Ad Standards Community Panel
PO Box 5110, Braddon ACT 2612
P (02) 6173 1500 | F (02) 6262 9833

AdStandards.com.au

Ad Standards Limited
ACN 084 452 666

Case Report

1. Case Number :	**0105-20**
2. Advertiser :	**Creative Content Australia**
3. Product :	**Community Awareness**
4. Type of Advertisement/Media :	**Internet - Social - Other**
5. Date of Determination	**25-Mar-2020**
6. DETERMINATION :	**Dismissed**

ISSUES RAISED

AANA Code of Ethics\2.6 Health and Safety

DESCRIPTION OF ADVERTISEMENT

This YouTube ad depicts a young man in a police interview room with a detective and a police officer.

The detective states, "So you were hacked, and they stole your passwords and private photos. Use one of those pirate sites did we? And you know that's illegal?"

The man responds, "Yeah but I'm the victim here."
The detective states, "The victim of your own crime."
The police officer asks, "All that for a free movie?"
And the detective states, "Sorry son, can't help you."
And the police office says, "Cos it wasn't free, was it? Cost him heaps."

The words, "Pirate sites expose you to hackers" appear on the screen, followed by "Piracy. You're exposed."

THE COMPLAINT
A sample of comments which the complainant/s made regarding this advertisement included the following:

This is in breach of point 2.6 of the AANA code of ethics, in that it depicts content contrary to prevailing community expectations of safety. If you are the victim of any

crime, including cybercrime due to lax cybersecurity behaviours, then you should report it to police and police will investigate that crime fairly and impartially. Discouraging people from reporting serious crimes if they believe they may themselves have committed a crime against a member of Creative Content Australia is contrary to prevailing community expectations of safety and undermines safety and suggests that police may be influenced by CCA to fail to investigate such cases.

THE ADVERTISER'S RESPONSE

Comments which the advertiser made in response to the complainant/s regarding this advertisement include the following:

I refer to your emails dated 12 and 13 March 2020 informing Creative Content Australia (CCA) about three complaints received in relation to CCA's 'Piracy. You're exposed' consumer campaign.

As requested, we have supplied a copy of the script, details of the CAD reference number and a digital copy of the campaign.

CCA takes its legal responsibilities under the AANA Advertiser Code of Ethics seriously and believes the campaign is at all times, in compliance with Section 2 of the Code.

RESPONSE TO THE AD STANDARDS COMPLAINTS
In your letter, you asked us to address all parts of Section 2 of the AANA Code of Ethics.

The complaints have been made under the following sections:
- *2.1 Discrimination or vilification*
- *2.6 Prevailing community standards on health and safety*

Our position is that none of the other parts of Section 2 are relevant to the Complaint. However, for completeness we provide the following comments:
- *2.2 Exploitive & Degrading Sexual Appeal - not applicable. There is no exploitive sexuality depicted in this commercial.*
- *2.3 Violence - not applicable. There is no violence or harm depicted within the TVC.*
- *2.4 Sex, Sexuality and nudity - not applicable. There is no sex or nudity depicted in the commercial.*
- *2.5 Language - not applicable. The commercial does not contain any offensive language.*

2.1 Discrimination or vilification
Discrimination – unfair or less favourable treatment.
Vilification – humiliates, intimidates, incites hatred, contempt or ridicule.

CCA is confident that the campaign does not unfairly discriminate against the young man who brings his cyber security concerns to the police. His complaint is not dismissed because he accessed copyright-infringing material from a pirate website. They are simply unable to assist him.
As evidenced in the European Union Intellectual Property Office report in 2019, there is little that can be done because "In many of these cases [customers targeted by phishing attempts or for disseminating malware on illegal digital content networks], the servers are located in different countries to those where the subscriptions are sold, making it particularly complicated for law enforcement authorities to detect the criminals behind them."

The complainant suggests that the police "refuse to take the report" and the "the loudest message in the campaign is that 'police will not help you'". The police do not "refuse" to help him. Detective Miller says "Sorry son, can't help you" – not "won't" help you. She empathises with his issue but there is, in reality, very little Australian authorities can do to take down these sites or to find the people behind their operation.

This is confirmed through a series of court cases where rightsholders obtained injunctions requiring Internet Service Providers to disable access to over 1,400 domains associated with online locations which had the primary purpose or effect of facilitating the infringement of copyright.

One prerequisite for obtaining such an injunction was that the location of these domains was outside of Australia. This condition was specifically added because creators (as well as users of these websites affected by malware) would have been able to rely on Australia's legislation – and if serious enough – the help of Australian law enforcement, for any online locations operating from within Australia. In our members' experience, it is incredibly rare and unusual to see infringement perpetrated from within Australia.

The EU IPO Report says that, "In many cases, increasingly sophisticated organised crime groups are behind the counterfeiting and piracy activities, illustrating the growing threat arising from this type of crime. Many of these organised crime groups are also involved in other criminal activities, including, in a limited number of cases, terrorism."

It is important to reiterate that, even though enforcement is exceptionally difficult, screen content piracy is a crime under the 1968 Copyright Act. This includes the illegal downloading and streaming of copyrighted screen content.

However, Jesse – the young pirate in the campaign – is not receiving unfair or less favourable treatment because of his online activity. It's the nature of that activity – operated by offshore criminals - which renders the police helpless. Nor does the campaign depict Jesse in a way which humiliates, intimidates, incites hatred, contempt or ridicules him.

Detective Rogers questions whether the "free movie" was worth the cost. While this may be interpreted as being chastening to the young pirate, the intention is to inform the public about the potential cost of piracy and raise a valid question about whether the loss of personal data is worth the saving of a few dollars – which is what it would have cost to view that content legally.

The second complainant argues that the campaign promotes an "adversarial relationship between police and victims by promoting a false narrative that authorities will not follow through on reports of legitimate criminal offending…". This is not the intent or effect of the campaign. The police, while stern, are not argumentative or antagonistic. They are direct and truthful when they say they cannot help him.

This campaign does not, as suggested, target "vulnerable" people. The campaign does not suggest or infer that all young men pirate, nor that all young men are likely to be exposed to cyber security breaches. Jesse, the onscreen pirate, is a young man because CCA research indicates that it is young men, aged 20-34, who are the most frequent and persistent content pirates and the campaign hopes they recognise their own behaviour when they see it.

CCA strongly believes that the public benefit of the campaign, in informing consumers about the existence of the cyber security risks associated with pirate sites, outweighs the minor embarrassment experienced by Jesse when his online activity is revealed.

2.6 Prevailing community standards on health and safety
All three complainants believe the campaign breaches 2.6 of the Code by "depicting content contrary to prevailing community expectations of safety". They suggest that the campaign discourages people from reporting crimes and suggest that "police may be influenced by CCA to fail to investigate such cases".

It is not possible or feasible for CCA to "influence" police investigations in any way. Copyright legislation enforcement is not a remit of CCA and the organisation, being purely educational, has absolutely no contact with police at any time.

The idea that police may be unable to assist victims who have been hacked after visiting pirate sites is factual. 2016 legislation allows the Federal Court to order Internet Service Providers (ISPs) to block websites found to be primarily engaged in facilitating access to copyright-infringing content. Of the 1,481 pirate-site domains blocked by the Court since the first case ruling in August 2017, ALL were operating offshore in jurisdictions beyond the reach of national courts, making it impossible for local law enforcement authorities to shut down the sites or detain the criminals behind it.

The need for the campaign is made more imperative by the ever-emerging proxy and mirror sites that emerge every time a pirate site is taken down or blocked.

One complainant suggests that CCA should have "[spelled] out exactly what piracy is, how it is an

offence, and what external risks you may be subjected to by using piracy sites specifically". This is not always feasible in a 30-second video that also aims to capture the attention of predominantly young males - the key demographic for this campaign. CCA research shows that they believe piracy is a victimless crime. The campaign needs to be both entertaining and attention-grabbing whilst also making a strong and compelling case about how they might in fact become a victim as a result of their online piracy behaviour.

The dedicated "Price of Piracy" website offers further evidence to back up the campaign messages and provides links to the research studies that underpin the campaign theme. The web address is present on all versions of the campaign – video, print, outdoor and website banners. All CCA research studies since 2010 are available on the Creative Content Australia website.
(https://www.creativecontentaustralia.org.au/research/2020)

The campaign aims to drive viewers to the website for more information by using the vehicle of what is an unlikely scenario.

We believe that a reasonable person would conclude CCA is not discouraging people to report cybercrime, but informing them that the jurisdiction of Australian enforcement authorities is limited when attempting to satisfactorily resolve these issues. We hope that consumers find this concerning and that they are prompted to seek further information about the campaign message.

We do not believe that the conclusion the complainants reached is a view likely to be shared by the wider community.

FINAL COMMENTS
While we respect the personal opinions of the complainants, CCA believes that the campaign is in full compliance with the AANA Code of Ethics, as well as real world community standards

CCA strongly believes the campaign does not discriminate against or vilify any person, does not depict material contrary to prevailing community standards on health and safety and therefore does not breach Sections 2.1 or 2.6 of the Code.

In light of the above, we request these complaints be dismissed.

Few products face the challenge of being unlawfully available, globally, to billions of consumers with an internet connection. In 2018 there were an estimated 5.4 billion downloads of pirated films and television shows and 21.4 billion visits to streaming piracy sites worldwide.
(Source: https://www.mediaplaynews.com/anti-piracy-group-adds-viacom-comcast/ (Citing USA Chamber of Commerce's Global Innovation Policy Center Research)

Despite the proliferation of legal content sites, these numbers are not reducing substantially year-on-year.

Online piracy of copyright content deprives rightsholders of their right to control the distribution of their
content, erodes the legitimate market for copyright content in the online space, hinders the development of new methods of delivering content to wider audiences at competitive rates by the film and television industry and causes significant financial losses to content creators.

For consumers, at best ignorant of these effects, at worst disdainful of them, it is becoming increasingly critical to encourage behavioural change by emphasising the personal consequences of their actions. These consequences are factual, valid and credible. This campaign brings them to the attention of online pirates and to the broader community whose friends or family are vulnerable to cybercrime due to their online activity.

We have been delighted with the support we have seen for this campaign, particularly from the creative industries – from writers, directors and producers, to cinema operators, television broadcasters, retail DVD stores and subscription service providers – whose livelihoods are most at risk from online piracy. While we are disappointed that complaints have arisen, we stand by the integrity of our message and the importance of disseminating this information to consumers.

BACKGROUND TO CREATIVE CONTENT AUSTRALIA
Creative Content Australia is a not-for-profit organisation committed to raising awareness about the value of screen content copyright and the impact of piracy on the creative industry. CCA's stakeholders – cinemas, film distributors, filmmakers, broadcasters and associated industry organisations – oppose the for-profit theft of copyrighted creative work which threatens Australian jobs and undermines business models.

CCA is fully funded by its stakeholders who represent the production, distribution and exhibition/broadcast sectors: the Australia New Zealand Screen Association (ANZSA), Australian Home Entertainment Distributors (AHEDA), Australian Directors Guild (ADG), Australian Independent Distributors Association (AIDA), Australian Writers' Guild (AWG), BBC Studios, Comscore, Deluxe, Foxtel, FetchTV, Independent Cinemas Association of Australia (ICA), the Media, Entertainment & Arts Alliance (MEAA), Motion Picture Association (MPA), Motion Picture Distributors Association of Australia (MPDAA) , National Association of Cinema Operators (NACO), Screen Producers Australia (SPA) and Screenrights.

To inform the debate about movie and TV theft, CCA commissions research that tracks the attitudes and behaviours of Australians aged 12-64 in regard to their access to screen content, both legal and illegal. With annual studies since 2008, our research data provides the most comprehensive picture of piracy available in Australia.

Using this research, CCA develops consumer campaigns which tap into the consumer consciousness, encouraging them to think about the consequences of piracy.

RESEARCH CONDUCTED BY CREATIVE CONTENT AUSTRALIA
CCA's 2019 research reveals that 21% of Australians aged 18+ continue to pirate movies and TV shows despite the increasing number of legally available content services and platforms.

Research respondents who admit to online piracy confirmed that they were experiencing increasing cyber security issues: with 62% of adults and 75% of persistent teen pirates experiencing cyber breaches after accessing pirated content. Those who pirate more frequently (persistent pirates) are significantly more likely to experience cyber issues than those who pirate less frequently (casual pirates).

INTERNATIONAL RESEARCH WHICH SUPPORTS CAMPAIGN
CCA's research data on cybersafety risks associated with pirate sites has been confirmed by a growing body of international consumer-group surveys, academic papers and peer-reviewed international studies – many exposing links between screen content piracy and criminal cyber activity.

A few relevant studies are outlined below.

2019: Intellectual Property Crime Threat Assessment 2019
https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_IP_Crime_Threat_Assessment_Report/2019_IP_Crime_Threat_Assessment_Report.pdf
Commissioned by the European Union Intellectual Property Office, this recent study concludes that one in four persons who stream illegally through a box or stick are affected by a virus or malware.
In many cases, increasingly sophisticated organised crime groups are behind the counterfeiting and piracy activities, illustrating the growing threat arising from this type of crime. Many of these organised crime groups are also involved in other criminal activities, including, in a limited number of cases, terrorism.
In many of these cases, the servers are located in different countries to those where the subscriptions are sold, making it particularly complicated for law enforcement authorities to detect the criminals behind them.

2019: Fishing in the Piracy Stream: How the Dark Web of Entertainment is Exposing Consumers to Harm
https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf
Digital Citizens Alliance investigation observed malware from the piracy apps stealing usernames and passwords, probing user networks and surreptitiously uploading data without consent. In North America, the 12 million active users of illicit devices (such as set top boxes and apps providing access to copyright-infringing content) have helped hackers bypass network security and offered a new avenue to exploit consumers.

2018: Identification and analysis of malware on selected suspected copyright-infringing websites

https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2018_Malware_Study/2018_Malware_Study_en.pdf
Installation of free programs to access copyright-infringing platforms is associated with malware and PUPs (potentially unwanted programs). These applications may compromise users' personal details and computer configuration. Through social engineering tricks, various kind of private data - such as payment card details, personally identifiable information and social media account credentials - may also be disclosed.

2018: Does Online Piracy make Computers Insecure? Evidence from Panel Data
https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/06/WEIS_2018_paper_57.pdf
In order to quantify the risk of piracy, researchers from Carnegie Mellon University observed the online activities of 253 people for a year. From actual user behavior in a real-world setting, after controlling for other activities, their unique dataset showed that visiting infringing sites is more likely to lead to malware on users' machines. It found strong evidence that doubling of the amount of time users spent on various infringing sites resulted in a 20% increase in malware count on their computers.

2015: Digital Bait: How Content Theft Site and Malware are Exploited by Cybercriminals to Hack into Internet Users' Computers and Personal Data
https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/digitalbait.pdf
After comparing a sample of approximately 800 infringing sites to a control group of 250 similarly situated non-infringing sites, the study found that:

- *1 out of every 3 infringing sites surveyed contained malware*
- *Visitors were 28 times more likely to get malware from an infringing site than on a similarly situated non-infringing site*
- *45% of the malware on the infringing sites surveyed was delivered passively - a process allowing visitors to the site to be infected without having to click a single link. These so-called drive-by downloads "infect users silently and can go completely undetected. 45% of malware payloads found on the sample sites downloaded invisibly in the background and did not require the user to do anything to confirm the download. Users did not need to download media or click on any pop-up advertisements to be infected by these attacks".*

2014: The 'Bogus Features' Lurking Behind Pirate Film and TV Sites
http://www.industrytrust.co.uk/press-releases/the-bogus-features-lurking-behind-pirate-film-and-tv-sites/
Incopro analysed thirty of the most frequently used infringing film/TV sites in the UK (based on Alexa Rankings) and found that 97% contained malware or credit card scams. Three in four visitors to the sites experienced problems with their device after visiting the sites. A second survey by ICM of 4,210 users in the UK aged 16+ found that offenders encountered the following problems after accessing content from infringing sites:

- *Viruses: 1 in 3 downloaded a virus on to their device.*

- *Malware: 28% downloaded malware on their device.*
- *Stolen data: Almost 1 in 5 lost personal data or had personal information stolen.*
- *Illicit material: 14% were exposed to material such as pornography or violent images.*

CCA CONSUMER CAMPAIGN 2020

The objective of the 2020 campaign is to credibly highlight the potential consequences of accessing movies and TV shows from pirate sites and to demonstrate that the risks associated with those sites are not worth it. CCA research shows that pirates are more likely to change their behaviour if they are confronted with a negative personal consequence of their actions, hence the focus of the campaign.

The campaign is a dramatisation of the young man's visit to the police station. It has been written and executed to dramatise the hopelessness of the situation the young man finds himself in. It has been written and produced to create a sense of unease in the hope that viewers will think twice about visiting sites that host copyright-infringing content.

Unsurprisingly, and as the evidence compiled above confirms, illegal pirate sites have long been associated with malware and cybercrime. The piracy ecosystem is built on making money from stolen screen content. Often uninformed of the risks, users of these sites are baited into trying something they think is free or cheap but comes with a hidden cost: fraud, viruses, loss of personal data and exposure to potentially unwanted programs or unsavoury online activity such as gambling and pornography.

Following a global campaign (https://tagtoday.net) in 2015 to help advertisers and their agencies keep their ads off websites that promoted or distributed counterfeit goods or pirated content, pirate site operators are increasingly reliant on advertising income from "dark web" activities, including gambling, pornography, drugs etc. To compensate for the loss of legitimate advertising revenue, many pirate sites sell user data to criminal enterprises or are paid to include links with the potential to infect users' computers with viruses and other malware, so that cyber criminals can gain access to the user's data. These downloads earn pirate site owners millions in annual revenue.
(Source: https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/goodstillbad.pdf)

Because these pirate sites operate beyond Australia's borders, the Australian Government and law enforcement can do little to influence the content on these websites. The CCA campaign is the creative industry's attempt to alert consumers to the dangers these sites pose to their cyber security.

Screen content piracy is a crime. Copyright offences include the illegal distribution "by way of communication" (which includes online downloading and streaming), manufacture or selling of copyrighted screen content all of which are a crime under

the 1968 Copyright Act. Copyright holders also have civil and/or criminal remedies against copyright infringement.

The majority of Australians agree that piracy is stealing/theft, as indicated in CCA's annual research study, making this clearly a "community standard".

CAMPAIGN PRODUCTION AND DISTRIBUTION
CCA's consumer campaigns are usually made using the goodwill of our members, stakeholders and industry professionals and organisations. Production costs are provided at exceptionally low or no-cost with crew, actors and post production facilities donating their time and facilities to facilitate this critical message.

The 2020 campaign was written by CCA, together with director Curtis Hill from GoodOil Films (http://goodoilfilms.com/). Curtis has directed two of CCA's previous campaigns:

- *2017: The Price of Piracy https://vimeo.com/219052229*
- *2018: Say No to Piracy https://vimeo.com/256002627*

We are fortunate to have access to the free services of OMD (https://www.omd.com/) who assist us with our media placements. Support for the campaign is generally requested directly by CCA board members leveraging their relationships with media outlets.

The campaign launched on Monday 24 February. CCA's members and associated media organisations, screen the campaign pro bono in cinemas, on Foxtel and FTA television and promote the message via the major news outlets – both in print and online.

A small budget is applied to the digital campaign utilising Search Engine Marketing, Youtube and Fandom and many industry associations and companies use their social media platforms to promote the campaign – which resulted in the screening on Facebook that prompted one of the complaints.

PROFESSIONAL CYBER SECURITY CONSULTANTS
CCA consulted with Bastien Treptel of Bastien Treptel, CEO of the CTRL Group, an information security expert. Mr Treptel was provided with numerous research reports and undertook his own research and testing of the basic premises of the campaign before agreeing to act as an advisor and spokesperson.

THE DETERMINATION

The Ad Standards Community Panel (Panel) considered whether this advertisement breaches Section 2 of the AANA Code of Ethics (the Code).

The Panel noted the complainant's concern that the advertisement may discourage people from reporting crimes to the police.

The Panel viewed the advertisement and noted the advertiser's response.

The Panel considered whether the advertisement complied with Section 2.1 of the Code which requires that 'advertisements shall not portray or depict material in a way which discriminates against or vilifies a person or section of the community on account of race, ethnicity, nationality, gender, age, sexual preference, religion, disability, mental illness or political belief.'

The Panel noted the Practice Note to Section 2.1 provides the following definitions:

"Discrimination – unfair or less favourable treatment.

Vilification – humiliates, intimidates, incites hatred, contempt or ridicule."

The Panel considered that the man shown to be reporting the crime is a young male.

The Panel noted the advertiser's response that the man in the advertisement is not seen receiving unfair or less favourable treatment because of his age, rather the nature of the activity he has undertaken has resulted in him being in a situation where police are unable to help.

The Panel considered that the age of the young man is not mentioned in the advertisement. The Panel considered that the comments made by the police are in reference to the man's actions, and are not a result of his age or gender. The Panel considered that the young man in the advertisement is not seen to receive unfair or less favourable treatment because of his age, and that he is not treated in a way which humiliates, intimidates, incites hatred, contempt or ridicule of the man because of his age.

The Panel considered that the advertisement did not portray or depict material in a way which discriminates against or vilifies a person or section of the community on account of their age and determined that the advertisement did not breach Section 2.1 of the Code

The Panel considered whether the advertisement complied with Section 2.6 of the Code. Section 2.6 of the Code states: "Advertising or Marketing Communications shall not depict material contrary to Prevailing Community Standards on health and safety".

The Panel noted the complainant's concern that the advertisement may discourage people from reporting crimes to the police.

The Panel noted the advertiser's response that the advertisement is based on the fact which shows that it is impossible for local law enforcement agencies to detain criminals behind websites operated off-shore and that therefore downloading

material through illegal channels makes you vulnerable to these criminals and leaves you without any way to have your cyber security protected or compensated.

A minority of the Panel considered that the advertisement does imply that the price of undertaking illegal activity is that you deserve to be a victim of a crime. The minority of the Panel considered that the advertisement treats the man in the advertisement as a criminal rather than a victim, and that the dismissive and unhelpful attitude of the police officers did lead to a suggestioncccc that people should not report crimes. A minority of the Panel considered that identity theft is a serious matter that should be reported to police, and that most members of the community would expect Police to treat the matter as serious and in need of investigation. A minority of the Panel consider that the attitude of the police in this advertisement may have the effect of discouraging people to report crimes of this nature, which would be contrary to prevailing community standards on victim safety.

The majority of the Panel considered that the police in the advertisement say that they 'can't help' rather than that they won't help, and that this is an indication they have little power to resolve cyber crimes . The majority of the Panel considered the purpose of the advertisement was to highlight the risks of accessing pirated material and that the police won't be able to prevent your personal information from being stolen, and may not be able to prosecute the criminals if it is. The majority of the Panel considered that most members of the community would understand this advertisement to be a warning to avoid pirating material, rather than a suggestion that crimes should not be reported to the police.

The majority of the Panel considered that the advertisement did not contain material which would be contrary to Prevailing Community Standards on health and safety.

The Panel determined that the advertisement did not breach Section 2.6 of the Code.

Finding that the advertisement did not breach any other section of the Code the Panel dismissed the complaint.