s47F

From: s47F
Sent: Wednesday, 10 October 2012 11:08 am
To s47F

s47F

Subject: Social media and the law working group

Dear All

I am seeking nominations from your jurisdiction for the social media and the law working group to be led by Victoria. We are seeking one nomination from the Attorneys-General portfolio and one nomination from the law enforcement side. We are looking at more senior level representation where nominees have authority to make decisions (for instance, director level). It is envisaged that most meetings of the working group will take place via teleconference.

Could you pls send details of your nominees to me (with a copy to Tilda Hum and Allison will) by **COB next Monday, 15 October.**

Thanks

s47F

Assistant Director
Civil Law Policy
Department of Justice

Phone s47F
Mobile
Email s47F

Help conserve resources by not printing this email.
PRIVATE & CONFIDENTIAL
The content of this e-mail and any attachments may be private and confidential, intended only for use of the individual or entity named. If you are not the intended recipient of this message you must not read, forward print, copy, disclose, use or store in any way the information this e-mail or any attachment contains.
If you are not the intended recipient, please notify the sender immediately and delete or destroy all copies of this e-mail and any attachments.
Our organisation respects the privacy of individuals. For a copy of our privacy policy please go to our website or contact us..

If you have received this transmission in error please notify us immediately by return e-mail and delete all copies. If this e-mail or any attachments have been sent to you in error, that error does not constitute waiver of any confidentiality, privilege or copyright in respect of information in the e-mail or attachments.

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

****

WARNING

This email message and any attached files may contain information that is confidential and subject of legal privilege intended only for use by the individual or entity to whom they are addressed. If you are not the intended recipient or the person responsible for delivering the message to the intended recipient be advised that you have received this message in error and that any use, copying, circulation, forwarding, printing or publication of this message or attached files is strictly forbidden, as is the disclosure of the information contained therein. If you have received this message in error, please notify the sender immediately and delete it from your inbox.

AFP Web site: http://www.afp.gov.au
****

If you have received this transmission in error please notify us immediately by return e-mail and delete all copies. If this e-mail or any attachments have been sent to you in error, that error does not constitute waiver of any confidentiality, privilege or copyright in respect of information in the e-mail or attachments.

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

Communiqué
Standing Council on Law and Justice
5 October 2012

The second meeting of the Standing Council on Law and Justice (**SCLJ**) for 2012 was held on 5 October 2012 in Brisbane, Queensland. The Queensland Attorney-General chaired the meeting. The Commonwealth, State and Territory Attorneys-General (excluding the ACT and Tasmania), the Commonwealth Minister for Home Affairs and Justice, the Queensland Minister for Police and Community Safety and the New Zealand Minister of Justice were in attendance. The ACT Government was in caretaker mode, and was represented by the Director-General of the Justice and Community Safety Directorate. The Tasmanian Attorney-General was represented by the Secretary of the Department of Justice.

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

Summary of Decisions

Interface between the Federal Family Courts and the State and Territory Child Welfare Authorities

Ministers noted the considerable work that the Commonwealth, States and Territories are undertaking to improve collaboration between the federal family courts and child welfare authorities.

Update on Australian Law Reform Commission National Classification Scheme Review

Ministers noted the recommendations made by the Australian Law Reform Commission in its Final Report on the Review of the National Classification Scheme and agreed officials would report back following further work on a number of recommendations to enable decisions to be made by Ministers about priority areas for reform at the next SCLJ meeting in April 2013.

Unexplained Wealth

Ministers agreed that the Senior Officers Group on Organised Crime will develop measures to improve asset confiscation laws and the identification and pursuit of unexplained wealth.

People Smuggling Offences

Ministers noted moves by the Commonwealth to implement the Expert Panel on Asylum Seekers Report recommendations on people smuggling crew issues, including the Attorney-General's direction to the Commonwealth Director of Public Prosecutions not to prosecute first time offenders, and lower culpability crew with an aggravated people smuggling offence involving mandatory minimum penalties.

Synthetic Drugs

Ministers noted that the Intergovernmental Committee on Drugs is overseeing work on emerging psychoactive and synthetic drugs.

Cyberbullying and Trolling

Ministers considered existing Commonwealth, State and Territory offences to deal with cyberbullying and agreed that they provide appropriate coverage but requested officers continue to monitor the adequacy of those laws. Ministers noted that existing protocols operate on the principle that state and territory police investigate cybercrimes against the person, which would include cases of cyberbullying amounting to criminal conduct.

Ministers noted the importance of cooperation with social media operators, and in particular noted recent progress in negotiations with Twitter. Further discussions will continue between governments, law enforcement agencies and social media operators.

Ministers also noted the progress of Australia's accession to the Council of Europe Cybercrime Convention following enactment of the *Cybercrime Legislation Amendment Act 2012* (Cth) in September 2012. Accession to the Convention will facilitate international cooperation in the investigation of cybercrime offences.

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

FOI - 39

The Commonwealth Attorney-General will also continue to develop, through the Quintet of Attorneys General and other fora, options to improve cooperation between law enforcement agencies and online social media providers.

Ministers noted the importance of education for Australians about ways to prevent and address cyberbullying.

Facebook and Privacy

Ministers requested that officers continue to monitor legislative developments in other jurisdictions to allow parents to access and edit the content of children's social networking accounts and report back to the SCLJ in the event legislative reforms are introduced on this issue either in domestic or international jurisdictions.

Social Media and the Law

Ministers noted the potential for social media to jeopardise the right to a fair trial, and in particular to compromise a jury trial and agreed to seek a coordinated national approach.

Ministers agreed that the issue be further considered by a working group of the SCLJ, chaired by Victoria, to provide recommendations to SCLJ following consultation with representatives of social media organisations, news media organisations, justice officials, law enforcements authorities and the courts. Recommendations are to be made on:

- model guidelines and warnings regarding prejudicial material for social media organisations;
- protocols between social media organisations, law enforcement agencies and courts for the removal of prejudicial material from content posted on social media; including opportunities to improve existing protocols;
- procedures for law enforcement agencies and courts to use social media to give warnings to or serve notices on social media users regarding prejudicial material;
- model jury directions that may be used when material that might be prejudicial has been in the public domain;

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

- legislative provisions relating to the conduct of juries, jury directions and offences, including prohibitions against jurors seeking information from extrinsic sources; and
- possible further empirical research about the effect on jurors of information from sources extrinsic to a trial.

National Legal Profession Reform

New South Wales and Victoria are continuing negotiations on this reform project.

National Online Reporting Facility for Cybercrime

Ministers endorsed the Business Case for the proposed Australian Cybercrime Online Reporting Network and gave in-principle agreement to proceed with the implementation of the facility, subject to consideration by the Standing Council on Police and Emergency Management.

Cross-Border Justice Scheme

Ministers discussed issues raised with the Commonwealth Government by the National Aboriginal and Torres Strait Islander Services about the operation of the Cross-Border Justice Scheme in Australia's central desert region. Ministers noted these issues had been considered by relevant jurisdictions, through the Cross-Border Justice Project Executive Group.

National Approach to Governments' Response to Senate Committee Report on Forced Adoptions

Ministers discussed the two recommendations of the Senate Committee Report on former forced adoption practices and policies that are about matters that fall under their portfolio responsibility.

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

Standing Council on Law and Justice Communiqué
Summary of Out of Session Decisions

Senate Committee Inquiry into the National Classification Scheme

Recommendations 8 and 21 of the Senate Legal and Constitutional Affairs Committee Report Review of the National Classification Scheme: Achieving the Right Balance were raised for Ministers' consideration.

Uniform Evidence Reform Tendency and Coincidence

Ministers requested that the Evidence Working Group consider issues regarding the operation of the tendency and coincidence provisions of the Model Uniform Evidence Bill and report back to Ministers.

SCLJ Annual Report

Ministers agreed to publicly release the SCLJ Annual Report for the 2011-2012 financial year.

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

Ellery, Jacqueline

From: s47F
Sent: Friday, 12 October 2012 9:22 AM
To: Ellery, Jacqueline
Subject: FW: Social Networking Sites (SNS) response to cyber safety and security issues [SEC=UNCLASSIFIED]
Attachments: Cooperative Arrangement for Complaints Handling on Social Network Sites + SNS Self Declarations.pdf; SNS response to cyber safety and security threats (table).docx

UNCLASSIFIED

Hi Jackie

As discussed. It appears Neil got this, but for your info, here it is. Let me know if you have any comments next week, and I can send through.

Cheers

s47F

s47F
Criminal Law Reform Section
Criminal Law & Law Enforcement Branch
Attorney-General's Department
2 - 4 National Circuit | Barton ACT 2600
T: s47F | W: www.ag.gov.au

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

From: s47F
Sent: Wednesday, 10 October 2012 4:19 PM
To:
Cc: s47F
Subject: FW: Social Networking Sites (SNS) response to cyber safety and security issues [SEC=UNCLASSIFIED]

UNCLASSIFIED

Colleagues

Further to our burgeoning collaboration on social media and law, attached and below is work from DBCDE that seems to engage with many of our social media issues.

I haven't read it closely enough to assess who is the logical area to lead on this – possibly TSLB or CrimJD given it comes out of cybersafety WG. Let me know what you think. In the mean time, I propose that each of the 4 branches consider their comments/ input – they want AGD advice by 19 Oct.

As discussed with Sarah and Catherine, on the SCLJ WG I'm happy to be the lead for the time being and we'll see how it evolves – seems to involve substantive issues for AJD, CrimJD & TSLB.

s47F

From: Rizvi, Abul [mailto:Abul.Rizvi@dbcde.gov.au]
Sent: Wednesday, 10 October 2012 3:58 pm
To: s47F
s47F
Cc: s47F
Subject: Social Networking Sites (SNS) response to cyber safety and security issues [SEC=UNCLASSIFIED]

Dear Colleagues

Further to the development of the protocol for the *Cooperative Arrangement for Complaints Handling on Social Networking Sites* through the Consultative Working Group on Cybersafety (attached for your information), the Department is now seeking to engage popular SNS to pin down with greater specificity how they will deal with a range of specific circumstances and how they will cooperate with relevant agencies.

As the next step in engaging with SNS, a draft table has been developed which provides an outline of some of the more serious issues which arise on their services and the different stages in the potential escalation of these issues. I would be grateful for your advice on whether this table adequately covers the range of serious circumstances and the escalation stages by Friday, 19 October. Once the table is agreed amongst relevant Commonwealth agencies, we propose to provide this table to popular SNS as the basis of a further discussion with them. I acknowledge that in some of the circumstances raised an SNS may say that it is dependent on the facts of the particular case but even still it would be worth testing (and seeing if a more detailed response could be later developed).

I note that a wide range of government agencies would have an interest in the issues raised in the table. I therefore propose that we meet at 10.30 am on Wednesday, 31 October at DBCDE Offices, 38 Sydney Avenue, Forrest to discuss this initiative and any comments you may have on the table before engaging with popular SNS. Also, if there is any other Commonwealth agency which you think should be included in these discussions can you please advise.

Regards

Abul

Abul Rizvi
Deputy Secretary
Phone +61 2 6271 7022 | Fax +61 2 6271 1515

Department of Broadband, Communications and the Digital Economy
38 Sydney Avenue, Forrest ACT 2603 | GPO Box 2154, Canberra ACT 2601

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

NOTICE: This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

This message has been content scanned by the Axway MailGate.
MailGate uses policy enforcement to scan for known viruses, spam, undesirable content and malicious code.
For more information on Axway products please visit www.axway.com.

If you have received this transmission in error please notify us immediately by return e-mail and delete all copies. If this e-mail or any attachments have been sent to you in error, that error does not constitute waiver of any confidentiality, privilege or copyright in respect of information in the e-mail or attachments.

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

SNS response to cyber safety and security threats

	Complaint by user to SNS	Issue raised in mainstream media	Government agencies (non-enforcement) raise with SNS	Law enforcement or regulator makes an informal request	Law enforcement or regulator makes a formal request	Court/ Tribunal decision
Serious threat of death or physical harm to person or damage to property (e.g. incitement to commit crime)						
Menacing or harassing content (e.g. trolls encourage victim to commit suicide)						
Privacy infringement (e.g. posting of topless photographs of the Duchess of Cambridge)						
Content prejudicial to a court proceeding (e.g. comments on the accused of a prominent criminal trial)						
Vilification (e.g. based on race, age, sex, sexual preference)						
Defamatory content						
Child pornography						
Other Offensive content likely to be rated refused classification of X18+						
False or misleading content (e.g. commercial information)						
Scams/phishing/fraud						

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

FOI - 46

Cooperative Arrangement for Complaints Handling on Social Networking Sites

SNS
Self Declarations from Facebook, YouTube, Microsoft and Yahoo!7

FREEDOM OF INFORMATION ACT 1982

Table of Contents

1 **Cooperative Arrangement for Complaints Handling on Social Networking Sites** 2

2 Background 3

3 Cooperative Arrangement Principles 4

4 Participating Social Networking Sites 5

5 Appendix 6

6 **SNS Self Declarations** 7

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

Cooperative Arrangement for Complaints Handling on Social Networking Sites

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

Background

Australia has a healthy and promising digital economy which is set to provide further growth and opportunity. In taking advantage of this opportunity, it is important that all Australians are equipped and empowered to be capable digital citizens.

Being a capable digital citizen is about having the necessary skills to be smart, safe and responsible online. Capable digital citizens have the skills and knowledge to take advantage of the opportunities of the online world while minimising the risks that can arise. Digital citizenship is also about being a positive contributor to online communities. For example, constructively sharing views, creating and rating content, commenting on articles and reporting content that may be inappropriate. These active modes of participation are to be preserved and encouraged.

Promoting digital citizenship requires a collaborative effort - it is a shared responsibility and we all have a role to play. There are a wide range of stakeholders including young people, parents, teachers, online service providers, the private sector, governments and non-governmental organisations. The most effective approach is for stakeholders to consult and collaborate.

The providers of Social Networking Sites (SNS) or services with SNS-like functionality, listed at the end of this document share a common goal to support and empower all Australians to be good digital citizens. In pursuit of this goal, they are recording here a cooperative arrangement for complaints handling on SNS that builds on existing cooperative processes. This arrangement is voluntary and non-binding. SNS recognise that a complaints handling system which is tangible, helps to build the confidence of users and promote good digital citizenship.

Implementation of this cooperative arrangement is to reflect the nature of each particular SNS and is to be assessed by each provider independently. This cooperative arrangement is intended to support the SNS' existing policies and processes, reflect understanding of how each SNS operates and provide for flexibility, noting the need to avoid a prescriptive approach.

This cooperative arrangement is not to impact on any law enforcement or Attorney-General's Department arrangements with the providers.

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

Principles

Policies for acceptable use

1. These providers will have in place policies for acceptable use, which may be referred to by terms such as community guidelines, terms of use, codes of conduct or similar. They will provide clear information about what constitutes inappropriate behaviour on the site. This information should be easily accessible and include information about the consequences of breaching the acceptable use policy.

Complaints mechanisms

2. These providers will have mechanisms for reporting inappropriate content, contact or behaviour as outlined in their policies for acceptable use. Providers will enable users to have access to information they need to make an effective report and, where appropriate, an indication of how reports are typically handled.

Review processes

3. These providers will have a process for reviewing and acting on complaints promptly, as appropriate in the circumstances. This process should be adapted to the scale at which the SNS operates. The providers will build systems and provide trained staff to assess issues on a case by case basis in accordance with the providers' policies. A user's non-compliance with policies for acceptable use may have consequences including removal of content, suspension or closure of their account. Sanctions for a breach of a provider's policies will in all cases be determined by the provider.

Child abuse material

4. These providers will remove child abuse material in accordance with the providers' child abuse policies as soon as they are made aware of it. Upon receipt of notification of alleged child abuse material, they will implement effective processes to expeditiously review that material and take such other actions as appropriate. They will continue to make referrals of this material to the appropriate authorities, including to law enforcement.

Identified contact person

5. These providers will have a contact person(s) with whom the Australian Government can discuss issues and any appropriate messaging to the community and media in response to issues as they arise. This is particularly important where an issue is of public interest and as such, requires prompt attention.

Education and awareness raising

6. These providers will encourage their users to understand the functionality on the site, including reporting tools. They will provide clear guidance designed to give people the tools, knowledge and skills to navigate their services safely.

7. These providers will take steps to help users be aware of the importance of being smart, safe and responsible online.

Collaboration with Government on education and awareness raising initiatives

8. These providers will contribute to, support and collaborate with the Australian Government, as appropriate, on relevant cybersafety initiatives.

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

Continued innovation

9. These providers will innovate to provide useful services that promote user safety.

Transparency

10. These providers will each provide information on how they give effect to this cooperative arrangement (see appendix).

11. These providers will meet with government officials on a bilateral basis every six months to discuss trends and emerging issues.

12. These providers will provide the Consultative Working Group on Cybersafety with information on trends and emerging issues every twelve months.

Participating SNS (as at 30 July 2012)

- Facebook
- Google (YouTube)
- Microsoft
- Yahoo

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

FOI - 52

Cooperative Arrangement for Complaints Handling on Social Networking Sites

Appendix
[SNS name]

In the interests of transparency, providers supporting the Cooperative Arrangement for Complaints Handling on Social Networking Sites agree to provide information on how they give effect to the Principles in relation to the social networking services they offer, using this form.

1. About the Social Networking Service(s)

   [Brief outline of the social networking services offered]

2. How will the provider give effect to the complaints handling aspect of the Cooperative Arrangement?

3. Other actions taken on implementation of these arrangements

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

FOI - 53

Social Networking Sites Self Declarations

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

Cooperative arrangement for complaints handling on social networking sites

Facebook

In the interests of transparency, providers supporting the Cooperative Arrangement for Complaints Handling on Social Networking Sites agree to provide information on how they give effect to the Principles in relation to the social networking services they offer, using this form.

1. About the Social Networking Service(s)

At Facebook, we have built a global communications platform embraced by hundreds of millions of people because we give them the power to share and connect, in the ways that they want, with the audiences that they want. People from around the world use Facebook to exchange photos, spread up-to-the-minute news, participate in the democratic process, and create and mobilize communities.

Facebook has also become an engine of economic growth and job creation: a recent study found that Facebook added more than €15 billion in value to the European Union in 2011, supporting more than 230,000 jobs.[1] In the U.S., a similar study found that applications built on Facebook's platform have contributed at least 182,744 new jobs and over $12.9 billion wages.[2] Like their overseas counterparts, Australian entrepreneurs and innovators have also built and expanded their businesses via Facebook. For example, the Australian fashion entrepreneur – MIISKA – built a sustainable business entirely on Facebook, attracting 1,000 unique buyers in the first 6 months and enjoying 100% of revenue being driven exclusively from Facebook.[3]

Nothing is more important to Facebook than keeping people safe. Facebook's mission is to make the world more open and connected. Our commitment to online safety enables us to fulfil that mission. If the experiences people have on Facebook are not positive, then the site will no longer be useful for them to connect and share and we will no longer fulfil our mission.

To support these and many more positive experiences on the site, Facebook promotes safety and security through a combination of policies, tools and awareness-raising initiatives.

One of Facebook's most important safeguards is our real name culture. We always have believed that people online are more likely to adhere to community rules and less likely to engage in negative, dangerous, or criminal behaviour when their real-world friends and families surround them. A culture of authentic identity also makes our service less attractive to predators and other bad actors who rarely use their real names and email addresses when engaging in nefarious activity. To protect this real name culture, creating an account using a fake name is a violation of our policies and is grounds for closing an account. We have tools to detect fake accounts; and we block the registration of accounts under common fake names.

Our real name culture supports and enables the special protections for minors that we have in place to help keep minors safe on our site.[4] Hence our Facebook Safety Center advises teens: *Help us keep the community safe by reporting fake profiles to Facebook if you ever see them.*

We receive tens of thousands of complaints each day from users complaining about inauthentic accounts and we remove those of which we become aware. We also have automated systems to detect obvious behaviours that are inauthentic, like sending a large number of friend requests

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER FREEDOM OF INFORMATION ACT 1982

or messages over a short space of time. In our experience, fake accounts are more likely to be associated with other harmful activity such as prohibited graphic content, spam, harassment and child predation.

The benefit of our real name culture for improved communications is borne out by the experience of media sites that have incorporated Facebook comments. They have seen the tone of comments improve, specifically: *"Trolls don't like their friends to know that they're trolls," explained Jimmy Orr, online managing editor of the Los Angeles Times. "By using Facebook, it has made a difference."* ***[5]***

In addition, in their recent Audit of Facebook Ireland, the entity with whom Australian users contract, the Irish Data Protection Commissioner confirmed Facebook's real name culture was a tool to promote child protection and online safety on the site.[6]

2. How will the company give effect to the complaints handling aspect of the Cooperative Arrangement?

Policies for acceptable use
Everyone who uses Facebook agrees to our Statement of Rights and Responsibility: https://www.facebook.com/terms.php at the time they sign up for the service. This prohibits the posting of content that is harmful, including hate speech, bullying and harassment. For a detailed explanation of what is and is not permitted, you can review our Community Standards: https://www.facebook.com/communitystandards

Complaints mechanisms
Our reporting infrastructure leverages the collective experience of the more than 900 million people on Facebook to keep an eye out for harmful or potentially dangerous content. We make it easy to report harmful or harassing content with "report" links on nearly every page on Facebook. More information about how to report content on Facebook is available here: https://www.facebook.com/report/

Facebook's reporting infrastructure was recently examined as part of the audit conducted by the Irish Data Protection Commissioner (DPC) of Facebook Ireland, the company with whom Facebook users in Australia contract when agreeing to the terms of use on the site.

As the Irish DPC explained about our reporting infrastructure:
"Facebook provides its users with a variety of ways to report abuses on the site. Users can go to the Help Centre and find pages of information about abuses to report. [Facebook Ireland] also has contextual reporting buttons on every page and associated with every piece of content. On every profile, there is a report link; on every photo there is a report link; and on every advertisement there is a way to report it. There is a means to report abuses included on every profile, photo and advertisement." ***[7]***

The Irish DPA concluded:
"We examined the accessibility of options available to a user who wishes to report an issue to Facebook. It is considered that it is straight-forward for a user to locate the 'Report Abuse' options via the 'help' drop down option on the user profile page and within 2 mouse clicks is within the 'Report Abuse or Policy Violations' of the Help Centre'." ***[8]***

And further:

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

"We are satisfied that [Facebook Ireland Ltd] has appropriate and accessible means in place for users and non-uses to report abuse on the site. We are also satisfied from our examination of the User Operations area that [Facebook Ireland Ltd] is committed to ensuring it meets its obligations in this respect." ***[9]***

Review processes
Our review process includes systems to prioritize the most serious reports and a trained team of reviewers who respond to reports and escalate them to law enforcement as needed. On a weekly basis, Facebook's internal safety teams review hundreds of thousands of reports globally through both manual and automated means. When people report content, we are quick to respond.

Child abuse material
We have a zero tolerance policy regarding child exploitative material on our platform and employ innovative and industry leading measures to prevent its dissemination. For example, in collaboration with Microsoft and the National Center for Missing and Exploited Children ("NCMEC") in the US, we also utilize a technology called PhotoDNA. PhotoDNA allows us to automatically identify, remove and report known abusive images to NCMEC, which coordinates with law enforcement authorities around the world for potential prosecution.

Identified contact person
Facebook has a confirmed contact person with whom the Australian Government can discuss issues and any appropriate messaging to the community and media in response to issues as they arise. This includes issues of public interest and similar issues that require prompt attention. It also allows Facebook to ensure that the Australian Government continues to receive up-to-date information about Facebook features, policies and initiatives.

Education and awareness raising
We provide educational materials through our Family Safety Center and blog that specifically address bullying prevention, and we have partnered with other organizations to educate young people about the responsibilities of digital citizenship and the dangers of abuse online. Our Family Safety Center provides detailed and helpful advice to help support parents and teachers in these conversations.[10]

We also maintain the Facebook Safety Page. Over 820,000 people have "Liked" our Safety Page,[11] which allows them to receive the latest in safety education directly in their Facebook News Feeds. We regularly post information, tips, articles, features, and dialogues about digital citizenship, as well as links to useful content from third-party experts. For example, earlier this year we posted an interview with Rosalie O'Neale, who works on the CyberSmart initiative run by the Australian Communications and Media Authority (ACMA).[12]

We believe online safety is a shared responsibility, which is why we partner with organisations globally to create the most robust and effective safety environment possible. We regularly engage with safety experts and non-profits that work to promote online safety to support their initiatives and to ensure that they have relevant information about Facebook's tools and policies to empower them in their own community engagement.

Facebook regularly engages directly with parents, teachers, and teens around the country. We have developed a program to do safety demonstrations for these audiences, as well as

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

members of government. Most recently we presented about Facebook, education and safety as part of the Queensland Catholic Education Commission's Student Protection In-Service Day.

Collaboration with Government on education and awareness raising initiatives
We are proud of our participation in various government initiatives to promote safety and privacy online. For example, we are a member of the Australian Government's Consultative Working Group to improve online safety. We also partnered in National Consumer Fraud Awareness Week for 2012, in Privacy Awareness Week for 2012 and in National Cybersafety Awareness Week 2012 – all initiatives organised by Australian government agencies -- by posting security and privacy tips to the Facebook Australia Page and by participating in various awareness-raising events held as part of these initiatives.

Continued innovation
Facebook continually innovates to improve our ability to create a space that empowers people to engage via the platform. Most recently, we have rolled out the following new safety features and initiatives:

- **Social Reporting:** Facebook believes in offering teens many options to manage their reputations, and to seek help should they ever encounter abuse on the site. A new tool we have pioneered called "Social Reporting" allows minors to directly notify others of content they want removed from Facebook, such as an unflattering or embarrassing photo posted by a friend. In cases where teens may feel threatened by posted content, the Social Reporting feature gives them the option to report the content to Facebook, to send a copy of the content to a trusted adult, or to block the person who posted it. More information about social reporting is included here: https://www.facebook.com/note.php?note_id=196124227075034

- **Support Dashboard**: a new tool designed to give people much better visibility and insight into the reports they make on Facebook. The Support Dashboard enables people to track their reports and informs them about the actions taken by our review team. We think this will help people better understand the reporting process and will educate them about how to resolve their issues. As people see which of their reports result in a removal of content, we believe users will be better equipped to make actionable reports. We have also posted about this to our Safety Page: https://www.facebook.com/notes/facebook-safety/more-transparency-in-reporting/397890383565083

- **"Ask Arturo" series**: as part of this series, we ask people to tell us about a situation in which they had to resolve a conflict that stemmed from an interaction on Facebook. Arturo Bejar supports the teams who handle reports of objectionable photos and posts on Facebook. Sometimes this content doesn't violate our Community Standards, but people may still wish for it to be removed. For people who have been in this situation, they can ask Arturo your question below. Each month, Arturo will tackle one tough problem, explaining how Facebook's policies apply and offering what he's learned from experts on conflict resolution. More information about the 'Ask Arturo' series is included here: https://www.facebook.com/notes/facebook-safety/ask-arturo-1-introduction/423179407702847

- **Other actions taken on implementation of these arrangements**

We offer a number of additional tools to ensure that individuals have a positive experience when using our site, including:

- **Inline privacy settings.** According to a recent Yahoo! study, 81 percent of teens use privacy controls when setting up an online profile.2 This is consistent with the findings from a survey

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER FREEDOM OF INFORMATION ACT 1982

undertaken by the Asia Pacific Privacy Authorities, in which over 80% of respondents said that they had used the privacy settings on their social networking site.[13] Facebook now also offers inline privacy settings, meaning that the settings can be adjusted at the point where the user decides to share a particular piece of information. We made the icons for each of the different privacy settings prominent and easy to identify, so that users can easily understand whom they are sharing with at that moment.

- **Age-appropriate sharing and visibility settings.** Facebook's privacy and visibility settings take into account the unique needs of people between the ages of 13 and 17, and are more restrictive than the settings for adults in nearly all cases. For example, a minor's sharing is automatically restricted to no more than the minor's friends and friends of those friends, or their networks, which are typically associated with their schools. Minors never have listings created for them in search engines off of Facebook, and the ability to share their location is automatically defaulted to "off." Unlike adults, minors can only be "tagged" on Facebook by their friends or the friends of those friends. Facebook's "Tag Review" feature, which is a privacy option that allows people to approve or reject tags that others add to their posts, is automatically turned "on" for minors.

- **Safeguards to avoid inappropriate contact between adults and minors.** Facebook employs robust tools to protect minors from unwanted contact and solicitation. For example, minors can only receive Messages on Facebook from friends or the friends of those friends, and never by strangers. Additionally, when a minor who is new to our service receives a friend request, we might interpose a message along the lines of "Only accept friend requests from people you really know" before the minor can confirm that he or she wants to accept the friend request. We also use innovative technical mechanisms to flag suspicious adult behaviour. For instance, if an adult sends an unusual number of friend requests to minors that are ignored or rejected, our warning systems might be triggered, which initiates a Facebook inquiry so that remedial action can be taken, if necessary.

- **Ongoing authentication checks.** We perform technical and community verification of users' accounts. Although we do not generally discuss the details publicly in order to limit attempts to compromise or circumvent the safeguards, we look for anomalous behaviour in the aggregate data produced by the Facebook community and employ automated systems to block inappropriate conduct, warn the user, or, when necessary, disable the offending account.

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

---

[1] More information can be found in the Deloitte Report: http://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/Industries/TMT/uk-tmt-media-facebook-europe-economic-impact-exec-summary.pdf
[2] More information can be found in the University of Maryland Study: http://www.rhsmith.umd.edu/digits/pdfs_docs/research/2011/AppEconomyImpact091911.pdf
[3] https://www.facebook.com/miishkafanpage
[4] https://www.facebook.com/help/?page=214189648617074
[5] http://www.poynter.org/latest-news/media-lab/social-media/143192/news-sites-using-facebook-comments-see-higher-quality-discussion-more-referrals/
[6] See page 137 http://dataprotection.ie/viewdoc.asp?DocID=1182
[7] *Irish Data Protection Commissioner*, Report of Audit – Facebook Ireland, 21 December 2011, page 137 (http://dataprotection.ie/viewdoc.asp?DocID=1182).
[8] *Id.*, page 141.

[9] *Id.*, page 139.
[10] Facebook, Family Safety Center, http://www.facebook.com/safety.
[11] Facebook, Facebook Safety, www.facebook.com/fbsafety
[12] https://www.facebook.com/note.php?note_id=360022794018509
[13] http://www.privacyawarenessweek.org/2011/survey_media_release.html

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

Cooperative arrangement for complaints handling on social networking sites

YouTube

In the interests of transparency, providers supporting the Cooperative Arrangement for Complaints Handling on Social Networking Sites agree to provide information on how they give effect to the Principles in relation to the social networking services they offer, using this form.

1. About the Social Networking Service

Google is deeply committed to protecting young people on the Internet and providing all of our users with a safe experience online through empowerment, education and protective measures. That's why we empower people with tools to help them choose what content they see online; provide educational materials on how to stay safe online; and protect through partnerships including with law enforcement and industry. We incorporate these three key principles across all Google products and services as broadly as possible. Google's Family Safety Center[1] and the YouTube Safety Center[2] are great resources for any user looking for safety tools and resources. They are one-stop shops for *teens, parents, teachers, and carers* about staying safe online. We've recently updated it to include advice from leading child safety organisations around the world, tips and ideas from parents at Google, as well as information on how to use the safety tools and controls built into Google products.

In relation to this protocol, there are social elements to our video sharing platform YouTube. YouTube is a user generated video sharing platform around which communities form, have discussion and interact. Bearing this in mind, Google provides information below about how it maintains these principles on the YouTube platform, where the relevant principles can be applied.

YouTube allows billions of people to discover, watch and share originally-created videos. YouTube provides a forum for people to connect, inform, and inspire others across the globe and acts as a distribution platform for original content creators and advertisers large and small.

Members of the YouTube community engage with one another by uploading, watching, favouriting, liking and commenting on videos, subscribing to channels, creating playlists and

[1] http://www.google.com.au/goodtoknow/familysafety/

[2] http://support.google.com/youtube/bin/request.py?&contact_type=abuse

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

sharing this activity. The following statistics particularly demonstrate the social nature of YouTube.

- 500 years of YouTube video are watched every day on Facebook, and over 700 YouTube videos are shared on Twitter each minute
- 100 million people take a social action on YouTube (likes, shares, comments, etc) every week
- Millions of subscriptions happen each day. Subscriptions allow you to connect with someone you're interested in — whether it's a friend, or the Sydney Opera House — and keep up on their activity on the site
- More than 50% of videos on YouTube have been rated or include comments from the community
- Millions of videos are favourited every day

2. How will the provider give effect to the complaints handling aspect of the Cooperative Arrangement

The following is an outline of how YouTube has considered the Cooperative Arrangement for complaints handling in relation to its Social Networking Service(s). This section will make reference to the recommendations made in the Principles document, where they are applicable and outline how they are applied.

1. Policies for acceptable use

YouTube's Terms of Service require all users to abide by our Community Guidelines before uploading videos. Our Community Guidelines are purposefully written in easy-to-understand language and are designed to provide users with clear advice on what content is acceptable and what is not (e.g., hate speech, pornography, images of drug abuse, and graphic violence). We have zero tolerance for predatory behaviour, harassment, revealing other users' personal information, or any activity that endangers safety or privacy. Users who repeatedly violate our Community Guidelines will have their accounts terminated.

Content deemed "age-restricted" after flagging and subsequent staff review is only viewable by signed-in users who represent that they are 18 years of age and older and who've clicked through a warning message.

Our Community Guidelines are clear about what is allowed on YouTube and what is not. There is, however, a category of content that is not illegal and does not breach our Terms of Service, but could still be inappropriate for users under the age of 18.[3] Should a user who is not signed into the service come across such a video they will be greeted with an interstitial page stating:

[3] http //support google com/youtube/bin/answer py?hl=en-GB&answer=92486

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

"This video or group may contain content that is inappropriate for some users, as flagged by YouTube's user community. To view this video or group, please verify that you are 18 or older by signing in or signing up[4]."

A user can then sign in and choose to watch the video or not. Only users with a birth date putting them over the 18 year old threshold will be allowed to watch the video. In order to prevent a teen from signing out of their account and then trying to create a new account with an older birth date, YouTube places a cookie on the user's browser preventing the user from re-registering with a different age.

Users under the age of 13 are prohibited from using YouTube and are blocked from creating accounts by a permanent cookie.

Within YouTube's safety tips page and the Terms of Service[5] it is clearly stated that the YouTube service is for people of 13 years and older. If, upon registration, a user puts a birth date that makes them under 13, they will be refused use of YouTube. In order to prevent a teen from trying to create a new account with an older birth date, YouTube places a cookie on the user's browser which prevents the user from registering with a different birth date.

Upon notification or if YouTube reasonably suspects that a particular user is less than 13 years old, that account will be closed. YouTube will send a confirming email to that user in those suspect cases.

2 & 3. Complaints Mechanisms and Review Processes

Every minute, 72 hours of video are uploaded to YouTube, totaling hundreds of thousands of videos every day. To handle this much content, we have developed an innovative and reliable community policing system that involves our users in helping us enforce You Tube's rules.

Millions of users report potential violations of our Community Guidelines by selecting the "Flag" link when they encounter inappropriate content. This reporting mechanism is straightforward and easily navigable for users of any age. Users are able to select from a list of over a dozen reasons for flagging a video and are given the opportunity to provide additional information, such as the specific time when the objectionable material appears in the video. Flagged videos are promptly reviewed for compliance with our Community Guidelines.

In addition to the aforementioned flagging mechanism to report content policy violations, YouTube has formal contact forms through which users can contact us directly regarding privacy, harassment and legal complaints.

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

[4] www.youtube.com/create_account
[5] http://www.youtube.com/t/terms

Dedicated YouTube staff review flagged content 24 hours a day, seven days a week, with a lot of content being reviewed in under one hour. If a user seeks more information on how we enforce our policies, there are additional details available in the Help Center[6].

Users whose content is flagged and removed pursuant to our Community Guidelines receive messaging specific to the policy violated. For instance, a user who violates our policies regarding Harmful & Dangerous Content would receive messaging tailored to that policy area.

If users submit a Harassment complaint via our Help & Safety Tool[7] they are informed, "We appreciate your bringing this to our attention. We will investigate your claim and take action if necessary. Thanks for helping us keep YouTube safe." If the content violates our policies regarding Harassment we notify the uploader as well.

If someone feels that their privacy has been violated on YouTube, a privacy complaint can be submitted to YouTube through our online tool[8]. We also accept complaints from parents or legal guardians of a minor child.

Throughout the Privacy Complaint Process the support team engages in correspondence with both the complainant and the uploader. We first email both the complainant and the uploader to confirm that a privacy complaint has been filed and to explain how reports are handled. In certain circumstances we ask either or both parties for additional information regarding the claim. After we review the complaint against our Community Guidelines, we take action as necessary and email the complainant regarding our decision. We likewise engage in email correspondence with users who submit impersonation and legal complaints. We confirm that we've received their complaint and notify them of the action taken.

We also offer our users tools to protect their privacy on the site, such as the ability to hide personal information, make videos private, remove videos from public listings, or share videos selectively with family and friends.

We respond immediately to threatening situations and report all instances of child abuse/exploitation to the National Center for Missing and Exploited Children (NCMEC).

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

4. Child abuse material

YouTube takes reports of illegal content on the site seriously. When we become aware that a video violates the law, we cooperate with law enforcement agencies quickly and in the proper

[6] http //www google com/support/youtube/bin/answer py?hl=en&answer=92486

[7] http //www youtube com/reportabuse

[8] http //support google com/youtube/bin/answer py?hl=en-GB&hlrm=en&answer=142443

legal framework. For example, we report all instances of child abuse/exploitation to the National Center for Missing and Exploited Children (NCMEC). Content that demonstrates imminent threats to life or limb can be reported to relevant law enforcement agencies. Content that is flagged or reported through the Help & Safety Tool is reviewed and dealt with appropriately.

On the Google-wide level, we actively support law enforcement efforts to keep kids safe online. Google has a specialized legal team dedicated to working with law enforcement officials, available 24 hours a day, 7 days a week.

We're also leveraging Google tools to combat online child abuse material. Throughout 2007, engineers used some of their 20% time to create innovative software tools[9]. The keys here were organization, scalability, and search. In particular, the tools we provided will aid in organizing and indexing the National Centre for Missing and Exploited Children's (NCMEC) information so that analysts can both deal with new images and videos more efficiently and also reference historical material more effectively. This task has been time-consuming, and NCMEC analysts were simply getting overwhelmed by all of the data they had to sift through to help NCMEC track down child predators through video and image search. With these tools, analysts will be able to more quickly and easily search NCMEC's large information systems to sort and identify files that contain images of child pornography. In addition, a new video tool we built streamlines analysts' review of video snippets.

Google has also donated Google Search Appliances[10] and hundreds of thousands of dollars of in-kind advertising each year through our Google Grants[11] program to NCMEC.

Google is a member of both NCMEC's Financial Coalition Against Child Pornography and its Technology Coalition. The Financial Coalition includes leading banks, credit card companies, third party payment companies and Internet services companies, and is dedicated to fighting child pornography/abuse over the Internet. The goal of the Financial Coalition Against Child Pornography is to eradicate commercial child pornography. NCMEC's Technology Coalition's mission is to develop and deploy technology solutions that disrupt the ability of predators to use the Internet to exploit children or traffic in child pornography/abuse material.

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

5. Identified contact person

YouTube's identified contact person is Google's representative on the Consultative Working Group on CyberSafety. This is the person with whom the Australian Government can discuss issues and any appropriate messaging to the community and media in response to issues as they arise.

[9] http://missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=3644
[10] http://www.google.com/enterprise/gsa/
[11] http://www.google.com/support/youtube/bin/answer.py?answer=126289

6 & 7. Education and awareness raising

YouTube as a video platform not only demonstrates its own safety features but also provides information to parents, teachers and young people on how to remain safe online, many of whom we partner with and support. Users are able to access YouTube's Community Guidelines[12], Help Center[13] and Safety Center[14] from every YouTube page. All of these pages are written in an easy to understand, user-friendly format.

The Help Center provides advice on a vast array of topics from changing personal settings to privacy complaint guidelines. Our dedicated Safety Center, linked to at the bottom of each page on our site, provides safety tips to our users, including advice on keeping personal videos private, teen safety, protecting online identities, appropriately managing interactions with other users, being responsible digital citizens, and using the community flagging system (see www.youtube.com/t/safety). We also provide Educator[15] and Parent Resources[16] pages which are targeted specifically at those audiences. From the Safety Center, it is possible to reach the Google Family Safety Center which offers additional tools and resources on a variety of topics. This information is made available to users, parents and teachers.

We also support child safety organisations' efforts to educate Internet users through new media, including YouTube. YouTube has partnered with many organisations in multiple countries and languages who have their own channels and whose expertise we've incorporated into our help resources and safety tips. Some examples are Kids Helpline[17], Bravehearts[18], Beat Bullying[19], Childnet[20], eEnfance[21], Save the Children[22], ICMEC[23], Ad Council[24] and others.

We also teamed up with online safety organisation iKeepSafe to develop a curriculum[25] that educators can use in the classroom to teach what it means to be a responsible online citizen. The curriculum is designed to be interactive, discussion filled and allow students to learn

[12] http://www.youtube.com/t/community_guidelines
[13] http://support.google.com/youtube/?hl=en
[14] http://support.google.com/youtube/bin/request.py?contact_type=abuse
[15] http://support.google.com/youtube/bin/answer.py?hl=en&answer=157105
[16] http://support.google.com/youtube/bin/answer.py?hl=en&answer=126289
[17] http://www.kidshelp.com.au/
[18] http://www.bravehearts.org.au/
[19] http://www.youtube.com/user/Beatbullying
[20] http://www.youtube.com/user/childnet
[21] http://www.youtube.com/user/eenfance
[22] http://www.youtube.com/user/savethechildrenuk
[23] http://www.youtube.com/user/DontYouForgetAboutMe
[24] http://www.youtube.com/user/adcouncil
[25] http://www.google.com/educators/digitalliteracy.html

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

through hands-on and scenario activities. The site also provides a resource booklet for both educators and students that can be downloaded in PDF form, presentations to accompany the lesson and animated videos to help frame the conversation. We've also launched a number of videos from our Safety Center, one[26] of which focuses exclusively on how to stay safe on YouTube.

YouTube always encourages users to employ a safe approach to personal information and privacy. YouTube does not have profile pages in the same way as social networking services, instead YouTube users use Channels to share user created content. YouTube does provide the option for users to make their channel private, share their videos privately to a limited number of people, or remove their videos from public listings. Users can also have the option to prevent videos being embedded on 3rd party pages, to prevent other sites from putting the user's video elsewhere on the web.

When setting up an account, users are advised in the Safety Tips, also accessible from every page, on how to protect their identity. Users are able to add some personal information on their channel should they choose to do so. In fact, the default information on a users channel shows the user name, not their actual name, but the user and channel name that is chosen when the user signs in. For example, you may be John Smith but choose to have a channel and user name of randomvideoviewer5 and his channel would become www.youtube.com/user/randomvideoviewer5. Once the user has set up their channel they have the option to add information through their account settings. Privacy settings are readily available to users regarding recent activity sharing[27] which allow a user to choose which information they wish to share. Help articles on 'Editing your Channel for Privacy' and related issues can be found in the Help Center. Users can also have the option to prevent videos being embedded on 3rd party pages, to prevent other sites from putting the user's video elsewhere on the web.

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

8. Collaboration with Government on education and awareness raising initiatives

YouTube, through its Google representative, is a member of the Consultative Working Group on Cybersafety and is committed to helping all Australians be smart, safe and responsible online.

Google works to promote the Australian Government's CyberSafety Help Button, including through its blog and Family Safety Center. Google also participates in cybersafety events and awareness activities organised by the Government, including Safer Internet Day, Privacy Awareness Week and National CyberSecurity Awareness Week. For example, for Safer Internet Day Google published advertisements promoting its safety tools in newspapers across Australia and online.

[26] http://www.youtube.com/watch?v=DQ5zJvA0NYY

[27] http://www.youtube.com/account_sharing

Google also distributes information about its safety tools through the Australian Communications Authority's Cybersmart program, and through events such as the CyberSafety Summit, the National Center Against Bullying Conference and consumer organisations such as ACCAN. We also meet with education institutions to raise awareness of the safety tools we make available, and how to report content on our services.

We support the part-Government funded Cooperative Research Centre for Youth and Wellbeing (YAW-CRC). The YAW-CRC contributes important research to this area, including research which is helping us understand how we as a community can harness the knowledge and skills of young people to help parents and guardians learn about the online world (see for example the YAW-CRC's *Living Lab study on Intergenerational Attitudes to Social Networking and Cybersafety*).

We also support non-government educational efforts to increase awareness about digital citizenship. In Australia we support non-profit organisations including The National Association for Prevention of Child Abuse and Neglect (NAPCAN), Inspire Foundation, The Alannah and Madeline Foundation, Kids Helpline and Bravehearts, to provide online public service announcements that promote access to resources about safety and other educational efforts. We actively support their efforts to raise awareness and educate people about digital citizenship. This includes our support for The Alannah and Madeline Foundation's eSmart Schools Program (http://www.amf.org.au/eSmart/).

9. Continued innovation

We are continually developing innovative tools to keep our community safe. For example, we use digital hashing technologies to prevent the re-upload of files that have been removed pursuant to policy violations. We also offer our users tools to protect their privacy on the site, such as the ability to hide personal information, make videos private, remove videos from public listings, or share videos selectively with family and friends. Our Help & Safety Tool lets users report concerns to the YouTube team (such as harassment, privacy violations and cyberbullying), block comments from specific other users and disable the video comments feature on videos.

YouTube specifically created Safety Mode[28], which allows users to choose not to see potentially objectionable content they may find offensive, to give parents additional controls over their teen's account. When users opt in to Safety Mode, videos with potentially objectionable content will not show up in video search, related videos, playlists, shows and movies. While no filter is 100% accurate, we use community flagging and hide objectionable comments to identify and

[28] http://support.google.com/youtube/bin/answer.py?hl=en-GB&answer=174084

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

hide inappropriate content. Like Google SafeSearch, Safety Mode on YouTube does not remove content from the site but rather keeps it off the page for users who opt in.

In order to make it less likely for users to stumble upon this type of content it are excluded from certain listings and areas of the site such as the "Most Viewed" page. YouTube has implemented automated systems to help classify content based on their content and meta-data and where videos are determined to be unsuitable for younger viewers, such content is demoted in browse pages, for example.

3. Other actions taken on implementation of these arrangements

This Self-Declaration is designed to provide information about how YouTube handles complaints and works to raise awareness about how to stay smart, safe and responsible online. YouTube, through its Google representative, is a member of the Consultative Working Group on CyberSafety and is committed to ongoing collaboration to help all Australians have a safe experience online.

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982

Cooperative arrangement for complaints handling on social networking sites

Microsoft Corporation

In the interests of transparency, providers supporting the Cooperative Arrangement for Complaints Handling on Social Networking Sites agree to provide information on how they give effect to the Principles in relation to the social networking services they offer, using this form.

1. **About the Social Networking Service(s)**

   Given that social networking services (SNS) are not defined in this Cooperative Arrangement, Microsoft interprets SNS to mean those services which have a primary purpose of facilitating broad and multi-modal interactions between users inside a single interface. Microsoft provides several services that may be considered SNS, catering to different consumer audiences, including:

   - Xbox Live which works with the Xbox gaming console to enable users to interact socially, play games and enjoy online content; and
   - Windows Live including tools such as Windows Live Messenger, Hotmail and SkyDrive

2. **How will the provider give effect to the complaints handling aspect of the Cooperative Arrangement?**

   Policies for Acceptable Use:
   Users of Microsoft's social networking services are required to accept standard terms of acceptable use in order to contribute to and participate in the services. An example of our terms of use policy for XBox Live can be found at: http://www.xbox.com/en-au/Legal/LiveTOU

   Complaints Mechanism:
   Clear and easy mechanisms are made available for users of Microsoft's services to make a complaint. For example, Microsoft's Live services have a Help Center where customers can report abuse, and with regard to XBox Live, there is a user interface onscreen enabling a player to instantly make a complaint regarding content or the activities of another player. Investigation into a complaint in this regard may lead to the suspension or banning of an offending player from XBox Live. This mechanism is detailed at http://support.xbox.com/en-AU/xbox-live/account-banning-and-player-feedback/chat-terms-of-use-conduct.

   Other social network services operated by Microsoft have similar capabilities for users to lodge complaints online or by contacting Microsoft through phone, email or chat. This is generally handled through Microsoft's local support channel with full details available at http://support.microsoft.com/?ln=en-au

   Child Abuse Material:
   Microsoft has existing procedures and policies in place for the removal of child abuse material and the appropriate notification of law enforcement. Microsoft is committed

THIS DOCUMENT IS RELEASED BY THE AUSTRALIAN FEDERAL POLICE UNDER THE FREEDOM OF INFORMATION ACT 1982