s22

From: s22
Sent: Monday, 18 March 2019 11:22 AM
To: Patteson, Carolyn
Cc: James Penprase; Mike Makin; Aaron o'neill
Subject: RE: Latest - heading to richard now [SEC=PROTECTED, DLM=Sensitive:Cabinet]

PROTECTED Sensitive: Cabinet

Thanks s22 ☺ Will make your other change.

Will cc you into the final going to Richard in the next 15 mins.

From: Patteson, Carolyn
Sent: Monday, 18 March 2019 11:13 AM
To: s22
Cc: Penprase, James ; Makin, Mike ; O'Neill, Aaron
Subject: Re: Latest - heading to richard now [SEC=PROTECTED, DLM=Sensitive:Cabinet]

Thank s22

s47C . I'd need to understand more practically how it works in the broadcast space currently. I'd also need to think about the powers for the OeSC.

Minor suggestion - the Prohibiting Streaming Services might be better above the Press Council Summit bit, it is fundamentally important.

Sent from my iPad

On 18 Mar 2019, at 11:03, s22 communications.gov.au> wrote:

PROTECTED Sensitive: Cabinet

streaming of terrorism material

Advice from the Office of the eSafety Commissioner

- The full-length video posted on 8Chan showing Tarrant's assault on the Al Noor Mosque in Riccarton would almost certainly fall within the RC category under the terror-advocacy provisions and the broader instruction in crime or violence provisions.
- Information from Google, Twitter and Facebook over the weekend is that they have worked to remove as much content as possible from their platforms. Facebook alone has removed something in the order of 1.5million videos of the attack.

- There are several other versions of the attack video circulating, including an edited version that stops as Tarrant raises his shotgun to fire at worshippers standing at the door of the Al Noor Mosque.

- These edited versions – depending very much on the context in which it is provided – may not be considered sufficiently detailed to be regarded as pro-terror advocacy. Arguably, they do not show a terrorist act within the meaning of section 100.1 of the Criminal Code, as required under section 9A of the Classification (Publications, Films and Computer Games) Act 1995.

- It is arguable that some of the edited versions may, however, still be considered sufficiently detailed to fall within the RC crime instruction category, as they could be seen as showing instruction in tactics, techniques and procedures.

- We have not been able to establish an Australian connection with respect to the hosting of the material. As such we are not empowered to take formal action.

- Material hosted via Australian news outlets may not have an Australian connection, as many of them are hosted overseas (even while employing .com.au country-level domains).

Arrangements for dealing with inappropriate material

Australia's classification system to address violent and extreme material

- Australia has a robust domestic Classification Scheme for films, computer games and certain publications.
- Australia relies on the Scheme to provide safeguards on material deemed extremist in nature and where appropriate, a Refused Classification (RC) rating is applied for material submitted for classification. This includes content promoting, inciting or instructing matters of crime of violence.
- The scheme is an inter-governmental arrangement whereby any changes to the scheme must be considered and agreed to by all ministers with responsibility for classification matters.

Video Games depicting violence

- Under Australian classification laws, a computer game must be classified before it can be sold. This includes games that are available via online storefronts.
- Computer games are classified by applying the Classification Act, the National Classification Code and the Guidelines.
    - The National Classification Code states that adults should be able to read, hear, see and play what they want, but minors should be protected from material likely to harm or disturb them, and that there is a need to take account of community concerns about depictions that condone or incite violence.
    - The Computer Games Guidelines state that a game is classified R 18+ if the violence is high impact. However, high impact violence that is visually depicted, frequently gratuitous, exploitative and offensive to a reasonable adult is not permitted at the R 18+ level.
    - The Computer Games Guidelines state that a game is Refused Classification if it contains:
        - Detailed instruction or promotion in matters of crime or violence.

        - Violence with a very high degree of impact which are excessively frequent, prolonged, detailed or repetitive.
- Under state and territory classification laws, a computer game which has been Refused Classification cannot be sold or advertised. It is also an offence to possess such a game in Western Australia. Enforcement of classification decisions is matter for the states and territories
- Online and mobile games apps can be classified by the International Age Rating Coalition (IARC) tool, used on participating storefronts (including Google Play, the Microsoft Store, Nintendo eShop, PlayStation Store and Oculus Store).
- The Department monitors a sample of games classified by the IARC tool, and the Classification Board can revoke the classification if it would have provided a different rating.
- Games have been Refused Classification by the IARC tool.
    - In 2017, a game titled *'Airplane Terrorist Simulator'* was Refused Classification because of terrorist related content. This demonstrates that the IARC tool is working for games that contain this type of content.
- Games that are Refused Classification by the IARC tool cannot be made available for sale on digital storefronts.
- Some digital storefronts such as Apple and Steam do not use the IARC tool. Steam has been known to provide games with high impact content.
- Since 2015-16, 5 games have been classified RC by the Classification Board, and none of these have been due to violence (these have been due to promoting drug use or paedophilia).
- The Computer Games Guidelines were most recently updated in 2012 to introduce the R 18+ category.
- Based on the Department's research with the Australian community and low complaints received, there is satisfaction with the standards for the classification of violent video games.

Working with digital platforms

Mechanisms for takedown

- Under the Online Content Scheme, the eSafety Office can take action in relation to material hosted in Australia that has been assessed against the National Classification Scheme as 'prohibited' or 'potential prohibited' (RC, X 18+, R 18+ or, in some cases, MA 15+).
- The RC category includes offensive depictions or descriptions of children and illegal content. However, it is important to note that what is considered prohibited/potential prohibited under Australian law may not be illegal in the jurisdiction where the content is hosted.
- While the eSafety Office does not have the power under the Online Content Scheme to issue a takedown notice to Facebook, which is based in the United States, it does work cooperatively with digital platforms to request removal of material that is clearly illegal in Australia and other jurisdictions.

Powers

- The eSafety Commissioner has the statutory power to direct Australian content hosts to remove prohibited online content if it is hosted in Australia.
- Overseas-hosted prohibited content, including adult content, is notified to vendors of accredited Family Friendly Filters.
- Reports about prohibited online content are prioritised and are referred to local and international civil and law enforcement partners for removal.

- If prohibited online content depicts information that could lead to the identification of either a victim or perpetrator, an immediate report will be made by the Office to the AFP.
- Pro-extremist content is notified to the Australian Federal Police or to state law counter-terrorism commands.

The ACMA

- The ACMA has commenced a formal investigation to examine whether content broadcast by commercial, national and subscription broadcasters on Friday's terrorist attack in Christchurch breached current rules.
- The ACMA's investigation will focus on any content from the perpetrator-filmed and live streamed footage of the shootings that was broadcast on Australian television.
- The ACMA is also concerned about content made available or linked to on broadcasters' websites. While this is currently beyond its regulatory remit, the ACMA is in close contact with the Australian Press Council as it reviews its members' coverage of the attack.
- In the first instance, the ACMA Chair will be writing to the CEOs of the commercial, national and subscription broadcasters requesting urgent information on the nature, extent and timing of the broadcast of content relating to the shootings, in particular from the day of the attack.
- The ACMA will also be requesting urgent meetings with the peak industry organisations—Free TV Australia and the Australian Subscription Television and Radio Association—to discuss whether current rules are providing adequate protections for Australian audiences.

Possible Next Steps

- This is a highly complex matter involving a perpetrator who has meticulously planned to maximise the spread of their content by exploiting the open nature of digital platforms.
- Domestic regulation can only go so far in addressing this as digital platforms are global entities.
- Close collaboration and cooperation with digital platforms is essential to identify, report and limit the spread of extremist material.

s47C [redacted]

s47C [redacted]

Briggs Review and Online Safety Charter

- The Briggs review of Online Safety legislation conducted in 2018 recommended the development of a new Online Safety Act, with an increased obligation for industry to be more proactive in addressing online harms to be passed into law in the second half of 2019. The Government has indicated in principle support.
- The Government is also consulting on a draft online safety charter which is intended to establish the Government's expectations for social media services, content hosts and other technology companies in enhancing online safety for Australian users.
- It will seek to articulate community expectations in relation to the identification and removal of harmful and illegal content, tackling abusive conduct, and improving transparency for users.
- The Government could strengthen the charter with a view to addressing live streaming of terrorist content.

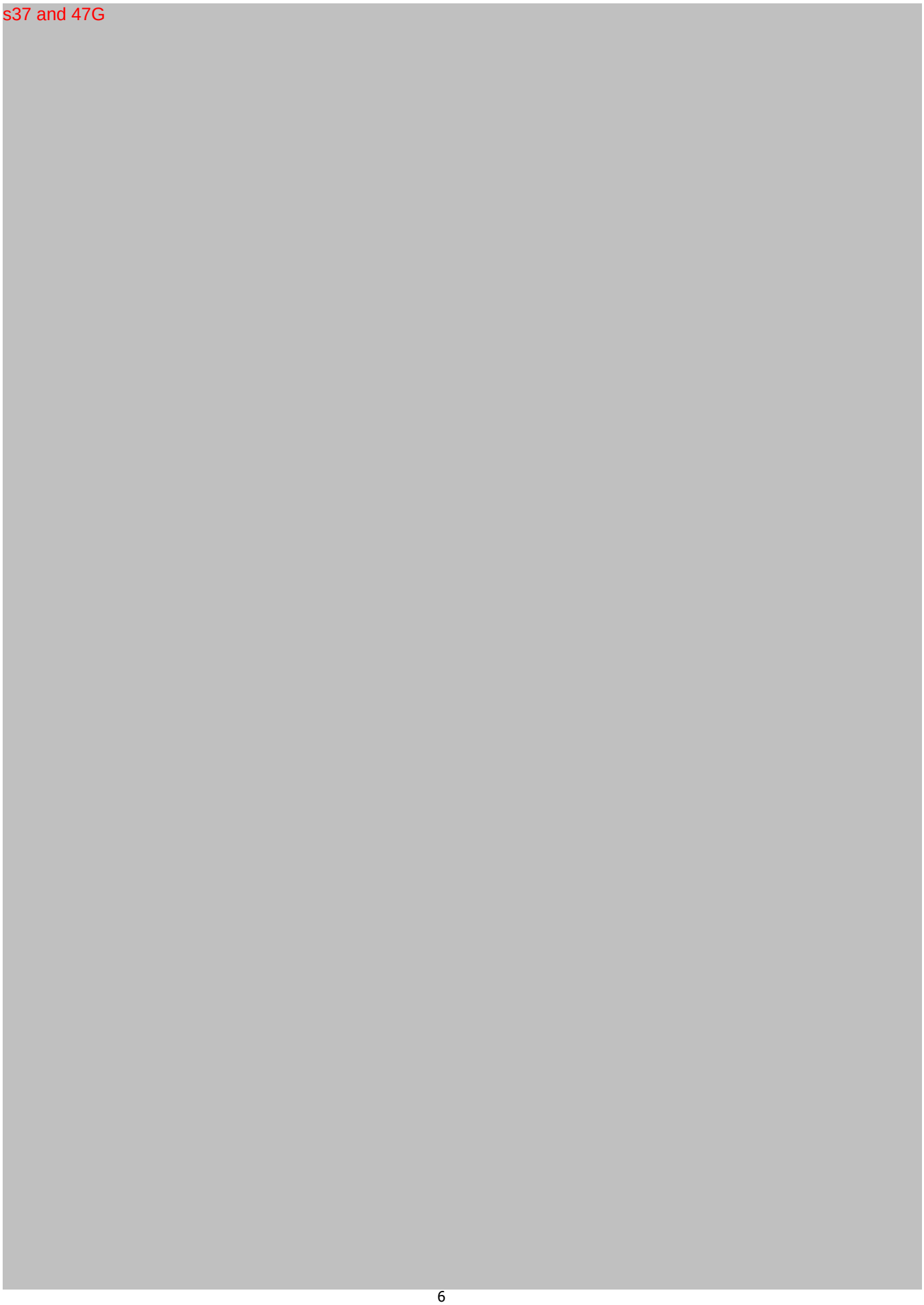
Prohibiting Streaming Services

- Prohibiting live streaming is not feasible as this functionality is widely available across any number of social media, OTT and telecommunication platforms.
- Overwhelmingly, live streaming services are used for legal purposes and have widespread business, consumer and personal uses.

ATTACHMENT A

Emails from Facebook – 17 March

s37 and 47G

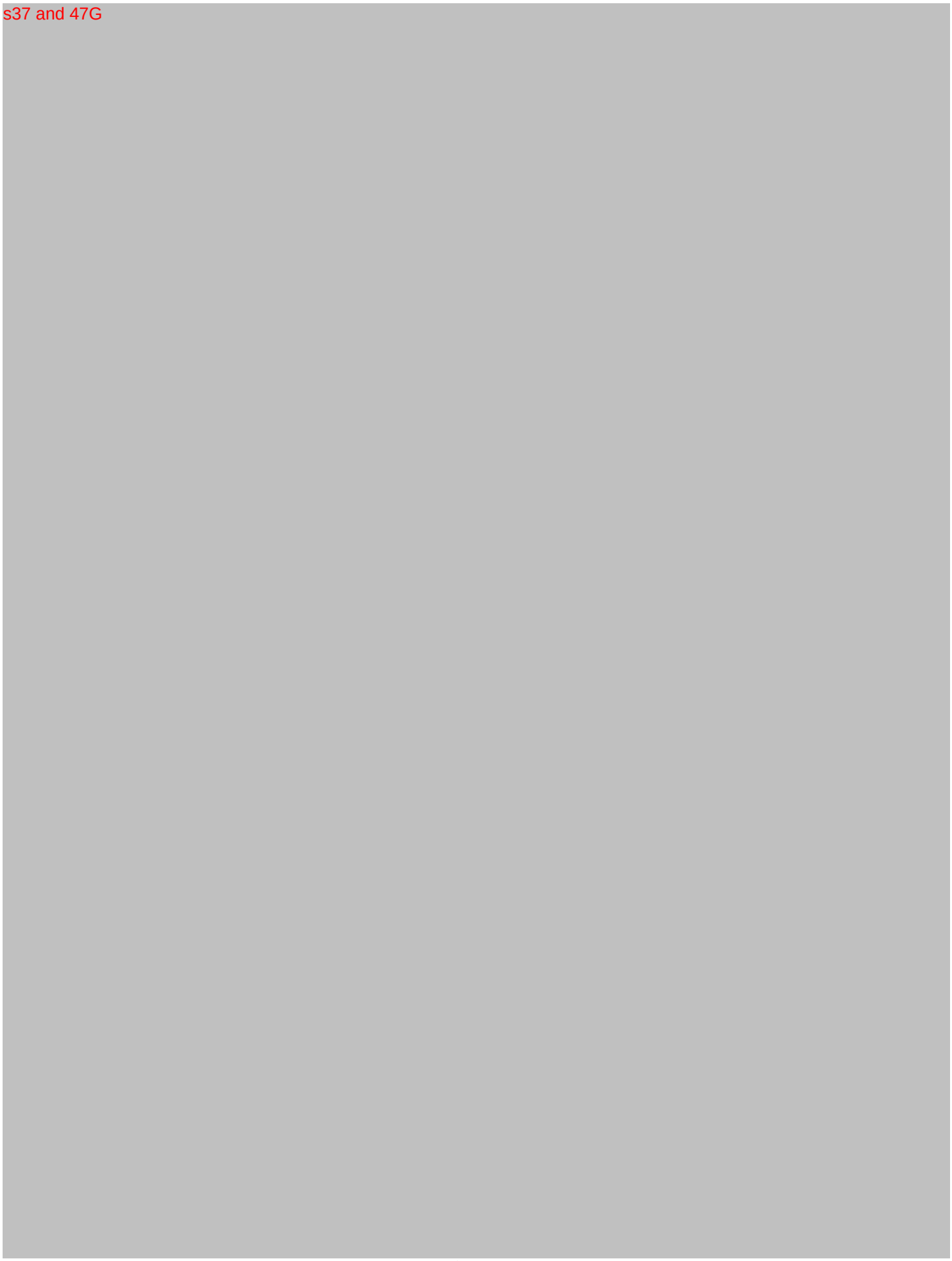



s37 and 47G

ATTACHMENT B

Emails from Facebook – 16 March

s37 and 47G



s37 and 47G

ATTACHMENT C

Online Content Scheme

The Online Content Scheme is set out in Schedules 5 and 7 of the *Broadcasting Services Act 1992* (BSA) and four industry codes. This is a coregulatory scheme with industry codes working together with a formal regulated complaints mechanism.

- Schedule 5 contains powers to take action against content hosted outside Australia.
- Schedule 7 contains powers to take action against content hosted within Australia.

The scheme was designed to meet the objects in subsection 3(1) of the BSA of:

(ha) to ensure designated content/hosting service providers respect community standards in relation to content; and

……

(k) to provide a means for addressing complaints about certain internet content; and

(l) to restrict access to certain internet content that is likely to cause offence to a reasonable adult; and

(m) to protect children from exposure to internet content that is unsuitable for children;

Prohibited content is that which what been classified by the Classification Board, and may include assessment for material that contains violence, language and themes such as terrorism and pornography. Prohibited content includes material to which criminal penalties apply (e.g. child pornography) or that has been classified as:

- Refused Classification (RC)
- X18+
- R18+ unless subject to a restricted access system
- MA15+ and is provided on a commercial basis unless subject to a restricted access system.

Potentially prohibited content is content that has not been classified but, if it was, is highly likely to be found to be prohibited.

Schedule 7 of the BSA defines 'content' as text, data, speech, music, sounds, visual images or any other form.

The eSafety Commissioner can investigate complaints about prohibited or potentially prohibited content and can:

- If content is hosted in Australia, order the take down of material using powers in schedule 7 of the BSA, or
- If content is hosted outside of Australia, report it to law enforcement and advise of links to the makers of internet filters using powers under Schedule 5 of the BSA.

The eSafety Commissioner is not able to classify material directly. Applications for classification of content can be made to the Classification Board by the host service provider, content service provider, links service provider or the eSafety Commissioner. Content is classified under the National Classification Code and classification guidelines.

CONCERNS ABOUT THE EFFECTIVENESS OF THE ONLINE CONTENT SCHEME

Issues with the Scheme as identified in the current and previous reviews are that the scheme is inflexible and overly prescriptive and not keeping up with changing technology. The industry codes that underpin the Scheme have not been reviewed since they were first developed in 2005 and 2008.

In 2012 the Australian Law Reform Commission recommended the establishment of a new classification scheme, administered by a single Commonwealth regulator that covered all media content across all platforms.

Submissions to the current review noted:

- The schedules overlap, are outdated, not fit for purpose and do not reflect current technologies or content delivery models and there is an inconsistent treatment of the same content across different platforms.
- The scheme has been more effective for content hosted in Australia with a high compliance rate. However this has become less relevant because of the migration of illegal content to offshore sites.
- Some submissions suggested that content should be classified by appropriately trained eSafety Office staff which would allow for quicker removal of content.
- The industry codes are out of date but the prescriptive nature of the schedules have prevented a meaningful overhaul of the codes by industry.

BACKGROUND

Outline of Schedule 5 of the BSA - Online Services

Schedule 5 was added to the BSA in 1999. The Schedule sets up a system for regulating certain aspects of the internet industry:

- If the eSafety Commissioner is satisfied that internet content hosted outside Australia is prohibited content or potential prohibited content, the Commissioner must:
    - if the eSafety Commissioner considers that the content is of a sufficiently serious nature to warrant referral to a law enforcement agency—notify the content to an Australian police force; and
    - notify the content to internet service providers so that the providers can deal with the content in accordance with procedures specified in an industry code or industry standard (for example, procedures for the filtering, by technical means, of such content).
- Bodies and associations that represent the internet service provider section of the internet industry may develop industry codes.
- The eSafety Commissioner has a reserve power to make an industry standard if there are no industry codes or if an industry code is deficient.

Outline of Schedule 7 of the BSA - Content Services

Schedule 7 was added to the BSA in 2007. The Schedule sets up a complaint mechanism for online content:

- A person may make a complaint to the eSafety Commissioner about prohibited content, or potential prohibited content, in relation to certain services.
- The Commissioner may take the following action to deal with prohibited content or potential prohibited content if it is hosted in Australia:
    - in the case of a hosting service—issue a take-down notice;
    - in the case of a live content service—issue a service-cessation notice;
    - in the case of a links service—issue a link-deletion notice.

- Content (other than an eligible electronic publication) is ***prohibited content*** if:
    - the content has been classified RC or X 18+ by the Classification Board; or
    - the content has been classified R 18+ by the Classification Board and access to the content is not subject to a restricted access system; or
    - the content has been classified MA 15+ by the Classification Board, access to the content is not subject to a restricted access system, the content does not consist of text and/or one or more still visual images, and the content is provided by a commercial service (other than a news service or a current affairs service); or
    - the content has been classified MA 15+ by the Classification Board, access to the content is not subject to a restricted access system, and the content is provided by a mobile premium service.
- Content that consists of an eligible electronic publication (an electronic edition of a book, magazine or newspaper) is ***prohibited content*** if the content has been classified RC, category 2 restricted or category 1 restricted by the Classification Board.
- Generally, content is ***potential prohibited content*** if the content has not been classified by the Classification Board, but if it were to be classified, there is a substantial likelihood that the content would be prohibited content.
- Bodies and associations that represent sections of the content industry may develop industry codes.
- The Commissioner has a reserve power to make an industry standard if there are no industry codes or if an industry code is deficient.
- The Commissioner may make determinations regulating certain content service providers and hosting service providers.

ATTACHMENT D

Excerpts from Commercial Television Industry Code of Practice and Subscription Broadcast Television Code of Practice

Commercial Television Industry Code of Practice

2.3 Exceptions

2.3.3 News Programs (including news flashes and news updates), Current Affairs Programs and Sports Programs and Program Promotions for news, Current Affairs or Sports Programs do not require classification and may be shown at any time, however a Licensee will exercise care in selecting material for broadcast, having regard to:

a) the likely audience of the Program or Program Promotion; and

b) any identifiable public interest reason for presenting the Program or Program Promotion.

2.6 Material not suitable for broadcast

2.6.1 A Licensee must not broadcast any material that cannot be classified MA15+ or any lower television classification.

Note: Material may be modified by a Licensee to ensure that it is suitable for broadcast, or for broadcast at particular times.

2.6.2 A Licensee must not broadcast any Program, Program Promotion, Community Service Announcement or Station ID which is likely, in all the circumstances, to provoke or perpetuate in, or by a reasonable person, intense dislike, serious contempt or severe ridicule against a person or group of people because of age, colour, gender, national or ethnic origin, disability, race, religion or sexual preference.

3.2 Material which may cause distress

3.2.1 In broadcasting a news or Current Affairs Program, a Licensee must:

a) not include material which, in the reasonable opinion of the Licensee, is likely to seriously distress or seriously offend a substantial number of viewers, having regard to the likely audience of the Program, unless there is a public interest reason to do so; and

b) include a spoken warning before a segment that contains material which, in the reasonable opinion of the Licensee, is likely to seriously distress or seriously offend a substantial number of viewers having regard to the likely audience of the Program; and

c) not broadcast reports of suicide or attempted suicide unless there is a public interest reason to do so, and exclude any detailed description of the method used, and exclude graphic details or images; and

d) exercise sensitivity in broadcasting images of or interviews with bereaved relatives or people who have witnessed or survived a traumatic incident; and

e) have regard to the feelings of relatives and viewers when including images of dead bodies or people who are seriously wounded, taking into account the relevant public interest.

Subscription Broadcast Television Code of Practice

2.1 General Programs

(a) Licensees will not broadcast any program which is likely in all the circumstances to provoke or perpetuate intense dislike, serious contempt or severe ridicule against a person or group of

persons on the grounds of age, colour, gender, national or ethnic origin, disability, race, religion or sexual preference.

2.2 News and Current Affairs Program

[…]

(b) In broadcasting news and current affairs programs to the extent practicable Licensees:

(i) must not present material in a manner which creates public panic;

(ii) must include only sparingly material likely to cause some distress to a substantial number of viewers;

(iii) must exercise sensitivity in broadcasting images of, or interviews with, bereaved relatives and survivors or witnesses of traumatic incidents;

(iv) will take all reasonable efforts to provide warnings when there are identifiable public interest reasons for broadcasting material which may seriously distress or seriously offend a substantial number of viewers;

(v) will only broadcast reports of suicide or attempted suicide where there is an identifiable public interest to do so and will exclude any detailed description of the method used and any graphic details and will not glamourise suicide in any way; and

(vi) will make reasonable efforts to correct significant errors of fact at the earliest opportunity.

(c) In broadcasting news and current affairs programs Licensees must not use material relating to a person's personal or private affairs, or which invades an individual's privacy, other than where there are identifiable public interest reasons for the material to be broadcast.

Note: The question of intrusion into private domains, such as bereavement or personal tragedy, is one of real difficulty for all providers of news and current affairs programs. It is a matter of balance between what should be reported in the interests of the general public and what, if reported, would cause an individual or group of individuals unnecessary anguish. It is noted that the ACMA has published advisory Privacy Guidelines for Broadcasters available on the ACMA website at www.acma.gov.au.

2.3 Program Promotions and News Updates

Licensees will have particular regard to the need to protect children from unsuitable material in program promotions, news updates and news promotions.

The content of program promotions, news updates and news promotions will be consistent with the classification of the programs (if classified) during which updates or promotions appear and will, where practicable, include classification information about the programs being promoted, (see Part 3 of these Codes).

ATTACHMENT E

Extract from draft Online Safety Charter – released for public comment on 16 February 2019

Draft Online Safety Charter

This Charter seeks to outline what the Australian Government, and the Australian community, expect of technology companies and online service providers operating in Australia in terms of protecting the most vulnerable in our community. It is underpinned by two fundamental principles:

1. Standards of behaviour online should reflect the standards that apply offline.
1. Content that is harmful to users, particularly children, should be appropriately restricted.

This Charter is directed towards technology firms that offer the opportunity for users in Australia to interact or connect, and technology firms whose services and products enable Australian users to access content and information. This includes social media services, internet service providers, search engine providers, content hosts, app developers, and gaming providers, among others. For the sake of simplicity, the Charter uses the term 'technology firms'.

Control and responsibility

Content identification

Technological solutions should be fully utilised by technology firms to identify illegal and harmful content, and these solutions should be supported by human resources as appropriate.

There should be a specific point of contact within each technology firm for the referral of complaints about illegal and harmful content or legal notices from Australian authorities. This point of contact should be equipped and trained to manage Australian referrals, with a good understanding of relevant Australian legal requirements.

Content moderation

The systems employed by technology firms should have the capability and capacity to moderate illegal and harmful content.

Where feasible, this should include a triaging system to ensure high risk content (e.g. content promoting self-harm or criminal activity) is addressed expeditiously and lower risk content is reviewed and actioned within a longer period (for example, within 24 hours).

This triaging system should ensure that complaints made by children, or by adults on behalf of children, are also expedited. Where appropriate, illegal, harmful or inappropriate content targeted towards a child should be removed immediately, and only reinstated once the complaint has been investigated and only if the complaint is not upheld.

The resources devoted to content moderation should be proportionate to the volume of content available to users and relevant to the Australian context. Human content moderators should meet minimum training standards.

Minimum timeframes should apply to the review and moderation of flagged content, whether identified from internal flags, user complaints or regulatory authorities.

Content removal

Content that is clearly and unambiguously illegal under Australian law should be removed proactively by technology firms

Content that has been determined to be in breach of terms of use, or identified by regulatory authorities to be illegal or harmful, should be removed within clearly stated minimum timeframes.

Technology firms should take steps to prevent the reappearance of illegal, harmful or offensive content that has been removed.

s22

Director / Digital Platforms / Digital Media and Copyright Branch
Department of Communications and the Arts
s22

2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra, ACT 2601

communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

I would like to acknowledge the traditional custodians of this land on which we meet, work and live. I recognise and respect their continuing connection to the land, waters and communities. I pay my respect to Elders past and present and to all Aboriginal and Torres Strait Islanders.

Doc 2

KENNA Allison

From: s22
Sent: Monday, 18 March 2019 5:22 PM
To: Patteson, Carolyn; James Penprase; s22 Mike Makin
Cc: Richard Eccles
Subject: FW: Summary - Google/YouTube Work Following Christchurch Tragedy [SEC=UNCLASSIFIED]

UNCLASSIFIED

FYI (this has been passed to the MO as well).

s22 – Richard Eccles – Deputy Secretary (Content, Arts, Strategy & Research)
Richard Windeyer – Deputy Secretary (Infrastructure & Consumer Affairs)
Department of Communications and the Arts
s22

2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra ACT 2601

communications.gov.au
@CommsAu

arts.gov.au
@artsculturegov

INTERNATIONAL YEAR OF INDIGENOUS LANGUAGES
www.arts.gov.au/IY2019

I would like to acknowledge the traditional custodians of this land on which we meet, work and live. I recognise and respect their continuing connection to the land, waters and communities. I pay my respect to Elders past and present and to all Aboriginal and Torres Strait Islanders.

From: Eccles, Richard
Sent: Monday, 18 March 2019 3:54 PM
To: s47F ; Mrdak, Mike ; Patteson, Carolyn

s22

Subject: RE: Summary - Google/YouTube Work Following Christchurch Tragedy [SEC=UNCLASSIFIED]

UNCLASSIFIED

Dear s47F

This is very useful – appreciate the update.

Richard

Richard Eccles
Deputy Secretary / Content, Arts, Strategy and Research
Department of Communications and the Arts
P s22

Richard.eccles@communications.gov.au

s22
1
s22

INTERNATIONAL YEAR OF INDIGENOUS LANGUAGES
www.arts.gov.au/IY2019

I would like to acknowledge the traditional custodians of this land on which we meet, work and live. I recognise and respect their continuing connection to the land, waters and communities. I pay my respect to Elders past and present and to all Aboriginal and Torres Strait Islanders.

communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

From: s47F
Sent: Monday, 18 March 2019 3:48 PM
To: Mrdak, Mike <Mike.Mrdak@communications.gov.au>; Eccles, Richard <Richard.Eccles@communications.gov.au>; Patteson, Carolyn <Carolyn.Patteson@communications.gov.au>
Cc: Middleton, Vicki <Vicki.Middleton@communications.gov.au>
Subject: Summary - Google/YouTube Work Following Christchurch Tragedy

Dear Mike, Richard and Carolyn,

s37 and 47G

s47G

s47G and 47F

Doc 3

s22

From: s22
Sent: Wednesday, 20 March 2019 5:18 PM
To: s22 media
Subject: FW: Final reply that is being sent in response to media enquiries [SEC=UNCLASSIFIED]

UNCLASSIFIED

As discussed

From: s22
Sent: Tuesday, 19 March 2019 4:57 PM
To: Penprase, James <James.Penprase@communications.gov.au>
Subject: Final reply that is being sent in response to media enquiries [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hi James,

The final version that has been issued to journalists is as follws.

s22

- There has been a sea change in the attitude of the community and governments to the regulation of the internet over the last decade. The clear view of our Government and the Australian community is that the same standards and rules that apply in the physical world should apply in the online world. The internet cannot be an ungoverned and safe space for terrorists and other criminals. This has been the guiding principle of this Government with the internet and why we have been continually adding to the enforcement powers of agencies, to protections for the community, and commissioned the ACCC to examine the entire digital platform market from end to end. The Government has been working locally and globally.

- The Prime Minister has written to the G20 President (Shinzo Abe) to express his concern at the continuing and unrestricted role played by internet technologies in this and other terrorist attacks. The Prime Minister has requested that leaders have an opportunity to discuss the issue as part of the Osaka G20 Summit agenda.

- It is imperative that the global community works together to ensure that technology firms meet their moral obligation to protect the communities which they serve and from which they profit.

- The Australian Government has been at the forefront of online safety legislative reform to enshrine the principle that the online world is not a safe place for terrorists. It's why we have legislated to give law enforcement agencies the same sort of crime fighting tools for encrypted communication that they have had for decades for phone services.

- Our Government established and appointed the world's first eSafety commissioner to be a one stop shop for advice, education and enforcement.

- We legislated the world's first kids' anti cyberbullying regime to give the eSafety Commissioner the powers to issue take down notices and fine individuals and digital platforms. We've legislated similar powers for the eSafety Commissioner in relation to the non-consensual sharing of intimate images.

- The eSafety Commissioner already has the power to direct Australian hosted websites to take down offensive material that would be refused classification such as those related to terrorist, child sex and drugs matters. Australian law enforcement agencies can also require Australian ISPs to block access to overseas hosted content using powers in section 313 of the Telecommunications Act 1997.

- And the eSafety Commissioner also has the power to advise Australian ISPs to include sites carrying material that would be refused classification in the list of filtering products where these are hosted overseas. And where sites are hosted in other jurisdictions the eSafety Commissioner works directly with platforms and overseas partner agencies to have material taken down.

- But more needs to be done.

- Even before the tragic events in Christchurch, the Government had released a draft Online Safety Charter for community consultation. The purpose of the Charter is to make clear to the platforms the Government's expectations on behalf of the community across a range of areas including the prevention and the taking down of offensive material through the better use of moderators, artificial intelligence and other technologies.

- At the time the draft Charter was issued I made clear that I expected the full cooperation of the platforms and that if this wasn't forthcoming, the Government would not hesitate to legislate as it has in areas such as encryption, kids' cyberbullying and the non-consensual sharing of intimate images.

- In the wake of Christchurch, Ministers have met with government agencies and while the initial focus has been on responding to immediate events and assisting New Zealand colleagues the Government has also started looking at measures to address the ways digital platforms were used and abused. As part of these efforts the Government will be calling together representatives of digital platforms, ISPs and government agencies next Tuesday.

- Digital platforms have evolved in what they can offer to the community and regrettably the worst elements of our society have also adapted their use. The time has come for those who own and manage platforms to accept a greater responsibility for how they are used. A best endeavours approach is no longer good enough. It's clear that while social media companies have cooperated with authorities to remove some of that disgusting content, more needs to be done. If they won't act, we need to.

Doc 4

s22

From: Patteson, Carolyn <Carolyn.Patteson@communications.gov.au>
Sent: Wednesday, 20 March 2019 3:35 PM
To: s22
Cc: James Penprase
Subject: Invitees - ISPs [SEC=UNCLASSIFIED]

UNCLASSIFIED

s22

Email text for the telcos and Communications Alliance with names and email addresses below – where we have them. I understand Lauren has email addresses for telco CEOs which are understandably tightly held.

Dear (CEO name),

The Australian Government would like to invite you to attend a summit to discuss government and industry responses to the sharing of content related to the terrorist attack in Christchurch on 15 March.

The summit will bring together representatives of Australian law enforcement and security agencies, internet service providers, social media platforms, regulators and officials from my department.

Representatives will be asked to outline the actions taken by their organisations in response to the shootings and the dissemination of footage from the attacks. Summit participants will then work collectively to identify what can be done to prevent the streaming and reposting of extremist material, both now and into the future.

The meeting will be held in Brisbane on 26 March from 1 -3 pm at Level 31, Eagle Street, Waterfront Place. We would like to confirm your representation by Friday, 22 March 2019. Please RSVP to Dr Carolyn Patteson, First Assistant Secretary, Content Division on (02) 6271 1418 or by email to Carolyn.Patteson@communications.gov.au.

An agenda for the meeting will be circulated once attendees are confirmed.

Telstra

s47F

Carolyn Patteson
First Assistant Secretary / Content
Department of Communications and the Arts
P +61 2 6271 1418

s47F
Email.carolyn.patteson@communications.gov.au
2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra, ACT 2601
communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

s22

From: Patteson, Carolyn <Carolyn.Patteson@communications.gov.au>
Sent: Friday, 22 March 2019 11:48 AM
To: James Penprase; s22
Subject: FW: Microsoft President Brad Smith in Australia [SEC=UNCLASSIFIED]

UNCLASSIFIED

FYI, we're adding Microsoft too. I s22 .

Carolyn Patteson
First Assistant Secretary / Content
Department of Communications and the Arts
P +61 2 6271 1418
s47F
Email.carolyn.patteson@communications.gov.au

2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra, ACT 2601

communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

s22


s22


s22

s22

IMPORTANT: This message, and any attachments to it, contains information that is confidential and may also be the subject of legal professional or other privilege. If you are not the intended recipient of this message, you must not review, copy, disseminate or disclose its contents to any other party or take action in reliance of any material contained within it. If you have received this message in error, please notify the sender immediately by return email informing them of the mistake and delete all copies of the message from your computer system.

Doc 6

s47C and 47G

s47C and 47G

s47C and 47G

DRAFT

s47C and 47G

s47C and 47G

s47C and 47G

s47C and 47G

DRAFT

s47C and 47G

MOTHERBOARD

ADVERTISEMENT

IN MODERATION

Documents Show How Facebook Moderates Terrorism on Livestreams

On Friday, at least 49 people were killed in terror attacks in New Zealand. Documents, sources, and interviews with senior Facebook employees show how difficult it is for social media companies to moderate live footage.

By Joseph Cox | Mar 15 2019, 12:58pm

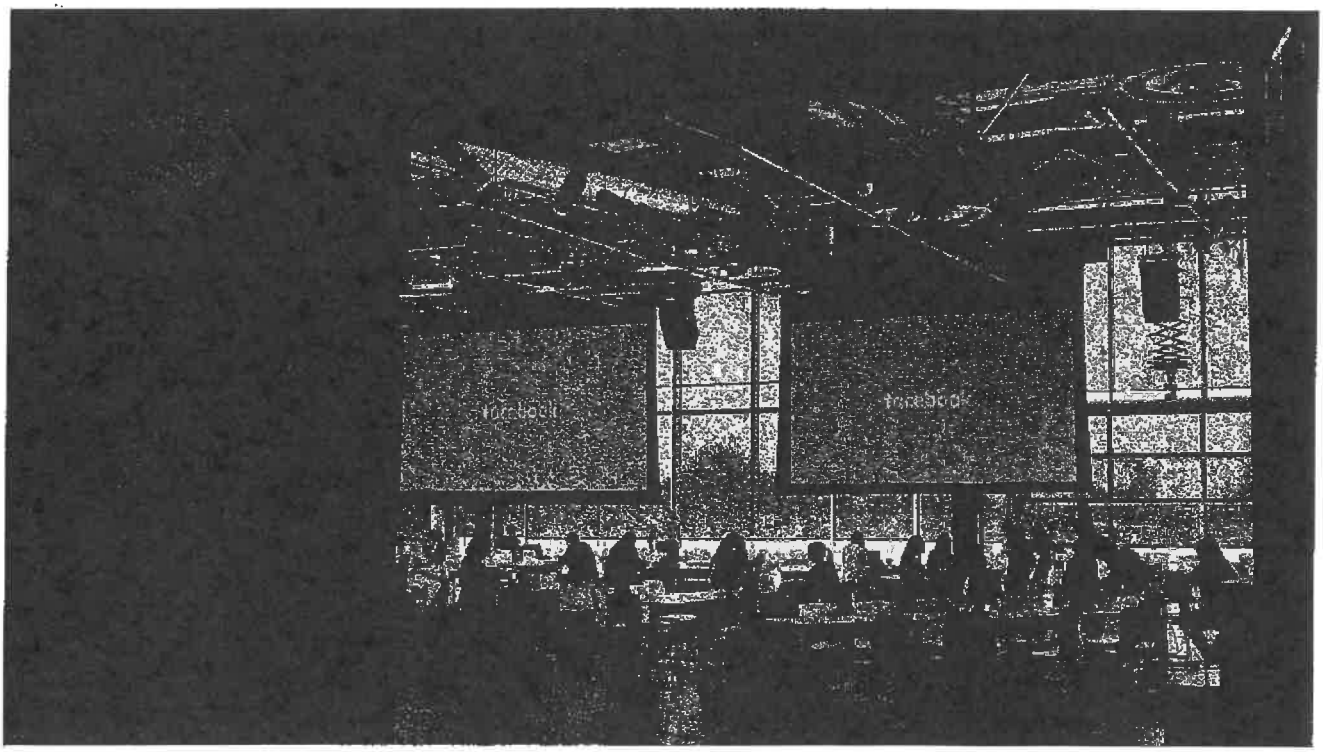


Image: Jason Koebler

SHARE TWEET

This piece is part of an ongoing Motherboard series on Facebook's content moderation strategies. You can read the rest of the coverage here.

ADVERTISEMENT

On Friday, at least **49 people were killed** in terror attacks against mosques in Christchurch, New Zealand. One apparent shooter broadcast the attack onto Facebook Live, the social network's streaming service. The footage was graphic, and Facebook deleted the attackers' Facebook and Instagram accounts, although archives of the video have spread across other online services.

The episode highlights the fraught difficulties in moderating live content, where an innocuous seeming video can quickly turn violent with little or no warning. Motherboard has obtained internal Facebook documents showing how the social media giant has developed tools to make this process somewhat easier for its tens of thousands of content moderators. Motherboard has also spoken to senior employees of Facebook as well as sources with direct knowledge of the company's moderation strategy, who described how Live was, and sometimes still is, a difficult type of content to keep tabs on.

"I couldn't imagine being the reviewer who had to witness that livestream in New Zealand," a source with direct knowledge of Facebook's content moderation strategies told Motherboard. Motherboard granted some sources in this story anonymity to discuss internal Facebook mechanisms and procedures.

Like any content on Facebook, be those posts, photos, or pre-recorded videos; users can report Live broadcasts that they believe contain violence, hate speech, harassment, or other terms of service violating behaviour. After this, content moderators will review the report, and make a decision on what to do with the Live stream.

ADVERTISEMENT

Ad

World Countries Quiz: Kno
than an Average American

HowStuffWorks V

According to an internal training document for Facebook content moderators obtained by Motherboard, moderators can 'snooze' a Facebook Live stream, meaning it will resurface to moderators again every 5 minutes, so they can check if anything has developed. Moderators also have the option to ignore it, essentially closing the report; delete the stream; and escalate the stream to a specialized team of reviewers to scrutinise if it contains a particular type of material such as terrorism. In the case of terrorism, escalation would flag the stream to Facebook's Law Enforcement Response Team (LERT), who work directly with police. In the Christchurch case, Facebook told Motherboard it had been in contact with New Zealand law enforcement since the start of this unfolding incident.

> ***Got a tip? You can contact this reporter securely on Signal on +44 20 8133 5190, OTR chat on jfcox@jabber.ccc.de, or email joseph.cox@vice.com.***

When escalating a potential case of terrorism in a livestream, moderators are told to fill in a selection of questions about the offending content: what is happening that indicates the user is a committing an act of terrorism? When has the user said indicated that harm will occur? Who is being threatened? Does the user show weapons in the video? What are the users' surroundings; are they driving a car?

On Friday, New Zealand Prime Minister Jacinda Ardern explicitly **described the Christchurch mosque shootings** as a terrorist attack.

Finally, moderators can also "mark" the stream with a variety of different labels, such as disturbing, sensitive, mature, or low quality, the training document obtained by Motherboard adds.

When reviewing streams, moderators may watch the live portion of the material itself as well as sections that already aired, and multiple moderators may work on the

same clip, each rewinding to the point the previous reviewer stopped, the document indicates.

WARNING SIGNS

ADVERTISEMENT

For Facebook Live video, moderators are told to watch out for "warning signs" which may show a stream is about to include violating content, the training document continues. These include evidence of a suicide attempt, with people saying goodbye, or talking about ending their life. The document also tells moderators to be on the lookout for "Evidence of human despair," such as "Crying, pleading, begging."

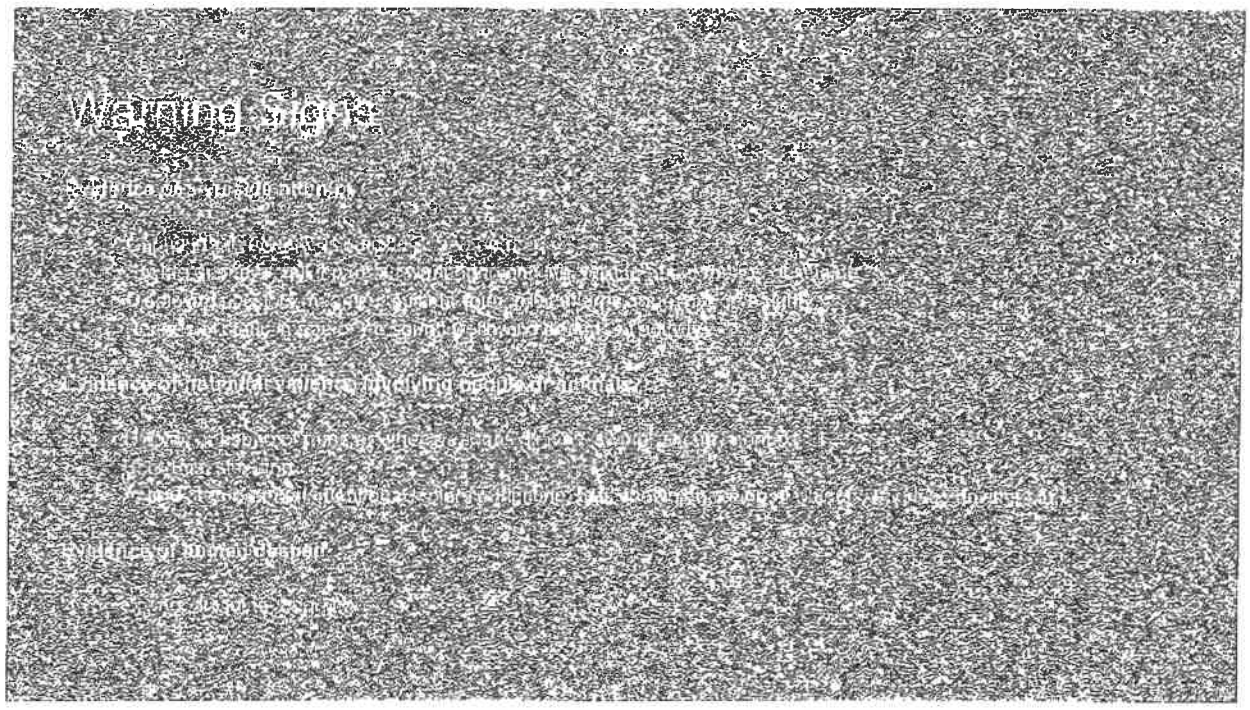
With relevance to the Christchurch stream and other terrorist attacks, some of those warning signs fall under "Evidence of potential violence involving people or animals." Specifically, that includes the "Display or sound of guns or other weapons (knives, swords) in any context," the document reads.

A second source with direct knowledge of Facebook's moderation strategy told Motherboard "Live streams can be slightly more difficult in that you're sometimes trying to monitor the live portion and review an earlier portion at the same time, which you can't really do with sound."

Of course, when it comes to weapons, and in particular guns, a stream's transition from non-violating to violent can happen in milliseconds. In this respect, the fact that users are easily able to broadcast acts of violence via Facebook Live is not an indication that the social media company isn't trying to find ways to moderate that content, but indicative of the difficulties that live broadcasts present to all platforms.

In a copy of the attack video viewed by Motherboard, the attacker shows several weapons right at the start of the stream, and they frequently reappear through the footage as the attacker drives to the mosque.

"I'm not sure how this video was able to stream for [17] minutes," the second source with direct knowledge of Facebook's content moderation strategies told Motherboard.



An internal Facebook slide obtained by Motherboard. Motherboard has reconstructed the slide to preserve source anonymity, but the language of the material remains intact. Image: Motherboard.

Because Live has had a rocky moderation history as Facebook learned to control it, the company has created tools to make moderators' jobs somewhat easier.

ADVERTISEMENT

"Facebook Live was something that ramped [up] quickly, that from a consumer experience was delivering great customer experiences. But there also was unearthing places we had to do better and were making mistakes, as violence and other policy violations were occurring," James Mitchell, the leader of Facebook's risk and response team, told Motherboard in late June last year in an interview at the company's headquarters.

In the same set of interviews, Neil Potts, Facebook's public policy director, **told Motherboard that moderation issues** "became really acute around the live products, Facebook Live, and suicides."

"We saw just a rash of self-harm, self-injury videos, go online, and we really recognized that we didn't have a responsive process in place that could handle those, the volume, now we've built some automated tools to help us better accomplish that," he added.

Justin Osofsky, Facebook's head of global operations, previously told Motherboard, "We then made a concerted effort to address it, and it got much better, by staffing more people, building more tools, evolving our policies."

One tool moderators have access to is an interface that gives them an overview of a Facebook Live stream, including a string of thumbnails to get a better idea of how a stream has progressed; a graph showing the amount of user engagement at particular points, and the ability speed up the footage or slow it down, perhaps if they want to skip to a part with violating content or take a moment to scrutinise a particular section of the footage.

"You know if this video's 10 minutes, at minute four and 12 seconds, all of a sudden people are reacting. Probably a pretty good sign to go and see what happened there." Osofsky added.

> **"I couldn't imagine being the reviewer who had to witness that livestream in New Zealand."**

ADVERTISEMENT

BOOK NOW

Judging by a watermark in the corner of the stream, in this case, the attacker appears to have used **an app called LIVE4**, which streams footage from a GoPro camera to Facebook Live.

"We were shocked by the news like everyone else," Alex Zhukov, CEO of LIVE4, told Motherboard in an email

"We are ready to work with law enforcement agencies to provide any information we have to help the investigation. And also Facebook representatives, to make sure the platform stays safe and is used only as it was intended. We will be blocking access to the app to anyone spreading evil. Unfortunately we [LIVE4] have no technical ability to block any streams while they are happening," he added.

Mia Garlick from Facebook New Zealand told Motherboard in a statement, "Our hearts go out to the victims, their families and the community affected by this horrendous act. New Zealand Police alerted us to a video on Facebook shortly after the livestream commenced and we quickly removed both the shooter's Facebook and Instagram accounts and the video. We're also removing any praise or support for the crime and the shooter or shooters as soon as we're aware. We will continue working directly with New Zealand Police as their response and investigation continues."

Jason Koebler contributed reporting.

Subscribe to our new cybersecurity podcast, CYBER.

MORE FROM MOTHERBOARD

SHARE TWEET

TAGGED: INSTAGRAM, TERRORISM, CHRISTCHURCH, HATE SPEECH, LIVESTREAMING, CONTENT MODERATION, LIVESTREAMING VIOLENCE, CONTENT MODERATORS, FACEBOOK CONTENT MODERATION

Watch This Next

© 2019 VICE MEDIA LLC

Doc 7

s22

From: s22
Sent: Friday, 22 March 2019 4:54 PM
To: James Penprase; s22
Subject: RE: Actions [SEC=UNCLASSIFIED]

UNCLASSIFIED

I've added to the annotated agenda brief.

From: Penprase, James
Sent: Friday, 22 March 2019 4:39 PM
To: s22
Subject: FW: Actions [SEC=UNCLASSIFIED]

UNCLASSIFIED

More from Google. For file please and use in outlining what they have been doing.

From: Eccles, Richard
Sent: Friday, 22 March 2019 11:58 AM
s22

Cc: Penprase, James <James.Penprase@communications.gov.au>; Patteson, Carolyn <Carolyn.Patteson@communications.gov.au>
Subject: RE: Actions [SEC=UNCLASSIFIED]

UNCLASSIFIED

For interest, this just in from Facebook.

s37 and 47G

In addition, we have shared more details about our technical work on artificial intelligence and blocking the video: https://newsroom.fb.com/news/2019/03/technical-update-on-new-zealand/. In terms of next steps, our work is focused on:

s37 and 47G

Please let me know if you have any further questions at this stage. We look forward to engaging further about these topics in more detail at the summit next Tuesday in Brisbane."

Richard Eccles
Deputy Secretary / Content, Arts, Strategy and Research
Department of Communications and the Arts
P +61 2 6271 1 s22

Richard.eccles@communications.gov.au

R s22

INTERNATIONAL YEAR OF INDIGENOUS LANGUAGES
www.arts.gov.au/IY2019

I would like to acknowledge the traditional custodians of this land on which we meet, work and live. I recognise and respect their continuing connection to the land, waters and communities. I pay my respect to Elders past and present and to all Aboriginal and Torres Strait Islanders.

communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

From: Eccles, Richard
Sent: Friday, 22 March 2019 11:11 AM
s22 [redacted]
Cc: Penprase, James <James.Penprase@communications.gov.au>; Patteson, Carolyn <Carolyn.Patteson@communications.gov.au>
Subject: Actions [SEC=UNCLASSIFIED]

UNCLASSIFIED

Dear all

Please use this address list to keep in touch.

As discussed, can each agency turn their mind to tangible outcomes and changes we would propose to platforms and ISPs.

As per the discussion, we propose that these outcomes would be grouped under the following elements:

1. Instantaneous or quicker takedown of violent and extreme material (or blocking of access);

2. Improving transparency of the actions the planforms and ISPs take in relation to violent and extreme material;

3. Holding platforms, ISPs, and individuals to account for the upload and distribution of violent and extreme material.

Thanks – lets all keep close on this.

Richard

Richard Eccles
Deputy Secretary / Content, Arts, Strategy and Research
Department of Communications and the Arts
P +61 2 6271 1534 s22 [redacted]

Richard.eccles@communications.gov.au

s22 [redacted]

I would like to acknowledge the traditional custodians of this land on which we meet, work and live. I recognise and respect their continuing connection to the land, waters and communities. I pay my respect to Elders past and present and to all Aboriginal and Torres Strait Islanders.

communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

SUMMIT ON RESPONSES TO THE SHARING OF CONTENT RELATED TO CHRISTCHURCH INCIDENT

ANNOTATED AGENDA AND BRIEFING

Date: Tuesday, 26 March 2019
Time: 1:00 to 3:00 pm
Venue: Level 31, 1 Eagle Street Waterfront Place, Brisbane, Queensland

Agenda	Timing	Description	Lead
1	1:00 – 1:05 pm (5 minutes)	Welcome	Prime Minister

PURPOSE OF ITEM

- Prime Minister to welcome attendees and outline the purpose of the Summit and its intended outcomes.

- The Prime Minister is expected to articulate the concerns of the Government in relation to the terrorist attack in New Zealand and the upload and dissemination of footage from the incident on social media and other websites.

Agenda	Timing	Description	Lead
2	1:05 – 1:15 pm (10 minutes)	Overview of expectations	Minister Fifield Minister Dutton Attorney-General Porter

PURPOSE OF ITEM

Ministers to outline their expectations from the Summit (around 2 minutes each).

TALKING POINTS

- (If PM present) I acknowledge Prime Minister Morrison – and I thank you for your leadership in progressing this Summit.
- (If Deputy High Commissioner of New Zealand is present) I also acknowledge the Deputy High Commissioner of New Zealand, Mr Llewellyn Roberts, and express my heartfelt condolences for the terrible events that occurred in Christchurch.
- My portfolio has played an active role in working with the platforms and the ISPs with respect to online safety. This is as it should be: online safety is a shared responsibility, with roles for individuals, industry and Government.
- We have regulated the platforms – for a simple reason: to protect Australia's best interests. In my portfolio we have done so in the areas of image-based abuse, cyberbullying, online gambling, copyright and piracy. And our classification system makes it clear what content should be banned – refused classification and removed for circulation.
- And I acknowledge the efforts of the platforms and ISPs to delete and block content from the Christchurch attack, and their willingness to cooperate with law enforcement agencies and Government in the wake of the attacks.
- Despite this, it is clear that more needs to be done, by all parties.
- Government must ensure that we have the right regulatory arrangements in place, and individuals, and the community, need to take responsibility for their actions online.
- But industry must do more to ensure that their services are not being weaponised by those that perpetrate such acts, and that this type of harmful content isn't able to be spread.
- That is what we are here to talk about today.
- As you know, we've sought to crystallise our expectations through the draft Online Safety Charter.
- The action we are looking for from industry is a subset of that work, relating specifically to violent and extreme material.
- As the Prime Minister has already outlined, we are seeking action in three areas:
    - Prevention and protection – including detecting, blocking, and instantaneous and faster takedown options for violent and extreme material.
    - Transparency – improving transparency of the actions taken by platforms and ISPs in relation to violent and extreme material.
    - Deterrence – enhancing responsibility for the upload and distribution of violent and extreme material by individuals, platforms and ISPs.
- Today we are seeking concrete actions and commitments from industry.

- If we don't get those, we will invariably need to turn to regulatory options. We've done so in the past, and won't hesitate to do so again.
- I hope today that we can agree on some tangible and practical measures to address the upload and dissemination of violent and extreme content, and curb the harm that this type of content to cause in our society.

Agenda	Timing	Description	Lead
3	1:15 – 1:30 pm (15 minutes)	Update from the digital platforms • Actions • Rules and standards • Lessons learned	Facebook Google Twitter

PURPOSE OF ITEM

For the digital platforms to provide a briefing on the actions taken in response to the attacks in Christchurch, the rules and standards that govern their services and lessons learned from the incident.

OUTLINE OF ACTIONS TAKEN BY INDUSTRY

Facebook

Facebook has advised that the first user report of the video of the attack came in **29 minutes after the video started**, and **12 minutes after the live broadcast ended**. s47G

s37 and 47G

Once it was aware of the video, Facebook marshalled a range of resources to attempt to keep it off its platform.

s37 and 47G

[redacted]

On Friday, 22 March, Facebook published a technical update on New Zealand which included details of its work to: use technology to improve video matching technology and react faster to this kind of video; identify and remove the content of over 200 white supremacist organisations globally; and experiment with sharing URLs with its partners in the Global Internet Forum to Counter Terrorism, as well as refining and improving collaboration in a crisis.

Google (YouTube)

s37 and 47G [redacted]

Twitter

Twitter has not provided an update on the actions that it took in response to the attacker's video. Twitter has been quoted in media reports as saying that the company had suspended the account of one of the suspects and was working to remove the video from its network, which violated its policies.

TALKING POINTS

- The Government appreciates that this heinous act caught all of us off guard.
- As I noted earlier, the Government appreciates the efforts of the platforms and ISPs to delete and block content from the Christchurch attack, and their willingness to cooperate with law enforcement agencies and Government in the wake of the attacks.
- Digital platforms are not the only place that this horrendous content was uploaded and shared. Sites like 4Chan, 8Chan and Kiwifarms were used by individuals to host this material.
- But the fact remains that the platforms – notably Facebook – were the **launching point** for the dissemination of this content by the perpetrator.
- The alleged gunman deliberately **exploited the openness of the platforms**, and used them as a means of **promoting this abhorrent act of terrorism**.

- And the platforms remain the key ways in which the bulk of our community access online content, including harmful content. With this scale and impact comes an unavoidable level of social responsibility.

POTENTIAL QUESTIONS

Facebook

a) Why did it take 29 minutes (12 minutes after the end of the video) for Facebook to begin the process of taking down copies of the video? How can this be improved?

b) Facebook has indicated that in the 24 hours following the incident, it has prevented the attempted upload of 1.2 million copies of the video, but than 300,000 slipped through. How did this happen?

c) How many attempted uploads of the video has Facebook blocked automatically (current figures), and how many has it had to take down once uploaded?

d) How many of those videos that required removal after upload needed to be reviewed by Facebook staff or contractors, and how many were removed with technology?

e) How did Facebook seek to work with other industry players in relation to 'hashed versions' of the video? When did this occur, and what were the results?

Google (YouTube)

a) How many searches related to the Christchurch attack occurred in the first 24 hours, and how many were seeking the video footage?

b) Did YouTube become aware of the existence of the video on its platform by user notification, advice from security agencies, or from internal sources?

c) When, precisely, did YouTube remove the first upload of the video footage, and how long after the attack was this?

d) How many attempted uploads of the video did YouTube block on the first 24 hours, and how many got through and needed to be removed once uploaded?

e) How did Google seek to work with other industry players in relation to 'hashed versions' of the video? When did this occur, and what were the results?

Twitter

a) Why hasn't Twitter provided some indication publically of the impact of the incident on its platform, and what actions it has taken?

b) How many times was the video uploaded by users to the Twitter platform in the first 24 hours of the incident? What action did Twitter take in relation to these uploads?

c) Did Twitter seek to block the upload of the video, and how soon after the incidence did this occur?

d) How many attempted uploads were blocked by Twitter, and how were they blocked?

e) How many times did users share links to the video footage? What action did Twitter take in relation to these tweets?

f) How many user accounts did you suspect or disable?

g) How did Twitter seek to work with other industry players in relation to 'hashed versions' of the video? When did this occur, and what were the results?

Agenda	Timing	Description	Lead
4	1:30 – 1:55 (25 minutes)	Update from the ISPs • Actions • Rules and standards • Lessons learned	Telstra Optus TPG Vodafone Communications Alliance

PURPOSE OF ITEM

For ISPs to provide a briefing on the actions taken in response to the attacks in Christchurch, the rules and standards that govern their services and lessons learned from the incident.

OUTLINE OF ACTIONS TAKEN BY INDUSTRY

- Telstra, Optus and Vodafone have voluntarily blocked sites hosting the Christchurch shooting video. The role of TPG is unclear, as no statements have been located.
- The blocked sites included 4chan, 8chan, Liveleaks, Zerohedge and Kiwi Farms. There was significant criticism of the blocking of Zerohedge, s47G s47G
- ISPs have reportedly been working with blocked websites to restore access once the video had been taken down. Media reports also suggest that the telecommunications industry is hopeful that this summit will bring clarity over the government's expectations about how they would react to any terrorist material being shared widely in future.

TALKING POINTS

- I commend those of you (Telstra, Vodafone and Optus) who took action voluntarily in response to the events in New Zealand to block access to sites hosting the abhorrent content until it was removed.
- This has played an important role in reducing the spread of the content throughout the Australian community.
- I appreciate that industry would like guidance from Government about when and how to act.
- Today I hope we can make a start to clarifying these arrangements and the systems that should be in place should unfortunate situations like this arise in the future.

POTENTIAL QUESTIONS

a) How many websites have each of you blocked?

b) How many have removed the offending content, and has access been restored? What is the process and timeframe for restoring access?

c) Did the ISPs share information with each other about the decision to block sites voluntarily? Was there industry-wide coordination?

d) What about smaller ISPs – did they undertake any blocking?

e) Did TPG block any of the sites?

Agenda	Timing	Description	Lead
5	1:55 – 2:55 pm (60 minutes)	Facilitated discussion: improving outcomes and commitments to reform. • Instantaneous or quicker takedown of violent and extreme material (or blocking of access). • Improving transparency of the actions taken by platforms and ISPs in relation to violent and extreme material. • Enhancing responsibility for the upload and distribution of violent and extreme material by individuals, platforms and ISPs.	All

PURPOSE OF ITEM

To seek commitments from the digital platforms and telecommunication industries that they will lift their game and do more to deal proactively and decisively with inappropriate content.

More detailed content is available at Attachment A.

TALKING POINTS AND QUESTIONS

Takedown

Talking Points
- I acknowledge the efforts of the digital platforms to find and remove the content once alerted. And we have heard about the difficulty of moderating live streams featuring abhorrent content.
- But the issue remains – digital platforms have set up service that we know can be exploited by terrorists to reach mass audiences.
- We also know that if even one copy of a video can reach an audience – that content can then be copied and reposted.

Questions
- Can platforms prioritise the development of better and more effective AI to detect extreme material?
- Can platforms put better mechanisms in place to identify users or accounts that spread violent and extreme material and prevent them from creating new accounts with the same intent?
- On human oversight – can platforms appoint Australian-based content moderators with the historical, political and cultural knowledge needed to make informed moderation decisions?

Transparency

Talking Points
- The draft Online Safety Charter would require technology forms to publish regular reports on content controls, complaints and compliance issues.
- I note and welcome the various transparency reports published by many digital platforms – however more granular detail would assist government to assess the effectiveness of actions taken.
- For example – it is not helpful to provide the number of pieces of offensive content taken down when we don't know the prevalence of graphic violence, hate speech or offensive content on the platform.

Questions

- Can platforms build greater awareness about the actions that users can take to quickly report abhorrent content?
- How can platforms increase the level of trust with users that their reports are taken seriously and will be acted on?

Responsibility

Talking Points

- Technology firms are no longer just the pipes that deliver content. There must be greater responsibility for the content that users can access and minimum thresholds for content control and moderation.
- Disturbingly, the events in Christchurch have also demonstrated that there are individuals who will make a determined effort to edit and re-upload appalling content. There needs to be a clear message sent that this behaviour is unacceptable.

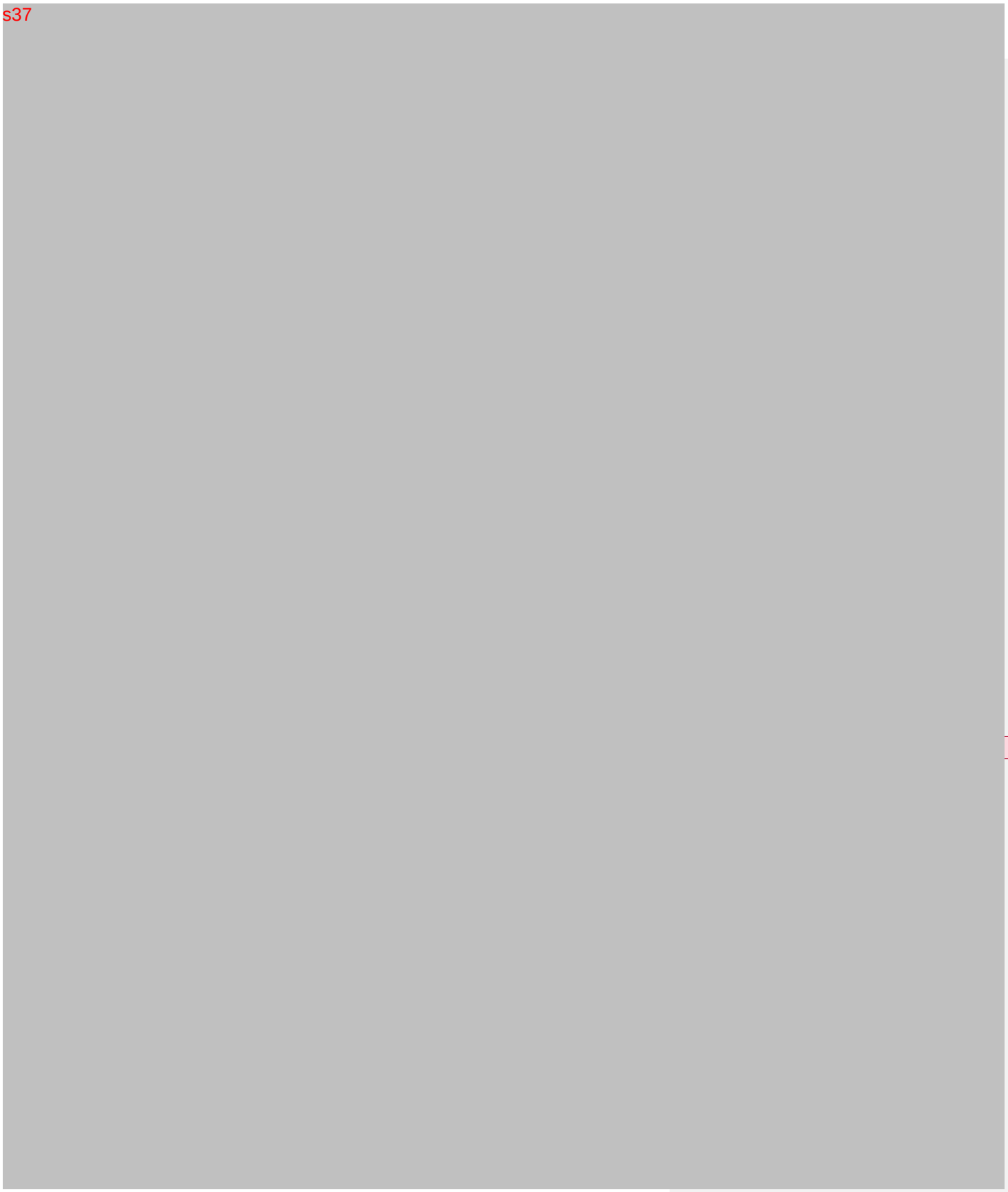
Questions

- Could the platforms do more to identify and demote content of users with a track record of engaging with violent or extreme material?
- Can platforms build stronger relationships with law enforcement and provide a designated, 24 hour contact point for responding to online safety concerns in Australia?
- Could technology companies formalise the share with government emergency plans for responding to these issues?

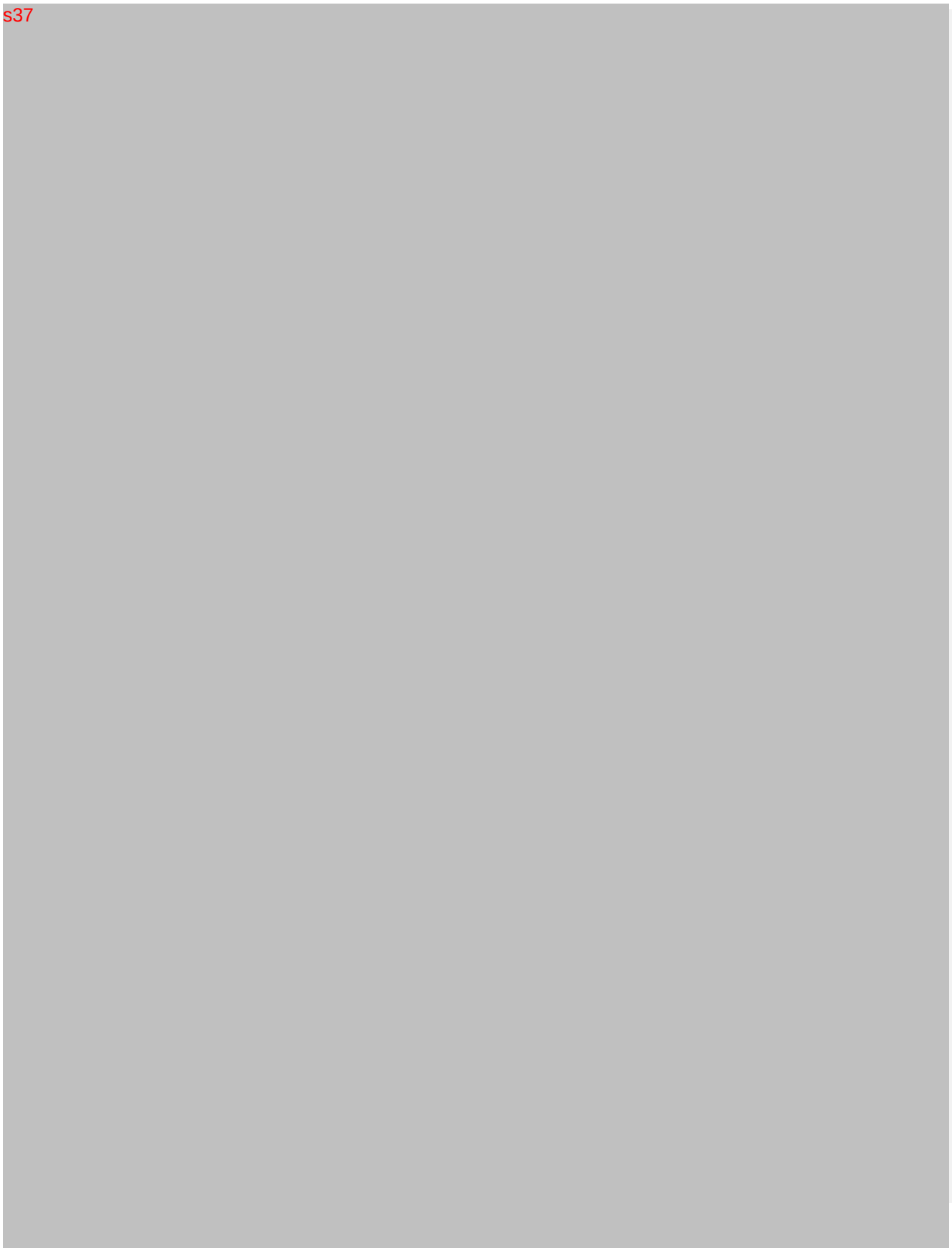
Agenda	Timing	Description	Lead
6	2:55 – 3:00 pm (5 minutes)	Close	Minister for Communications

PURPOSE OF ITEM

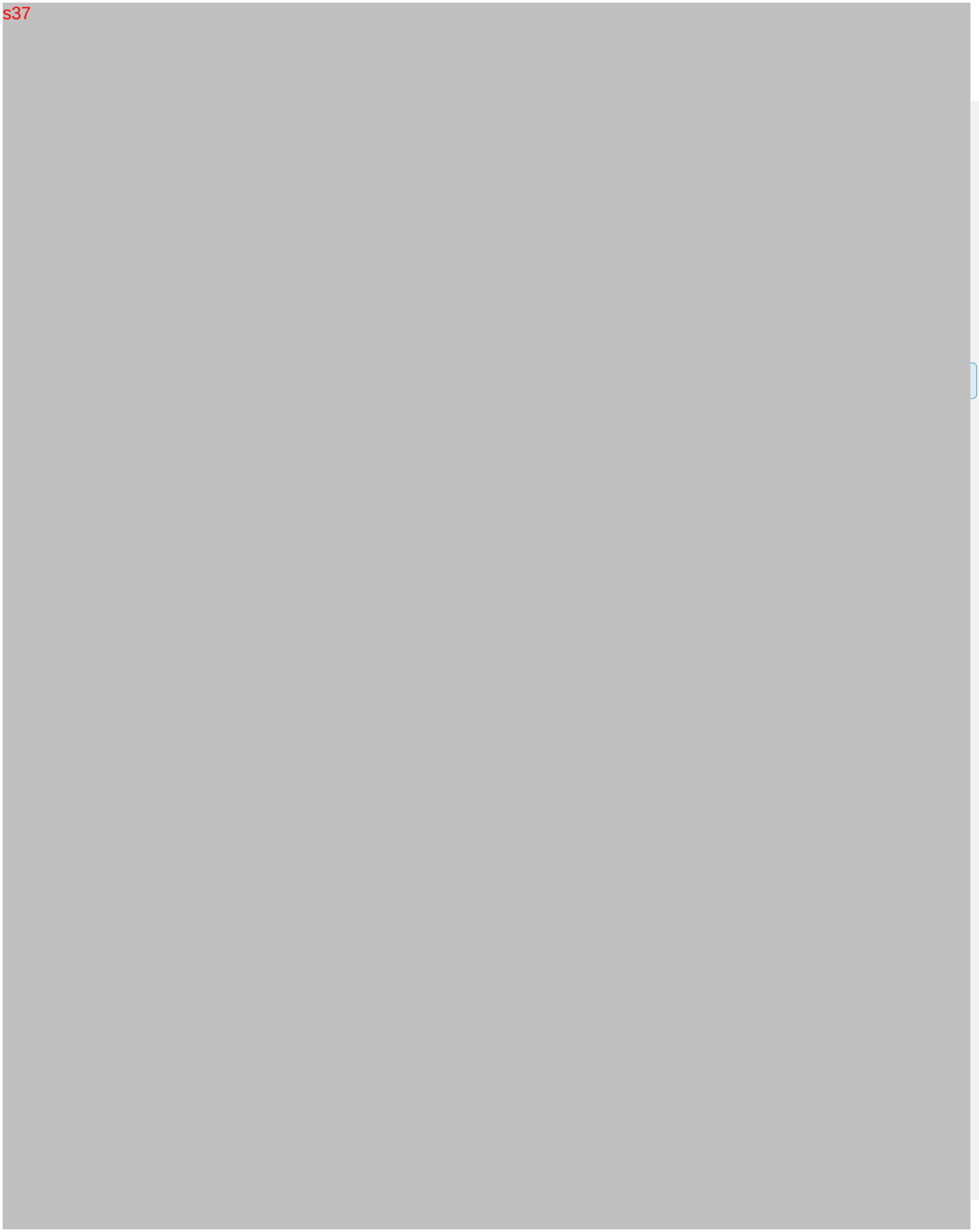
TALKING POINTS

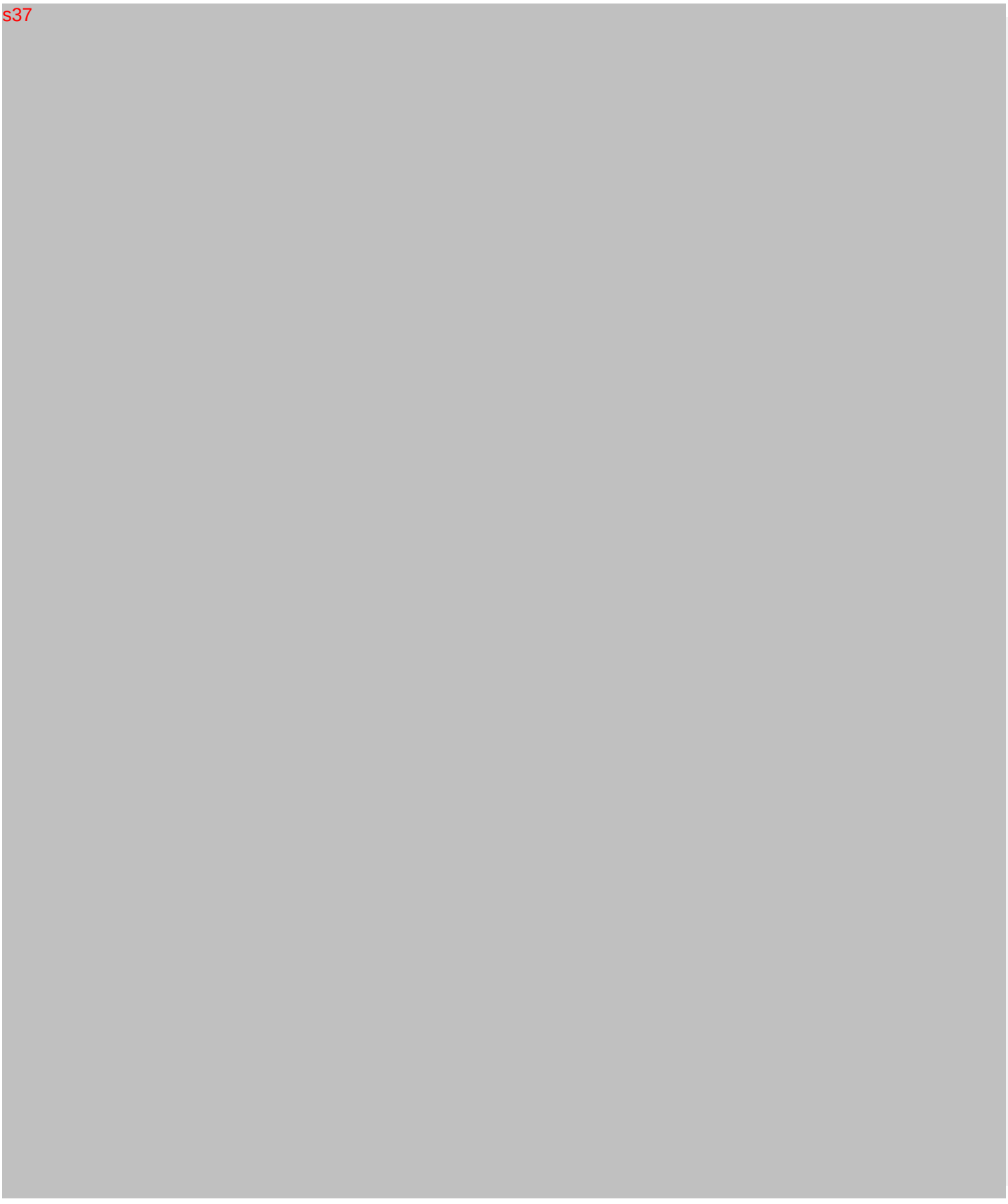

s37

s37


s37

s37




s37

s22

From: Patteson, Carolyn <Carolyn.Patteson@communications.gov.au>
Sent: Monday, 25 March 2019 5:28 PM
To: s22
Cc: James Penprase
Subject: Agenda for tomorrow [SEC=UNCLASSIFIED]
Attachments: Agenda - Summit of Violent Terrorist Material - 26 March 2019 - FINAL.docx

UNCLASSIFIED

Dear s22,
Please find attached the agenda for the meeting in Brisbane tomorrow. I look forward to seeing you both there.
Regards,

Carolyn Patteson
First Assistant Secretary / Content
Department of Communications and the Arts
P +61 2 6271 1418
s22
Email.carolyn.patteson@communications.gov.au
2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra, ACT 2601
communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

MEETING WITH DIGITAL PLATFORMS, INTERNET SERVICE PROVIDERS AND GOVERNMENT ON VIOLENT TERRORIST MATERIAL ONLINE

Date: Tuesday, 26 March 2019

Time: 1:00 to 3:00 pm

Venue: Level 31, 1 Eagle Street Waterfront Place, Brisbane, Queensland

AGENDA

Agenda	Timing	Description	Lead
1	1:00 – 1:05 pm (5 minutes)	Introduction	Prime Minister
2	1:05 – 1:15 pm (10 minutes)	Overview of expectations	Minister Fifield Minister Dutton Attorney General
3	1:15 – 1:30 pm (15 minutes)	Response from the digital platforms • Actions • Rules and standards • Lessons learned	Facebook Google Twitter
4	1:30 – 1:55 (25 minutes)	Response from the ISPs • Actions • Rules and standards • Lessons learned	Telstra Optus Vodafone TPG Comms Alliance
5	1:55 – 2:55 pm (60 minutes)	Facilitated discussion: improving outcomes and protections for the community • **Prevention and protection** – including detecting, blocking, and instantaneous and faster takedown options for violent terrorist material. • **Transparency** – improving transparency of the actions taken by platforms and ISPs in relation to violent terrorist material. • **Deterrence** – enhancing responsibility for the upload and distribution of violent terrorist material by individuals, platforms and ISPs.	All (led by Minister Fifield)
6	2:55 – 3:00 pm (5 minutes)	Close	Minister Fifield

KENNA Allison

From: Patteson, Carolyn <Carolyn.Patteson@communications.gov.au>
Sent: Monday, 25 March 2019 5:33 PM
To: s22 tpgtelecom.com.au
Cc: James Penprase
Subject: Agenda for meeting in Brisbane tomorrow [SEC=UNCLASSIFIED]
Attachments: Agenda - Summit of Violent Terrorist Material - 26 March 2019 - FINAL.docx

UNCLASSIFIED

Dear s22

Thank you for reaching out before and confirming that you will be attending the meeting in Brisbane tomorrow. The agenda for it is attached.

It is highlighted on top of the agenda, but it is being held from 1-3pm, Level 31, Waterfront Place, 1 Eagle St, Brisbane.

Please do not hesitate to contact me if I can be of any help in the meantime.

Regards,

Dr Carolyn Patteson
First Assistant Secretary / Content
Department of Communications and the Arts
P +61 2 6271 1418
s22
Email.carolyn.patteson@communications.gov.au
2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra, ACT 2601
communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

MEETING WITH DIGITAL PLATFORMS, INTERNET SERVICE PROVIDERS AND GOVERNMENT ON VIOLENT TERRORIST MATERIAL ONLINE

Date: Tuesday, 26 March 2019

Time: 1:00 to 3:00 pm

Venue: Level 31, 1 Eagle Street Waterfront Place, Brisbane, Queensland

AGENDA

Agenda	Timing	Description	Lead
1	1:00 – 1:05 pm (5 minutes)	Introduction	Prime Minister
2	1:05 – 1:15 pm (10 minutes)	Overview of expectations	Minister Fifield Minister Dutton Attorney General
3	1:15 – 1:30 pm (15 minutes)	Response from the digital platforms • Actions • Rules and standards • Lessons learned	Facebook Google Twitter
4	1:30 – 1:55 (25 minutes)	Response from the ISPs • Actions • Rules and standards • Lessons learned	Telstra Optus Vodafone TPG Comms Alliance
5	1:55 – 2:55 pm (60 minutes)	Facilitated discussion: improving outcomes and protections for the community • **Prevention and protection** – including detecting, blocking, and instantaneous and faster takedown options for violent terrorist material. • **Transparency** – improving transparency of the actions taken by platforms and ISPs in relation to violent terrorist material. • **Deterrence** – enhancing responsibility for the upload and distribution of violent terrorist material by individuals, platforms and ISPs.	All (led by Minister Fifield)
6	2:55 – 3:00 pm (5 minutes)	Close	Minister Fifield

KENNA Allison

From: Patteson, Carolyn <Carolyn.Patteson@communications.gov.au>
Sent: Monday, 25 March 2019 5:34 PM
To: s22
Cc: James Penprase
Subject: Agenda for tomorrow [SEC=UNCLASSIFIED]
Attachments: Agenda - Summit of Violent Terrorist Material - 26 March 2019 - FINAL.docx

UNCLASSIFIED

Dear John,
Please find attached the agenda for the meeting tomorrow in Brisbane. We look forward to seeing you there.
Regards,

Carolyn Patteson
First Assistant Secretary / Content
Department of Communications and the Arts
P +61 2 6271 1418
s22
Email.carolyn.patteson@communications.gov.au
2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra, ACT 2601
communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

MEETING WITH DIGITAL PLATFORMS, INTERNET SERVICE PROVIDERS AND GOVERNMENT ON VIOLENT TERRORIST MATERIAL ONLINE

Date: Tuesday, 26 March 2019

Time: 1:00 to 3:00 pm

Venue: Level 31, 1 Eagle Street Waterfront Place, Brisbane, Queensland

AGENDA

Agenda	Timing	Description	Lead
1	1:00 – 1:05 pm (5 minutes)	Introduction	Prime Minister
2	1:05 – 1:15 pm (10 minutes)	Overview of expectations	Minister Fifield Minister Dutton Attorney General
3	1:15 – 1:30 pm (15 minutes)	Response from the digital platforms • Actions • Rules and standards • Lessons learned	Facebook Google Twitter
4	1:30 – 1:55 (25 minutes)	Response from the ISPs • Actions • Rules and standards • Lessons learned	Telstra Optus Vodafone TPG Comms Alliance
5	1:55 – 2:55 pm (60 minutes)	Facilitated discussion: improving outcomes and protections for the community • **Prevention and protection** – including detecting, blocking, and instantaneous and faster takedown options for violent terrorist material. • **Transparency** – improving transparency of the actions taken by platforms and ISPs in relation to violent terrorist material. • **Deterrence** – enhancing responsibility for the upload and distribution of violent terrorist material by individuals, platforms and ISPs.	All (led by Minister Fifield)
6	2:55 – 3:00 pm (5 minutes)	Close	Minister Fifield

KENNA Allison

From: Patteson, Carolyn <Carolyn.Patteson@communications.gov.au>
Sent: Monday, 25 March 2019 5:37 PM
To: s22
Cc: James Penprase
Subject: Agenda for tomorrow [DLM=For-Official-Use-Only]
Attachments: Agenda - Summit of Violent Terrorist Material - 26 March 2019 - FINAL.docx

For Official Use Only

Dear s22

I'm sorry we haven't spoken again in the last couple of days, but please find attached the agenda for the meeting in Brisbane tomorrow. I look forward to meeting you in person then. Please reach out if there is anything further I can provide in the meantime.

Regards,

Carolyn Patteson
First Assistant Secretary / Content
Department of Communications and the Arts
P +61 2 6271 1418
s22
Email.carolyn.patteson@communications.gov.au
2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra, ACT 2601
communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

MEETING WITH DIGITAL PLATFORMS, INTERNET SERVICE PROVIDERS AND GOVERNMENT ON VIOLENT TERRORIST MATERIAL ONLINE

Date: Tuesday, 26 March 2019

Time: 1:00 to 3:00 pm

Venue: Level 31, 1 Eagle Street Waterfront Place, Brisbane, Queensland

AGENDA

Agenda	Timing	Description	Lead
1	1:00 – 1:05 pm (5 minutes)	Introduction	Prime Minister
2	1:05 – 1:15 pm (10 minutes)	Overview of expectations	Minister Fifield Minister Dutton Attorney General
3	1:15 – 1:30 pm (15 minutes)	Response from the digital platforms • Actions • Rules and standards • Lessons learned	Facebook Google Twitter
4	1:30 – 1:55 (25 minutes)	Response from the ISPs • Actions • Rules and standards • Lessons learned	Telstra Optus Vodafone TPG Comms Alliance
5	1:55 – 2:55 pm (60 minutes)	Facilitated discussion: improving outcomes and protections for the community • **Prevention and protection** – including detecting, blocking, and instantaneous and faster takedown options for violent terrorist material. • **Transparency** – improving transparency of the actions taken by platforms and ISPs in relation to violent terrorist material. • **Deterrence** – enhancing responsibility for the upload and distribution of violent terrorist material by individuals, platforms and ISPs.	All (led by Minister Fifield)
6	2:55 – 3:00 pm (5 minutes)	Close	Minister Fifield

Doc 13

s22

From: Patteson, Carolyn <Carolyn.Patteson@communications.gov.au>
Sent: Monday, 25 March 2019 5:29 PM
To: s22
Cc: James Penprase
Subject: Agenda for tomorrow [SEC=UNCLASSIFIED]
Attachments: Agenda - Summit of Violent Terrorist Material - 26 March 2019 - FINAL.docx

UNCLASSIFIED

Dear s22

Please find attached the agenda for the meeting in Brisbane tomorrow. We look forward to seeing you there.

Regards,

Carolyn Patteson
First Assistant Secretary / Content
Department of Communications and the Arts
P +61 2 6271 1418
s22
Email.carolyn.patteson@communications.gov.au
2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra, ACT 2601
communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

MEETING WITH DIGITAL PLATFORMS, INTERNET SERVICE PROVIDERS AND GOVERNMENT ON VIOLENT TERRORIST MATERIAL ONLINE

Date: Tuesday, 26 March 2019

Time: 1:00 to 3:00 pm

Venue: Level 31, 1 Eagle Street Waterfront Place, Brisbane, Queensland

AGENDA

Agenda	Timing	Description	Lead
1	1:00 – 1:05 pm (5 minutes)	Introduction	Prime Minister
2	1:05 – 1:15 pm (10 minutes)	Overview of expectations	Minister Fifield Minister Dutton Attorney General
3	1:15 – 1:30 pm (15 minutes)	Response from the digital platforms • Actions • Rules and standards • Lessons learned	Facebook Google Twitter
4	1:30 – 1:55 (25 minutes)	Response from the ISPs • Actions • Rules and standards • Lessons learned	Telstra Optus Vodafone TPG Comms Alliance
5	1:55 – 2:55 pm (60 minutes)	Facilitated discussion: improving outcomes and protections for the community • **Prevention and protection** – including detecting, blocking, and instantaneous and faster takedown options for violent terrorist material. • **Transparency** – improving transparency of the actions taken by platforms and ISPs in relation to violent terrorist material. • **Deterrence** – enhancing responsibility for the upload and distribution of violent terrorist material by individuals, platforms and ISPs.	All (led by Minister Fifield)
6	2:55 – 3:00 pm (5 minutes)	Close	Minister Fifield

KENNA Allison

From: Patteson, Carolyn <Carolyn.Patteson@communications.gov.au>
Sent: Monday, 25 March 2019 5:25 PM
To: s22 twitter.com
Cc: James Penprase
Subject: Agenda for tomorrow [SEC=UNCLASSIFIED]
Attachments: Agenda - Summit of Violent Terrorist Material - 26 March 2019 - FINAL.docx

UNCLASSIFIED

Dear Kara,
Please find attached the agenda for the meeting in Brisbane tomorrow. We look forward to seeing you there.
Regards,

Carolyn Patteson
First Assistant Secretary / Content
Department of Communications and the Arts
P +61 2 6271 1418
s22
Email.carolyn.patteson@communications.gov.au
2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra, ACT 2601
communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

MEETING WITH DIGITAL PLATFORMS, INTERNET SERVICE PROVIDERS AND GOVERNMENT ON VIOLENT TERRORIST MATERIAL ONLINE

Date: Tuesday, 26 March 2019

Time: 1:00 to 3:00 pm

Venue: Level 31, 1 Eagle Street Waterfront Place, Brisbane, Queensland

AGENDA

Agenda	Timing	Description	Lead
1	1:00 – 1:05 pm (5 minutes)	Introduction	Prime Minister
2	1:05 – 1:15 pm (10 minutes)	Overview of expectations	Minister Fifield Minister Dutton Attorney General
3	1:15 – 1:30 pm (15 minutes)	Response from the digital platforms • Actions • Rules and standards • Lessons learned	Facebook Google Twitter
4	1:30 – 1:55 (25 minutes)	Response from the ISPs • Actions • Rules and standards • Lessons learned	Telstra Optus Vodafone TPG Comms Alliance
5	1:55 – 2:55 pm (60 minutes)	Facilitated discussion: improving outcomes and protections for the community • **Prevention and protection** – including detecting, blocking, and instantaneous and faster takedown options for violent terrorist material. • **Transparency** – improving transparency of the actions taken by platforms and ISPs in relation to violent terrorist material. • **Deterrence** – enhancing responsibility for the upload and distribution of violent terrorist material by individuals, platforms and ISPs.	All (led by Minister Fifield)
6	2:55 – 3:00 pm (5 minutes)	Close	Minister Fifield

KENNA Allison

From: Patteson, Carolyn <Carolyn.Patteson@communications.gov.au>
Sent: Monday, 25 March 2019 5:30 PM
To: s22 Vodafone Australia; s22
Cc: James Penprase
Subject: Agenda for tomorrow [SEC=UNCLASSIFIED]
Attachments: Agenda - Summit of Violent Terrorist Material - 26 March 2019 - FINAL.docx

UNCLASSIFIED

Dear s22,
Please find attached the agenda for the meeting in Brisbane tomorrow. We look forward to meet with your CEO and Dan then.
Regards,

Carolyn Patteson
First Assistant Secretary / Content
Department of Communications and the Arts
P +61 2 6271 1418
s22
Email.carolyn.patteson@communications.gov.au
2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra, ACT 2601
communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

MEETING WITH DIGITAL PLATFORMS, INTERNET SERVICE PROVIDERS AND GOVERNMENT ON VIOLENT TERRORIST MATERIAL ONLINE

Date: Tuesday, 26 March 2019

Time: 1:00 to 3:00 pm

Venue: Level 31, 1 Eagle Street Waterfront Place, Brisbane, Queensland

AGENDA

Agenda	Timing	Description	Lead
1	1:00 – 1:05 pm (5 minutes)	Introduction	Prime Minister
2	1:05 – 1:15 pm (10 minutes)	Overview of expectations	Minister Fifield Minister Dutton Attorney General
3	1:15 – 1:30 pm (15 minutes)	Response from the digital platforms • Actions • Rules and standards • Lessons learned	Facebook Google Twitter
4	1:30 – 1:55 (25 minutes)	Response from the ISPs • Actions • Rules and standards • Lessons learned	Telstra Optus Vodafone TPG Comms Alliance
5	1:55 – 2:55 pm (60 minutes)	Facilitated discussion: improving outcomes and protections for the community • **Prevention and protection** – including detecting, blocking, and instantaneous and faster takedown options for violent terrorist material. • **Transparency** – improving transparency of the actions taken by platforms and ISPs in relation to violent terrorist material. • **Deterrence** – enhancing responsibility for the upload and distribution of violent terrorist material by individuals, platforms and ISPs.	All (led by Minister Fifield)
6	2:55 – 3:00 pm (5 minutes)	Close	Minister Fifield

Doc 16

From: Eccles, Richard <Richard.Eccles@communications.gov.au>
Sent: Monday, 25 March 2019 8:31 AM
To: Patteson, Carolyn; James Penprase
Cc: Mrdak, Mike
Subject: FW: Brad Smith blog [SEC=UNCLASSIFIED]
Attachments: NZ Draft Blog Version 7.docx

UNCLASSIFIED

This is a good article from Microsoft – clearly indicates their intent to be serious in terms of change following Christchurch.

I've spoken with s47F – this will be the basis of a discussion with them later in the week. They cannot do tomorrow – Brad Smith had previously committed to be in NZ – and that understandably takes priority.

We should add this to the pack for the Min. I will send also to

Richard

Richard Eccles
Deputy Secretary / Content, Arts, Strategy and Research
Department of Communications and the Arts
P +61 2 6271 1534 s22

Richard.eccles@communications.gov.au

s22

INTERNATIONAL YEAR OF INDIGENOUS LANGUAGES
www.arts.gov.au/IY2019

I would like to acknowledge the traditional custodians of this land on which we meet, work and live. I recognise and respect their continuing connection to the land, waters and communities. I pay my respect to Elders past and present and to all Aboriginal and Torres Strait Islanders.

communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

From: [s22 @microsoft.com]
Sent: Sunday, 24 March 2019 11:21 AM
To: Eccles, Richard
Subject: Brad Smith blog

Hey Richard

I wanted to share with you a blog Brad is proposing to post tomorrow morning on Microsoft's thoughts post Christchurch.

It would be great to get your thoughts on this - do you think the tone hits the mark? Whilst this is not predominantly an issue on our platform we are trying to take a leadership role within the industry but at the same time we want to be politically sensitive.

Any thoughts you have on this would be greatly appreciated.

s22

DRAFT: Version 7

A Tragedy that Calls for More than Words:
The Need for the Tech Sector to Learn and Act After Events in New Zealand

Four months ago, when our team at Microsoft first made plans for a visit to New Zealand that began yesterday, we did not expect to arrive on the heels of a violent attack that would kill innocent civilians, horrify a nation and shock the world. Like so many other people around the globe, across Microsoft we mourn the victims and our hearts go out to their families and loved ones. This includes two of the individuals killed who were part of the broader Microsoft partner community.

We appreciate the gravity of the moment. This is a time when the world needs to stand with New Zealand.

Words alone are not enough. Across the tech sector, we need to do more. Especially for those of us who operate social networks or digital communications tools or platforms that were used to amplify the violence, it's clear that we need to learn from and take new action based on what happened in Christchurch.

As an industry, tech companies created new services to bring out the best – not the worst – in people. To break down boundaries, not sow division. But as with virtually every technology ever invented, people are using digital services for both good and ill. Unfortunately, individuals are using online platforms to bring out the darkest sides of humanity.

The problem has multiple dimensions. We've seen online platforms and digital tools used to help recruit people to violent ideologies. These same tools have been used to incite and organize violent attacks on innocent people. And as we saw in Christchurch, we've seen digital platforms used to amplify the impact of attacks through the widespread sharing of violent images and videos around the world.

While Microsoft's services were not used nearly to the same degree as other platforms to spread the video from Christchurch, we too need to take stock. Regardless of whether a particular technology played a big, small or no part in this event, across the industry we all can and need to be part of the solution. There is a role for everyone to play. That should be one of the most important lessons from Christchurch.

What should we do?

To start, we should acknowledge that no one yet has all the answers. This is an area in which companies across the tech sector need to learn, think, work and act together. Competition is obviously indispensable to a vibrant technology sector. But when it comes to saving human lives and protecting human rights, we should act in a united way and enable every company large and small to move faster.

Ultimately, we need to develop an industry-wide approach that will be principled, comprehensive and effective. The best way to pursue this is to take new and concrete steps quickly in ways that build upon what already exists.

There are in fact important recent steps on which we can build. Just over two years ago, thanks in part to the leadership and urging of the British and the European Commission, four companies – YouTube, Facebook, Twitter and Microsoft – came together to create the Global Internet Forum to Counter Terrorism (GIFCT). Among other things, the group's members have created a shared hash database of terrorist content and developed photo and video matching and text-based machine learning techniques to identify and thwart the spread of violence on their platforms. These technologies were used more than a million times in 24 hours to stop the distribution of the video from Christchurch.

While these are vital steps, one of the lessons from New Zealand is that the industry rightly will be judged not only by what it prevented, but by what it failed to stop. And from this perspective, there is clearly much more that needs to be done. As Prime Minister Ardern noted last week, gone are the days when tech companies can think of their platforms akin to a postal service without regard to the responsibilities embraced by other content publishers. Even if the law in some countries gives digital platforms an exemption from decency requirements, the public rightly expects tech companies to apply a higher standard.

There are at least three areas where we should focus our efforts.

First, we need to focus on prevention. We need to take new steps to stop perpetrators from posting and sharing acts of violence against innocent people. New and more powerful technology tools can contribute even more than they have already. We must work across the industry to continue advancing technologies like PhotoDNA and other AI-based image scanning techniques to identify and apply digital hashes (a kind of digital identifier). This can enable us more granularly to improve the ability to remove violent video content. For example, while video hashes allow automated tools to detect additional copies already flagged as violent, we need to further improve this technology so that it can better identify and catch *edited* versions of the same video.

We should also pursue new steps beyond the posting of content. For example, we should explore browser-based solutions – building on ideas like safe search – to block the accessing of such content at the point when people attempt to view it.

We should pursue all these steps with a community spirit that will share our learning and technology across the industry through open source and other collaborative mechanisms. This is the only way for the tech sector as a whole to do what will be required to be more effective.

We also should recognize that technology cannot solve this problem by itself. We need to consider and discuss additional controls or other measures that human beings working at tech companies should apply when it comes to the posting of this type of violence. There are legal responsibilities that need to be considered as well. It's a complicated topic with important sensitivities in some parts of the tech sector. But it's an issue whose importance can no longer be avoided.

Second, we need to respond more effectively to moments of crisis. Even with better progress, we cannot afford to assume that there will never be another tragedy. The tech sector should consider creating a "major event" protocol, in which technology companies would work from a joint virtual command center during a major incident. This would enable all of us to share information more quickly and directly, helping each platform and service to move more proactively, while simultaneously ensuring that we avoid restricting communications that are in the public interest, such as reporting from news organizations.

We should also discuss whether to define a category of agreed "confirmed events," upon which tech companies would jointly institute additional processes to detect and prevent sharing of these types of violent content. We should consider the pros and cons, for example, of the short-term application in these circumstances of a brief delay for some live video streaming that would better enable efforts to identify and stop this content, while exempting from this restriction live reporting by journalists.

Finally, we should work more broadly to advance digital civility online. As many have noted, while much of the focus in recent days rightly has been on the use of contemporary tools to amplify this violence, the language of hate has existed for decades and even centuries. While we must take new and urgent technology steps to improve online safety, we will never succeed entirely if people fail to address the deeper problems or conclude that the standards of civility they follow in the real world fail to apply in cyberspace.

Working on digital civility has been a passion for many employees at Microsoft, who have recognized that the online world inevitably reflects the best and worst of what people learn offline. In many ways, anonymity on the internet can free people to speak and behave in ways they never would in person. This is why we believe it's important to continue to promote four tenets to live by when engaging online. Namely, we all need to treat others how we want to be treated, respect each other's differences, pause before replying, and stand up for ourselves and for others. This too is an area on which we can build further.

We all need to come together and move faster.

This is the type of serious challenge that requires broad discussion and collaboration with people in governments and across civil society around the world. It also requires us to expand and deepen industry wide groups focused on these issues, including key partners from outside the industry.

Finally, we hope this will become a moment that brings together leaders from across the tech sector.

It's sometimes easy amidst controversy for those not on the hot seat to remain silent and on the sideline. But we believe this would be a mistake. Across the tech sector we can all contribute ideas, innovate together and help develop more effective approaches.

The question is not just what technology did to exacerbate this problem, but what technology and tech companies can do to help solve it. Put in these terms, there is room – and a need – for everyone to help.

Doc 17

KENNA Allison

From: Penprase, James <James.Penprase@communications.gov.au>
Sent: Monday, 25 March 2019 11:14 AM
To: s47F
Cc: Richard Eccles; Patteson, Carolyn; s47F
s22
Subject: RE: Summit on Violent Terrorist Material - Briefing Pack [DLM=For-Official-Use-Only]
Attachments: DRAFT Online Safety Charter.pdf; Australia's media laws and regulations applicable to digital platforms.docx; Master Briefing Pack.docx

For Official Use Only

Dear Luke, Damien

Please find attached a full briefing pack for the Minister for Tuesday's Summit. Two background documents are also included.

This morning we are calling the relevant industry participants to confirm the purpose of the summit and the expectations of Government. We will also be providing them with a copy of the agenda.

Any questions, or if you need anything else, please let us know.

Regards

James

James Penprase
Assistant Secretary / Digital Media and Copyright
Department of Communications and the Arts
P +61 2 6271 1932
s47F
james.penprase@communications.gov.au

2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra, ACT 2601

AUSTRALIA'S MEDIA LAWS AND REGULATIONS APPLICABLE TO DIGITAL PLATFORMS

March 2019

For Official Use Only

Contents

Introduction

The provision of online media services in Australia is governed by a broad statutory framework. This generally extends to services based overseas but available to consumers in Australia. The Australian Government's expectation is that digital platforms, such as search engine providers, social media platforms and other aggregators of digital content, will comply with these laws and regulations, including by actively cooperating with Australian regulators.

This paper outlines the key elements of this framework, and provides links to further information.

Electoral communications and authorisation requirements

Laws/regulations/codes
Commonwealth Electoral Act 1918
Commonwealth Electoral (Authorisation of Voter Communication) Determination 2018
Referendum (Machinery Provisions) Act 1984
*Australian Broadcasting Corporation Act 1983**
*Broadcasting Services Act 1992**
*Special Broadcasting Service Act 1991**
**(For TV and radio only):*

Under the above laws, a person intending to communicate regarding an electoral, referendum or political matter (electoral communication) must ensure the communication is appropriately authorised. An electoral communication is the communication of 'electoral matter'. That is, a matter that is communicated, or intended to be communicated, for the dominant purpose of influencing the way electors vote in an election of a member of the House of Representatives or of Senators for a State or Territory.

The regime is applicable to online content that appears on a digital platform. It will apply if there is the communication of 'electoral matter':

- in the form of 'paid for' advertisements, including where all or only part of the distribution or production of the advertisement was 'paid for';
- in the form of promotional items, such as stickers, fridge magnets, leaflets, flyers, pamphlets, notices, posters and how-to-vote cards; or
- by, or on behalf of, a disclosure entity, that is intended to affect voting in a federal election.

More information is available at the following website:
https://www.aec.gov.au/About_AEC/Publications/Backgrounders/authorisation.htm.

Foreign Interference

Laws/regulations/codes
Foreign Influence Transparency Scheme Act 2018

The scheme in the *Foreign Influence Transparency Scheme Act 2018* introduces registration obligations for persons and entities who have arrangements with, and undertake certain activities on behalf of, foreign principals. Whether a person or entity is required to register will depend on who the foreign principal is, the nature of the activities undertaken, the purpose for which the activities are undertaken, and in some cases, whether the person has held a senior public position in Australia.

A digital platform will be subject to the scheme provided all requirements under the scheme are met and no exemptions apply. The requirement to register will be applicable to digital platforms if they engage in registrable activities including parliamentary lobbying, general political lobbying, communications activity or disbursement activity.

More information is available at the following websites:
Attorney-General's Department (www.ag.gov.au)
Australian Federal Police (www.afp.gov.au)

Online safety – prohibited content

Laws/regulations/codes
Schedules 5 and 7 of the Broadcasting Services Act 1992

Schedules 5 and 7 of the *Broadcasting Services Act 1992* contain a legislated take-down regime supported by industry codes that enable filtering (voluntary) through the Family Friendly Filter scheme (Communications Alliance has responsibility for the industry codes). The Scheme distinguishes between content hosted in Australia and content hosted overseas.

The regime applies to content accessed through the internet, mobile phones and convergent devices, and applies to content delivered through emerging content services such as subscription-based internet portals, chat rooms, live audio-visual streaming, and link services.

In 2017-18, the Office of the eSafety Commissioner referred 10,229 items of internet content hosted overseas to filter vendor.

More information is available at the following website:
https://www.communications.gov.au/policy/policy-listing/online-content-regulation

Online safety – cyberbullying

Laws/regulations/codes
Enhancing Online Safety Act 2015

The *Enhancing Online Safety Act 2015* establishes a complaints service for young Australians who experience serious cyberbullying. It gives the Commissioner the power to investigate complaints about serious cyberbullying material targeted at an Australian child. It also establishes a two-tiered scheme for the rapid removal of cyberbullying material from participating social media services.

Google+, Facebook, Instagram and Youtube are 'Tier two services', which are legally required to comply with a notice issued by the eSafety Commissioner to remove cyberbullying material, or face civil penalties.

A civil penalties scheme applies to hosting service providers including providers of a social media service, relevant electronic services (messaging services) and designated internet services.

More information is available at the following website:
https://esafety.gov.au/esafety-information/esafety-issues/cyberbullying

Online safety – image-based abuse

Laws/regulations/codes
Enhancing Online Safety Act 2015 *Criminal Code Act 1995, ss 474.17 and 474.17A* *State/Territory laws*

The *Enhancing Online Safety Act 2015* establishes a civil penalties scheme for the non-consensual sharing of intimate images. The civil penalties scheme applies to hosting service providers including providers of a social media service, relevant electronic services (messaging services) and designated internet services.

The *Criminal Code Act 1995* contains criminal offences relating to using a carriage service to menace, harass or cause offence, including aggravated offences involving private sexual material.

More information is available at the following website:
https://www.esafety.gov.au/image-based-abuse/legal/whats-the-law-in-my-state-territory

Copyright

Laws/regulations/codes
Copyright Act 1968

The *Copyright Act 1968* enables copyright owners to privately enforce their rights in Australian courts through the following actions:

- civil actions for direct or authorising copyright infringement; and
- injunctions to block access to foreign pirate websites.

Australian copyright owners have also used the US 'safe harbour' scheme to request the takedown of infringing content from online service providers, including digital platforms (e.g. Youtube).

Platforms containing user generated content have been successfully sued in Australia for direct and authorising copyright infringement (see *Pokemon v Redbubble* [2017] FCA 1541[1]). More information about possible copyright infringement issues relating to user generated content is available at: https://www.copyright.org.au/ACC_Prod/ACC/Information_Sheets/Websites___User-Generated_Content.aspx?WebsiteKey=8a471e74-3f78-4994-9023-316f0ecef4ef

Defamation

Laws/regulations/codes
Nationally-uniform State defamation law (e.g. NSW *Defamation Act 2005*)

Defamation is a communication from one person to at least one other that harms the reputation of an identifiable third person, where the communicator (the publisher) has no legal defence. A complainant can take civil action against the publisher of defamatory material.

Australian defamation laws are applicable to digital platforms, such as social media services. For example, the Australian High Court has ruled that a defamation case can be brought against Google LLC in Australia (*Trkulja v Google LLC* [2018] HCA 25). In terms of social media platforms, the Federal Court of Australia has also awarded damages for tweets that contained defamatory material (Hockey v Fairfax Media Publications Pty Limited [2015] FCA 652).

[1] See at: http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2017/2017fca1541

Privacy

Laws/regulations/codes
Privacy Act 1988

Under the *Privacy Act 1988*, Australian Privacy Principle entities (APP entities), are subject to the following key requirements relating to personal information:

- publishing privacy policies;
- rules relating to collection, notification, use and disclosure;
- direct marketing;
- security; and
- access to, and correction of, information.

Serious data breaches are required to be reported to Office of the Australian Information Commissioner (OAIC) and affected parties. Complainants can make complaint about privacy breaches to the OAIC which can also initiate its own investigations.

Digital Platforms with an Australian presence will be 'APP entities' and subject to the Privacy Act unless they are a small business. For example, in April 2018, the OAIC opened a formal investigation into Facebook, following confirmation from Facebook that the information of over 300,000 Australian users may have been acquired and used without authorisation. https://www.oaic.gov.au/media-and-speeches/statements/facebook-and-cambridge-analytica

More information is available at the following website:
www.oaic.gov.au

Advertising

Laws/regulations/codes
Codes of conduct adopted by: • Australian Association of National Advertisers (AANA) • Australian Food and Grocery Council (AFGC) • Federal Chamber of Automotive Industries (FCAI)

Advertisements in Australia are self-regulated under industry codes and complaints are handled by Ad Standards.

Ad Standards must take into account the relevant industry codes when evaluating complaints from the public regarding advertisements. If the Ad Standards Community Panel upholds a complaint, it will ask an advertiser to remove or amend the offending advertisement as soon as possible. The decisions of Ad Standards are not underpinned by any legislative powers.

Digital platforms such as Google and Facebook are members of the Australian Association of National Advertisers, and new digital platforms that begin operating in Australia that use advertisements would be expected to also become part of these self-regulatory arrangements.

More information is available at the following website:
Australian Association of National Advertisers (www.aana.com.au/)
Ad Standards (www.adstandards.com.au/)

Gambling promotions during live sports

Laws/regulations/codes
Schedule 8 to the *Broadcasting Services Act 1992* *Broadcasting Services (Online Content Service Provider Rules) 2018*

The *Broadcasting Services (Online Content Service Provider Rules) 2018* seek to limit the exposure to child audiences of all gambling promotional content during live sporting events streamed online. There are restrictions on gambling advertising during live sport at all times, but stricter requirements between 5.00 am to 8.30 pm when children are more likely to be watching.

These rules would apply to digital platforms as they apply to online content services that provide live (or near live) coverage of sporting events, unless the service falls within a particular exemption.

More information is available at the following website:
https://www.acma.gov.au/Industry/Internet/Internet-content/Gambling-advertising/faqs-gambling-ads-during-live-streamed-sports

Illegal interactive gambling services

Laws/regulations/codes
Interactive Gambling Act 2001

The *Interactive Gambling Act 2001* (IGA) creates an offence to provide or advertise prohibited or unlicensed interactive gambling services to Australian residents.

Prohibited interactive gambling services include online casinos, online slot machines and online wagering services that accept 'in-play' betting on sports events. Unlicensed regulated interactive gambling services include online wagering services provided without a licence issued by an Australian state or territory. The IGA also prohibits certain interactive wagering services providers from providing or facilitating the provision of credit to their customers.

The IGA would apply to digital platforms proposing to provide the above services to customers in Australia.

More information is available at the following website: (https://www.acma.gov.au/Industry/Internet/Internet-content/Interactive-gambling/internet-gambling)

DEPARTMENT OF COMMUNICATIONS AND THE ARTS

To: Minister Fifield

MEETING WITH DIGITAL PLATFORMS, INTERNET SERVICE PROVIDERS (ISP's) AND GOVERNMENT ON VIOLENT TERRORIST MATERIAL ONLINE

Date: Tuesday, 26 March 2019
Time: 1:00 to 3:00 pm
Venue: Level 31, 1 Eagle Street Waterfront Place, Brisbane, Queensland

BRIEFING PACK

1. Agenda
2. Key Attendees
3. Potential Actions and Commitment (identified by Commonwealth Agencies)
4. Annotated Agenda and Briefing
   - Background note
   - Speaking points
   - Issues to propose to platforms and ISPs
5. Further Background Material
   - Australia's online content regulation
   - Action taken by platforms and ISPs
   - Draft blog from Microsoft (not yet published)
   - Excerpts from relevant regulation

Other material

- Draft Online Safety Charter
- Australia's media laws and regulations applicable to digital platforms

PART 1: AGENDA

Agenda	Timing	Description	Lead
1	1:00 – 1:05 pm (5 minutes)	Introduction	Prime Minister
2	1:05 – 1:15 pm (10 minutes)	Overview of expectations	Minister Fifield Minister Dutton Attorney General
3	1:15 – 1:30 pm (15 minutes)	Response from the digital platforms · Actions · Rules and standards · Lessons learned	Facebook Google Twitter
4	1:30 – 1:55 (25 minutes)	Response from the ISPs · Actions · Rules and standards · Lessons learned	Telstra Optus TPG Vodafone Comms Alliance
5	1:55 – 2:55 pm (60 minutes)	Facilitated discussion: improving outcomes and protections for the community · Prevention and protection – including detecting, blocking, and instantaneous and faster takedown options for violent terrorist material. · Transparency – improving transparency of the actions taken by platforms and ISPs in relation to violent terrorist material. · Deterrence – enhancing responsibility for the upload and distribution of violent terrorist material by individuals, platforms and ISPs.	All (led by Minister Fifield)
6	2:55 – 3:00 pm (5 minutes)	Close	Minister Fifield

PART 2: KEY Attendees

Note: We have reiterated to platforms the importance of sending people who are in a position to discuss these matters and commit to tangible action as a result. Some attendees might change.

Ministers

1. Prime Minister
2. Minister for Communications and the Arts
3. Attorney-General
4. Minister for Home Affairs

Government

5. PM&C – Martin Parkinson
6. DoCA – Mike Mrdak
7. Home Affairs – Mike Pezullo
8. AGD – Chris Moraitis
9. ASIO – Duncan Lewis
10. AFP – Andrew Colvin
11. OeSC – Julie Inman-Grant
12. ACMA – Nerida O'Loughlin

NZ Officials

13. Deputy High Commissioner to Australia - Mr Llewellyn Roberts

Platforms

14. Google s47F
15. Facebook – s47F
    s47F
16. Twitter - s47F

ISPs

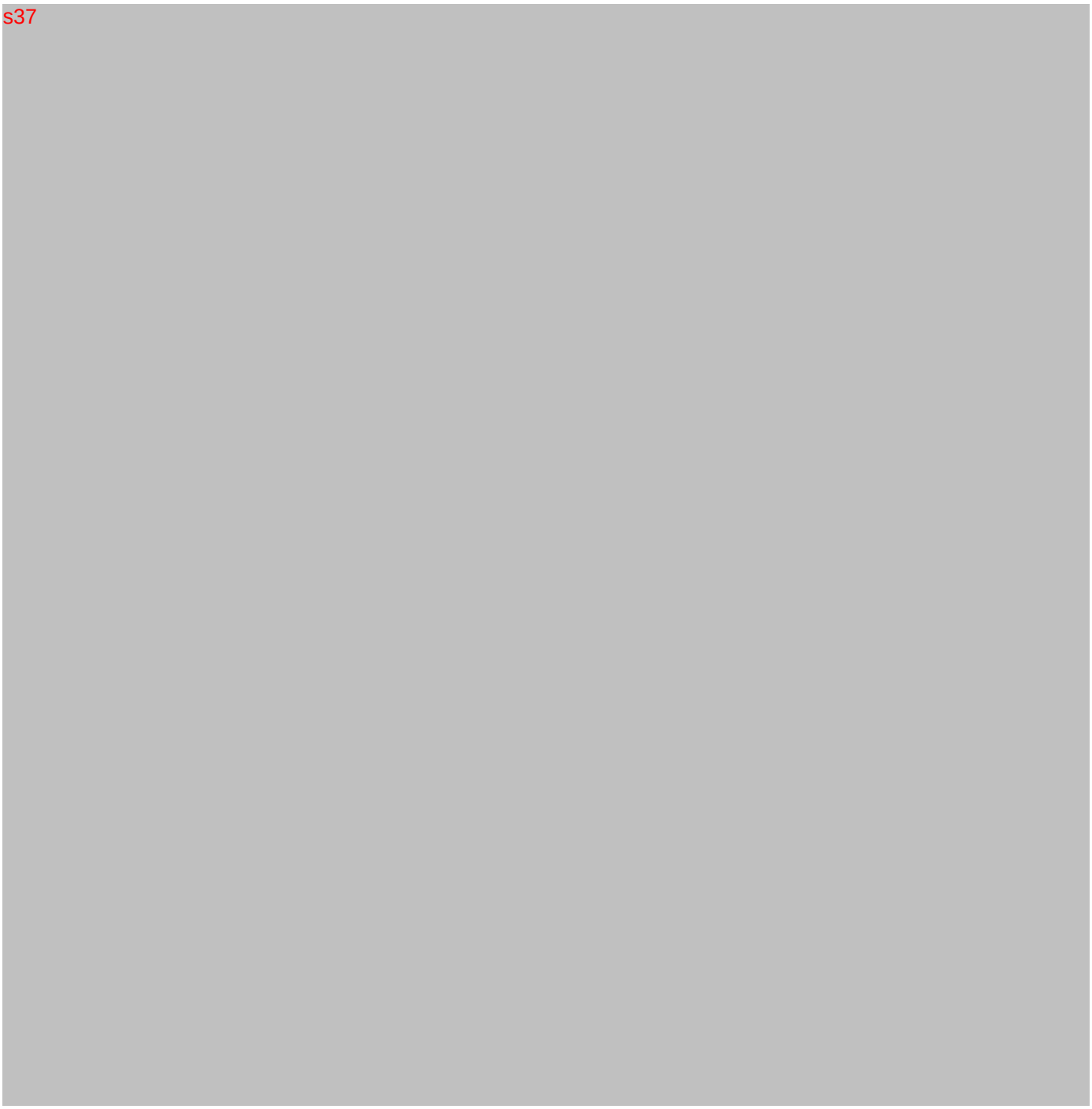
17. Telstra – (s47F
    Govt Relations)
18. Vodafone – s47F
19. Optus – s47F
20. TPG – s47F (TBC)
21. Comms Alliance – s47F

PART 3: POTENTIAL ACTIONS AND COMMITMENTS

Note: these possible actions have been identified by Commonwealth Agencies as options to put to the ISPs and Platforms for specific, tangible action. Agenda Items 3, 4 and 5 cover.

1. PREVENTION AND PROTECTION – DETECTING, BLOCKING, AND INSTANTANEOUS AND FASTER TAKEDOWN OPTIONS FOR VIOLENT TERRORIST MATERIAL

s37



f) Product design – platforms to commit to incorporating safety protections into their services from the design phase to mitigate risks (Safety-by-Design).

2. TRANSPARENCY – IMPROVING TRANSPARENCY OF THE ACTIONS TAKEN BY PLATFORMS IN RELATION TO VIOLENT TERRORIST MATERIAL

g) Standards development – platforms to commit to engage broadly with in-country experts and key stakeholders in relation to the development and application of their own online safety standards and terms of use.

h) Reporting – platforms to compile and publish regular reports and data, specific to Australia, on:
   i. content controls, including the type of content is identified, moderated and/or prevented from being uploaded, how it was identified, and the action taken; and
   ii. complaints, including the number of complaints received, investigated and resolved, the time taken to resolve complaints, the category of complaint, the action taken and generalised demographic information (including, where known, age, geographic location of complainants), and any appeals/ arbitration processes.

3. DETERRENCE – ENHANCING RESPONSIBILITY FOR THE UPLOAD AND DISTRIBUTION OF VIOLENT TERRORIST MATERIAL BY INDIVIDUALS, PLATFORMS AND ISPs.

i) User reporting – platforms to deploy clear, visible and intuitive reporting mechanisms on live streaming services that are triaged immediately in relation to extreme violent content (in addition to suicide, terrorism and child sexual abuse material). Platforms to push reporting mechanisms and remind users of the importance of reporting content to keep others safe.

j) Moderators: Platforms to ensure they employ sufficient moderators to handle the volume of requests in accordance with timeframe expectations, and that these moderators have adequate support in dealing with this content.

k) Warning notices – platforms to issue warning notices to live streaming users who may be posting violent content that their service may be cut off.

l) Moderation triggers – platforms to implement 'moderation triggers' in circumstances where live-stream content on a platform service is drawn from anonymous sites such as 4chan or 8chan.

m) Disabling comments – platforms to agree to provide an option for site owners to turn off notifications / comments where they are experiencing high levels of offensive or violent commentary in response to the posting or reporting of content on their social media sites.

n) Predictive search – platforms to ensure that after a terrorist attack users are not prompted to search for live footage.

o) Problematic websites – platforms to demote content links to websites that host violent terrorist footage

PART 4: ANNOTATED AGENDA AND BRIEFING

Agenda	Timing	Description	Lead
1	1:00 – 1:05 pm (5 minutes)	Welcome	Prime Minister

PURPOSE OF ITEM

- Prime Minister to welcome attendees and outline the purpose of the Summit and its intended outcomes.

- The Prime Minister is expected to articulate the concerns of the Government in relation to the terrorist attack in New Zealand and the upload and dissemination of footage from the incident on social media and other websites.

Agenda	Timing	Description	Lead
2	1:05 – 1:15 pm (10 minutes)	Overview of expectations	Minister Fifield Minister Dutton Attorney-General Porter

PURPOSE OF ITEM

Ministers to outline their expectations from the Summit (around 2 minutes each).

TALKING POINTS

- (If PM present) I acknowledge Prime Minister Morrison – and I thank you for your leadership in progressing this Summit.
- (If Deputy High Commissioner of New Zealand is present) I also acknowledge the Deputy High Commissioner of New Zealand, Mr Llewellyn Roberts, and express my heartfelt condolences for the terrible events that occurred in Christchurch.
- My portfolio has played an active role in working with the platforms and the ISPs with respect to online safety. This is as it should be: online safety is a shared responsibility, with roles for individuals, industry and Government.
- We have regulated the platforms – for a simple reason: to protect Australia's best interests. In my portfolio we have done so in the areas of image-based abuse, offensive and harmful content, cyberbullying, online gambling, illegal interactive gambling products, copyright, piracy and electoral communications.
- Our classification system makes it clear what content should be banned. Content refused classification must be removed from circulation.
- I acknowledge the efforts of the platforms and ISPs to delete and block content from the Christchurch attack, and their willingness to cooperate with law enforcement agencies and Government in the wake of the attacks.
- Despite this, it is clear that more needs to be done, by all parties.
- Government must ensure that we have the right regulatory arrangements in place, and individuals, and the community, need to take responsibility for their actions online.
- But industry must do more to ensure that their services are not being weaponised by those that perpetrate such acts, and that this type of harmful content isn't able to be spread.
- That is what we are here to talk about today.
- As you know, we've sought to crystallise our expectations through the draft Online Safety Charter.
- The action we are looking for from industry is a subset of that work, relating specifically to violent terrorist material.
- As the Prime Minister has already outlined, we are seeking action in three areas:

  - Prevention and protection – including detecting, blocking, and instantaneous and faster takedown options for violent terrorist material.
  - Transparency – improving transparency of the actions taken by platforms and ISPs in relation to violent terrorist material.
  - Deterrence – enhancing responsibility for the upload and distribution of violent terrorist material by individuals, platforms and ISPs.

- Today we are seeking concrete actions and commitments from industry. If we don't get those, we will invariably need to turn to regulatory options. We've done so in the past, and won't hesitate to do so again.
- I hope today that we can agree on some tangible and practical measures to address the upload and dissemination of violent terrorist content, and curb the harm that this type of content to cause in our society.

Agenda	Timing	Description	Lead
3	1:15 – 1:30 pm (15 minutes)	Update from the digital platforms • Actions • Rules and standards • Lessons learned	Facebook Google Twitter

PURPOSE OF ITEM

For the digital platforms to provide a briefing on the actions taken in response to the attacks in Christchurch, the rules and standards that govern their services and lessons learned from the incident.

BACKGROUND: OUTLINE OF ACTIONS TAKEN BY INDUSTRY

s47G and s37

s47G and s37

s47G

Twitter

Twitter has not provided an update on the actions that it took in response to the attacker's video.

Twitter has been quoted in media reports as saying that the company had suspended the account of one of the suspects and was working to remove the video from its network, which violated its policies.

TALKING POINTS

- The Government appreciates that this heinous act in some respects caught all of us off guard. And as I noted earlier, we appreciate the efforts of the platforms and ISPs to delete and block content from the Christchurch attack, and their willingness to cooperate with law enforcement agencies and government in the wake of the attacks.

- Digital platforms are not the only places that this content was uploaded and shared. Sites like 4Chan, 8Chan and Kiwifarms were used by individuals to host this material.

- But the fact remains that the platforms – notably Facebook – were the **launching point** for the dissemination of this content by the perpetrator.

- The alleged gunman deliberately **exploited the openness of the platforms**, and used them as a means of **promoting this abhorrent act of terrorism**.

- Moreover, the platforms remain the key vehicles through which the community at larger discovers and shares content, including harmful content. With this scale and impact comes an unavoidable level of social responsibility.

POTENTIAL QUESTIONS

Facebook

a) Why did it take 29 minutes (12 minutes after the end of the video) for Facebook to begin the process of taking down copies of the video? How can this be improved?

b) Facebook has indicated that in the 24 hours following the incident, it has prevented the attempted upload of 1.2 million copies of the video, but than 300,000 slipped through. How did this happen?

c) How many attempted uploads of the video has Facebook blocked automatically (current figures), and how many has it had to take down once uploaded?

d) How many of those videos that required removal after upload needed to be reviewed by Facebook staff or contractors, and how many were removed with technology?

Google (YouTube)

a) How many searches related to the Christchurch attack occurred in the first 24 hours, and how many were seeking the video footage?

b) Did YouTube become aware of the existence of the video on its platform by user notification, advice from security agencies, or from internal sources?

c) When, precisely, did YouTube remove the first upload of the video footage, and how long after the attack was this?

d) How many attempted uploads of the video did YouTube block on the first 24 hours, and how many got through and needed to be removed once uploaded?

Twitter

a) Why hasn't Twitter provided some indication publically of the impact of the incident on its platform, and what actions it has taken?

b) How many times was the video uploaded by users to the Twitter platform in the first 24 hours of the incident? What action did Twitter take in relation to these uploads?

c) Did Twitter seek to block the upload of the video, and how soon after the incidence did this occur?

d) How many attempted uploads were blocked by Twitter, and how were they blocked?

e) How many times did users share links to the video footage? What action did Twitter take in relation to these tweets?

f) How many user accounts did you suspect or disable?

All

a) Did the platforms work together in relation to 'hashed versions' of the video? Was this through the auspices of the Global Internet Forum to Counter Terrorism, or some other mechanism? What were the results?

Agenda	Timing	Description	Lead
4	1:30 – 1:55 (25 minutes)	Update from the ISPs • Actions • Rules and standards • Lessons learned	Telstra Optus TPG Vodafone Communications Alliance

PURPOSE OF ITEM

- For ISPs to provide a briefing on the actions taken in response to the attacks in Christchurch, the rules and standards that govern their services and lessons learned from the incident.

BACKGROUND: OUTLINE OF ACTIONS TAKEN BY INDUSTRY

- Telstra, Optus and Vodafone have voluntarily blocked sites hosting the Christchurch shooting video. The role of TPG is unclear, as no statements have been located.

- The blocked sites included 4chan, 8chan, Liveleaks, Zerohedge and Kiwi Farms. There was significant criticism of the blocking of Zerohedge, s47G s47G

- ISPs have reportedly been working with blocked websites to restore access once the video had been taken down. Media reports also suggest that the telecommunications industry is hopeful that this summit will bring clarity over the government's expectations about how they would react to any terrorist material being shared widely in future.

TALKING POINTS

- I commend those of you (Telstra, Vodafone and Optus) who took action voluntarily in response to the events in New Zealand to block access to sites hosting the abhorrent content until it was removed.

- This has played an important role in reducing the spread of the content throughout the Australian community.

- I appreciate that industry would like guidance from Government about when and how to act.

- Today I hope we can make a start to clarifying these arrangements and the systems that should be in place should unfortunate situations like this arise in the future.

POTENTIAL QUESTIONS

a) How many websites have each of you blocked?

b) How many have removed the offending content, and has access been restored? What is the process and timeframe for restoring access?

c) Did the ISPs share information with each other about the decision to block sites voluntarily? Was there industry-wide coordination?

d) What about smaller ISPs – did they undertake any blocking?

e) Did TPG block any of the sites?

f) How do you think ISPs can play a stronger role in assisting to block content of the nature we saw – content that under any circumstances would be refused classification.

Agenda	Timing	Description	Lead
5	1:55 – 2:55 pm (60 minutes)	Facilitated discussion: improving outcomes and protections for the community. • Prevention and protection – including detecting, blocking, and instantaneous and faster takedown options for violent terrorist material. • Transparency – improving transparency of the actions taken by platforms and ISPs in relation to violent terrorist material. • Deterrence – enhancing responsibility for the upload and distribution of violent terrorist material by individuals, platforms and ISPs.	All (led by Minister Fifield)

PURPOSE OF ITEM

- To seek commitments from the digital platforms and telecommunication industries that they will lift their game and do more to deal proactively and decisively with inappropriate content.

- To discuss and agree specific proposals – those developed by Government and (if forthcoming) proposals from industry. You might choose to ask Facebook to go first – we understand they are prepared to make strong commitments.

PLEASE REFER TO MATERIAL AT ITEM 3 OF THIS PACK

TALKING POINTS

- I want to hear from industry now on specific commitments you are prepared to make now – here, in this room.

- We have some ideas which we are prepared to put forward – but my preference is to hear from you first.

- In responding, can we focus on specific commitments, relating to:

  a) Prevention and protection
  b) Transparency
  c) Deterrence

PREVENTION AND PROTECTION

- We have heard about the difficulty of moderating live streams featuring abhorrent content.

- But the issue remains – digital platforms have set up service that we know can be exploited by terrorists to reach mass audiences.

- We also know that if even one copy of a video can reach an audience – that content can then be copied and reposted.

TRANSPARENCY

- I note and welcome the various transparency reports published by many digital platforms.

- However, more granular detail would assist Government to assess the effectiveness of actions taken.

- For example – it is not helpful to provide the number of pieces of offensive content taken down, when we don't know the overall prevalence of graphic violence, hate speech or offensive content on the platform.

DETERRENCE

- Platforms are not just pipes that deliver content. There must be greater responsibility for the content that users can access, and minimum thresholds for content control and moderation.

- Disturbingly, the events in Christchurch have also demonstrated that there are individuals who will make a determined effort to edit and re-upload appalling content. There needs to be a clear message sent that this behaviour is unacceptable.

Agenda	Timing	Description	Lead
6	2:55 – 3:00 pm (5 minutes)	Close	Minister Fifield

PURPOSE OF ITEM

To conclude the discussion and summarise the key actions / commitments agreement through the Summit, and any further work / actions to the undertaken by the parties.

TALKING POINTS

- We are currently out for consultation on our On-Line Safety Charter. I would encourage all players here to outline the commitments made today in their submission.
- I will turn to (tba) to provide an overview of the commitments – to ensure we are all on the same page.
- The next steps will be pivotal. This cannot be the end of the conversation.

PART 5: BACKGROUND INFORMATION

ATTACHMENT 1
AUSTRALIAN ONLINE CONTENT ARRANGEMENTS

Australia's classification system to address violent and extreme material

- Australia has a robust domestic Classification Scheme for films, computer games and certain publications.
- Australia relies on the Scheme to provide safeguards on material deemed extremist in nature and where appropriate, a Refused Classification (RC) rating is applied for material submitted for classification. This includes content promoting, inciting or instructing matters of crime of violence.
- The RC category includes offensive depictions or descriptions of children and illegal content. However, it is important to note that what is considered prohibited/potential prohibited under Australian law may not be illegal in the jurisdiction where the content is hosted.
- The scheme is an inter-governmental arrangement whereby any changes to the scheme must be considered and agreed to by all ministers with responsibility for classification matters.

Legality of video

- The full-length video posted on 8Chan showing Tarrant's assault on the Al Noor Mosque in Riccarton would certainly fall within the RC category under the terror-advocacy provisions and the broader instruction in crime or violence provisions.
- There are several other versions of the attack video circulating, including an edited version that stops as Tarrant raises his shotgun to fire at worshippers standing at the door of the Al Noor Mosque.
- These edited versions – depending very much on the context in which it is provided – may not be considered sufficiently detailed to be regarded as pro-terror advocacy.
- It is arguable that some of the edited versions may, however, still be considered sufficiently detailed to fall within the RC crime instruction category, as they could be seen as showing instruction in tactics, techniques and procedures.

Mechanisms for takedown

- The eSafety Commissioner has the statutory power to direct Australian content hosts to remove prohibited online content if it is hosted in Australia under the Online Content Scheme.
- While the eSafety Office does not have the power under the Scheme to issue a takedown notice to Facebook, which is based in the United States, it does work cooperatively with digital platforms to request removal of material that is clearly illegal in Australia and other jurisdictions.

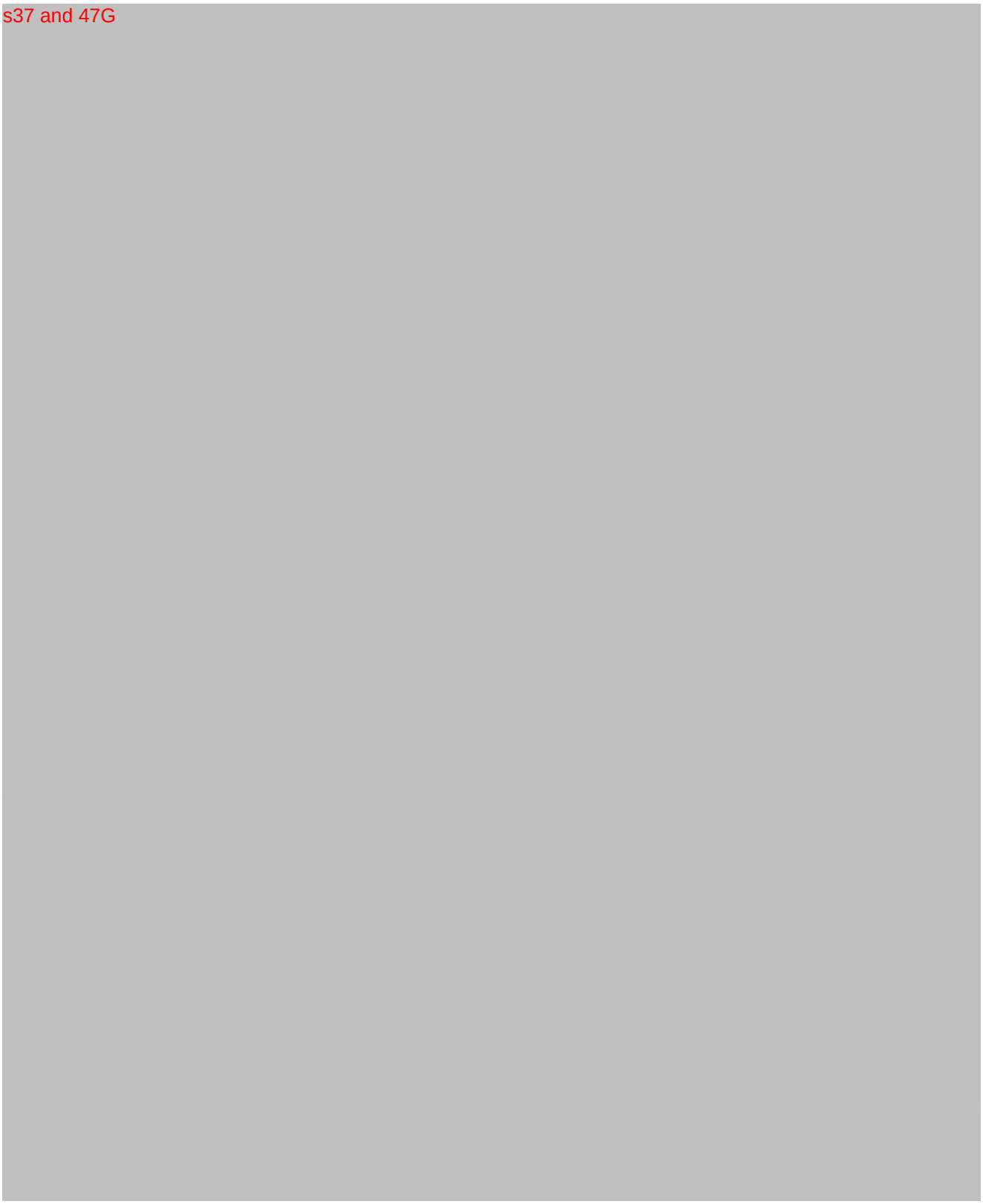
- Reports about prohibited online content are referred to local and international civil and law enforcement partners for investigation and removal.
- If prohibited online content depicts information that could lead to the identification of either a victim or perpetrator, an immediate report will be made by the Office to the AFP.
- Pro-extremist content is notified to the Australian Federal Police or to state law counter-terrorism commands.
- There are separate protocols that guide the relationship between law enforcement, intelligence agencies and platforms.
- Overseas-hosted prohibited content is notified to vendors of accredited Family Friendly Filters.

(Excerpts from relevant regulation are at Attachment 3)

ATTACHMENT 2
ACTION TAKEN BY INDUSTRY

Information received from Facebook

s37 and 47G



s37 and 47G

s47G

s47G and s37

[redacted]

Internet Service Provider response

- Media reports (Guardian Australia, AFR – 20 March) indicate that Telstra, Vodafone and Optus have all confirmed that they are actively blocking Australian customers from accessing websites that are hosting the Christchurch attacker's video.
- Communications Alliance Chief Executive John Stanton is quoted as saying: "Due to the extraordinary circumstances, several large ISPs in Australia have taken the decision to voluntarily implement temporary blocks of websites that continue to host footage of the Christchurch terrorist attack video. These ISPs have sought to balance community expectations to remove access to the video with the need to minimise any inconvenience that may arise from legitimate content being blocked as an unavoidable, temporary consequence."
- ISPs have been working with blocked websites to restore access once the video had been taken down.

ATTACHMENT 3
DRAFT BLOG FROM MICROSOFT (NOT YET RELEASED)

DRAFT: Version 7

A Tragedy that Calls for More than Words: The Need for the Tech Sector to Learn and Act After Events in New Zealand

Four months ago, when our team at Microsoft first made plans for a visit to New Zealand that began yesterday, we did not expect to arrive on the heels of a violent attack that would kill innocent civilians, horrify a nation and shock the world. Like so many other people around the globe, across Microsoft we mourn the victims and our hearts go out to their families and loved ones. This includes two of the individuals killed who were part of the broader Microsoft partner community.

We appreciate the gravity of the moment. This is a time when the world needs to stand with New Zealand.

Words alone are not enough. Across the tech sector, we need to do more. Especially for those of us who operate social networks or digital communications tools or platforms that were used to amplify the violence, it's clear that we need to learn from and take new action based on what happened in Christchurch.

As an industry, tech companies created new services to bring out the best – not the worst – in people. To break down boundaries, not sow division. But as with virtually every technology ever invented, people are using digital services for both good and ill. Unfortunately, individuals are using online platforms to bring out the darkest sides of humanity.

The problem has multiple dimensions. We've seen online platforms and digital tools used to help recruit people to violent ideologies. These same tools have been used to incite and organize violent attacks on innocent people. And as we saw in Christchurch, we've seen digital platforms used to amplify the impact of attacks through the widespread sharing of violent images and videos around the world.

While Microsoft's services were not used nearly to the same degree as other platforms to spread the video from Christchurch, we too need to take stock. Regardless of whether a particular technology played a big, small or no part in this event, across the industry we all can and need to be part of the solution. There is a role for everyone to play. That should be one of the most important lessons from Christchurch.

What should we do?

To start, we should acknowledge that no one yet has all the answers. This is an area in which companies across the tech sector need to learn, think, work and act together. Competition is obviously indispensable to a vibrant technology sector. But when it comes to saving human lives and protecting human rights, we should act in a united way and enable every company large and small to move faster.

Ultimately, we need to develop an industry-wide approach that will be principled, comprehensive and effective. The best way to pursue this is to take new and concrete steps quickly in ways that build upon what already exists.

There are in fact important recent steps on which we can build. Just over two years ago, thanks in part to the leadership and urging of the British and the European Commission, four companies – YouTube, Facebook, Twitter and Microsoft – came together to create the Global Internet Forum to Counter Terrorism (GIFCT). Among other things, the group's members have created a shared hash database of terrorist content and developed photo and video matching and text-based machine learning techniques to identify and thwart the spread of violence on their platforms. These technologies were used more than a million times in 24 hours to stop the distribution of the video from Christchurch.

While these are vital steps, one of the lessons from New Zealand is that the industry rightly will be judged not only by what it prevented, but by what it failed to stop. And from this perspective, there is clearly much more that needs to be done. As Prime Minister Ardern noted last week, gone are the days when tech companies can think of their platforms akin to a postal service without regard to the responsibilities embraced by other content publishers. Even if the law in some countries gives digital platforms an exemption from decency requirements, the public rightly expects tech companies to apply a higher standard.

There are at least three areas where we should focus our efforts.

First, we need to focus on prevention. We need to take new steps to stop perpetrators from posting and sharing acts of violence against innocent people. New and more powerful technology tools can contribute even more than they have already. We must work across the industry to continue advancing technologies like PhotoDNA and other AI-based image scanning techniques to identify and apply digital hashes (a kind of digital identifier). This can enable us more granularly to improve the ability to remove violent video content. For example, while video hashes allow automated tools to detect additional copies already flagged as violent, we need to further improve this technology so that it can better identify and catch *edited* versions of the same video.

We should also pursue new steps beyond the posting of content. For example, we should explore browser-based solutions – building on ideas like safe search – to block the accessing of such content at the point when people attempt to view it.

We should pursue all these steps with a community spirit that will share our learning and technology across the industry through open source and other collaborative mechanisms. This is the only way for the tech sector as a whole to do what will be required to be more effective.

We also should recognize that technology cannot solve this problem by itself. We need to consider and discuss additional controls or other measures that human beings working at tech companies should apply when it comes to the posting of this type of violence. There are legal responsibilities that need to be considered as well. It's a complicated topic with important sensitivities in some parts of the tech sector. But it's an issue whose importance can no longer be avoided.

Second, we need to respond more effectively to moments of crisis. Even with better progress, we cannot afford to assume that there will never be another tragedy. The tech sector should consider creating a "major event" protocol, in which technology companies would work from a joint virtual command center during a major incident. This would enable all of us to share information more quickly and directly, helping each platform and service to move more proactively, while simultaneously ensuring that we avoid restricting communications that are in the public interest, such as reporting from news organizations.

We should also discuss whether to define a category of agreed "confirmed events," upon which tech companies would jointly institute additional processes to detect and prevent sharing of these types of violent content. We should consider the pros and cons, for example, of the short-term application in these circumstances of a brief delay for some live video streaming that would better enable efforts to identify and stop this content, while exempting from this restriction live reporting by journalists.

Finally, we should work more broadly to advance digital civility online. As many have noted, while much of the focus in recent days rightly has been on the use of contemporary tools to amplify this violence, the language of hate has existed for decades and even centuries. While we must take new and urgent technology steps to improve online safety, we will never succeed entirely if people fail to address the deeper problems or conclude that the standards of civility they follow in the real world fail to apply in cyberspace.

Working on digital civility has been a passion for many employees at Microsoft, who have recognized that the online world inevitably reflects the best and worst of what people learn offline. In many ways, anonymity on the internet can free people to speak and behave in ways they never would in person. This is why we believe it's important to continue to promote four tenets to live by when engaging online. Namely, we all need to treat others how we want to be treated, respect each other's differences, pause before replying, and stand up for ourselves and for others. This too is an area on which we can build further.

We all need to come together and move faster.

This is the type of serious challenge that requires broad discussion and collaboration with people in governments and across civil society around the world. It also requires us to expand and deepen industry wide groups focused on these issues, including key partners from outside the industry.

Finally, we hope this will become a moment that brings together leaders from across the tech sector.

It's sometimes easy amidst controversy for those not on the hot seat to remain silent and on the sideline. But we believe this would be a mistake. Across the tech sector we can all contribute ideas, innovate together and help develop more effective approaches.

The question is not just what technology did to exacerbate this problem, but what technology and tech companies can do to help solve it. Put in these terms, there is room – and a need – for everyone to help.

ATTACHMENT 4
EXCERPTS FROM RELEVANT REGULATION

Online Content Scheme

The Online Content Scheme is set out in Schedules 5 and 7 of the *Broadcasting Services Act 1992* (BSA) and four industry codes. This is a coregulatory scheme with industry codes working together with a formal regulated complaints mechanism.

- Schedule 5 contains powers to take action against content hosted outside Australia.
- Schedule 7 contains powers to take action against content hosted within Australia.

The scheme was designed to meet the objects in subsection 3(1) of the BSA of:

(ha) to ensure designated content/hosting service providers respect community standards in relation to content; and

.....

(k) to provide a means for addressing complaints about certain internet content; and

(l) to restrict access to certain internet content that is likely to cause offence to a reasonable adult; and

(m) to protect children from exposure to internet content that is unsuitable for children;

Prohibited content is that which what been classified by the Classification Board, and may include assessment for material that contains violence, language and themes such as terrorism and pornography. Prohibited content includes material to which criminal penalties apply (e.g. child pornography) or that has been classified as:

- Refused Classification (RC)
- X18+
- R18+ unless subject to a restricted access system
- MA15+ and is provided on a commercial basis unless subject to a restricted access system.

Potentially prohibited content is content that has not been classified but, if it was, is highly likely to be found to be prohibited.

Schedule 7 of the BSA defines 'content' as text, data, speech, music, sounds, visual images or any other form.

The eSafety Commissioner can investigate complaints about prohibited or potentially prohibited content and can:

- If content is hosted in Australia, order the take down of material using powers in schedule 7 of the BSA, or
- If content is hosted outside of Australia, report it to law enforcement and advise of links to the makers of internet filters using powers under Schedule 5 of the BSA.

The eSafety Commissioner is not able to classify material directly. Applications for classification of content can be made to the Classification Board by the host service provider, content service provider, links service provider or the eSafety Commissioner. Content is classified under the National Classification Code and classification guidelines.

Concerns about the effectiveness of the online content scheme

Issues with the Scheme as identified in the current and previous reviews are that the scheme is inflexible and overly prescriptive and not keeping up with changing technology. The industry codes that underpin the Scheme have not been reviewed since they were first developed in 2005 and 2008.

In 2012 the Australian Law Reform Commission recommended the establishment of a new classification scheme, administered by a single Commonwealth regulator that covered all media content across all platforms.

Submissions to the current review noted:

- The schedules overlap, are outdated, not fit for purpose and do not reflect current technologies or content delivery models and there is an inconsistent treatment of the same content across different platforms.
- The scheme has been more effective for content hosted in Australia with a high compliance rate. However this has become less relevant because of the migration of illegal content to offshore sites.
- Some submissions suggested that content should be classified by appropriately trained eSafety Office staff which would allow for quicker removal of content.
- The industry codes are out of date but the prescriptive nature of the schedules have prevented a meaningful overhaul of the codes by industry.

Outline of Schedule 5 of the BSA - Online Services

Schedule 5 was added to the BSA in 1999. The Schedule sets up a system for regulating certain aspects of the internet industry:

- If the eSafety Commissioner is satisfied that internet content hosted outside Australia is prohibited content or potential prohibited content, the Commissioner must:
    - if the eSafety Commissioner considers that the content is of a sufficiently serious nature to warrant referral to a law enforcement agency—notify the content to an Australian police force; and
    - notify the content to internet service providers so that the providers can deal with the content in accordance with procedures specified in an industry code or industry standard (for example, procedures for the filtering, by technical means, of such content).
- Bodies and associations that represent the internet service provider section of the internet industry may develop industry codes.
- The eSafety Commissioner has a reserve power to make an industry standard if there are no industry codes or if an industry code is deficient.

Outline of Schedule 7 of the BSA - Content Services

Schedule 7 was added to the BSA in 2007. The Schedule sets up a complaint mechanism for online content:

- A person may make a complaint to the eSafety Commissioner about prohibited content, or potential prohibited content, in relation to certain services.
- The Commissioner may take the following action to deal with prohibited content or potential prohibited content if it is hosted in Australia:
    - in the case of a hosting service—issue a take-down notice;

  - in the case of a live content service—issue a service-cessation notice;
  - in the case of a links service—issue a link-deletion notice.

- Content (other than an eligible electronic publication) is ***prohibited content*** if:
  - the content has been classified RC or X 18+ by the Classification Board; or
  - the content has been classified R 18+ by the Classification Board and access to the content is not subject to a restricted access system; or
  - the content has been classified MA 15+ by the Classification Board, access to the content is not subject to a restricted access system, the content does not consist of text and/or one or more still visual images, and the content is provided by a commercial service (other than a news service or a current affairs service); or
  - the content has been classified MA 15+ by the Classification Board, access to the content is not subject to a restricted access system, and the content is provided by a mobile premium service.
- Content that consists of an eligible electronic publication (an electronic edition of a book, magazine or newspaper) is ***prohibited content*** if the content has been classified RC, category 2 restricted or category 1 restricted by the Classification Board.
- Generally, content is ***potential prohibited content*** if the content has not been classified by the Classification Board, but if it were to be classified, there is a substantial likelihood that the content would be prohibited content.
- Bodies and associations that represent sections of the content industry may develop industry codes.
- The Commissioner has a reserve power to make an industry standard if there are no industry codes or if an industry code is deficient.
- The Commissioner may make determinations regulating certain content service providers and hosting service providers.

Excerpts from Commercial Television Industry Code of Practice and Subscription Broadcast Television Code of Practice

Commercial Television Industry Code of Practice

2.3 Exceptions

2.3.3 News Programs (including news flashes and news updates), Current Affairs Programs and Sports Programs and Program Promotions for news, Current Affairs or Sports Programs do not require classification and may be shown at any time, however a Licensee will exercise care in selecting material for broadcast, having regard to:

a) the likely audience of the Program or Program Promotion; and

b) any identifiable public interest reason for presenting the Program or Program Promotion.

2.6 Material not suitable for broadcast

2.6.1 A Licensee must not broadcast any material that cannot be classified MA15+ or any lower television classification.

Note: Material may be modified by a Licensee to ensure that it is suitable for broadcast, or for broadcast at particular times.

2.6.2 A Licensee must not broadcast any Program, Program Promotion, Community Service Announcement or Station ID which is likely, in all the circumstances, to provoke or perpetuate in, or by a reasonable person, intense dislike, serious contempt or severe ridicule against a person or group of people because of age, colour, gender, national or ethnic origin, disability, race, religion or sexual preference.

3.2 Material which may cause distress

3.2.1 In broadcasting a news or Current Affairs Program, a Licensee must:

a) not include material which, in the reasonable opinion of the Licensee, is likely to seriously distress or seriously offend a substantial number of viewers, having regard to the likely audience of the Program, unless there is a public interest reason to do so; and

b) include a spoken warning before a segment that contains material which, in the reasonable opinion of the Licensee, is likely to seriously distress or seriously offend a substantial number of viewers having regard to the likely audience of the Program; and

c) not broadcast reports of suicide or attempted suicide unless there is a public interest reason to do so, and exclude any detailed description of the method used, and exclude graphic details or images; and

d) exercise sensitivity in broadcasting images of or interviews with bereaved relatives or people who have witnessed or survived a traumatic incident; and

e) have regard to the feelings of relatives and viewers when including images of dead bodies or people who are seriously wounded, taking into account the relevant public interest.

Subscription Broadcast Television Code of Practice

2.1 General Programs

(a) Licensees will not broadcast any program which is likely in all the circumstances to provoke or perpetuate intense dislike, serious contempt or severe ridicule against a person or group of persons on the grounds of age, colour, gender, national or ethnic origin, disability, race, religion or sexual preference.

2.2 News and Current Affairs Program

[...]

(b) In broadcasting news and current affairs programs to the extent practicable Licensees:

(i) must not present material in a manner which creates public panic;

(ii) must include only sparingly material likely to cause some distress to a substantial number of viewers;

(iii) must exercise sensitivity in broadcasting images of, or interviews with, bereaved relatives and survivors or witnesses of traumatic incidents;

(iv) will take all reasonable efforts to provide warnings when there are identifiable public interest reasons for broadcasting material which may seriously distress or seriously offend a substantial number of viewers;

(v) will only broadcast reports of suicide or attempted suicide where there is an identifiable public interest to do so and will exclude any detailed description of the method used and any graphic details and will not glamourise suicide in any way; and

(vi) will make reasonable efforts to correct significant errors of fact at the earliest opportunity.

(c) In broadcasting news and current affairs programs Licensees must not use material relating to a person's personal or private affairs, or which invades an individual's privacy, other than where there are identifiable public interest reasons for the material to be broadcast.

Note: The question of intrusion into private domains, such as bereavement or personal tragedy, is one of real difficulty for all providers of news and current affairs programs. It is a matter of balance between what should be reported in the interests of the general public and what, if reported, would cause an individual or group of individuals unnecessary anguish. It is noted that the ACMA has published advisory Privacy Guidelines for Broadcasters available on the ACMA website at www.acma.gov.au.

2.3 Program Promotions and News Updates

Licensees will have particular regard to the need to protect children from unsuitable material in program promotions, news updates and news promotions.

The content of program promotions, news updates and news promotions will be consistent with the classification of the programs (if classified) during which updates or promotions appear and will, where practicable, include classification information about the programs being promoted, (see Part 3 of these Codes).

Extract from draft Online Safety Charter – released for public comment on 16 February 2019

Draft Online Safety Charter

This Charter seeks to outline what the Australian Government, and the Australian community, expect of technology companies and online service providers operating in Australia in terms of protecting the most vulnerable in our community. It is underpinned by two fundamental principles:

1. Standards of behaviour online should reflect the standards that apply offline.
2. Content that is harmful to users, particularly children, should be appropriately restricted.

This Charter is directed towards technology firms that offer the opportunity for users in Australia to interact or connect, and technology firms whose services and products enable Australian users to access content and information. This includes social media services, internet service providers, search engine providers, content hosts, app developers, and gaming providers, among others. For the sake of simplicity, the Charter uses the term 'technology firms'.

Control and responsibility

Content identification

Technological solutions should be fully utilised by technology firms to identify illegal and harmful content, and these solutions should be supported by human resources as appropriate.

There should be a specific point of contact within each technology firm for the referral of complaints about illegal and harmful content or legal notices from Australian authorities. This point of contact should be equipped and trained to manage Australian referrals, with a good understanding of relevant Australian legal requirements.

Content moderation

The systems employed by technology firms should have the capability and capacity to moderate illegal and harmful content.

Where feasible, this should include a triaging system to ensure high risk content (e.g. content promoting self-harm or criminal activity) is addressed expeditiously and lower risk content is reviewed and actioned within a longer period (for example, within 24 hours).

This triaging system should ensure that complaints made by children, or by adults on behalf of children, are also expedited. Where appropriate, illegal, harmful or inappropriate content targeted towards a child should be removed immediately, and only reinstated once the complaint has been investigated and only if the complaint is not upheld.

The resources devoted to content moderation should be proportionate to the volume of content available to users and relevant to the Australian context. Human content moderators should meet minimum training standards.

Minimum timeframes should apply to the review and moderation of flagged content, whether identified from internal flags, user complaints or regulatory authorities.

Content removal

Content that is clearly and unambiguously illegal under Australian law should be removed proactively by technology firms

Content that has been determined to be in breach of terms of use, or identified by regulatory authorities to be illegal or harmful, should be removed within clearly stated minimum timeframes.

Technology firms should take steps to prevent the reappearance of illegal, harmful or offensive content that has been removed.

Attachment A—Draft Online Safety Charter

This Charter seeks to outline what the Australian Government, and the Australian community, expect of technology companies and online service providers operating in Australia in terms of protecting the most vulnerable in our community. It is underpinned by two fundamental principles:

1. Standards of behaviour online should reflect the standards that apply offline.
2. Content that is harmful to users, particularly children, should be appropriately restricted.

This Charter is directed towards technology firms that offer the opportunity for users in Australia to interact or connect, and technology firms whose services and products enable Australian users to access content and information. This includes social media services, internet service providers, search engine providers, content hosts, app developers, and gaming providers, among others. For the sake of simplicity, the Charter uses the term 'technology firms'.

1. Control and responsibility

1.1 Content identification

Technological solutions should be fully utilised by technology firms to identify illegal and harmful content, and these solutions should be supported by human resources as appropriate.

There should be a specific point of contact within each technology firm for the referral of complaints about illegal and harmful content or legal notices from Australian authorities. This point of contact should be equipped and trained to manage Australian referrals, with a good understanding of relevant Australian legal requirements.

1.2 Content moderation

The systems employed by technology firms should have the capability and capacity to moderate illegal and harmful content.

Where feasible, this should include a triaging system to ensure high risk content (e.g. content promoting self-harm or criminal activity) is addressed expeditiously and lower risk content is reviewed and actioned within a longer period (for example, within 24 hours).

This triaging system should ensure that complaints made by children, or by adults on behalf of children, are also expedited. Where appropriate, illegal, harmful or inappropriate content targeted towards a child should be removed immediately, and only reinstated once the complaint has been investigated and only if the complaint is not upheld.

The resources devoted to content moderation should be proportionate to the volume of content available to users and relevant to the Australian context. Human content moderators should meet minimum training standards.

Minimum timeframes should apply to the review and moderation of flagged content, whether identified from internal flags, user complaints or regulatory authorities.

1.3 Content removal

Content that is clearly and unambiguously illegal under Australian law should be removed proactively by technology firms.

Content that has been determined to be in breach of terms of use, or identified by regulatory authorities to be illegal or harmful, should be removed within clearly stated minimum timeframes.

Technology firms should take steps to prevent the reappearance of illegal, harmful or offensive content that has been removed.

2. Improving the user experience

2.1 User behaviour

Clear minimum standards for online behaviour should be set and applied consistently across services and service providers.

- Behaviour standards should be visible, easy to find and easy to understand.
- Behaviour standards should be reviewed regularly to ensure they remain fit-for-purpose and user-friendly.
- There should be meaningful and material consequences for breaches of behaviour standards, including account suspension, access restrictions and banning of repeat offenders.
- Banned users should not be able to open a new account in a different name or register a different user name.

2.2 User support

User reporting and complaints systems should be easy to find, understand and complete.

They should include a swift acknowledgement of each complaint and outline expected response timeframes.

They should provide regular updates to complainants and affected users (including the person being complained about), enable decisions to be reviewed, and provide full information to users on how to refer complaints to regulatory authorities in Australia.

Online safety resources should be actively promoted to users, age-appropriate and easy to understand. This should include mental health and other support services, where appropriate.

2.3 Account control

Instructions about how to adjust settings, including privacy settings, should be easy to find, understand and follow.

Users should be able to freeze their account in real time.

Users under 16 years should be required to secure parental or guardian consent to open an account or register as a user. Verifying parental consent should require more than just ticking a box.

Parental control settings should be easy to use and difficult to circumvent.

2.4 Content management

Users should be given full control of content safety options, such as the ability to delete unwanted comments, easily remove content, selectively hide content they no longer want to be visible and impose self-restrictions on uploading content such as time of day lockouts or type of content (for example, videos or images).

3. Built-in Child Safety

3.1 Default settings and age guidance

All products and services (including apps and games), and devices marketed to children, marketed as being appropriate for children, or that are likely to appeal to children, should default to the most restrictive safety and privacy settings at initial use or set up, and should include age guidance.

3.2 Supply chain

App and game supply points should require developers and suppliers to certify that they have considered built-in child safety and any relevant SbD principles before accepting apps and games for distribution.

Information about privacy, online safety and parental control settings should be available at all relevant points in the supply chain, including point-of-purchase (including by download), registration, account creation and first use.

4. Accountability and transparency

4.1 Reporting and compliance

Technology firms should engage broadly with experts and key stakeholders in relation to the development and application of online safety standards.

Technology firms should publish regular reports on:

- content controls, including the type of content is identified, moderated and/or prevented from being uploaded, how it was identified, and the action taken;
- complaints, including the number of complaints received, investigated and resolved, the time taken to resolve complaints, the category of complaint, the action taken and generalised demographic information (including, where known, age and geographic location of complainants); and
- compliance with the standards in this Charter, identifying any gaps and outlining the proposed approach to improving safety outcomes in relation to these gaps.

For firms with a significant presence in Australia, a local version of these reports should be published and the underlying data should be made available to relevant Australian authorities on request.

User safety considerations and practices should be embedded in the leadership structures, operating practices and governance arrangements for technology firms, and appropriate policies and procedures should be core business for all individuals who work within technology firms.

KENNA Allison

From: Patteson, Carolyn <Carolyn.Patteson@communications.gov.au>
Sent: Monday, 25 March 2019 12:07 PM
To: Richard Eccles
Cc: James Penprase
Subject: All ISPs called - s47G [SEC=UNCLASSIFIED]

UNCLASSIFIED

Richard,
Have talked to all ISPs and the Comms Alliance. All grateful for run through and ready to talk specifics.
s47G

Odds and sods:

- We can access the venue from 10am onwards no problems
- HA have lined up 4 helpers and they've got my details. I've asked them to arrive about 12:20 so we can talk to them and then we can have them ready to escort from 12:30 onwards – might have a few delegates arriving early depending on flights etc

Carolyn Patteson
First Assistant Secretary / Content
Department of Communications and the Arts
P +61 2 6271 1418
Email.carolyn.patteson@communications.gov.au
2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra, ACT 2601
communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

s22

From: s22 communications.gov.au>
Sent: Monday, 25 March 2019 3:37 PM
To: media
Cc: s22
Subject: Summit Talking Points [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hi Media Team,

Could you provide these talking points to media at Home Affairs s22

We will be updating these tomorrow.

Cheers,

Summit on Responses to the Sharing of Content Related to the Christchurch Incident

- The Australian Government has invited representatives to attend a summit to be held in response to the Christchurch incident on 26 March.
- The summit will bring together representatives of Australian law enforcement and security agencies, internet service providers, social media platforms, regulators and government officials.
- Representatives will be asked to detail the actions taken by their organisations in response to the shootings and the dissemination of footage from the attacks.
- Summit participants will then work collectively to identify what can be done to prevent the streaming and reposting of extremist material, both now and into the future.

Cheers,

s22

Director / Platforms and Partnerships / Digital Media and Copyright Branch
Department of Communications and the Arts
s22 munications.gov.au

2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra, ACT 2601

communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

I would like to acknowledge the traditional custodians of this land on which we meet, work and live. I recognise and respect their continuing connection to the land, waters and communities. I pay my respect to Elders past and present and to all Aboriginal and Torres Strait Islanders.

s22

From: s22 @communications.gov.au>
Sent: Tuesday, 26 March 2019 10:05 AM
To: James Penprase
Cc: s22
Subject: Info from AGs [DLM=For-Official-Use-Only]

For Official Use Only

Hi James,

AGD has called us to advise that they met with the AG yesterday s47C

AGD will circulate a revised Bill for comments. We are seeking some information for them about who the Online Safety Act and the Online Content Scheme applies to.

Regards,

s22
Director / Platforms and Partnerships / Digital Media and Copyright Branch
Department of Communications and the Arts
s22 munications.gov.au

2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra, ACT 2601

communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

I would like to acknowledge the traditional custodians of this land on which we meet, work and live. I recognise and respect their continuing connection to the land, waters and communities. I pay my respect to Elders past and present and to all Aboriginal and Torres Strait Islanders.

Doc 21
Has Sound file attachment

s22

From: s22 ommunications.gov.au>
Sent: Tuesday, 26 March 2019 4:44 PM
To: James Penprase; s22 ;
s22
Subject: Presser: Summit Outcomes [SEC=UNCLASSIFIED]
Attachments: AUTH0109.m4a

UNCLASSIFIED

Dear colleagues,

I've attached the audio file. The announcements were:

1. There will be a taskforce established that will report to PM&C, consisting of representatives of: DOCA, AGD and DHA. Representatives will also be sought from the platforms and ISPs.

The taskforce will develop practical measures including short and long-term responses to :
Identify more quickly
Take down more quickly
Greater transparency from platforms

2. The government is not dissuaded from pursuing a legislative solution to the "live streaming of serious criminal offending". Legislation will be developed 'in parallel' with the work of the taskforce.

Regards,

s22

Director / Platforms and Partnerships / Digital Media and Copyright Branch
Department of Communications and the Arts

s22

2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra, ACT 2601

communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

I would like to acknowledge the traditional custodians of this land on which we meet, work and live. I recognise and respect their continuing connection to the land, waters and communities. I pay my respect to Elders past and present and to all Aboriginal and Torres Strait Islanders.

SUMMIT ON RESPONSES TO THE SHARING OF CONTENT RELATED TO CHRISTCHURCH INCIDENT

Date: Tuesday, 26 March 2019

Time: 1:00 to 3:00 pm

Venue: Level 31, 1 Eagle Street Waterfront Place, Brisbane, Queensland

AGENDA

Agenda	Timing	Description	Lead
1	1:00 – 1:05 pm (5 minutes)	Introduction	Prime Minister
2	1:05 – 1:15 pm (10 minutes)	Overview of expectations	Minister Fifield Minister Dutton Attorney General
3	1:15 – 1:30 pm (15 minutes)	Response from the digital platforms • Actions • Rules and standards • Lessons learned	Facebook Google Twitter
4	1:30 – 1:55 (25 minutes)	Response from the ISPs • Actions • Rules and standards • Lessons learned	Telstra Optus TPG Vodafone Comms Alliance
5	1:55 – 2:55 pm (60 minutes)	Facilitated discussion: improving outcomes and protections for the community • **Prevention and protection** – including detecting, blocking, and instantaneous and faster takedown options for violent terrorist material. • **Transparency** – improving transparency of the actions taken by platforms and ISPs in relation to violent terrorist material. • **Deterrence** – enhancing responsibility for the upload and distribution of violent terrorist material by individuals, platforms and ISPs.	All (led by Minister Fifield)
6	2:55 – 3:00 pm (5 minutes)	Close	Minister Fifield

SUMMIT CALLED IN RESPONSE TO THE CHRISTCHURCH SHOOTINGS

BRISBANE – 26 MARCH 2019

COMMUNIQUÉ

At today's summit, hosted by Prime Minister, the Hon Scott Morrison MP, participants provided updates on their efforts to detect, delete or block multimedia content filmed by the perpetrator of the Christchurch shootings, including new legislation to criminalise the uploading or live streaming of multimedia content by perpetrators of terrorist acts and their supporters.

Summit participants agreed that they were united on the need to restrict access to multimedia content made by the perpetrators of terrorism. This content is intended to humiliate and degrade victims of terrorism, inflame social tensions and encourage copycat and revenge attacks.

Representatives of social media companies updated summit participants on their efforts to detect, delete and prevent footage created by the Christchurch attacker from being shared on their platforms.

Facebook removed the attacker's video and personal accounts following contact from the New Zealand Police. In the first 24 hours, 1.5 million re-uploads of the attack were removed from the platform globally. More than 1.2 million of these were videos blocked at upload. Variants of the video were identified and removed using a mixture of audio analysis technology and human oversight. Facebook has identified, blocked and shared more than 800 visually distinct videos with members off the Global Internet Forum to Counter-Terrorism (GIFCT) to prevent these videos from appearing on a wide range of other platforms.

Google activated a safety warning that included the contact details for the New Zealand Police at the top of search results for any person searching 'Christchurch' or related queries. YouTube terminated the attacker's account and then established a 24 hour incident team to identify and remove tens of thousands of copies of the video from being uploaded, many of which were stopped by automated systems. YouTube launched authoritative ranking to ensure that for queries related to the incident, authoritative content was prioritised (such as from news sites). Hundreds of accounts were terminated that were designed to either promulgate the attacker's footage or to express sympathy with the perpetrator. Finally, YouTube suspended the ability to search or filter searches by upload date. This was an unprecedented step to prevent violative videos from being discovered while YouTube worked to address the volume of attempted uploads.

Internet service providers including Telstra, Vodafone and Optus made an independent decision to introduce temporary blocking of a range of websites hosting the perpetrator's video. The temporary blocks will remain in place until the videos are removed.

The actions taken by digital platforms and internet service providers to reduce access to the attacker's video are acknowledged by government. However, despite these efforts, there remain numerous individuals who persist in exploring new ways to distribute the video widely. In order to address this issue, the Attorney-General, the Hon Christian Porter MP briefed summit participants on a range of new criminal offenses designed to prevent the spread of abhorrent online material.

[Legislation details…]

Summit participants affirmed that international websites that choose to continue hosting the perpetrator's video are an enduring problem which will require an international response. While the 'fringe' nature of these websites means they do not attract mass audiences, their role in bringing

together like minded individuals in forums where acts of terrorism can be glorified, promoted and encouraged cannot be ignored. Addressing these sites will require a coordinated, international effort. The Prime Minister will pursue an international approach to this issue at the G20 meeting in Osaka, Japan.

THE HON SCOTT MORRISON MP
PRIME MINISTER OF AUSTRALIA

SENATOR THE HON MITCH FIFIELD
MINISTER FOR COMMUNICATIONS AND THE ARTS

JOINT MEDIA RELEASE

Online and technology firms need to do more

26 March 2019

The Australian Government is committed to ensuring that digital platforms and services are not used as weapons by terrorists, and has today called on industry to do more to protect our citizens from harm.

“The attack in Christchurch on 15 March 2019 has brought into sharp focus how modern technology can be used to disseminate content that is clearly unacceptable in our society,” the Prime Minister said.

“Today the Australian Government met with senior representatives of the digital platforms and the telecommunications industry to agree how we can do better to make sure that this offensive and harmful content is not promulgated.”

The discussions involved representatives from Google, Facebook, Twitter, Telstra, Optus, Vodafone, TPG, and the Communications Alliance, along with the Attorney-General, the Hon Christian Porter MP, the Minister for Home Affairs, the Hon Peter Dutton MP, and relevant Government officials.

Minister for Communications Mitch Fifield said that the discussions were highly productive.

“The Government acknowledges the actions taken by the digital platforms and internet service providers to remove or block access to the attacker’s video,” Minister Fifield said.

“But much more is needed. We need to know that in the future the digital platforms and telecommunications providers will take greater responsibility for how their services are used,” he said.

At the meeting the Prime Minister articulated the two key areas where the Government, and community, expect industry to lift their game.

Firstly, ensuring that industry implements prevention measures to immediately detect, and remove or block access to, violent and extreme content.

Secondly, seeking a commitment that industry will be more transparent about the actions they take to deal with such inappropriate content.

The Prime Minister also emphasised to industry that there would be consequences if industry fail to meet the mark.

Media contacts:

Morrison: Name | Phone | Email
Fifield: Geraldine Mitchell | 0407 280 476 | Geraldine.Mitchell@communications.gov.au

Authorised by Senator Mitch Fifield, Liberal Party of Australia, Parliament House, Canberra

“Cooperation is better than regulation, but we will regulate if necessary,” the Prime Minister said.

“We have done so in the past to protect the Australian community online, and we won’t hesitate to do so again, he said.”

“Our current community consultations on the Government’s draft Online Safety Charter have never been more important,” Minister Fifield said.

“This is the vehicle by which we can continue to make our expectations clear and work collaboratively with the digital platforms and internet service providers to realise the benefits of a connected world while protecting our citizens from its harms.”

Despite these cooperative efforts by industry and regulators alike, there are those who persist in exploring new ways to distribute offensive violent material.

The horrendous events of 15 March in Christchurch make that abundantly clear.

The Australian Government will be introducing a new range of criminal offences designed to prevent the spread of extreme violent online material, and impose clear and meaningful penalties on those that do.

“We will continue to put Australia and Australians first, but we recognise that this is a global issue which needs a coordinated international effort, the Prime Minister said.

“This Government will continue to pursue this issue at the G20 meeting in Osaka, Japan later this year.”

Doc 25

s22

From: Penprase, James <James.Penprase@communications.gov.au>
Sent: Wednesday, 27 March 2019 10:20 AM
To: s47F

s47F

Cc: Patteson, Carolyn; ; Richard Eccles;
Subject: RE: Deputy Secretary Summit Debrief [DLM=For-Official-Use-Only]
Attachments: TASKFORCE - Outline of Possible First Paper.docx; Summit Debrief Agenda.docx; TASKFORCE - Draft Terms of Refence - 27 March 2019.docx

For Official Use Only

Dear all

Please find attached three short papers for today's post-summit debrief. An agenda, a draft terms of reference for the Taskforce, and a possible first paper for the initial meeting. These are very much a first cut (prepared this morning), but are a start.

Regards

James

James Penprase
Assistant Secretary / Digital Media and Copyright
Department of Communications and the Arts
P +61 2 6271 1932
s47F
james.penprase@communications.gov.au

2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra, ACT 2601

Summit Debrief

Agenda Items:

1. Debrief from Summit (All)
2. Governance arrangements for Task Force (PM&C)
3. Terms of Reference (All)
4. Potential actions and commitments (All)
5. Next Steps (DoCA/PM&C)

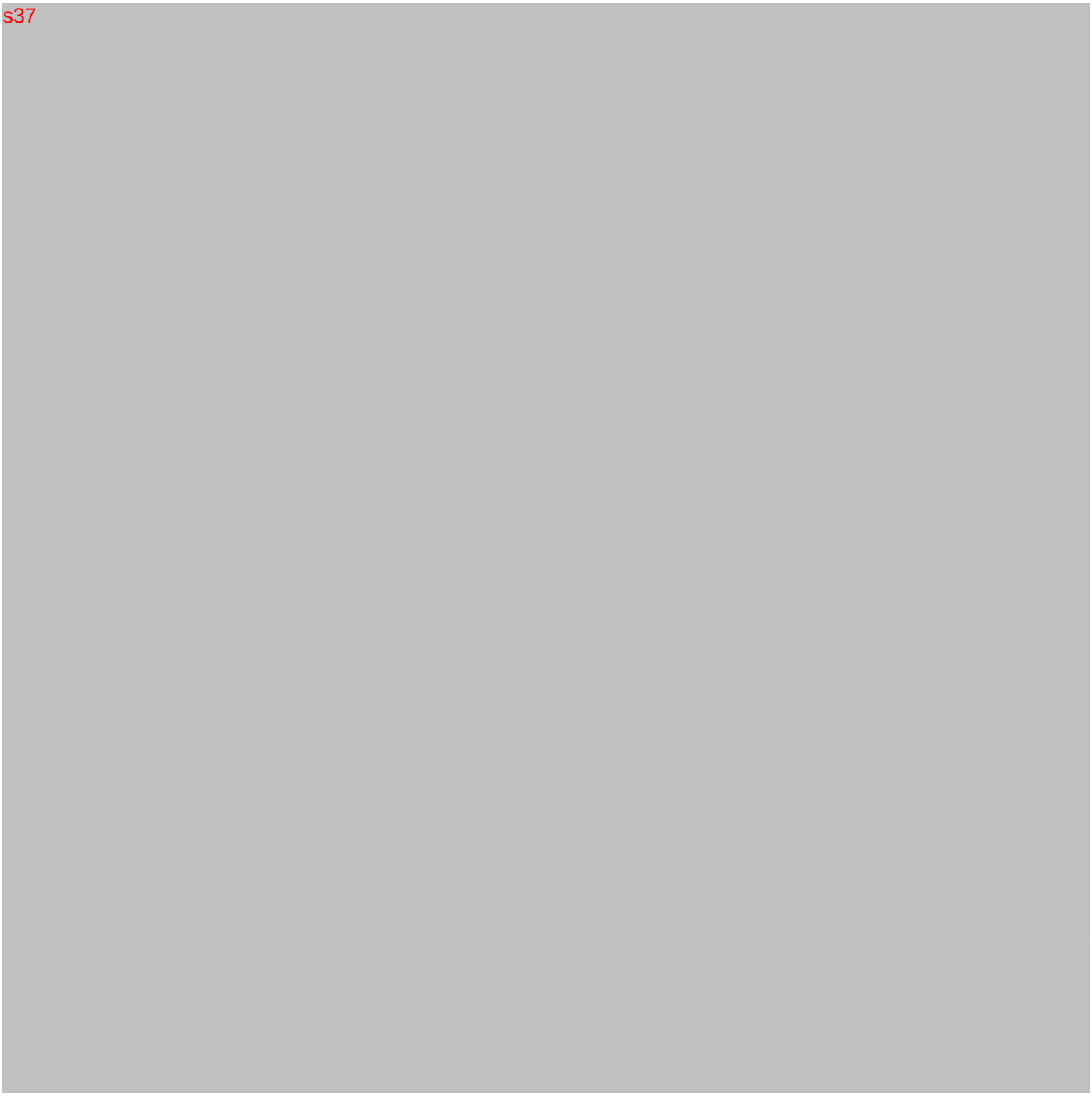
Attachments:

1. Draft ToR for Task Force
2. Discussion paper – Potential actions and commitments

TASKFORCE ON VIOLENT TERRORIST AND EXTREME MATERIAL ONLINE POTENTIAL AGENDA PAPER

1. PREVENTION AND PROTECTION – DETECTING, BLOCKING, AND INSTANTANEOUS AND FASTER TAKEDOWN OPTIONS FOR VIOLENT TERRORIST MATERIAL

s37



f) Product design – platforms to commit to incorporating safety protections into their services from the design phase to mitigate risks (Safety-by-Design).

2. TRANSPARENCY – IMPROVING TRANSPARENCY OF THE ACTIONS TAKEN BY PLATFORMS IN RELATION TO VIOLENT TERRORIST MATERIAL

g) Standards development – platforms to commit to engage broadly with in-country experts and key stakeholders in relation to the development and application of their own online safety standards and terms of use.

h) Reporting – platforms to compile and publish regular reports and data, specific to Australia, on:
   i. content controls, including the type of content is identified, moderated and/or prevented from being uploaded, how it was identified, and the action taken; and
   ii. complaints, including the number of complaints received, investigated and resolved, the time taken to resolve complaints, the category of complaint, the action taken and generalised demographic information (including, where known, age, geographic location of complainants), and any appeals/ arbitration processes.

3. DETERRENCE – ENHANCING RESPONSIBILITY FOR THE UPLOAD AND DISTRIBUTION OF VIOLENT TERRORIST MATERIAL BY INDIVIDUALS, PLATFORMS AND ISPs.

i) User reporting – platforms to deploy clear, visible and intuitive reporting mechanisms on live streaming services that are triaged immediately in relation to extreme violent content (in addition to suicide, terrorism and child sexual abuse material). Platforms to push reporting mechanisms and remind users of the importance of reporting content to keep others safe.

j) Moderators: Platforms to ensure they employ sufficient moderators to handle the volume of requests in accordance with timeframe expectations, and that these moderators have adequate support in dealing with this content.

k) Warning notices – platforms to issue warning notices to live streaming users who may be posting violent content that their service may be cut off.

l) Moderation triggers – platforms to implement 'moderation triggers' in circumstances where live-stream content on a platform service is drawn from anonymous sites such as 4chan or 8chan.

m) Disabling comments – platforms to agree to provide an option for site owners to turn off notifications / comments where they are experiencing high levels of offensive or violent commentary in response to the posting or reporting of content on their social media sites.

n) Predictive search – platforms to ensure that after a terrorist attack users are not prompted to search for live footage.

o) Problematic websites – platforms to demote content links to websites that host violent terrorist footage

TASKFORCE ON VIOLENT TERRORIST AND EXTREME MATERIAL ONLINE
Draft Terms of Reference

The Government has established a Taskforce on Violent Terrorist and Extreme Material Online to develop concrete actions and measures to combat the spread of violent terrorist and extreme content on digital platforms and other internet services. This is part of Australia's efforts to take a leadership role fighting the exploitation of internet technologies for terrorist purposes, which will be also be pursued through the G20 forum. The Taskforce will be comprised of representatives from relevant government departments and agencies, digital platforms and ISPs.

Terms of Reference

1. To provide advice to Government on practical, tangible and effective measures and commitments to combat the upload and dissemination of violent terrorist content online, with a specific focus on:

    i. **prevention and protection** – detecting, blocking and instantaneous and faster takedown of violent terrorist material;

    ii. **transparency** – improving the transparency of actions of digital platforms in identifying and removing violent terrorist material, and ensuring such content does not resurface; and

    iii. **deterrence** – enhancing the responsibility for the upload and distribution of violent terrorist material by platforms, ISPs and individuals.

2. To provide advice to Government on the incorporation of these tangible and concrete measures and commitments in the Online Safety Charter, which is due to be finalised in mid-2019.

s22

From: s22 communications.gov.au>
Sent: Wednesday, 27 March 2019 2:34 PM
To: James Penprase
Cc: s22
Subject: Summit Talking Points [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hi James,

The Department of Home Affairs are after updated talking points following the Summit yesterday. Are the following OK?

Summit on Responses to the Sharing of Content Related to the Christchurch Incident

- On 26 March, the Australian Government hosted a summit to respond to the live streaming of shootings in Christchurch.
- The summit brought together representatives of Australian law enforcement and security agencies, internet service providers, social media platforms, regulators and government officials.
- Following the summit, the Australian Government announced that it would form a taskforce to develop short and medium-term solutions to address the live streaming of extremist content.
- The taskforce will include representatives from:
  - Department of the Prime Minister and Cabinet
  - Department of Communications and the Arts
  - Department of Home Affairs
  - The Attorney-General's Department
  - Relevant social media platforms and internet service providers.
- [DHA to seek content from AGD about pursuing legislative solutions]

Cheers,
s22

s22
Director / Platforms and Partnerships / Digital Media and Copyright Branch
Department of Communications and the Arts
s22

2 Phillip Law Street, Canberra ACT 2601
GPO Box 2154 Canberra, ACT 2601

communications.gov.au / @CommsAu
arts.gov.au / @artsculturegov

I would like to acknowledge the traditional custodians of this land on which we meet, work and live. I recognise and respect their continuing connection to the land, waters and communities. I pay my respect to Elders past and present and to all Aboriginal and Torres Strait Islanders.

Doc 27

s22

From: Eccles, Richard <Richard.Eccles@communications.gov.au>
Sent: Thursday, 4 April 2019 11:31 PM
To: s47F ; Patteson, Carolyn; James Penprase
Subject: s22
Attachments: Letter to Mr Mrdak.pdf; ATT00001.htm

FYI

s22

s47G

s47G

s47G

s37

1. **PREVENTION AND PROTECTION – DETECTING, BLOCKING, AND INSTANTANEOUS AND FASTER TAKEDOWN OPTIONS FOR VIOLENT TERRORIST MATERIAL**

s37 and 47G

b) Content removal – platforms to prioritise removing violent terrorist material once it is notified to them, or otherwise identified through improved internal identification and moderation process. Platforms to pursue instantaneous removal of all content previously identified as violent terrorist content.

c) Content blocking – ISPs, subject to notices issued under a new / enhanced notification process, to immediately block domains that have been identified as consistently hosting / streaming violent terrorist content.

s37 and 47G

e) Response network – the Government to lead the development of a high speed emergency response contact network for Government, ISPs and platforms. Government will need to consider the structure and role, including the integration of the enhanced notification process outline above. But for the industry, this would involve:
   i. ISPs and platforms establishing processes to share information with each other and law enforcement or regulators of identified violent terrorist material, including the online locations of such material;
   ii. ISPs and platforms to develop, formalise and share with Government emergency plans for responding to these issues; and
   iii. ISPs and platforms committing to providing a designated, Australian 24 hour contact point for responding to law enforcement and regulators in relation to online safety; and
   iv. ISPs and platforms to work with law enforcement agencies to help identify wilful distributors of wilful distributors of violent terrorist content, such that legal consequences can be more consistently enforced

f) Product design – platforms to commit to incorporating safety protections into their services from the design phase to mitigate risks (Safety-by-Design).

2. TRANSPARENCY – IMPROVING TRANSPARENCY OF THE ACTIONS TAKEN BY PLATFORMS IN RELATION TO VIOLENT TERRORIST MATERIAL

g) Standards development – platforms to commit to engage broadly with in-country experts and key stakeholders in relation to the development and application of their own online safety standards and terms of use.

h) Reporting – platforms to compile and publish regular reports and data, specific to Australia, on:
   i. content controls, including the type of content is identified, moderated and/or prevented from being uploaded, how it was identified, and the action taken; and
   ii. complaints, including the number of complaints received, investigated and resolved, the time taken to resolve complaints, the category of complaint, the action taken and generalised demographic information (including, where known, age, geographic location of complainants), and any appeals/ arbitration processes.

3. DETERRENCE – ENHANCING RESPONSIBILITY FOR THE UPLOAD AND DISTRIBUTION OF VIOLENT TERRORIST MATERIAL BY INDIVIDUALS, PLATFORMS AND ISPs.

i) User reporting – platforms to deploy clear, visible and intuitive reporting mechanisms on live streaming services that are triaged immediately in relation to extreme violent content (in addition to suicide, terrorism and child sexual abuse material). Platforms to push reporting mechanisms and remind users of the importance of reporting content to keep others safe.

j) Moderators: Platforms to ensure they employ sufficient moderators to handle the volume of requests in accordance with timeframe expectations, and that these moderators have adequate support in dealing with this content.

k) Warning notices – platforms to issue warning notices to live streaming users who may be posting violent content that their service may be cut off.

l) Moderation triggers – platforms to implement 'moderation triggers' in circumstances where live-stream content on a platform service is drawn from anonymous sites such as 4chan or 8chan.

m) Disabling comments – platforms to agree to provide an option for site owners to turn off notifications / comments where they are experiencing high levels of offensive or violent commentary in response to the posting or reporting of content on their social media sites.

n) Predictive search – platforms to ensure that after a terrorist attack users are not prompted to search for live footage.

o) Problematic websites – platforms to demote content links to websites that host violent terrorist footage

Snapshot of Australian Government Online Responsibilities

Communications	**Attorney-General's**	**Home Affairs**	**Prime Minister and Cabinet**	**Department of Defence**	**Australian Electoral Commission**	**Social Services**	**Education and Training**
Agencies: • Office of the eSafety Commissioner • Australian Communications and Media Authority	*Agencies:*	*Agencies:* • Australian Federal Police • Australian Security Intelligence Organisation	*Agencies:* • Office of National Intelligence	*Agencies:* • Australian Signals Directorate • Australian Cyber Security Centre	*Agencies:*	*Agencies:*	*Agencies:*
Issues: • Online Safety including: o Cyberbullying o Image-based abuse o Offensive and harmful content o Online safety education • Copyright • Online advertising • Gambling promotions during live sport • Illegal interactive gambling services • Electoral communications (for broadcasting)	*Issues:* • National security and counter-terrorism • Child sexual abuse material • Foreign interference transparency scheme • Defamation • Privacy	*Issues:* • Breaches of the Criminal Code: Use of carriage service to menace, harass or cause offence • Commonwealth offences for prohibited online content include extremist propaganda and terrorist material • Collection of domestic intelligence, investigation of counter-terrorism and security threats	*Issues:* • Online Safety for Aboriginal and Torres Strait Islander communities • Improving online safety for women • ONI is responsible for enterprise level management of the National Intelligence Community	*Issues:* • Defending Australia from cyber threats • Coordination of Australian cyber capabilities to improve cyber resilience	*Issues:* • Ensuring electoral communication (including online communication) is appropriately authorised	*Issues*: • National Plan to Reduce Violence against Women and their Children • Funding organisations that provide education and support on technology-facilitated abuse	*Issues*: • National Safe Schools Framework • Information and resources for students through the Student Wellbeing Hub • COAG Bullying and Cyberbullying Senior Officials Working Group

Summit Paper

The events of Christchurch on 15 March 2019 have brought into stark relief a series of current vulnerabilities in the role that modern technology plays in supporting content and actions that are so clearly unacceptable to society.

KEY ISSUES

A future model of collaboration must see digital platforms and technology companies take responsibility in three general areas:

1. In ensuring content meets standards acceptable to the community.

2. To proactively discover and moderate inappropriate content.

3. To respond to referred instances of inappropriate content.

The extent to which each of the players currently takes responsibility for these matters varies greatly. But what is clear is that current levels of responsibility are insufficient.

These platforms are no longer just 'dumb pipes' that deliver unmoderated content developed by others. Sophistication of algorithm based activity has assisted each to grow rich - very rich – Google had global revenue of US$110 billion in 2017 of which AU$3 billion is from customers in Australia. Facebook earnt AU$1.3 billion in advertising revenue from the 13 million Australian subscribers in the same year. These platforms are amassing a greater market share of content, advertising and data resources. It is time that this sophistication is used to better achieve the three elements of responsibility outlined above.

Correspondingly, Government must be much clearer in its expectations. Recent history has shown that we have needed to regulate - to intervene in this market - for one simple reason: digital platforms have failed to act in a manner that approximates Australia's community standards. We have shown that although we live in a global economy, we can and will put the interests of our people first and foremost.

The pendulum has swung. Governments no longer consider platforms beyond regulation. Over the past three years the Government has begun to regulate the platforms in areas such as gambling advertising, copyright and piracy, online safety, electoral compliance and privacy. We have made it clear: unless your own standards reflect our national interest, we will regulate.

Similarly, society is no longer prepared to accept the power they yield unquestioned and unfettered (including in areas such as privacy, on-line safety and scamming).

So much more is needed.

The regulatory framework in relation to terrorist activity, extreme violence and human exploitation exists in some form. But the nature of regulation and the nature of the rapidly changing digital environment means government will likely be playing catch-up constantly. It will be hard for regulation to constantly evolve at the same pace as changes in on-line and digital communications.

Against this background, any future construct must be defined by best possible regulation; a shared understanding of community standards; clear protocols for discovery and referral of inappropriate activity and content; and (ambitiously) goodwill. There will need to be consequences for non-compliance.

DRAFT

The Government is currently consulting on an Online Safety Charter which will establish the Government's expectations for social media services, content hosts and other technology companies. The Government sees the Charter as the vehicle to drive the needed changes on these issues.

Legislative change will also be required to introduce new offences to prevent the dissemination of abhorrent audio-visual depictions of acts of violence that the perpetrator or their associates have recorded. These will deny offenders the opportunity to leverage interest in the event on social media platforms to further spread their propaganda messages.

OBJECTIVES OF THE SUMMIT

The objective of the Summit is to get a commitment from the digital platforms and telecommunications industry that they will lift their game and do more to deal proactively and decisively with inappropriate content.

The Summit should result in a greater understanding of the following:

1. Government's expectations of the digital platforms and ISPs in upholding community standards and proactively identifying and removing inappropriate content.
2. The tools and approaches that digital platforms and internet service providers can utilise in dealing with the dissemination of abhorrent material.
3. How government and technology companies can work together.
4. To identify lessons that could inform government action if required.

SUMMIT ATTENDEES

The Summit will bring together Ministers, Australian Government law enforcement, security and policy officials and senior representatives from the digital platforms and internet service providers. Invited attendees include:

Ministers

1. Prime Minister
2. Minister for Communications and the Arts
3. Attorney-General
4. Minister for Home Affairs

Officials

5. PM&C – Martin Parkinson
6. DoCA – Mike Mrdak
7. OeSC – Julie Inman-Grant
8. ACMA – Nerida O'Loughlin
9. AFP – Andrew Colvin
10. ASIO – Duncan Lewis
11. Home Affairs – Mike Pezzullo
12. AGD – Chris Moraitis

Platforms

13. Google
14. Facebook
15. Twitter

DRAFT

ISPs

16. Telstra – s47F
17. Vodafone – s47F
18. Optus – s47F
19. TPG – s47F
20. Communications Alliance – s47F

BROAD STRUCTURE OF SUMMIT

The agenda for the Summit has been structured to enable Government to make clear its expectations about the handling of harmful or offensive content and to foster a shared understanding of actions taken in response to the events of 15 March 2019. The focus will be on taking the lessons learned and framing a way forward. The Government is looking for stronger collaboration and commitments from the digital platforms and the ISPs to act on inappropriate material efficiently and effectively. If necessary the Government will regulate and there will be consequences for non-compliance.

Agenda

1. Welcome by the Prime Minister
2. Overview of expectations (Minister Fifield, Minister Dutton, Attorney-General)
3. Update from Digital Platforms (Facebook, Google, Twitter):
    a. Actions
    b. Rules and Standards
    c. Lessons Learnt
4. Update from ISPs (ISPs, Communications Alliance)
    a. Actions
    b. Rules and Standards
    c. Lessons Learnt
5. Facilitated Discussion: Lessons learned focusing on: (all)
    a. Ensuring content meets standards acceptable to the community
    b. To proactively discover and moderate inappropriate content
    c. To respond to referred instances of inappropriate content
6. Meeting Close (Government)

DRAFT

BACKGROUND INFORMATION

s47G and s37

[redacted]


s37 and 47G


s47G and s37


s47G

s47G

Internet Service Provider Response

- Media reports (Guardian Australia, AFR – 20 March) indicate that Telstra, Vodafone and Optus have all confirmed that they are actively blocking Australian customers from accessing websites that are hosting the Christchurch attacker's video.
- Communications Alliance Chief Executive John Stanton is quoted as saying: "Due to the extraordinary circumstances, several large ISPs in Australia have taken the decision to voluntarily implement temporary blocks of websites that continue to host footage of the Christchurch terrorist attack video. These ISPs have sought to balance community expectations to remove access to the video with the need to minimise any inconvenience that may arise from legitimate content being blocked as an unavoidable, temporary consequence."
- ISPs have been working with blocked websites to restore access once the video had been taken down.

Australian Online Content Arrangements

Australia's classification system to address violent and extreme material

- Australia has a robust domestic Classification Scheme for films, computer games and certain publications.
- Australia relies on the Scheme to provide safeguards on material deemed extremist in nature and where appropriate, a Refused Classification (RC) rating is applied for material submitted for classification. This includes content promoting, inciting or instructing matters of crime of violence.
- The RC category includes offensive depictions or descriptions of children and illegal content. However, it is important to note that what is considered prohibited/potential prohibited under Australian law may not be illegal in the jurisdiction where the content is hosted.
- The scheme is an inter-governmental arrangement whereby any changes to the scheme must be considered and agreed to by all ministers with responsibility for classification matters.

Legality of video

- The full-length video posted on 8Chan showing Tarrant's assault on the Al Noor Mosque in Riccarton would almost certainly fall within the RC category under the terror-advocacy provisions and the broader instruction in crime or violence provisions.
- There are several other versions of the attack video circulating, including an edited version that stops as Tarrant raises his shotgun to fire at worshippers standing at the door of the Al Noor Mosque.
- These edited versions – depending very much on the context in which it is provided – may not be considered sufficiently detailed to be regarded as pro-terror advocacy. Arguably, they do not show a terrorist act within the meaning of section 100.1 of the Criminal Code, as required under section 9A of the Classification (Publications, Films and Computer Games) Act 1995.

DRAFT

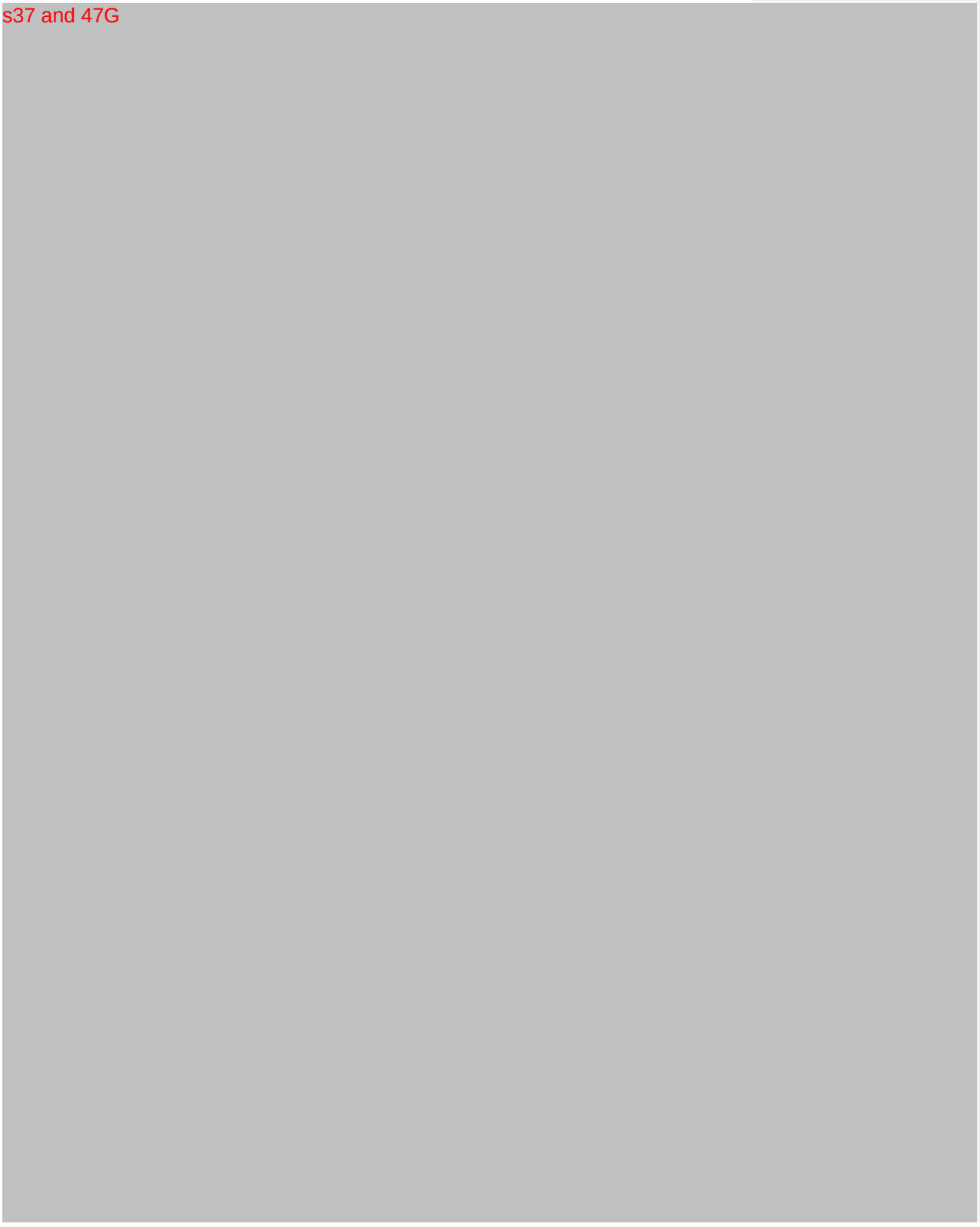
- It is arguable that some of the edited versions may, however, still be considered sufficiently detailed to fall within the RC crime instruction category, as they could be seen as showing instruction in tactics, techniques and procedures.

Mechanisms for takedown

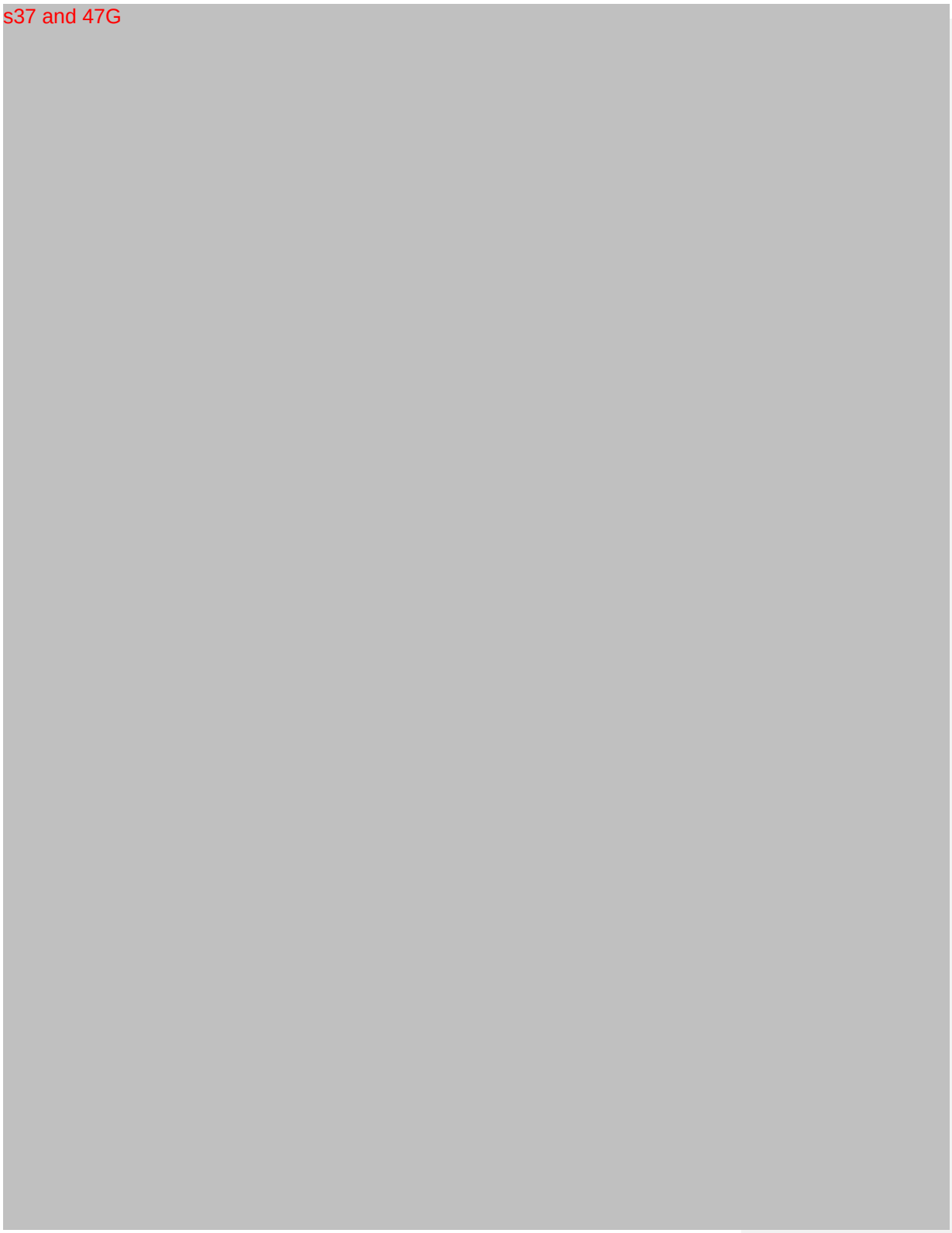
- The eSafety Commissioner has the statutory power to direct Australian content hosts to remove prohibited online content if it is hosted in Australia under the Online Content Scheme.
- While the eSafety Office does not have the power under the Scheme to issue a takedown notice to Facebook, which is based in the United States, it does work cooperatively with digital platforms to request removal of material that is clearly illegal in Australia and other jurisdictions.
- Reports about prohibited online content are referred to local and international civil and law enforcement partners for investigation and removal.
- If prohibited online content depicts information that could lead to the identification of either a victim or perpetrator, an immediate report will be made by the Office to the AFP.
- Pro-extremist content is notified to the Australian Federal Police or to state law counter-terrorism commands.
- There are separate protocols that guide the relationship between law enforcement, intelligence agencies and platforms.
- Overseas-hosted prohibited content is notified to vendors of accredited Family Friendly Filters.

DRAFT

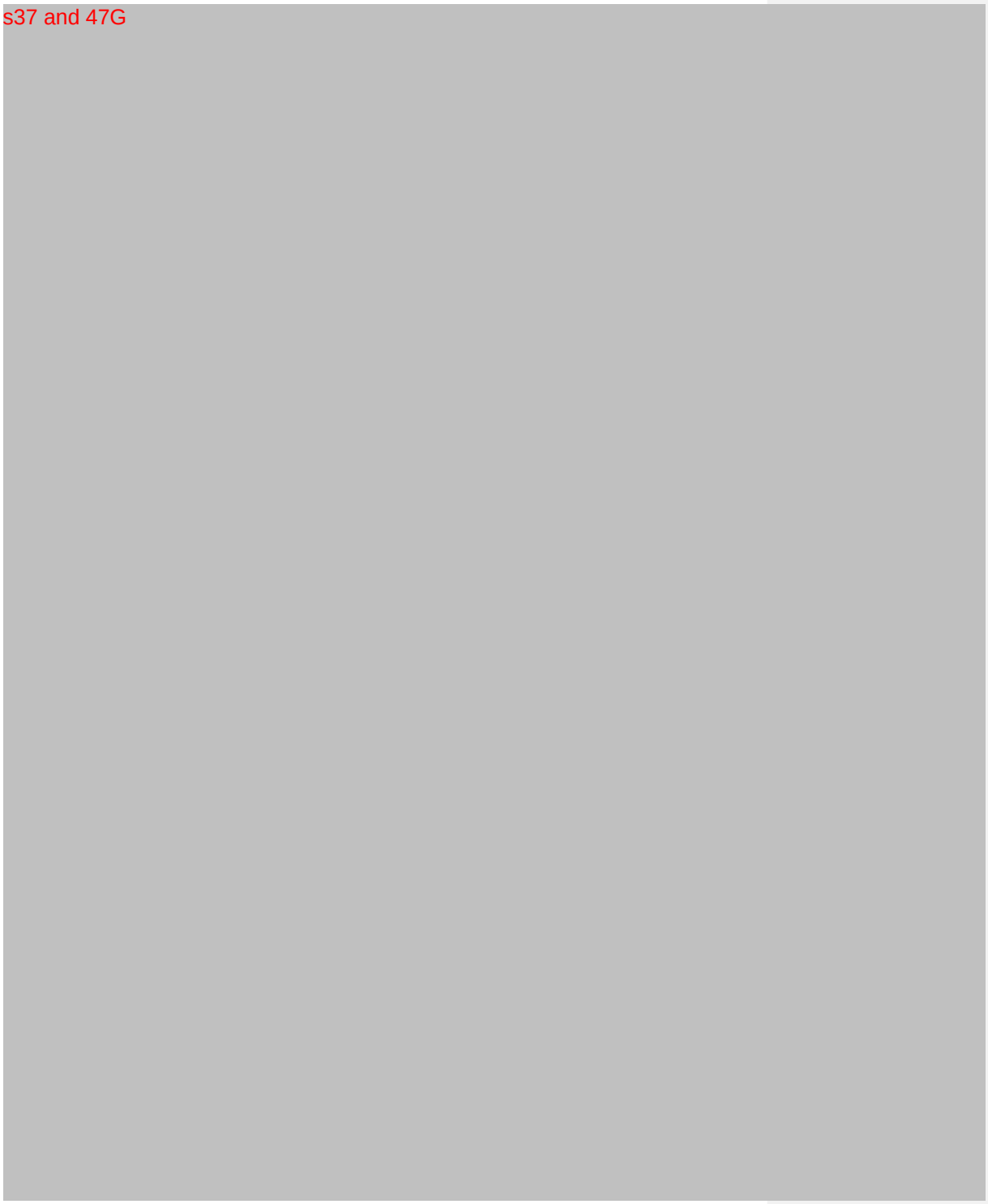
s37 and 47G



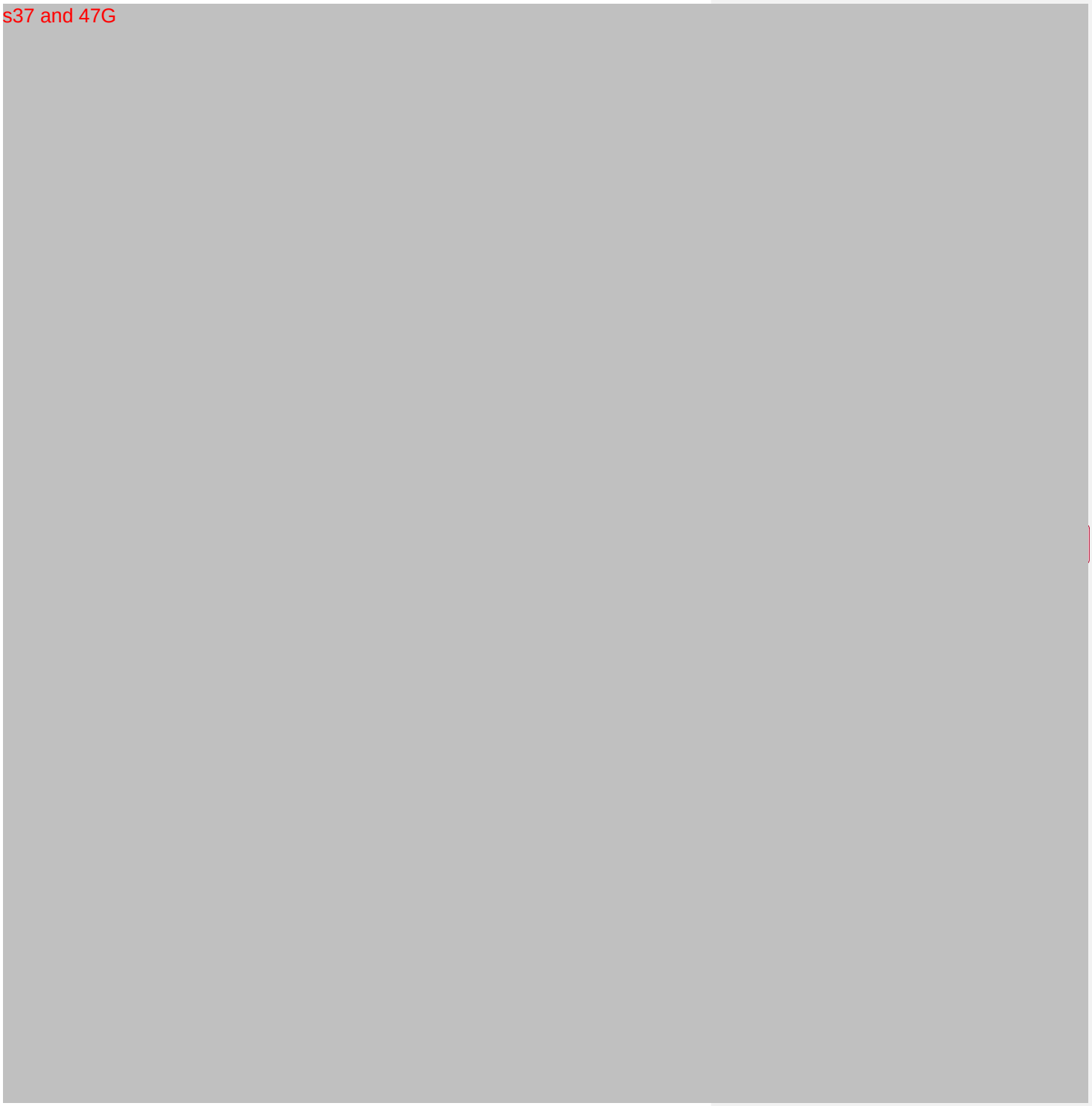
s37 and 47G



s37 and 47G



s37 and 47G



s37 and 47G