for your consideration. If you have any questions please contact Katherine Lane on 0447620694.

Yours sincerely

Australian Privacy Foundation

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors and is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, SubCommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby AC CMG and The Hon Elizabeth Evatt AC, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90) http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-) http://www.privacy.org.au/Campaigns/Media/