Summary of Recommendations

The following sections summarise recommendations that appear with background explanation and context throughout this report.

Recommendations to Create a Partnership Between Industry and Government

Number	Page	Recommendation
20	57	Serious hate speech, that which makes threats of violence or incites either violence or hatred, should be immediately reported to authorities. Other forms of hate speech should be removed by the platform, but a log of the incident including the user's account and IP address should be recorded. Users should be informed when a platform takes action against them and should be warned repeated breaches could lead to a report being made to authorities. Where platform sanctions prove ineffective at altering behaviour, the history of breaches and IP address of the user should be referred to authorities.
21	58	Once a user has been referred to authorities by a platform, a summary of any further hate speech incidents involving that user on that platform should be notified to authorities periodically (for example monthly) by the platform.
22	58	Once a user has been referred to authorities, the authorities should seek to convert the IP address into details of the accountholder and add it to the record. Where the account holder is a company, the company should be notified with a request to identify the specific user.
23	58	Where a company cannot provide information on the person who committed a breach of the law against serious or repeated hate speech, assistance should be provided. Where a company will not provide information on the person who committed a breach of the law against serious or repeated hate speech, the company itself should be liable to corporate fines.
24	58	Users referred to authorities by platforms for repeated breaches that do not involve incitement to hate or violence should initially be issued a warning, potentially after a discussion with authorities centering around user actions. Further breaches should lead to escalating fines. If fines fail to provide a deterrent, more serious measures including imprisonment should be available.
25	58	Legal exemptions should be provided for researchers from government agencies and departments, academia and civil society engaged in testing the effectiveness of both platform and government agency responses. Such exemptions may require prior approval of the research by one or more authorised people or agencies who are independent of the enforcement system.

Recommendations for Content Services

Number	Page	Recommendation
3	27	All services that allow users to upload or post content should have clearly visible mechanisms for reporting to the service provider any content that violates the terms of such services.
19	56	All companies that allow hosting of user generated content should have a process to receive reports from the public related to material promoting terrorism and this process should ensure rapid review.

4	27	All services that allow users to upload or post content should allow content to be reported anonymously to the service provider and by anyone who can see the content. If content is visible without having an account, then it should be reportable without having an account.
5	27	To assisting with lawful counter terrorism investigations, all services that allow users to upload or post content should maintain logs for at least 24 hours. Where a user reports content, log details related to the original uploader / poster of that content should be maintained for a further period of at least 7 days.
7	30	Livestreaming and video hosting sites should provide reporting options that allow the rapid identification, and a priority response, to reports of actual violence, extremism or unfolding crime.
8	30	Platforms should publish their target response time for reviewing and responding to reports of content flagged by users as potential violent extremist content or whichever broader category the platform choses which includes violent extremist content. Platforms should also publish their average response time to reports in this category on a regular, e.g. monthly, basis.
11	47	When a violent extremist attack is livestreamed the platform that was used to stream the incident and / or host the initial video of the incident should provide transparency on exactly when the livestream and/or video was first reported to them and when exactly they acted to remove it.
12	47	Platforms should take all reasonable steps to facilitate and encourage the reporting of material depicting and promoting violent extremism, as well as all other reasonable steps to identify such material themselves. They should expeditiously remove such material once they become aware of it. Provided the above steps are taken, there should be a clear safe harbour, protecting platforms from liability for material they are unaware they are hosting.
37	109	Hosting services that do not outright prohibit the use of their services to incite hate, should at a minimum ensure they do not serve content inciting hate to users in countries where such incitement is unlawful.

We additionally make the following recommendation, but flag it as particularly controversial:

36	109	Content services should create mechanisms that enable them to restrict access to specific content on their service for users from countries where that content is illegal. This will ensure content services have the technical capacity to respect national sovereignty and comply with national laws. There may be circumstances where a content service refuses to comply with national laws, for example, if the national laws conflict with customary international law, international treaties to protect human rights, or legal obligations in the content services own jurisdiction.

This goes to the question of state sovereignty and the role of Internet technology as a disrupter. Foreign interference that undermines a government's power or control is justifiable in circumstances where the power is being used contrary to universal human rights. Other cases are more controversial as they may advance the interests of some states against the interests of others. Questions of cyber dissidents, whistle blowers and Smart Power come in to play. A general discussion can be seen in Section 1.2.

Recommendations for Suppliers to Content Services

Number	Page	Recommendation
1	25	Where an image board is hosted in a country and the site, or a board within it, actively promotes hate speech which is unlawful in that country, the hosting provider once it is aware of this, should take action to terminate the hosting.
2	25	Where a domain name is registered in a country, and the owner actively uses the site at that domain for the purpose of promoting hate speech which is unlawful in that country, the domain name should be terminated by the domain name registrar.
32	105	Decisions by technology companies not to do business with a site should be such that a change to the ownership, brand, domain name or IP address will not circumvent the ban.
34	105	All companies providing Internet infrastructure should have clear terms of service which prohibit the use of their service for inciting hate or violence. They should also give notice that the service may be terminated without notice for serious breaches of this rule. Companies may further wish to require that any customer they provide a service to, includes a similar statement in its terms of service.

Recommendations for Law Makers

Number	Page	Recommendation
6	28	Laws and policies designed to prevent the spread of extremist material need to be flexible enough to cover content consisting of a link which directly or indirectly will lead to the material.
38	109	Governments should consider law reforms to create a system of sanctions that could be imposed on companies outside their jurisdiction who, after suitable notice, continue to provide unlawful content inciting hatred or violent extremism to users in that country, in breach of the country's law. Such law reform could also create sanctions that impose penalties for any company within the country's jurisdiction who engage in business with a company on the sanctions list.

Recommendations for Executive Government

Number	Page	Recommendation
35	107	Governments continue to contribute to the costs of security for Jewish communal institutions and provide additional support at times of increased risk such as during Yom Kippur.
33	105	Decisions by governments to restrict access to a site should be robust enough that a change to the ownership, brand, domain name or IP address of the banned site will not circumvent the restriction. Government may need to monitor and update identification details to enforce such restrictions.

Recommendations for Civil Society

Number	Page	Recommendation

18	56	Civil society organisations should redact or avoid naming hosting services that are making terrorist content available, but should confidentially report such content to key stakeholders in government, industry and civil society.
9	33	Those responding to antisemitic manifestations and incidents should make use of the International Holocaust Remembrance Alliance's *Working Definition of Antisemitism.*

Recommendations for Australia

Number	Page	Recommendation
10	33	Australia should join with other IHRA member countries in formally adopting the International Holocaust Remembrance Alliance's *Working Definition of Antisemitism* for domestic use.
26	63	The eSafety Commissioner should refer all unclassified Abhorrent Violent Material for classification by the Classification Board. This should become a standard part of the process when new Abhorrent Violent Material is identified.
27	63	The eSafety Commissioner should refer to the Classification Board for classification the manifesto documents from the terrorist attacks in Halle, Poway and El Paso as was done in the case of Christchurch.
28	63	The eSafety Commissioner should announce when terrorist related material that has a risk of going viral has been given an RC rating and should advise the public to report any online copies to the eSafety Commissioner and not to share it.
29	63	In Australia, consideration should be given to creating a civil penalty regime for sharing material classified RC that promotes terrorism. Suitable exemptions should apply for those acting reasonably and in good faith for the purpose of journalism, scientific research or law enforcement.
30	63	The Classification Board should restore the previous tool that allowed more detailed interrogation of Classification Board decisions, specifically, it should allow all decisions in a given period for a particular classification, to be listed.
31	63	The Classification Board should ensure either the title or a useful description is provided for material which is given an RC classification. This is necessary as the public cannot comply with a ban if the banned content cannot be identified.

Recommendations for Specific Companies or Organisations

Number	Page	Recommendation
14	53	Google should commit to supporting the "Christchurch Call" across all parts of the business without exception. This includes preventing Google's search engine being used to access material promoting terrorism.
15	55	Through the Global Internet Forum to Counter Terrorism (GIFCT), technology companies should provide a contact mechanism that is staffed 24/7 and available to assist any platform whose technology is abused to share manifestos or live streaming.
16	56	Access to the *Terrorist Content Analytics Platform* should be available to researchers after they are vetted, to ensure they represent legitimate research efforts in government, academia or civil society.

17	56	The *Terrorist Content Analytics Platform* or a similar service should offer a tool for archiving and preserving online content for use by law enforcement and in legal proceedings. Adding content should be available to the public, but accessing archived content should be restricted to vetted people from government, academia and civil society.
13	51	Telegram should join GIFCT and implement a system to remove videos from its platform which are registered in the GIFCT Hashing database.

Recommendations for the Public

Number	Page	Recommendation
39	113	The public are urged not to share content from terrorist attacks such as manifestos or videos. If seen, this content should be reported to the relevant authorities, in Australia this being the eSafety Commissioner.