

NOTICE OF FILING

Details of Filing

Document Lodged:	Affidavit - Form 59 - Rule 29.02(1)
Court of Filing	FEDERAL COURT OF AUSTRALIA (FCA)
Date of Lodgment:	7/05/2024 8:42:47 AM AEST
Date Accepted for Filing:	8/05/2024 10:56:43 AM AEST
File Number:	NSD474/2024
File Title:	ESAFETY COMMISSIONER v X CORP.
Registry:	NEW SOUTH WALES REGISTRY - FEDERAL COURT OF AUSTRALIA

Registrar

Important Information

This Notice has been inserted as the first page of the document which has been accepted for electronic filing. It is now taken to be part of that document for the purposes of the proceeding in the Court and contains important information for all parties to that proceeding. It must be included in the document served on each of those parties.

The date of the filing of the document is determined pursuant to the Court's Rules.

AFFIDAVIT

**FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NEW SOUTH WALES
DIVISION: GENERAL**

NO NSD 474 OF 2024

ESAFETY COMMISSIONER

Applicant

X CORP.

Respondent

Affidavit of: Toby Allan Dagg

Address: Level 5, The Bay Centre, 65 Pirrama Road, Pyrmont NSW 2009

Occupation: General Manager

Date affirmed: 6 May 2024

Contents:

Document Number	Details	Paragraph(s) of affidavit referring to annexure(s)	Page
1.	Affidavit of Toby Allan Dagg in support of application for interlocutory injunction affirmed on 6 May 2024.		
2.	Annexure TAD-29 being an extract of the EU Internet Forum report published in October 2023	25	25
3.	Annexure TAD-30 being a Social Media News article dated 1 February 2024 entitled 'Social Media Statistics Australia – January 2024'	26	33
4.	Annexure TAD-31 being a traffic analytics report from Semrush measuring visits by Australian users on any device dated 5 May 2024	28	38
5.	Annexure TAD-32 being two screenshots taken on 4 May 2024 of a URL subject to an informal request made to X Corp (Example 1)	37	40
6.	Annexure TAD-33 being a screenshot taken on 23 April 2024 of a URL subject to an informal request made to X Corp (Example 2)	43	42

Filed on behalf of the Applicant, eSafety Commissioner

File ref: 24003626

Prepared by: Matthew Garey
AGS lawyer within the meaning of s 551 of the *Judiciary Act*
1903

Address for Service:
The Australian Government Solicitor,
Level 10, 60 Martin Place, Sydney, NSW 2000
Matthew.Garey@ags.gov.au

Telephone: 02 9581 7625
Lawyer's Email:
Matthew.Garey@ags.gov.au
Facsimile: 02 6169 3054

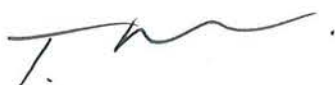
Document Number	Details	Paragraph(s) of affidavit referring to annexure(s)	Page
7.	Annexure TAD-34 being two screenshots taken on 2 May 2024 of a URL subject to an informal request made to X Corp (Example 3)	49	44
8.	Annexure TAD-35 being a screenshot of results of a Google search for 'best VPNs to access Twitter' taken 6 May 2024	50	46
9.	Annexure TAD-36 being five screenshots taken on 5 May 2024 depicting access to the Video while not logged into any registered X account	68	48
10.	Annexure TAD-37 being three screenshots taken on 5 May 2024 depicting access to the Video while logged in to an Adult Account with Location Services on	69	52
11.	Annexure TAD-38 being 29 screenshots taken on 5 May 2024 depicting access to the Video while logged in to an Underage Account	70	56
12.	Annexure TAD-39 being 31 screenshots taken on 5 May 2024 depicting access to the Video in a private browser without logging in to a registered X account	71	86
13.	Annexure TAD-40 being 22 screenshots taken on 5 May 2024 depicting access to the Video in a private browser while logged in to an Adult Account	72	104
14.	Annexure TAD-41 being a Security.org article dated 23 January 2024 entitled '2024 VPN Trends, Statistics, and Consumer Opinions'	73	127
15.	Annexure TAD-42 being a Comparitech article dated 9 February 2021 entitled 'VPN Market Report 2024: Who's got the biggest VPN market share	74	134
16.	Annexure TAD-43 being a Comparitech article dated 30 April 2024 entitled '8 Best VPNs for Australia for fast streaming and privacy (2024)'	75	162
17.	Annexure TAD-44 being a Comparitech article dated 15 March 2024 entitled 'How to remove geo-blocking with a VPN and change your location'	76	207

I, Toby Allan Dagg of level 5, The Bay Centre, 65 Pirrama Road, Pyrmont 2009 in the State of New South Wales, General Manager, affirm:

1. I am the General Manager of the Regulatory Operations Group within the Office of the eSafety Commissioner (**eSafety**) and I am authorised to make this affidavit on behalf of the Applicant, the eSafety Commissioner (**Commissioner**).
2. I make this affidavit on the basis of my own knowledge and belief, save where otherwise stated. Where I depose to any matter based on information provided to me, I believe it to be true.
3. I have previously affirmed an affidavit in this proceeding dated 22 April 2024 (**First Affidavit**). I adopt the defined terms in my First Affidavit.

ESAFETY'S RESPONSE TO THE VIDEO

4. At approximately 8.30pm on 15 April 2024, I spoke by phone with the acting Executive Manager of the Investigations Branch. He told me words to the effect that "eSafety's team of on-call investigations staff are being recalled to duty to monitor major social media platforms and notify the material to their providers" in response to the alleged stabbing at a church in Wakeley in Sydney. Therefore, from about 9.00pm on 15 April 2024, a team of eSafety investigators within the Investigations Branch was monitoring the circulation of the Video on major platforms.
5. By 9:00am on Tuesday 16 April 2024 that team had identified approximately 100 URLs on X and 50 URLs on Facebook that appeared to link to the Video. These amounted to by far the largest volume of readily identifiable forms of the Video on any site or platform being monitored, which included, amongst others, TikTok, Instagram, Snapchat, Facebook, Reddit and Telegram.
6. When seeking to minimise the harm or likely harm from online distribution of material such as the Video, eSafety's approach includes monitoring and identifying major platforms on which the material is being distributed and quickly taking action in relation to those platforms.
7. In my experience with eSafety investigations, it is necessary to act quickly in relation to such content being shared on large social media platforms, to limit to the extent possible the proliferation of the material across those platforms, where it can build momentum and go viral (meaning that the information propagates rapidly on a service and the Internet more broadly, including other social media platforms).
8. Viral material is typically shared widely and has a high degree of engagement by users. Should that occur in the circumstances of class 1 material, it would significantly increase the number of Australians potentially exposed to harm from viewing the content.
9. eSafety has a range of informal and formal compliance options when seeking to remove or limit access to illegal and restricted online content. It may approach online service providers informally to remove material in the first instance, where this may be



the fastest means to achieve removal of the material, resulting in fewer Australians being exposed to harmful online content.

10. In addition to the action eSafety took in relation to the Video on X described in my First Affidavit, it also took action across a range of other major online services in relation to distribution of the Video. These included Reddit Inc (**Reddit**), operator of the Reddit platform, Meta Platforms, Inc (**Meta**), operator of Facebook and Instagram, and Telegram FZ-LLC (**Telegram**), operator of Telegram.

OTHER NOTICES ISSUED IN RELATION TO THE VIDEO

11. Between 16 April and 25 April 2024, eSafety issued removal notices pursuant to sections 109 and 110 the Act to several online service providers and hosting service providers in relation to the distribution of the Video. Those entities were:
 - a) Meta. I am informed that Meta complied with the notice within 1 hour of the notice being given.
 - b) Rumble Canada Inc. I am informed that no response was received. I am informed that the material appears to have been geo-blocked.
 - c) Nocix LLC. I am informed that no response was received. I am informed that the notice was not complied with.
 - d) Amarutu Technology Ltd. I am informed that no response was received. I am informed that the notice was not complied with.
 - e) Verasel Inc. I am informed that no response was received. However, I am informed that the notice was complied with.
 - f) Google LLC. Of the three items identified in the notice I am informed that one item was geo-blocked, and the other two were removed.
 - g) X Corp.
12. Between 19 April and 23 April 2024, eSafety issued link deletion notices pursuant to section 124 of the Act to key search engine service providers in relation to links containing the Video:
 - a) Google LLC, in relation to Google Search
 - b) Microsoft Corporation, in relation to Bing.
13. I have set out the detail of some of the actions taken by eSafety in relation to other platforms below.



Reddit Inc

14. On 16 April 2024, eSafety contacted Reddit to request, on an informal basis, that it remove the Video from 14 URLs at which the content of the Video could be located on the Reddit platform.
15. eSafety received a response from Reddit on the same day to the effect that the Video had been removed from the 14 URLs for violating Reddit's Content Policy.
16. eSafety investigators subsequently confirmed to me that the URLs could no longer be accessed by them on Reddit, including via use of a VPN set to the United States.

Meta Platforms, Inc.

17. On 16 April 2024, eSafety contacted Meta via Meta's reporting webform to notify it of URLs on Facebook at which the Video was available.
18. In each case eSafety received responses from Meta stating the Video had been removed.
19. eSafety investigators subsequently informed me that they were no longer able to access the content of those URLs, including via use of a VPN set to the United States.
20. I have set out further detail in relation to eSafety's approach in respect of Meta at paragraph 56 and 57 of the First Affidavit.

Telegram

21. On 16 April 2024 eSafety contacted Telegram in relation to 18 URLs on the Telegram platform at which footage contained in the Video was available.
22. eSafety investigators subsequently informed me that they were no longer able to access the content of those URLs.

PRIORITISING ONLINE SERVICES DURING A RESPONSE

23. Based upon my experience and observations as a user of X and through my role at eSafety as an investigator of online services, some of the features of X as a social media platform that facilitate the rapid sharing and spread of material include the following:
 - a) its design is based on short-form text posts, allowing for fast, near real-time responses to events
 - b) by default, posts on X are visible to any user on the service, not just those who follow a specific account. The 'retweet' button allows for any user to immediately re-broadcast a post to their own followers, potentially enabling exponential increase to the reach of a tweet in just moments.



24. It is my experience, having led operational responses to incidents such as livestreamed terror attacks, that it is necessary in such a response to prioritise an assessment of how material of concern (such as class 1 material) is circulating on those online services most commonly used by Australians. My experience of such operations is that material is often shared on major social media services such as Facebook and X before entering secondary distribution channels to sites promoting 'gore' and death-related content, or violent extremism. 'Gore' sites are websites dedicated to sharing and disseminating extremely violent material, including material depicting a person engaging in a terrorist act, murder, attempts to murder and torture.
25. I am also aware of the findings of a 2022/2023 study commissioned by the European Commission and published as part of the EU Internet Forum on the role and effects of the use of algorithmic amplification to spread terrorist, violent extremist and borderline content. The final report was published in October 2023 and found that:
- a) Twitter had the highest findability score of terrorist and violent extremist material out of a group of YouTube, Facebook, Instagram, Twitter and TikTok (the platforms analysed in the study) (pages 2 and 63 of Annexure TAD-29).
 - b) Twitter showed the highest level of amplification of such material (pages 2 and 95 of Annexure TAD-29). I understand that findability in this study refers to how many pieces of content a motivated user can find during a targeted search on the platform within a limited time window.
 - c) Terrorist and violent extremist content is shared more widely on Twitter (page 77 of Annexure TAD-29).

A true copy of an extract of the EU Internet Forum report published in October 2023 is annexed hereto and labelled **Annexure TAD-29**.

26. On 6 May 2024, I accessed and reviewed a publicly accessible webpage published by Social Media News on 1 February 2024 entitled 'Social Media Statistics Australia – January 2024' which is available at <https://www.socialmedianews.com.au/social-media-statistics-australia-january-2024/>. The page states that:

Now that Elon Musk has full control over Twitter, which has now been renamed to X – we have actually seen user growth to the platform with 250 million + monthly active users, globally.

...

Social Media Statistics Australia – January 2024

...

7. X, formerly Twitter – 6,000,000 Monthly Active Australian Users approx.

A true copy of the webpage 'Social Media Statistics Australia – January 2024' is annexed hereto and labelled **Annexure TAD-30**.

27. I am informed by a member of eSafety's strategic communications team and believe that the member, whose functions include website analytics, accessed eSafety's account with Semrush on Sunday 5 May 2024. I am informed by the member of



eSafety's strategic communications team and believe Semrush is a widely used tool in the online content industry, providing a range of reports including traffic measurement.

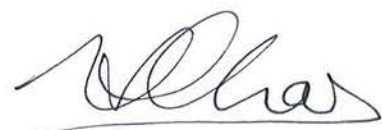
28. I am informed by the member of eSafety's strategic communications team and believe that the member of staff downloaded a traffic analytics report from Semrush that measured visits by Australian users on any device to each of the services identified in the affidavit of Justin Quill affirmed on 2 May 2024 as well as visits to the twitter.com website for the period 1 January to 31 March 2024.

A true copy of the traffic analytics report from Semrush measuring visits by Australian users on any device is annexed hereto and labelled **Annexure TAD-31**.

29. The services and platforms identified in paragraphs 11 to 22 above were prioritised as part of eSafety's response to the Wakeley attack for several reasons. These include prioritisation based on the size of a service and its ease of use, the preferences of users seeking to exploit the material for ideological ends, and the nature of public reports made to the Commissioner about class 1 material.
30. In my experience, in formulating an initial response to an event such as what happened in Wakeley, eSafety seeks to limit or suppress distribution of class 1 material online. This suppression is to primarily achieve the goal of reducing the likelihood of harm being experienced by users of online services who encounter the material inadvertently while using the service. The Commissioner does not (and cannot) 'police' the internet. To the extent that class 1 material can be located elsewhere online than the locations prioritised by the Commissioner through exercise of regulatory functions, this reflects the size and complexity of the internet. eSafety does not seek to remove all possible instances of an item of material from every site or platform online. If a person undertakes a concerted effort to locate the Video, they will likely succeed in that attempt. eSafety's emphasis is on reducing the likelihood of the material being easily discovered by Australian end-users and widely distributed.

X CORP'S PREVIOUS REMOVAL OF MATERIAL FROM X

31. There have been a number of instances in which eSafety has issued informal requests to X Corp for the removal of content that the Commissioner considers to be class 1 material under the Act.
32. In some of those instances, X Corp has responded to those requests by either removing the material and/or suspending the X user's account. I have set out three examples below:
- a) Example one shows that X, following an informal removal request by eSafety, removed the Video and suspended the account of the user who posted the Video: Paragraphs 33 to 37 below.
 - b) Example two shows that X, following an informal removal request by eSafety, within 24 hours suspended the account of the user who posted a video depicting a motor vehicle accident where police officers in Australia were killed: Paragraphs 38 to 43 below.



- c) Example three shows that X, following an informal request by eSafety, removed a video depicting an alleged terror attack in the United States and suspended the account of the user who posted the video: Paragraphs 44 to 49 below.

Example one

33. On 15 April 2024 at 8:47pm AEST, eSafety received a complaint about the Video.
34. On 26 April 2024 at approximately 10:45am AEST, an investigator at eSafety sent an informal removal request to X Corp for the removal of the video at the URL via X Corp's Law Enforcement Request reporting portal at <https://help.twitter.com/en/forms/law-enforcement/report-illegal-content>.
35. On 26 April 2024 at 10:47am AEST, an automated response from 'Twitter' was received at online@esafety.gov.au, confirming receipt of eSafety's request to remove content and noting that the request had been escalated to the appropriate team and would be reviewed and responded to as soon as possible.
36. On 26 April 2024 at 4:03pm AEST, an automated response from 'Twitter' was received at online@esafety.gov.au confirming that the team was now investigating the matter.
37. On 4 May 2024, eSafety investigators accessed the URL included in the informal request and confirmed that the account that posted the Video had been suspended by X. I am informed by the Executive Manager of Investigations and believe that the eSafety investigators took the following steps to access the URL:
- a) eSafety investigators input the link into the Chrome web browser while logged into an X account. A page appeared that showed the words: "This Post is from a suspended account."
- A screenshot of the URL when accessed without a VPN on 4 May 2024 is annexed hereto and labelled 'Image 1' in **Annexure TAD-32**.
- b) eSafety investigators then checked the URL using an active NordVPN connection to create the appearance that the device's internet traffic was originating from the US. The investigators identified that the material had been removed, with text appearing stated: "This Post violated the X Rules."

A screenshot of the URL when accessed with NordVPN on 4 May 2024 is annexed hereto and labelled 'Image 2' in **Annexure TAD-32**.

Example two

38. On 23 April 2024, eSafety received a complaint about the availability of a video depicting a motor vehicle accident where police officers in Australia were killed.
39. On 23 April 2024 at 2:25pm AEST, an investigator at eSafety sent an informal removal request to X Corp for the removal of the video at the URL via X Corp's Law Enforcement Request reporting portal at <https://help.twitter.com/en/forms/law-enforcement/report-illegal-content>.



40. On 23 April 2024 at 2:26pm AEST, an automated response from 'Twitter' was received at online@esafety.gov.au, confirming receipt of eSafety's request to remove content and noting that the request had been escalated to the appropriate team and will be reviewed and responded to as soon as possible.
41. On 23 April 2024 at 2:56pm AEST, an automated response from 'Twitter' was received at online@esafety.gov.au confirming that the team was now investigating the matter.
42. On 23 April 2024 at 3:16pm AEST, an email from 'Twitter' was received at online@esafety.gov.au confirming that the account which had posted the video had been suspended for violating Terms of Service.
43. On 23 April 2024 at 4:35pm AEST, an eSafety investigator accessed the URL included in the informal request and confirmed that the video had been removed and the account that posted the video had been suspended. I am informed by the Manager of the Illegal and Restricted Content team and believe that the investigators took the following steps to do so:

- a) With Nord VPN turned on and set to the US, the investigator accessed the URL at approximately 4:36pm using the Chrome web browser without logging in to a registered X account. The URL did not contain the Video and contained the following text: "Hmm...this page doesn't exist. Try searching for something else."


A true copy of the screenshot taken on 23 April 2024 at approximately 4:36pm is annexed hereto and labelled 'Image 1' of **Annexure TAD-33**.

- b) With Nord VPN turned on and set to the US, the investigator accessed the URL at approximately 4:40pm using the Chrome web browser after logging in to a registered X account. The URL did not contain the Video and contained the following text: "This Post is from a suspended account."

A true copy of the screenshot taken on 23 April 2024 at approximately 4:40pm is annexed hereto and labelled 'Image 2' of **Annexure TAD-33**.

Example three

44. On 24 April 2024 at 5:57pm AEST, eSafety received a complaint about the availability of a video depicting an alleged terror attack in the United States in May 2022.
45. On 26 April 2024, an investigator at eSafety sent an informal removal request to X Corp for the removal of the video at the URL via X Corp's Law Enforcement Request reporting portal at <https://help.twitter.com/en/forms/law-enforcement/report-illegal-content>.
46. On 26 April 2024 at 1:00 pm AEST, an automated response from 'Twitter' was received at online@esafety.gov.au, confirming receipt of eSafety's request to remove content and noting that the request has been escalated to the appropriate team and will be reviewed and responded to as soon as possible.



47. On 26 April 2024 at 3:33pm AEST, an automated response from 'Twitter' was received at online@esafety.gov.au confirming that the team was now investigating the matter.
48. On 27 April 2024 at 5:34pm, an email from 'Twitter' was received at online@esafety.gov.au confirming that the account which had posted the video had been suspended for violating Terms of Service.
49. On 2 May 2024, eSafety investigators accessed the URL included in the informal request and confirmed that the video had been removed and the account that posted the video had been suspended. I am informed that the investigators took the following steps to do so:

- a) Investigators input the link into an Edge browser on a computer while logged into an X account. A page appeared that showed the words "This Post is from a suspended account."

A screenshot of the URL when accessed without a VPN on 2 May 2024 is annexed hereto and labelled 'Image 1' in **Annexure TAD-34**.

- b) On 4 May 2024, investigators then checked the URL in Chrome using an active NordVPN to create the appearance that the internet traffic was originating from the US. A page appeared that showed the words "This Post is from a suspended account."

A screenshot of the URL when accessed with a VPN on 4 May 2024 is annexed hereto and labelled 'Image 2' in **Annexure TAD-34**.

ABILITY OF AUSTRALIAN COMMUNITY TO VIEW THE VIDEO ON X USING A VPN

50. On 6 May 2024, I directed the Manager of the Illegal and Restricted Content team at eSafety to use a web browser to navigate to the search engine 'Google' at the following web address: <https://www.google.com/>. I am informed that the Manager typed in the words 'best VPNs to access Twitter' into the search field. A number of VPN names came up, including the following:

- a) NordVPN
- b) Proton VPN
- c) CyberGhost
- d) SurfShark VPN
- e) Express VPN

A true copy of the results of the search using the Google search engine is annexed hereto and labelled **Annexure TAD-35**.



51. I am informed by an investigator in the Illegal and Restricted Content team, to identify that the Video could be accessed on at least some of the 65 URLs contained in the Removal Notice in the following ways (each of them while using a VPN).
- a) First, while using NordVPN, where investigators were logged into a registered X account where the 'Birth date' of the account was over the age of 18 (**Adult Account**): Paragraphs 52 to 67 below;
 - b) Second, while using NordVPN where I was not logged into any registered X account: Paragraph 68 below.
 - c) Third, while using NordVPN where I was logged into an Adult Account with an Australian mobile number, my 'Country' set to Australia and my 'Precise location' shared with X: Paragraph 69 below.
 - d) Fourth, while using Norton Secure VPN, where an investigator was logged into a registered X account where the 'Birth date' of the account was under the age of 18 (**Underage Account**): Paragraph 70 below.
 - e) Fifth, while using NordVPN where an investigator cleared their 'cache' and 'cookies' before using an 'Incognito' browser without logging into a registered X account: Paragraph 71 below.
 - f) Sixth, while using NordVPN where an investigator cleared their 'cache' and 'cookies' before using an 'Incognito' browser while logged into an Adult Account: Paragraph 72 below.

Accessing the Video while logged in to an Adult Account

52. I am informed and believe that on the following dates, investigators in the Illegal and Restricted Content Team in Sydney, Australia undertook reviews of the URLs identified in the Notice and were able to access the Video using a VPN:
- a) On 26 April 2024, using Norton Secure VPN: Paragraphs 53 to 55 below.
 - b) On 29 April 2024, 30 April 2024, 1 May 2024, 2 May 2024, 3 May 2024 and 5 May, using NordVPN: Paragraphs 56 to 64 below.
 - c) On 6 May, using CyberGhost VPN: Paragraphs 65 to 67 below.
 - d) On 6 May, using Proton VPN: Paragraphs 65 to 67 below.
 - e) On 6 May, using SurfShark VPN: Paragraphs 65 to 67 below.
 - f) On 6 May, using Express VPN: Paragraphs 65 to 67 below.
53. I am informed by the Executive Manager of Investigations and believe that on 26 April 2024, an investigator in the Illegal and Restricted Content Team undertook a review of each of the 65 URLs identified in the Notice using a VPN to confirm whether the



material identified in the Notice had been placed behind a notice in accordance with the orders made by Justice Kennett on 24 April 2024.

54. I am informed by the Executive Manager of Investigations that the investigator undertook the following steps to do so:
- a) the investigator activated the Norton Secure VPN such that the IP address was made to appear as though it originated in the United States of America.
 - b) the investigator accessed the X app on an iPad.
 - c) using the list of URLs identified in the Notice, the investigator accessed each URL individually, which opened up the location in the X app.
55. The investigator identified that 64 of the URLs were still accessible in Australia using the Norton Secure VPN. Two URLs were no longer found to contain the material identified in the Notice. Material at one of the URLs has been removed with text appearing in a browser stating: 'Hmm...this page doesn't exist. Try searching for something else.' and text in the X app stating: "This post has been deleted." Therefore, 62 of the URLs in the Notice contained the Video when accessed using the Norton Secure VPN.
56. I am informed that on 29 April 2024, an investigator in the Illegal and Restricted Content Team undertook a review of each of the 65 URLs identified in the Notice using a VPN.
57. I am informed by the Executive Manager of Investigations that to do so, the investigator undertook the following steps:
- a) the investigator activated the NordVPN such that the IP address was made to appear as though it originated in the United States of America.
 - b) the investigator logged into X via the Google Chrome browser.
 - c) using the list of URLs identified in the Notice, the investigator accessed each URL individually, via the browser.
58. I am further informed by the Executive Manager of Investigations that the investigator identified that 64 of the URLs were still accessible in Australia using the NordVPN. Two URLs, being the same two URLs as in paragraph 55 were no longer found to contain the material identified in the Notice. Material at one of the URLs, being the same URL as in paragraph 55, has been removed with text appearing in a browser stating: 'Hmm...this page doesn't exist. Try searching for something else.' Therefore, 62 of the URLs in the Notice contained the Video when accessed using the NordVPN.
59. I am informed that on 30 April 2024, 1 May 2024 and 2 May 2024, an investigator in the Illegal and Restricted Content Team undertook a review of each of the 65 URLs identified in the Notice using a VPN. To do so, the investigator undertook the steps set out in paragraph 57 above. The investigator identified the same results as set out in paragraph 58 above.



60. I am informed that on 3 May 2024, an investigator in the Illegal and Restricted Content Team undertook a review of each of the 65 URLs identified in the Notice using a VPN. To do so, the investigator undertook the steps set out in paragraph 57 above.
61. I am further informed that the investigator identified that 64 of the URLs were still accessible in Australia using the NordVPN. Two URLs were no longer found to contain the material identified in the Notice. Material at one of the URLs has been removed with text appearing in a browser stating: 'Hmm...this page doesn't exist. Try searching for something else.' Two URLs had removed the post containing the material identified in the Notice. Therefore, 60 of the URLs in the Notice contained the Video when accessed using the NordVPN.
62. I am informed that on 5 May 2024, an investigator in the Illegal and Restricted Content Team undertook a review of each of the 65 URLs identified in the Notice using a VPN.
63. I am informed that, to do so, the investigator undertook the following steps:
- a) the investigator activated the NordVPN such that the IP address was made to appear as though it originated in the United States of America.
 - b) the investigator logged into X via the Chrome browser.
 - c) using the list of URLs identified in the Notice, the investigator accessed each URL individually, via the browser.
64. I am further informed that the investigator identified that 64 of the URLs were still accessible in Australia using the NordVPN. Two URLs were no longer found to contain the material identified in the Notice. Material at one of the URLs has been removed with text appearing in a browser stating: 'Hmm...this page doesn't exist. Try searching for something else.' Two URLs had removed the post containing the material identified in the Notice. Therefore, 60 of the URLs in the Notice contained the Video when accessed using the NordVPN.
65. I am informed that on 6 May 2024, investigators in the Illegal and Restricted Content Team undertook a review of a sample of 20 of the 65 URLs identified in the Notice using each of the following VPN services:
- a) CyberGhost VPN.
 - b) Proton VPN.
 - c) SurfShark VPN.
 - d) Express VPN
66. I am informed that, to do so, the investigator undertook the following steps:
- a) The investigator navigated to the 'Privacy and security' settings on the Chrome browser and cleared the 'cookies' and 'cache'.



'Cookies' are files installed and stored on devices during sessions of activity on the internet. 'Cookies' store information on devices between sessions of activity on the internet.

'Cache' is a working storage or memory space for files to allow for quicker loading. Web browsers hold copies of recently visited websites to avoid repeatedly transferring the same static data and only download any changes.

- b) the investigator activated the CyberGhost VPN, Proton VPN, SurfShark VPN or Express VPN such that the IP address was made to appear as though it originated in the United States of America.
 - c) the investigator logged into X via the Chrome browser on a laptop running Windows 11.
 - d) using the list of URLs identified in the Notice, the investigator accessed a sample of 20 of the URLs individually, via the Chrome browser.
67. I am further informed that the investigator identified that each of the URLs were still accessible using each of the CyberGhost VPN, the Proton VPN, SurfShark VPN and Express VPN and contained the Video. The investigator did not observe any warning or content label overlaid onto the Video at any of the 20 URLs.

Accessing the Video while not logged into any registered X account

68. Between approximately 8:45pm and 9:30pm on 5 May 2024 in Sydney, Australia, I took the following steps:

- a) I opened a Chrome browser on a laptop computer operating Windows 11 Home Edition.
- b) I then navigated to X at the following web address: <https://twitter.com>.
- c) I then confirmed that I was not logged in to X with a registered account.

A true copy of a screenshot of the X sign-in page is annexed hereto and labelled 'Image 1' of **Annexure TAD-36**.

- d) I then opened the NordVPN service (**NordVPN**), which I had purchased for use on the laptop computer from www.nordvpn.com.
- e) I then used NordVPN to create the appearance that my web traffic originated in the United States. The following IP address was assigned to my device by NordVPN: 185.169.0.28.

A true copy of a screenshot of the NordVPN is annexed hereto and labelled 'Image 2' of **Annexure TAD-36**.



f) I then navigated to the following NordVPN web address:
<https://nordvpn.com/what-is-my-ip/>. That web address identifies the location from which a user's web traffic appears to be originating.

g) I then saw that my web traffic appeared to be originating from Santa Clara, California.

A true copy of the screenshot of my IP address location is annexed hereto and labelled 'Image 3' of **Annexure TAD-36**.

h) I then input each of the 65 URLs contained in the Notice into the Chrome browser on the laptop computer.

i) Of the 65 URLs, in respect of 45 of them I saw the following text: 'Hmm...this page does not exist'.

j) Of the 65 URLs, 20 of them contained the Video. Each of those 20 posts contained a warning label which appeared to be overlaid on material beneath it.

A true copy of an example of a screenshot with the warning label is annexed hereto and labelled 'Image 4' of **Annexure TAD-36**.

k) Underneath the above text was the word 'Show'. I clicked the word 'Show' on each of the 20 posts. After clicking the word 'show', I was able to view the Video.

A true copy of an example of a screenshot with the warning label is annexed hereto and labelled 'Image 5' of **Annexure TAD-36**.

Accessing the Video while logged in to an Adult Account with Location Services on

69. Between approximately 7:45pm and 8:45pm on 5 May 2024 in Sydney, Australia, I took the following steps:

a) I opened the X application on an iPhone 13 running iOS 16.3.1.

b) I then confirmed that the iPhone 13 iOS settings had 'Location Services' toggled 'on'. I understand that by having 'Location Services' toggled 'on' means that the iPhone 13 would use GPS and other means to determine the approximate location of the device.

c) I then confirmed that I was logged in to X with a registered account.

d) I then navigated to the 'Account' settings of my registered account on the X app.

e) I then confirmed that the 'Account' settings of my registered account on the X app:

i. in the field titled 'Phone', included my Australian mobile number which began with the following dialling code unique to Australia: +61.



- ii. in the field titled 'Country', recorded that I was in Australia.
- f) I then navigated to the 'Location information' settings of my registered account on the X app.
- g) I then confirmed that the 'Location information' settings of my registered account on the X app had enabled the 'Precise location'.

I saw that 'Precise location' in the 'Location information' settings of my registered account on the X app was described as: 'If enabled, X will collect, store and use your device's precise location, such as GPS information. This lets X improve your experience – for example, showing you more local content, ads, and recommendation'.

- h) I then opened NordVPN, which I had purchased for use on the iPhone 13 from www.nordvpn.com.
- i) I then used NordVPN to create the appearance that my web traffic originated in the United States.
- j) I then navigated to each of the URLs contained in the Removal Notice into the X app on the iPhone 13.
- k) Of the 65 URLs, in respect of 46 of them I saw the following text: 'This post is unavailable. Learn more'.
- l) Of the 65 URLs, 19 of them contained the Video. I did not observe any warning or content label overlaid onto the Video at any of the 19 URLs. I was able to view the Video.

A true copy of screenshots of three of these posts is annexed hereto and labelled 'Image 1' to 'Image 3' in **Annexure TAD-37**.

Accessing the Video while logged in to an Underage Account

70. I am informed by an investigator in the Illegal and Restricted Content Team at eSafety that between about 12:44pm and 3:58pm on 5 May 2024 in Sydney, Australia, an eSafety investigator took the following steps:

- a) The investigator opened the Norton Secure VPN application on an iPad device, which had been purchased for use on that iPad device from Sydney, Australia.
- b) The investigator used Norton Secure VPN to create the appearance that the web traffic on the iPad device originated in the United States. The following IP address was assigned to the iPad device by Norton VPN: 18.117.149.210.

A true copy of a screenshot of Norton VPN is annexed hereto and headed 'Image 1' in **Annexure TAD-38**.



- c) The investigator then opened the X app on the iPad device. The investigator then logged into an X registered account set up by eSafety. At the time of setting up the account, the 'Birth date' input by investigators was 10 September 2010 (**Underage Account**).

A true copy of a screenshot of the Underage Account profile is annexed hereto and labelled 'Image 2' in **Annexure TAD-38**.

- d) After logging into the Underage Account, the investigator navigated to a sample of 19 of the 65 URLs contained in the Notice in the X app on the iPad device.
- e) Of the 19 URLs, in respect of 11 of them the investigator saw the following text: 'Age-restricted graphic content. This content might not be appropriate for people under 18 years old. Learn more'.

A true copy of a screenshot of the 11 URLs is annexed hereto and labelled 'Image 19' to 'Image 29' in **Annexure TAD-38**.

- f) Of the 19 URLs, eight of them contained the Video. Each of those eight posts contained a warning label which appeared to be overlaid on material beneath it.
- i. In respect of three of the eight posts containing the Video, the warning label stated:

Content warning: Sensitive content

The author labelled this post as containing sensitive content.

A true copy of those three posts is annexed hereto and labelled 'Image 3', 'Image 13' and 'Image 15' in **Annexure TAD-38**.

- ii. In respect of five of the eight posts containing the Video, the warning label stated:

Content warning: Graphic Content

X labeled this post as containing Graphic Content.

A true copy of those five posts is annexed hereto and labelled 'Image 5', 'Image 7', 'Image 9', 'Image 11', 'Image 17' in **Annexure TAD-38**.

- g) Underneath the above text was the word 'Show'. The investigator clicked the word 'Show' on each of the eight posts. After clicking the word 'show', the investigator was able to view the Video.
- h) Underneath each of the eight posts, the investigator saw the following text: 'Share this post with anyone, even if they aren't on X yet'.



A true copy of the posts after clicking 'Show' to reveal the Video is annexed hereto and labelled 'Image 4', 'Image 6', 'Image 8', 'Image 10', 'Image 12', 'Image 14', 'Image 16', 'Image 18' in **Annexure TAD-38**.

Accessing the Video in a private browser without logging in to a registered X account

71. I am informed by an investigator in the Illegal and Restricted content team that between about 5:32pm and 7:18pm on 5 May 2024 in Sydney, Australia, an investigator at eSafety took the following steps:

- a) The investigator opened a Chrome browser on a laptop computer operating Windows 11.
- b) The investigator then navigated to the 'Privacy and security' settings on the Chrome browser and cleared the 'cookies' and 'cache'.

'Cookies' are files installed and stored on devices during sessions of activity on the internet. 'Cookies' store information on devices between sessions of activity on the internet.

'Cache' is a working storage or memory space for files to allow for quicker loading. Web browsers hold copies of recently visited websites to avoid repeatedly transferring the same static data and only download any changes.

A true copy of a screenshot of cache settings is annexed hereto and headed 'Image 1' in **Annexure TAD-39**.

- c) The investigator then entered an 'Incognito' Chrome browser. Using an 'Incognito' browser is intended to prevent the browser from saving a user's browsing history, cookies, site data and other information to the device.
- d) In an 'Incognito' Chrome browser, the investigator then opened NordVPN, which had been purchased for use on the laptop computer from Sydney, Australia.
- e) The investigator then used NordVPN to create the appearance that the web traffic from the 'Incognito' Chrome browser originated in the United States. The following IP address was assigned to the laptop by Norton VPN: 185.187.168.64.

A true copy of a screenshot of NordVPN is annexed hereto and headed 'Image 2' in **Annexure TAD-39**.

- f) The investigator then navigated to X at the following web address:
<https://twitter.com>.
- g) The investigator then confirmed that the 'Incognito' Chrome browser was not logged in to X with a registered account.
- h) The investigator then input a sample of 20 of the URLs contained in the Notice into the 'Incognito' Chrome browser on the laptop computer.



- i) Of the 20 URLs, in respect of 11 of them they saw the following text: 'Hmm...this page doesn't exist. Try searching for something else'.

A true copy of those 11 posts is annexed hereto and labelled 'Image 21' to 'Image 31' in **Annexure TAD-39**.

- j) Of the 20 URLs, nine of them contained the Video. Each of those nine posts contained a warning label which appeared to be overlaid on material beneath it.
- k) In respect of three of the nine posts containing the Video, the warning label stated:

'Content warning: Sensitive content

The author labelled this post as containing sensitive content.'

A true copy of those three posts is annexed hereto and labelled 'Image 3', 'Image 13' and 'Image 15' in **Annexure TAD-39**.

- l) In respect of six of the nine posts containing the Video, the warning label stated:

'Content warning: Graphic Content

X labeled this post as containing Graphic Content.'

A true copy of those six posts is annexed hereto and labelled 'Image 5', 'Image 7', 'Image 9', 'Image 11', 'Image 17' and 'Image 19' in **Annexure TAD-39**.

- m) Underneath the above text was the word 'Show'. Investigators clicked the word 'Show' on each of the 20 posts. After clicking the word 'show', Investigators were able to view the Video.

A true copy of those 20 posts is annexed hereto and labelled 'Image 4', 'Image 6', 'Image 8', 'Image 10', 'Image 12', 'Image 14', 'Image 16', 'Image 18', 'Image 20' in **Annexure TAD-39**.

Accessing the Video in a private browser while logged in to an Adult Account

72. I am informed by an investigator in the Illegal and Restricted content team that between about 4:10pm and 5.32pm on 5 May 2024 in Sydney, Australia, an investigator at eSafety took the following steps:

- a) The investigator opened a Chrome browser on a laptop computer operating Windows 11.
- b) The investigator then navigated to the 'Privacy and security' settings on the Chrome browser and cleared the 'cookies' and 'cache'.



'Cookies' are files installed and stored on devices during sessions of activity on the internet. 'Cookies' store information on devices between sessions of activity on the internet.

'Cache' is a working storage or memory space for files to allow for quicker loading. Web browsers hold copies of recently visited websites to avoid repeatedly transferring the same static data and only download any changes.

A true copy of a screenshot of cache settings is annexed hereto and headed 'Image 1' in **Annexure TAD-40**.

- c) The investigator then entered an 'Incognito' Chrome browser. Using an 'Incognito' browser is intended to prevent the browser from saving a user's browsing history, cookies, site data and other information to the device.
- d) In an 'Incognito' Chrome browser, the investigator then opened NordVPN, which had been purchased for use on the laptop computer from Sydney, Australia.
- e) The investigator then used NordVPN to create the appearance that the web traffic from the 'Incognito' Chrome browser originated in the United States. The following IP address was assigned to the laptop by NordVPN: 185.169.0.126.

A true copy of a screenshot of the NordVPN is annexed hereto and headed 'Image 2' in **Annexure TAD-40**.

- f) The investigator then navigated to X at the following web address:
<https://twitter.com>.
- g) The investigator then logged in using an X registered account set up by investigators. At the time of setting up the account, the 'Birth date' input by investigators was 17 July 1990.
- h) The investigator then input a sample of 20 of the URLs contained in the Removal Notice into the 'Incognito' Chrome browser on the laptop computer.
- i) Posts on X appeared when the investigator input each of the 20 URLs. The posts contained the Video. The investigator did not observe any warning or content label overlaid onto the Video at any of the 20 URLs. The investigator was able to view the Video.

A true copy of those 20 posts is annexed hereto and labelled 'Image 3' to 'Image 22' in **Annexure TAD-40**.

PREVALENCE OF VPN TECHNOLOGY

73. On 6 May 2024, I accessed and reviewed a publicly accessible webpage published by Security.org on 23 January 2024 entitled '2024 VPN Trends, Statistics, and Consumer Opinions' (**Security Org Page**) which is available at <https://www.security.org/resources/vpn-consumer-report-annual/>. The Security Org Page states that:



"Here are a few key insights from this year's report:

- VPNs have continued to grow in use and recognition: 95% of adults are now familiar with the technology, and 46% use VPNs. This means as many as 105 million Americans have VPNs today.
- The most popular VPNs were NordVPN, Proton VPN, and Google One VPN, which has surged in popularity since Google began offering it free with cloud storage subscriptions and Pixel 7 phones last year.
- About half of all users rely on VPNs for work or business applications, and an equal number use them on personal devices.
- Nearly 40% of users rely on VPNs to prevent tracking from search engines or social media sites. As many as 10 million American adults could begin using VPNs in 2024, underscoring the growing recognition of the significance of online privacy.

...

Far and away the most popular VPN among personal users in our study was NordVPN. NordVPN delivers privacy through features such as an automatic kill switch and Double VPN, which doubles the VPN encryption for extra privacy. NordVPN has also kept its promise not to keep IP addresses and VPN usage logs, which could improve trust among its users."

A true copy of the Security Org Page is annexed hereto and labelled **Annexure TAD-41**.

74. On 6 May 2024, I accessed and reviewed a publicly accessible webpage which appears to have been published by Comparitech on 9 February 2021 entitled 'VPN Market Report 2024: Who's got the biggest VPN market share?' (**Comparitech Market Report**) which is available at <https://www.comparitech.com/blog/vpn-privacy/vpn-market-share-report/>. The Comparitech Market Report states that:

"Which VPN has the greatest market share?

To find out, we looked at a number of factors, including how much each VPN has been searched for in Google, how "trendy" each VPN is, how big a social following each VPN has, how many website visits they're getting, and how many downloads and reviews they're getting on the App Store and Google Play.

...

NordVPN.

With almost 1.8 million searches per month, NordVPN is the most-searched VPN on Google. ExpressVPN comes second with 1.1 million, closely followed by Hotspot Shield with 1.04 million.

...

Out of the top 20 VPNs we've analyzed, the 5 with the most interest over the last year (from January to December 2019) are NordVPN, ExpressVPN, Hotspot Shield, Turbo VPN, and Psiphon.

We can see that NordVPN has, on average, been the most popular. The number of searches increases from August with a particular peak in October (which coincides with NordVPN's news of a data center breach).

...



Overall, then, NordVPN and ExpressVPN continue to hold a large share of the market but they are sharing this with the likes of Turbo VPN and Hotspot Shield, which also have huge followings. Out of these four, Turbo VPN is the only free service."

A true copy of the Comparitech Market Report is annexed hereto and labelled **Annexure TAD-42.**

75. On 6 May 2024, I accessed and reviewed a publicly accessible webpage published by Comparitech on 30 April 2024 entitled '8 Best VPNs for Australia for fast streaming and privacy (2024)' (**Comparitech Best VPNs page**) which is available at <https://www.comparitech.com/blog/vpn-privacy/best-vpn-australia/>. The Comparitech Best VPNs page states that:

"Are you tired of not being able to access streaming services in Australia or while abroad? A Virtual Private Network (VPN) could be your answer. With VPN usage on the rise within the country and among Australians traveling abroad, choosing a reliable service that meets your needs is crucial.

...

Best VPNs for Australia:

NordVPN: The best VPN for Australia. Best in class on security, with thousands of very fast, secure VPN servers to choose from. Works great with streaming sites like Netflix and includes a 30-day money-back guarantee.

...

A VPN, or virtual private network, encrypts a device's internet traffic and routes it through an intermediary server in a location of the user's choosing. This can allow Australians to access blocked content that's geo-locked in their own country. It can also provide a private tunnel through which P2P filesharing applications can be used."

A true copy of the Comparitech Best VPNs page is annexed hereto and labelled **Annexure TAD-43.**

76. On 6 May 2024, I accessed and reviewed a publicly accessible webpage published by Comparitech on 15 March 2024 entitled 'How to remove geo-blocking with a VPN and change your location' (**Comparitech Removal page**) which is available at <https://www.comparitech.com/blog/vpn-privacy/beat-geo-blocking-vpn/>. The Comparitech Removal page states that:

"How to avoid geo-blocking with a VPN

With the right VPN, it's easy to access region-locked services abroad. Just follow the steps below.

Here's how to get around geo-blocking using a VPN:

- 1. Start by signing up for a suitable VPN. We particularly recommend NordVPN, but Surfshark and ExpressVPN are two versatile, high-performance alternatives.*
- 2. Download and install the VPN app, taking care to get the right version for your device.*
- 3. Connect to one of your VPN's servers in the appropriate country. For example, you'll need to use a British server to unblock BBC iPlayer or a US one for Hulu.*
- 4. Log in to your chosen service and play previously geo-blocked content. In most cases, it should start immediately, but if not, clear your browser's cache and cookies, then refresh the page.*



...

When might I encounter geo-blocking?

...

Another situation in which you may encounter geo-blocking is when trying to access content that's restricted, banned, or against the law in your current location. This doesn't necessarily mean that you're up to no good; some countries just have different values, leading them to block things like gambling, dating, and social media sites.

...

How can websites and services tell which country I'm in?

Most of the time, services rely entirely on the user's real IP address to tell where they are in the world. However, more advanced platforms often employ additional verification measures. They could cross-reference your IP address with GPS location data if you're using a mobile device, for instance, or check your IP address against a list of known VPN servers.

...

Why isn't my VPN unblocking a particular service?

Some platforms have stricter geo-blocking than others. For instance, a local TV live stream likely won't have advanced geo-restriction and VPN-detection features built in. However, Netflix, an international network worth billions of dollars, absolutely does. This is why some users encounter errors like "You seem to be using an unblocker or proxy" when accessing geo-blocked services with a VPN.

...

What services can I access abroad with a VPN?

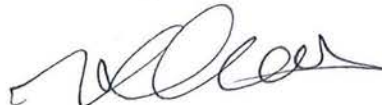
With the right VPN, you can access a huge variety of geo-blocked sites and services from anywhere in the world. Below, we've listed some of the types of geo-restricted content you can unblock: ...

- Social media (Facebook, Twitter, Instagram)

...

Roundup - best VPNs for beating geo blocking

1. NordVPN®



A true copy of the Comparitech Removal page is annexed hereto and labelled
Annexure TAD-44.

Affirmed by the deponent

at Pymont

in the State of NSW

on 6 May 2024



Before me:

Signature of witness:



Name of witness:

Ahram Choi

Qualification of witness:

Solicitor

ANNEXURE TAD-29

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NSW
DIVISION: GENERAL

NO NSD 474 OF 2024

ESAFETY COMMISSIONER

Applicant

X CORP

Respondent

The following 7 pages is the annexure marked TAD-29 referred to in the affidavit of
Toby Allan Dagg made on 6 May 2024 before me:


.....
Signature


.....
Qualification



DG HOME

EU Internet Forum: Study on the Role and Effects of the Use of Algorithmic Amplification to Spread Terrorist, Violent Extremist and Borderline Content

Final Report

Study commissioned by DG HOME,
drafted by Fincons, Trust Lab and Tremau,
in the context of the EU Internet Forum.
October – 2023

Abstract

The European Commission (DG HOME) commissioned this study for the European Union Internet Forum. The study examines the degree to which the five leading social media platforms in the EU, and in particular their recommender systems which proactively present content to users, algorithmically amplify terrorist and violent extremist content to online users. The study also examines the extent to which recommender systems amplify Borderline content, such as some forms of hate speech leading to violent extremism, disinformation and other forms of legal, but harmful content, that could lead to the creation of online filter bubbles, and recruitment and radicalisation of online users. The study analyses Facebook, Instagram, TikTok, Twitter and YouTube, covering eight markets/languages in the EU. The study was conducted from July 2022 to May 2023. Prior to this Final Report, the team submitted an Inception Report and two Interim Reports that complement this report.

Executive Summary

The European Commission (DG HOME) commissioned this study, performed by Trust Lab in collaboration with Tremau and coordinated by Fincons Group, which examines the degree to which five leading social media platforms and their recommender systems¹ amplify harmful Terrorist and Violent Extremist (TVE) content and “Borderline” content² to online users.

The Report reflects the study of Facebook, Instagram, TikTok, Twitter and YouTube, that operate in eight markets/languages, namely, Arabic, English, French, German, Italian, Polish, Russian and Spanish. The study looked at: (1) the extent to which a platform’s recommender system algorithmically amplifies TVE and Borderline content to users, and the impact of the dissemination of such content on a user’s journey to radicalisation; and (2) the extent to which a platform’s recommender system leads to the creation of online “filter bubbles”³ and the impact on a user’s adoption of violent extremist beliefs.

This study was a collaboration between Trust Lab, Professor Theodoros Evgeniou, Professor of Decision Sciences and Technology Management at INSEAD, who researched the risk of radicalisation linked to the dissemination of TVE content, and Fincons Group which handled project coordination.

¹ Recommender systems, also known as content curation systems, are the systems that prioritise content or make personalised content recommendations to online users. A key component of the recommender system is its recommender algorithm that determines the content a user will be served.

² As noted by the EU Internet Forum in its *Year in Review 2022*: “Borderline content, also known as harmful, but legal content, is content that comes close to infringing on the community guidelines of social media platforms or laws regulating online illegal content. Some of the most common types of Borderline content identified in the EU are anti-establishment/anti-institutions, antisemitic, anti-trans, misogynistic, anti-migrants, racist, or against COVID-19 measures.”

³ “Filter bubble” refers to a homogeneous feed/recommended content, caused by the algorithmic amplification of certain content types on a given platform. The higher proportion of similar content, the deeper/larger the filter bubble.

The European Commission's DG CONNECT has also been involved in the development of the study. The study was conducted from July 2022 to May 2023.

The study methodology is novel and discussed in Section 3.2 of the Report. Internal proprietary platform data (including algorithms), data, bots and Application Programming Interface (API) queries, which are common for this type of study, were not used. Trust Lab worked with human analysts to simulate motivated users intentionally seeking TVE content. The simulation was designed to ensure consistency and comparability across all platforms by the use of keyword lists, controlling for the amount of time exposed to each platform and repeating the experiments many times with different agents, thus increasing the likelihood of replicating the study's findings.

To address the six tasks defined by the study's sponsors, the following metrics were used:

- Findability: How easy is it to find harmful content, measured in the count of harmful posts during a one-hour interval?
- Removal Rate: What is the amount/percentage of harmful content removed by the platform?
- Removal Time: How much time did it take for harmful content to be removed by the platform?
- User Sentiment: What is the public (crowdsourced) perception of the appropriateness of harmful content, measured on a 5-point Likert scale?
- Amplification (filter bubble size): What is the amount of Bad Topic (TVE-related content, but not necessarily harmful content), Bad Content (TVE content), and Borderline content in a user's feed, measured as a percentage of the first 30 posts in the feed?

FINDINGS

Trust Lab's analysis found significant amounts of TVE content across all the major social media platforms as well as markets/languages. In addition, evidence of algorithmic amplification of TVE content on those platforms was also confirmed. The study identified significant differences in TVE-related performance and behaviour across all platforms and markets. The study's key findings include the following:

1. Evidence of amplification. The study validates the hypothesis that increased interaction with TVE content and Borderline content results in higher amplification of such content to users. All the platforms showed amplification of TVE-promoting content in their feeds. The percentage of TVE content in each platform's feed did not exceed 10% on average. Across all markets and platforms, the amplification of TVE content increased by 18% and Borderline content by 65%⁴. Twitter showed the highest level of amplification, YouTube ranked the second highest in amplifying TVE content, while TikTok showed the least. Regarding country and languages, platforms show the most TVE amplification occurring for Polish and German and for content related to Left-Wing political affiliation and younger Age Groups.

2. Findability Scores. Twitter had the highest findability scores of TVE content among the five platforms, and YouTube had the lowest findability score. Italian TVE content had the highest

⁴ This is the average percentage change between the first and third (final) amplification measurements across all languages and platforms. See the methodology, Section 3.2, for more details.

findability score of all languages when measured across all platforms. Violent Left-Wing TVE content had a significantly higher Findability score than other TVE types.

3. Removal Rates. More than 90% of the TVE content found by Trust Lab remained on the platforms by the end of the evaluation period 8 weeks later. TikTok removed more TVE content than the other platforms; Twitter and YouTube removed the least. Arabic TVE content was removed more frequently than the other languages, while Italian TVE content was removed less.

4. Borderline Content. Repeated cycles of user interaction and evaluation suggest that the amplification of Borderline content grows over time and at a higher rate than TVE content.

5. Variability across platforms and demographic blindspots. Each platform behaves differently in recommending TVE content with similar user features and behaviours. All platforms tended to recommend TVE at increasing rates as users interacted more with it, regardless of its TVE rating. Left-Wing politically oriented recommendations were far less likely to be removed by platforms than other groups. TikTok had a significantly low rate of success in amplifying TVE content to users, while Twitter and YouTube had the highest, with the former recommending most to Right-Wing and the latter recommending TVE content even to users with low rates of interaction. Ultimately, analysis based on user demographics and platform engagement data is still inconclusive to determine the full scope of how recommender algorithms operate on the back-end; more transparency and research is needed.

6.4 Task 1: Findability Charts

6.4.1 Findability per Platform

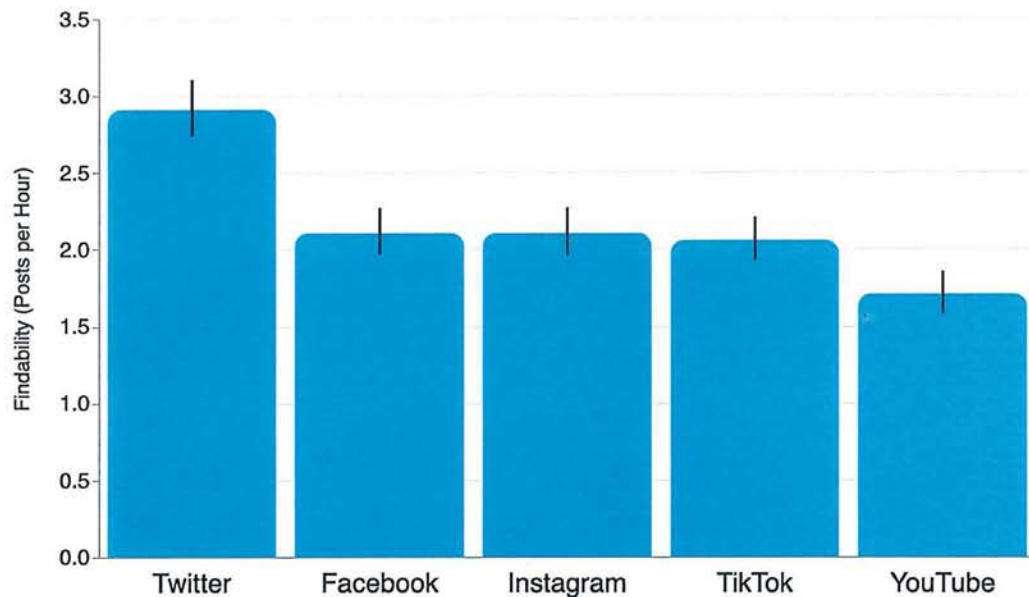


Figure A.6.4.1

The Findability Score is the average amount of content a motivated user can find on a given platform in a one-hour search period. The black lines in the bars represent 90% confidence intervals.

	Facebook	Instagram	TikTok	Twitter
YouTube	0.0012	0.0014	0.0030	0.0000
Twitter	0.0000	0.0000	0.0000	
TikTok	0.7036	0.7137		
Instagram	0.9930			

Table A.6.4.1

P-values on Findability per Platform

$\alpha = 0.01$ (Bonferroni correction from 0.05)

6.7 Task 1: User Engagement Charts and P-Values

6.7.1 Average Number of Shares

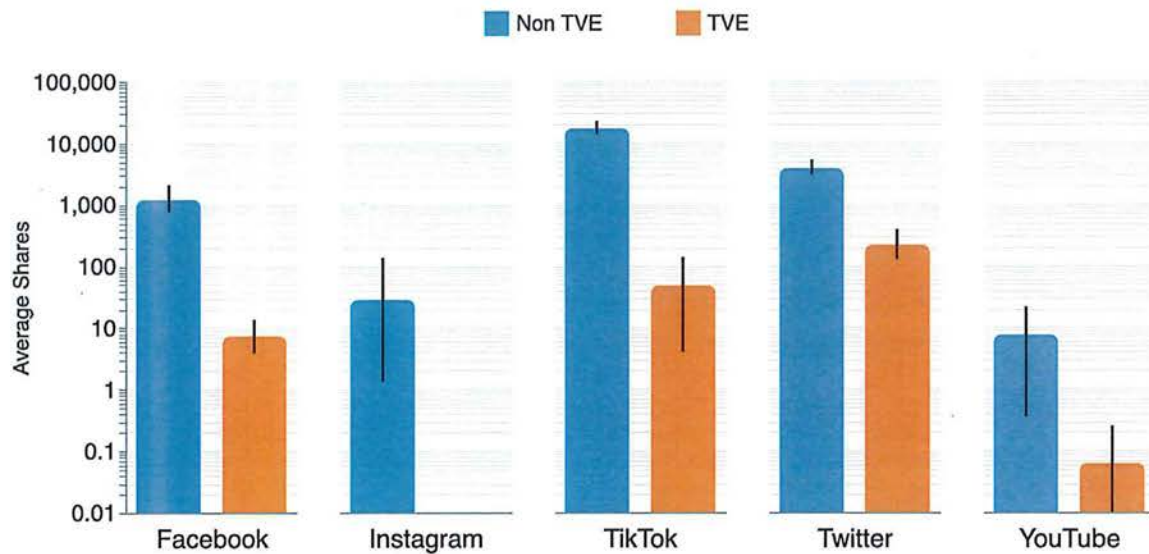


Figure A.6.7.1

This chart shows the average number of shares for TVE and non-TVE content on different platforms. The black lines in the bars represent 90% confidence intervals. Note that the Interaction charts all use a log scale instead of a linear scale.²⁹

²⁹ Since the range of values in these charts is very high, it would be difficult to visualise the bars that have lower values. Taking the logarithm makes the values closer in range on the log scale and hence easier to visualise the chart as a whole. Therefore, for the interaction charts, we are using log scales.

6.11.2 Amplification Average Percent of Bad Content in Feed per Platform

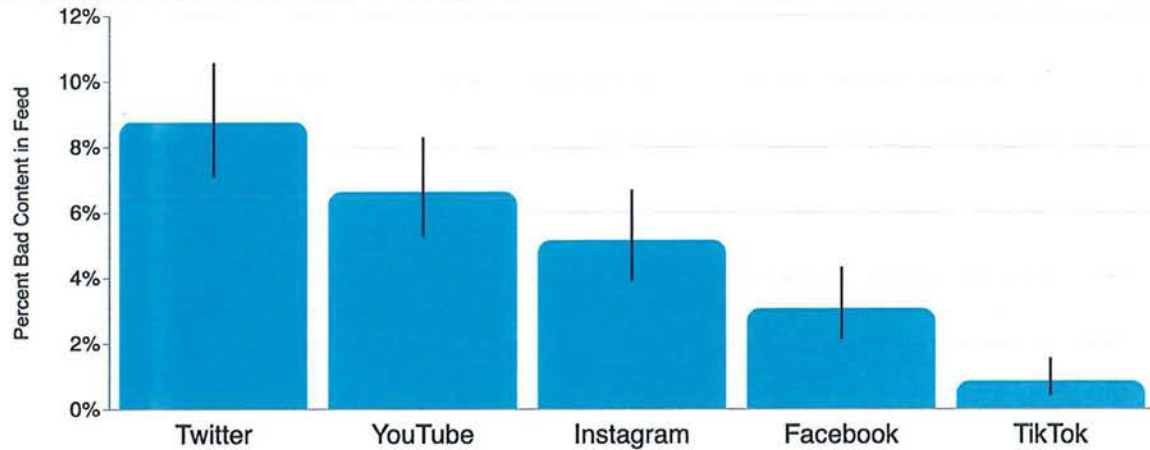


Figure A.6.11.2

This chart shows the average percentage of Bad (TVE) Content in the feeds of respective platforms. The black lines in the bars represent 90% confidence intervals.

	Facebook	Instagram	TikTok	Twitter
YouTube	0.0522	0.2201	0.4963	0.2536
Twitter	0.3872	0.9027	0.6548	
TikTok	0.2019	0.5803		
Instagram	0.4703			

Table A.6.11.2

P-values on Amplification Average Percent of Bad Content in Feed per Platform

$\alpha = 0.01$ (Bonferroni correction from 0.05)

ANNEXURE TAD-30

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NSW
DIVISION: GENERAL

NO NSD 474 OF 2024

ESAFETY COMMISSIONER

Applicant

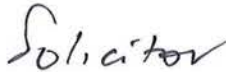
X CORP

Respondent

The following 4 pages is the annexure marked TAD-30 referred to in the affidavit of
Toby Allan Dagg made on 6 May 2024 before me:



Signature



Qualification

Filed on behalf of the Applicant, eSafety Commissioner
Prepared by: Matthew Garey
AGS lawyer within the meaning of s 55I of the *Judiciary Act 1903*

Address for Service:
The Australian Government Solicitor,
Level 10, 60 Martin Place, Sydney, NSW 2000
Matthew.Garey@ags.gov.au

File ref: 24003626

Telephone: 02 9581 7625
Lawyer's Email:
Matthew.Garey@ags.gov.au
Facsimile: 02 6169 3054

- Authors
- Events
- Jobs
- Advertise
- Contact
- POST A SPONSORED ARTICLE

[Send us a tip](#) 

[AUSTRALIAN SOCIAL MEDIA STATISTICS](#) | [SOCIAL MEDIA AGENCY](#) | [SOCIAL MEDIA EVENTS](#)

Social Media Statistics Australia – January 2024

[David Correll](#) on February 1, 2024 | [Australia](#) | [1 Comment](#)

January 2024 – Readers please note: On the 1st of every month we post a new social media report, the below report is not our latest figures. [Please see here the most up to date report.](#)

Now that Elon Musk has full control over Twitter, which has now been renamed to X – we have actually seen user growth to the platform with 250 million + monthly active users, globally.

Social Media users in Australia are some of the most active in the world, with a total of around 60% of the country's population an active user on Facebook, and 50% of the country logging onto Facebook at least once a day Google tried to compete with Facebook but never made significant progress to attract a large and active audience. They did have a security issue where user data was exposed and the incident was kept quiet for several months. As a result Google Plus has been shut down. This isn't entirely surprising as this social network never really gained traction in Australia.

Video is also a very popular medium in Australia with around 18 million Australian visitors to the YouTube website every month.

Social Media Statistics Australia – January 2024

1. Facebook – 19,000,000 Monthly Active Australian Users (steady)
2. YouTube – 18,000,000 Unique Australian Visitors per month (UAVs)
3. WhatsApp – 12,000,000 Active Australian Users
4. Instagram – 10,000,000 Monthly Active Australian Users (FB/ Instagram data)
5. LinkedIn – 6,500,000 Monthly Active Australian Users approx
6. Snapchat – 6,400,000 Monthly Active Australian Users (Snapchat data)
7. X, formerly Twitter – 6,000,000 Monthly Active Australian Users approx
7. WordPress.com – 5,100,000
9. Tinder – 4,000,000 Australian users (my estimation)
10. Tumblr – 3,700,000
11. WeChat – 2,900,000 Monthly Active Australian Users approx – (my estimation)
12. TripAdvisor – 2,800,000
13. TikTok – 2,000,000
14. Yelp – 1,500,000
15. Blogspot- 1,200,000
16. Hinge – 1,000,000
17. Flickr – 450,000
18. Pinterest – 290,000
19. Reddit – 110,000
20. MySpace – 70,000
21. RenRen – 70,000 Monthly Active Australian Users approx – (my estimation)
22. StumbleUpon – 39,000
23. Weibo – 35,000 Monthly Active Australian Users approx – (my estimation)
24. Digg – 10,000
25. Foursquare/Swarm – 9,000
26. Periscope – 9,000
27. Delicious – 7,000

Google Plus has been shut down worldwide

Stats Source: [Vivid Social – Social Media Agency](#).

(All figures represent the number of Unique Australian Visitors [UAVs] to that website over the monthly period – unless otherwise stated above. Facebook Data includes users of desktop, mobile, application and messenger services).

Australian Facebook Users As A Percentage Of The Total Population

According to the [Australian Bureau of Statistics Population Clock](#) there are now approximately 26 million Australians.

Facebook's recent data shows there are now 17 million active Australians on Facebook. Therefore approximately 65% of the total Australian population is an active Facebook user. This is a huge number.

Facebook Demographics in Australia

Age Bracket	Number of Users*
13 – 17	1,100,000
18 – 25	3,500,000
25 – 39	6,300,000
40 – 55	4,300,000
55 – 64	1,700,000
65+	1,500,000

*approx numbers of total users, not all necessarily active over the last month

Penetration of the Australian Population

Approximately:

- 6 in 10 Australians use Facebook
- 1 in 2 Australians uses Facebook on a daily basis
- 1 in 2 Australians use YouTube
- 1 in 3 Australians use Instagram
- 1 in 4 Australians use Snapchat

Global Stats of Interest

- Facebook Monthly Active Users (Worldwide) – 2.98 billion
- Facebook Daily Active Users (Worldwide) – 1.23 billion
- Instagram Monthly Active Users (Worldwide) – 600 million
- Instagram Daily Active Users (Worldwide) – 500 million
- LinkedIn Registered Users (Worldwide) – 467 million
- Snapchat Daily Active Users (Worldwide) – 161 million

Key Points to Note:

- TikTok has seen a quick rise in Australia, particularly amongst the age group of 13-17 years old.
- Instagram has re-introduced the Likes for photos in Australia after high demand. This feature is optional.
- Due to a security flaw, user data being exposed and overall small user update – Google Plus has been shut down.
- Snapchat has grown significantly in Australia and now has 6.4 million monthly active users and 4.5 million daily active users in Australia.
- Approximately 50% of the Australian population logs into Facebook on a daily basis.
- WhatsApp has close to 10 million active users in Australia
- Tier 2 and 3 networks such as Flickr, Pinterest, Google Plus, StumbleUpon whilst have more popularity in the US, have not caught mainstream use in Australia. As a result, Google Plus was shut down worldwide.
- A large proportion of the Chinese community in Australia use Chinese social media tools like WeChat, RenRen and Weibo and these networks are growing.
- LinkedIn now reports there are 10 million + registered users in Australia. According to our research – just over half of this number log in every month.

Contribute data – Do you have any of your own research from your work or social media agency than can help us with our Australian stats? Feel free to [contact us](#) and share your information. Otherwise feel free to leave a comment below and if suitable we will include this data in our reports.

Latest statistics – every month we post a new report with the latest statistics in Australia, [view our archive](#) to find the most up to date information.

Want to source our stats/ copy and paste them onto your website? Our work is licensed under [Creative Commons License CC BY-ND 3.0](#).

You are welcome to copy and paste our data, just include the following text and links at the start or end of your article:

Statistics compiled by [SocialMediaNews.com.au](#) for January 2024. Source: [Vivid Social - Social Media Agency](#). Figures correct as of 31/01/24.

Related Articles:

- [Social Media Statistics Australia - March 2024](#)
- [Social Media Statistics Australia - February 2024](#)
- [Social Media Statistics Australia - April 2024](#)
- [Social Media Statistics Australia - October 2023](#)
- [Social Media Statistics Australia - December 2023](#)



David Correll : Editor and Founder of SocialMediaNews.com.au. I also run a [Social Media Agency](#) where I do consulting work and Social Media Management. Connect with me: [Twitter](#) | [LinkedIn](#) | [Facebook](#) or [contact me here](#). Alternatively, you can send me an email at david@socialmedianews.com.au

Are you looking for a Social Media Agency, Consultant or Advisor?

Our Social Media Agency, [Vivid Social](#) is a specialist advisory service that helps companies large and small across Australia plan their social media & SEO strategies and execute their campaigns with realistic and achievable goals.

Need more?

We also offer an outsourced and contract **Social Media Director** service for companies large and small across Australia. Does your business need high-level advice, regular monthly input and feedback on your social media campaigns? Simply email us on info@vividsocial.com.au

In addition, we can help with **web design, hosting, graphic design** and **general web consulting**.

Does your business need a new website? We can build you a basic site in 3 business days. We can do everything for you - build you a website, host it, create a logo, and of course provide ongoing support and updates. [Visit our website](#) to find out more.



1 Comment

Login



Join the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name



Share

Best Newest Oldest



Cosette Paneque

3 months ago

Have you collected any data about the use of alternatives to X, such as Mastodon, Threads, and Bluesky? I'm curious if they're not on the list because the use numbers are so low, or data is unavailable, and we don't know.

0 0 Reply Share

Subscribe

Privacy

Do Not Sell My Data

SUBSCRIBE TO SOCIAL MEDIA NEWS

subscribe via email

Or get our [Monthly Email Newsletter](#).

Follow Social Media News Australia



MONTHLY NEWSLETTER SIGNUP

* indicates required

Email Address *

First Name

Last Name

Subscribe

Copyright 2010 - 2024 socialmedianews.com.au. All rights reserved. Various stock images and photography used under license from [Shutterstock](#).
Social Media News Australia has been created by [David Correll](#). Content Licensed under [Attribution-NoDerivs 3.0 \(CC BY-ND 3.0\)](#)
[Contact Us](#) | [Sitemap](#) | [Privacy Policy](#) | [Terms and Conditions](#)

ANNEXURE TAD-31

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NSW
DIVISION: GENERAL

NO NSD 474 OF 2024

ESAFETY COMMISSIONER

Applicant

X CORP

Respondent

The following 1 page is the annexure marked TAD-31 referred to in the affidavit of
Toby Allan Dagg made on 6 May 2024 before me:



.....
Signature



.....
Qualification

Filed on behalf of the Applicant, eSafety Commissioner
Prepared by: Matthew Garey
AGS lawyer within the meaning of s 551 of the *Judiciary Act 1903*

Address for Service:
The Australian Government Solicitor,
Level 10, 60 Martin Place, Sydney, NSW 2000
Matthew.Garey@ags.gov.au

File ref: 24003626

Telephone: 02 9581 7625
Lawyer's Email:
Matthew.Garey@ags.gov.au
Facsimile: 02 6169 3054

Bulk Analysis Jan – Mar 2024 Australia All devices

Target	Visits	Unique Visitors	Pages / Visit	Avg. Visit Duration	Bounce Rate
gettr.com	8,485	6,591	1.28	2:52	82.68%
wechat.com	668,863	396,031	1.32	3:55	79.31%
odysee.com	1,662,461	505,644	1.32	19:49	80.41%
douyin.com	2,109,210	706,284	2.71	16:00	58.89%
telegram.org	2,618,347	1,269,799	1.81	9:31	52.30%
yandex.com	4,457,064	1,579,410	2.52	9:11	53.10%
bitchute.com	6,588,191	1,125,172	1.53	15:36	75.85%
vk.com	6,807,501	2,569,692	2.62	9:13	54.91%
rumble.com	15,623,687	3,276,779	2.39	14:06	55.65%
9gag.com	25,031,698	1,698,106	1.99	23:09	65.38%
tiktok.com	104,147,733	40,915,875	1.99	12:23	67.71%
twitter.com	271,799,146	56,293,237	2.05	26:03:00	68.66%
instagram.co m	316,709,076	72,185,117	2.09	18:59	67.66%
reddit.com	591,205,830	95,533,325	2.13	16:33	66.98%
youtube.com	5,009,362,507	213,107,495	6.24	39:07:00	33.64%

ANNEXURE TAD-32

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NSW
DIVISION: GENERAL

NO NSD 474 OF 2024

ESAFETY COMMISSIONER

Applicant

X CORP

Respondent

The following 1 page is the annexure marked TAD-32 referred to in the affidavit of
Toby Allan Dagg made on 6 May 2024 before me:



.....
Signature



.....
Qualification

Image 1 of Annexure TAD-32



This Post is from a suspended account. [Learn more](#)



ArtsCulture @ArtsandCulture · Apr 15
Thousands. He has a huge following.



1



264



helloooo @speakshelloo · Apr 16
This is horrific.



1

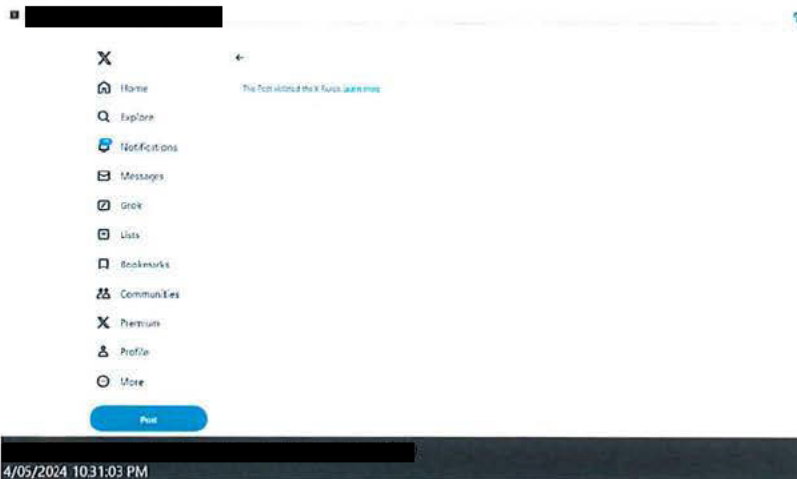


2

118



Image 2 of Annexure TAD-32



ANNEXURE TAD-33

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NSW
DIVISION: GENERAL

NO NSD 474 OF 2024

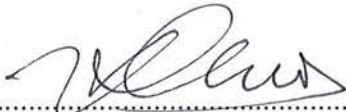
ESAFETY COMMISSIONER

Applicant

X CORP

Respondent

The following 1 page is the annexure marked TAD-33 referred to in the affidavit of
Toby Allan Dagg made on 6 May 2024 before me:



Signature



Qualification

Filed on behalf of the Applicant, eSafety Commissioner
Prepared by: Matthew Garey
AGS lawyer within the meaning of s 551 of the *Judiciary Act 1903*

Address for Service:
The Australian Government Solicitor,
Level 10, 60 Martin Place, Sydney, NSW 2000
Matthew.Garey@ags.gov.au

File ref: 24003626

Telephone: 02 9581 7625
Lawyer's Email:
Matthew.Garey@ags.gov.au
Facsimile: 02 6169 3054

Image 1 of Annexure TAD-33

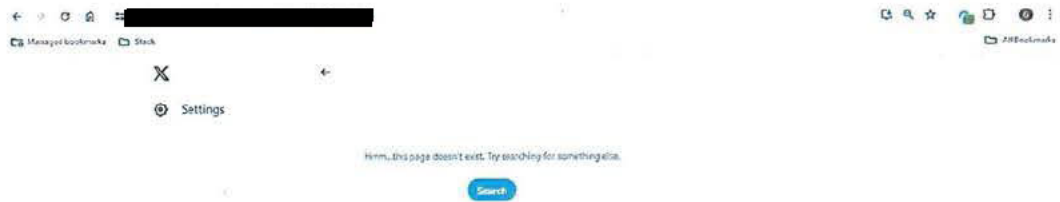
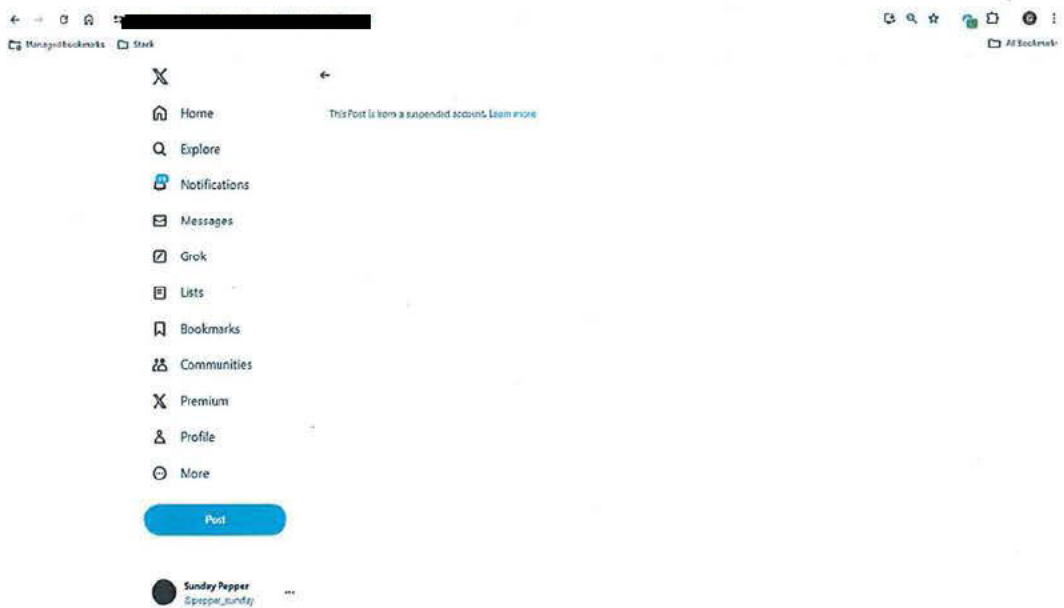


Image 2 of Annexure TAD-33



ANNEXURE TAD-34

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NSW
DIVISION: GENERAL

NO NSD 474 OF 2024

ESAFETY COMMISSIONER

Applicant

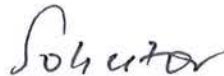
X CORP

Respondent

The following 1 page is the annexure marked TAD-34 referred to in the affidavit of
Toby Allan Dagg made on 6 May 2024 before me:



.....
Signature



.....
Qualification

Filed on behalf of the Applicant, eSafety Commissioner
Prepared by: Matthew Garey
AGS lawyer within the meaning of s 55I of the *Judiciary Act 1903*

Address for Service:
The Australian Government Solicitor,
Level 10, 60 Martin Place, Sydney, NSW 2000
Matthew.Garey@ags.gov.au

File ref: 24003626

Telephone: 02 9581 7625
Lawyer's Email:
Matthew.Garey@ags.gov.au
Facsimile: 02 6169 3054

Image 1 of Annexure TAD-34

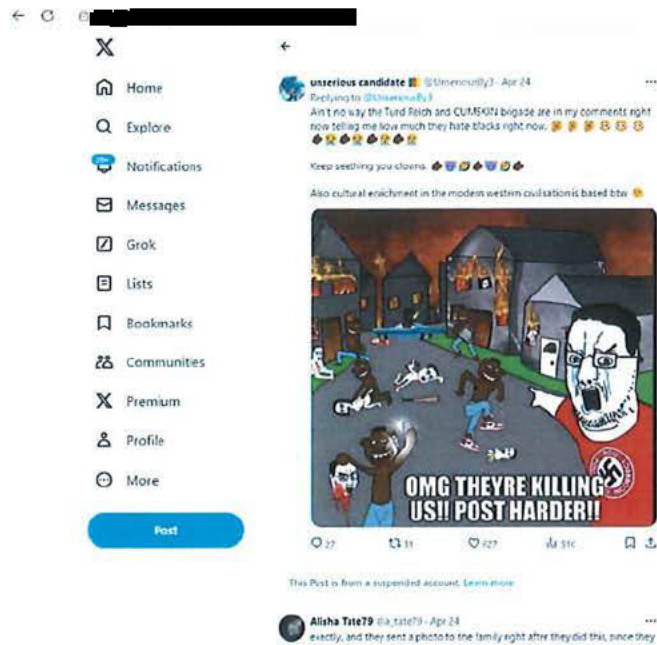
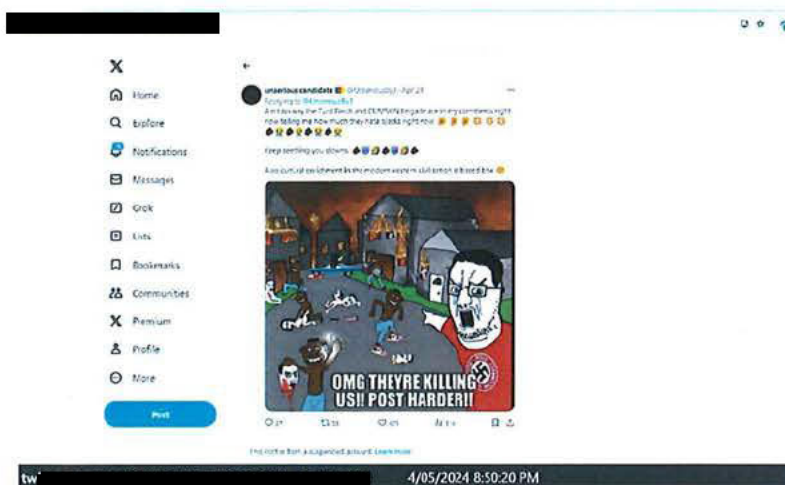


Image 2 of Annexure TAD-34



ANNEXURE TAD-35

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NSW
DIVISION: GENERAL

NO NSD 474 OF 2024

ESAFETY COMMISSIONER

Applicant

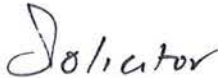
X CORP

Respondent

The following 1 page is the annexure marked TAD-35 referred to in the affidavit of
Toby Allan Dagg made on 6 May 2024 before me:



.....
Signature



.....
Qualification

Filed on behalf of the Applicant, eSafety Commissioner
Prepared by: Matthew Garey
AGS lawyer within the meaning of s 551 of the *Judiciary Act 1903*

Address for Service:
The Australian Government Solicitor,
Level 10, 60 Martin Place, Sydney, NSW 2000
Matthew.Garey@ags.gov.au

File ref: 24003626

Telephone: 02 9581 7625
Lawyer's Email:
Matthew.Garey@ags.gov.au
Facsimile: 02 6169 3054



ANNEXURE TAD-36

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NSW
DIVISION: GENERAL

NO NSD 474 OF 2024

ESAFETY COMMISSIONER

Applicant

X CORP

Respondent

The following 3 pages is the annexure marked TAD-36 referred to in the affidavit of
Toby Allan Dagg made on 6 May 2024 before me:



.....
Signature



.....
Qualification

Filed on behalf of the Applicant, eSafety Commissioner
Prepared by: Matthew Garey
AGS lawyer within the meaning of s 55I of the *Judiciary Act 1903*

Address for Service:
The Australian Government Solicitor,
Level 10, 60 Martin Place, Sydney, NSW 2000
Matthew.Garey@ags.gov.au

File ref: 24003626

Telephone: 02 9581 7625
Lawyer's Email:
Matthew.Garey@ags.gov.au
Facsimile: 02 6169 3054

×



Sign in to X

 Sign in with Apple

or

Phone, email, or username
 

Next

Forgot password?

Don't have an account? [Sign up](#)

Image 2 of Annexure TAD-36

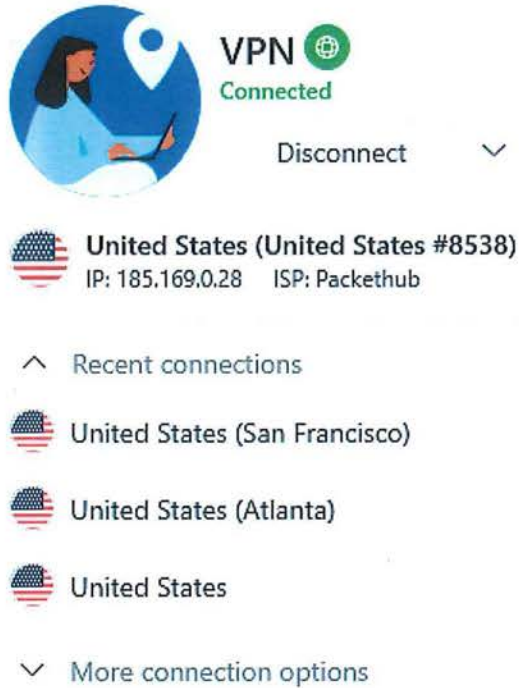


Image 3 of Annexure TAD-36

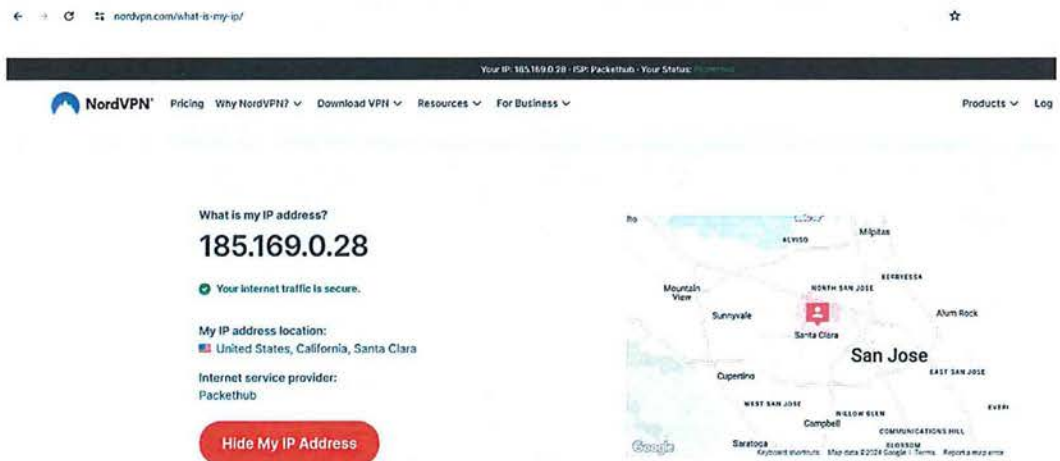


Image 4 of Annexure TAD-36

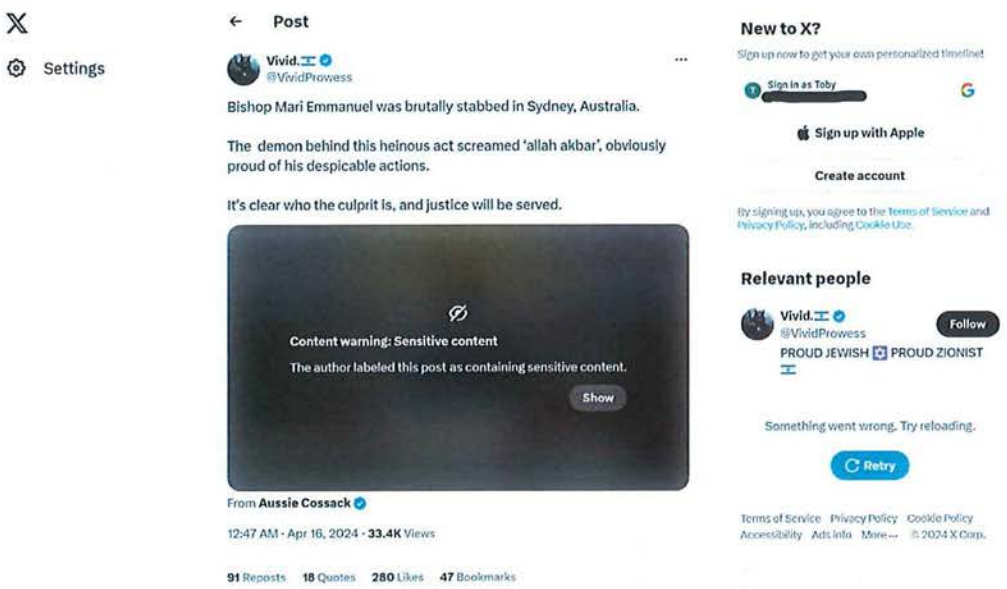


Image 5 of Annexure TAD-36



ANNEXURE TAD-37

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NSW
DIVISION: GENERAL

NO NSD 474 OF 2024

ESAFETY COMMISSIONER

Applicant

X CORP

Respondent

The following 3 pages is the annexure marked TAD-37 referred to in the affidavit of
Toby Allan Dagg made on 6 May 2024 before me:



Signature



Qualification

Filed on behalf of the Applicant, eSafety Commissioner
Prepared by: Matthew Garey
AGS lawyer within the meaning of s 551 of the *Judiciary Act 1903*

Address for Service:
The Australian Government Solicitor,
Level 10, 60 Martin Place, Sydney, NSW 2000
Matthew.Garey@ags.gov.au

File ref: 24003626

Telephone: 02 9581 7625
Lawyer's Email:
Matthew.Garey@ags.gov.au
Facsimile: 02 6169 3054

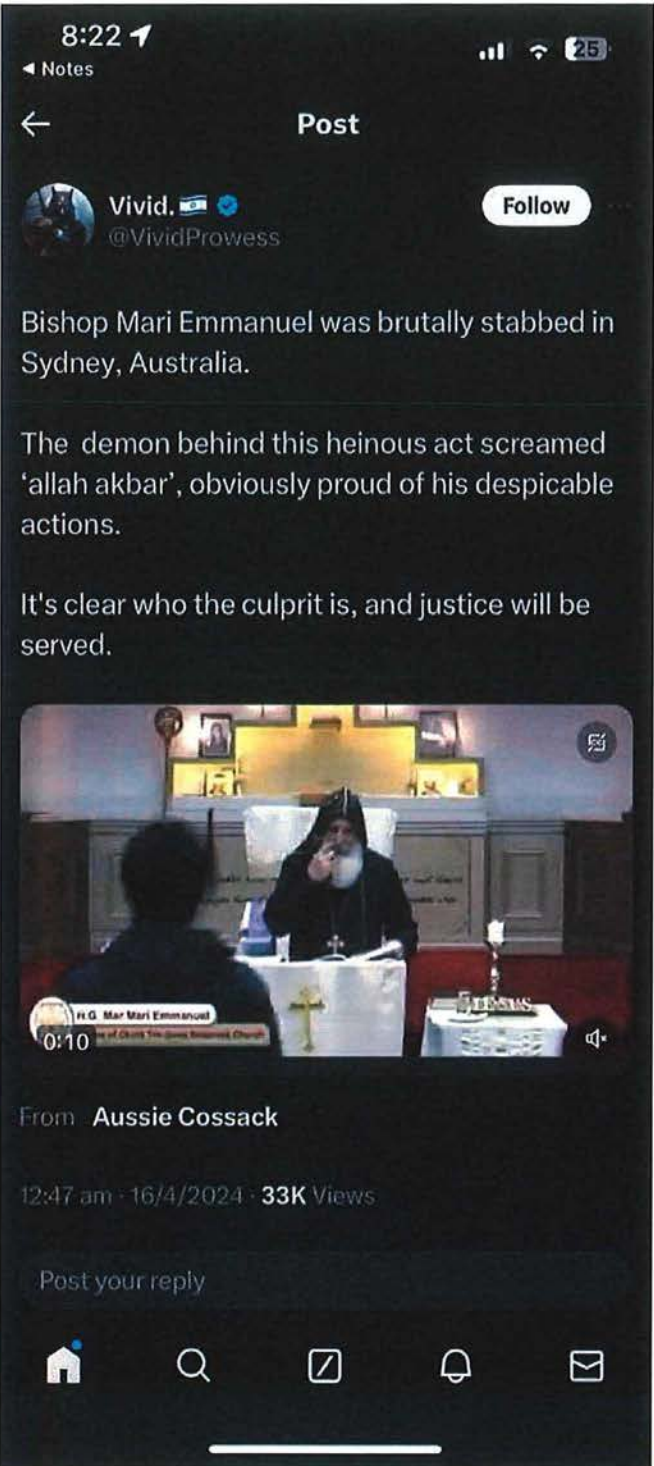
Image 1 of Annexure TAD-37



Image 2 of Annexure TAD-37



Image 3 of Annexure TAD-37



ANNEXURE TAD-38

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NSW
DIVISION: GENERAL

NO NSD 474 OF 2024

ESAFETY COMMISSIONER

Applicant

X CORP

Respondent

The following 29 pages is the annexure marked TAD-38 referred to in the affidavit of
Toby Allan Dagg made on 6 May 2024 before me:



.....
Signature



.....
Qualification

Filed on behalf of the Applicant, eSafety Commissioner
Prepared by: Matthew Garey
AGS lawyer within the meaning of s 551 of the *Judiciary Act 1903*

Address for Service:
The Australian Government Solicitor,
Level 10, 60 Martin Place, Sydney, NSW 2000
Matthew.Garey@ags.gov.au

File ref: 24003626

Telephone: 02 9581 7625
Lawyer's Email:
Matthew.Garey@ags.gov.au
Facsimile: 02 6169 3054

Image 1 of Annexure TAD-38

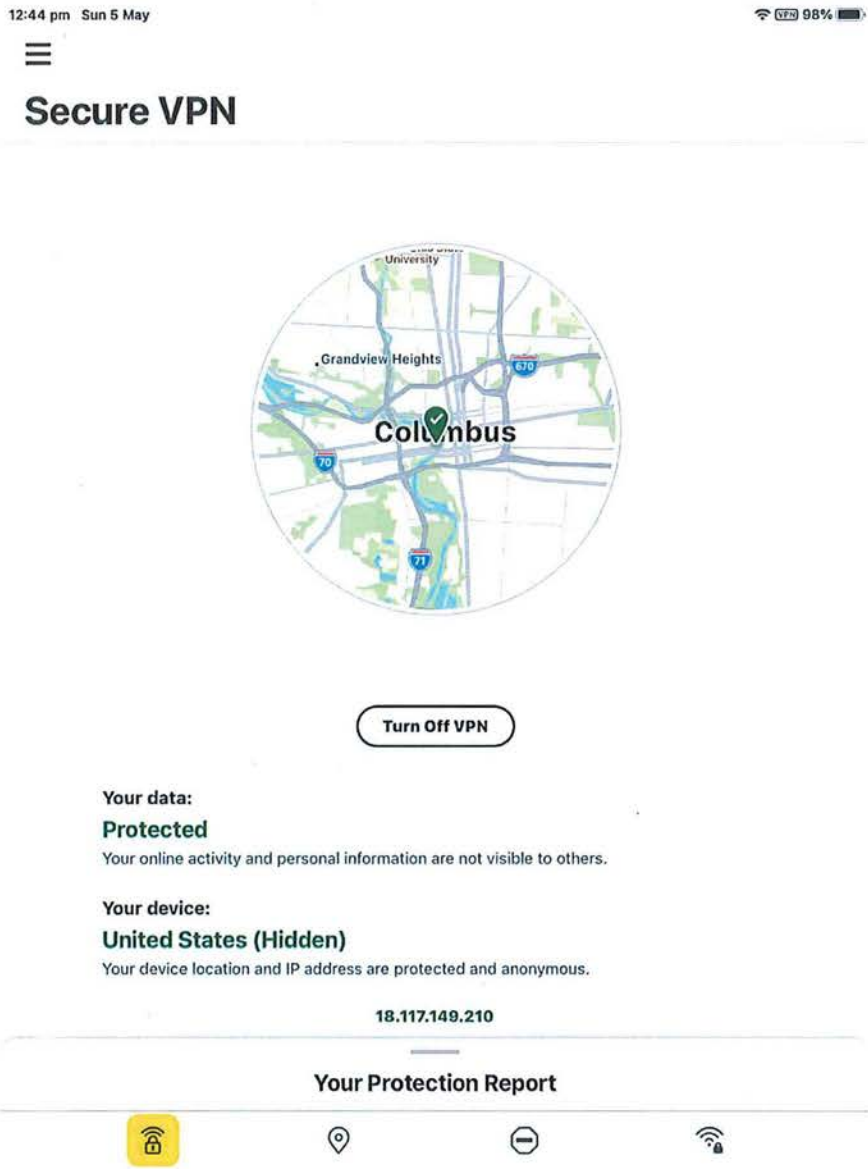



Image 2 of Annexure TAD-38

Firefox 1:49 pm Sun 5 May 89%

Cancel

Edit profile

Save



Name

Bio

Add a bio to your profile

Location

Add your location

Website

Add your website

Birth date

10 September 2010

Switch to Professional

War
Wa
udio
igina
ollow

Image 3 of Annexure TAD-38

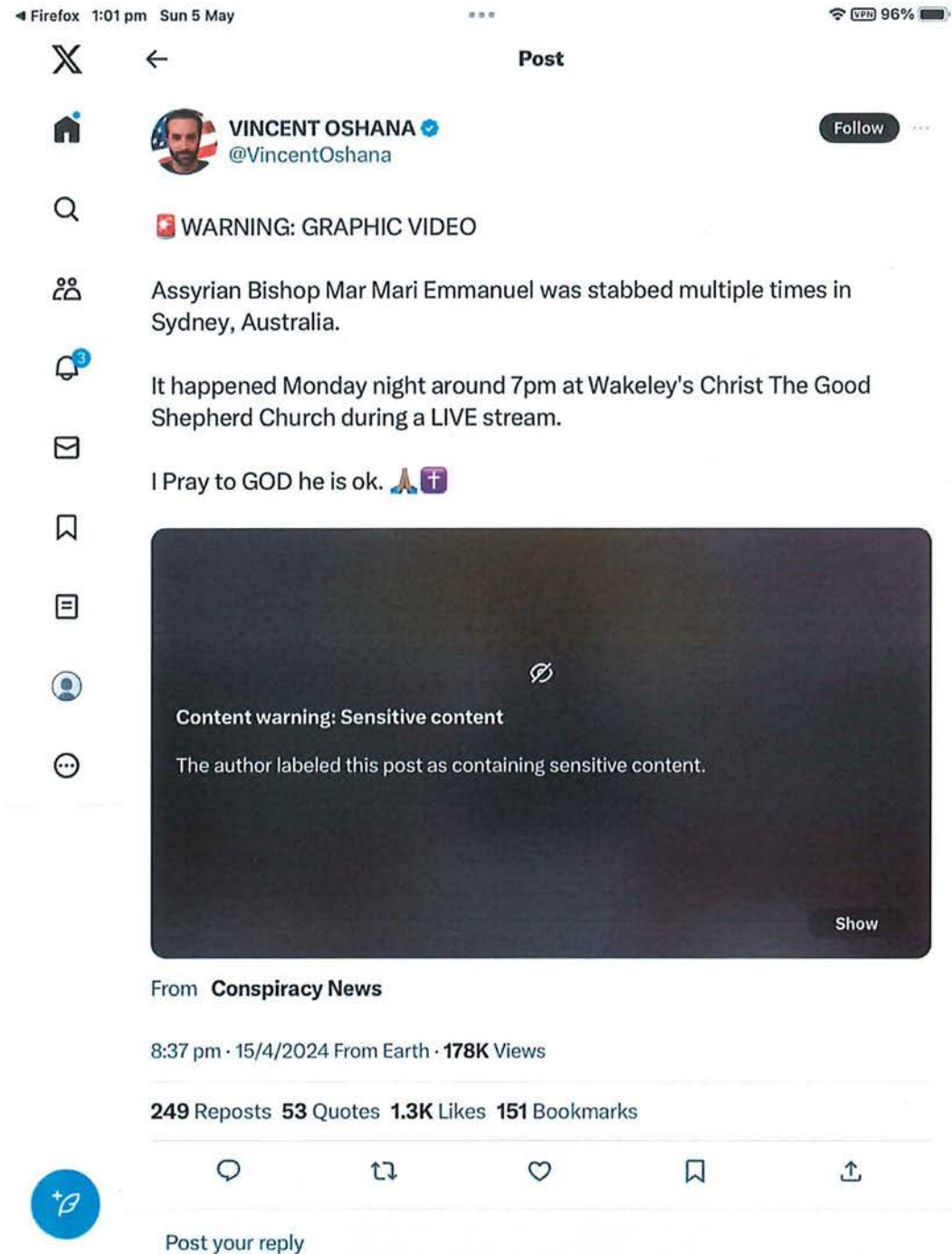








Image 4 of Annexure TAD-38





Image 5 of Annexure TAD-38







Firefox 1:27 pm Sun 5 May VPN 93%


  **Post**

  **Steven** 
@nogulagsagain 

 This is in Sydney now.


 We don't want his.



Content Warning: Graphic Content






X labeled this post as containing Graphic Content.








From **mark leach**

8:48 pm · 15/4/2024 From Earth · **222K** Views

399 Reposts **61** Quotes **2K** Likes **201** Bookmarks

 Share this post with anyone, even if they aren't on X yet 

  **Bitcoin Aussie**  @aussie_btc · 15/4/2024
Still bullish on Sydney property - analysis coming in SMH shortly

Post your reply

Image 6 of Annexure TAD-38



Image 7 of Annexure TAD-38

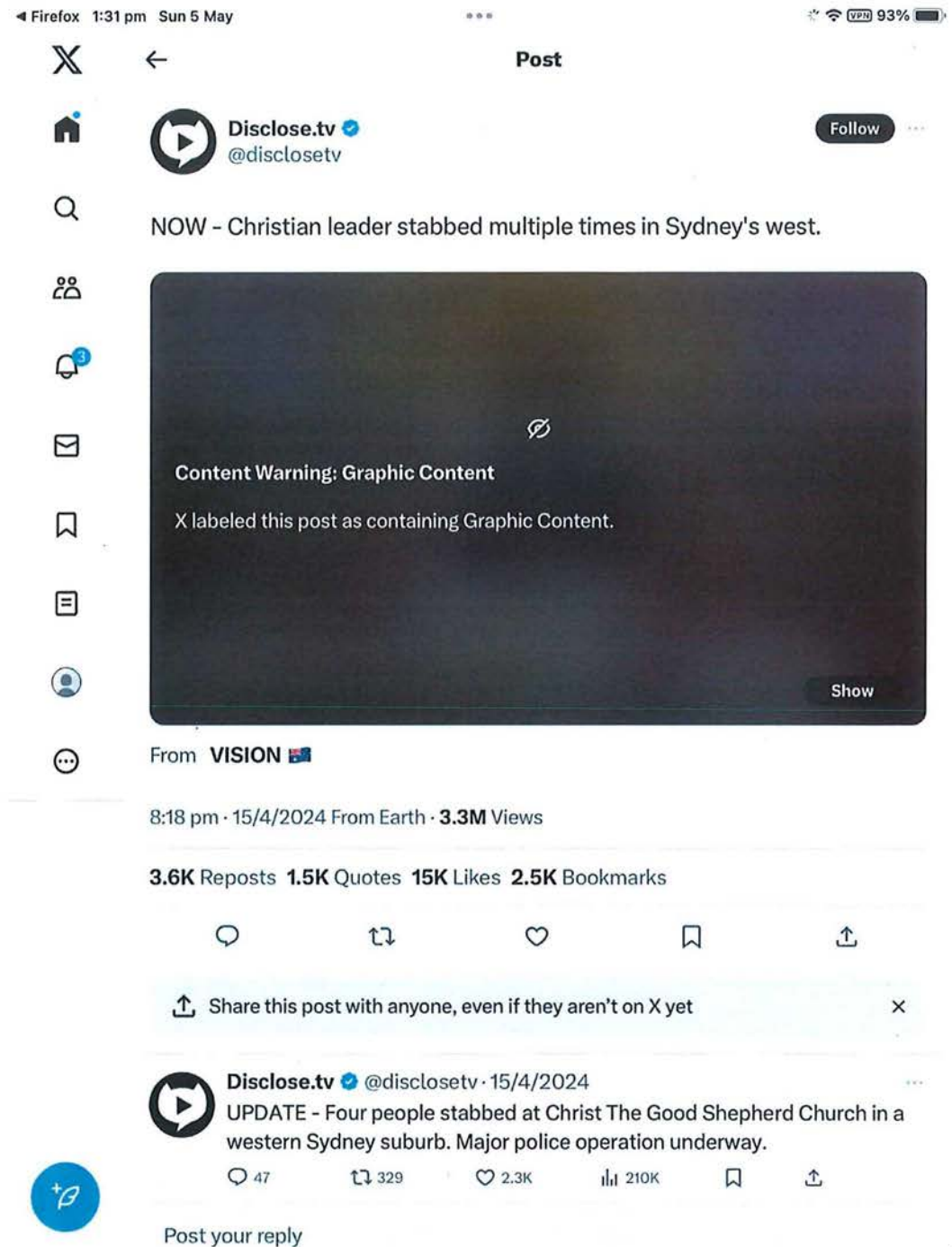


Image 8 of Annexure TAD-38

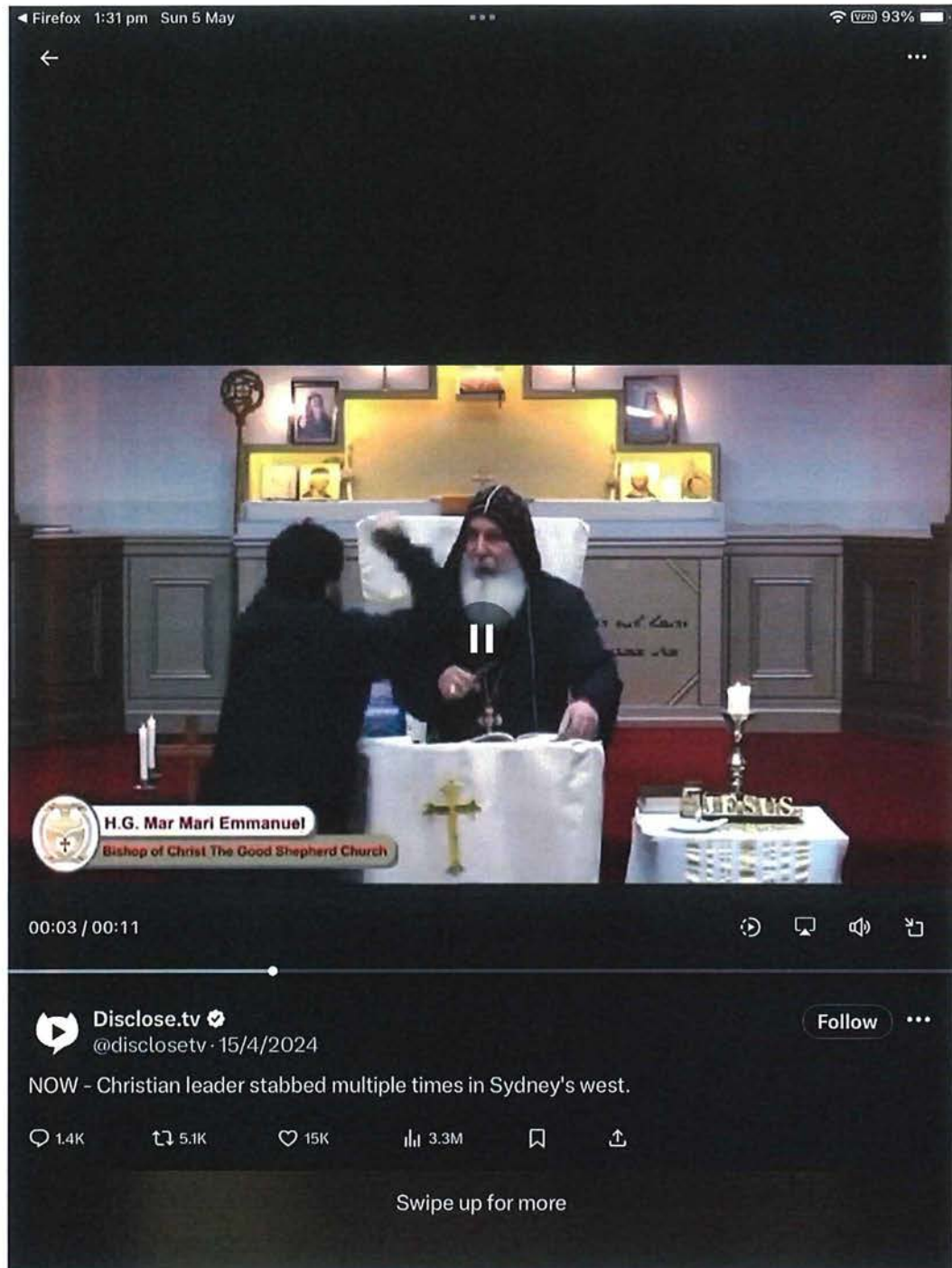


Image 9 of Annexure TAD-38

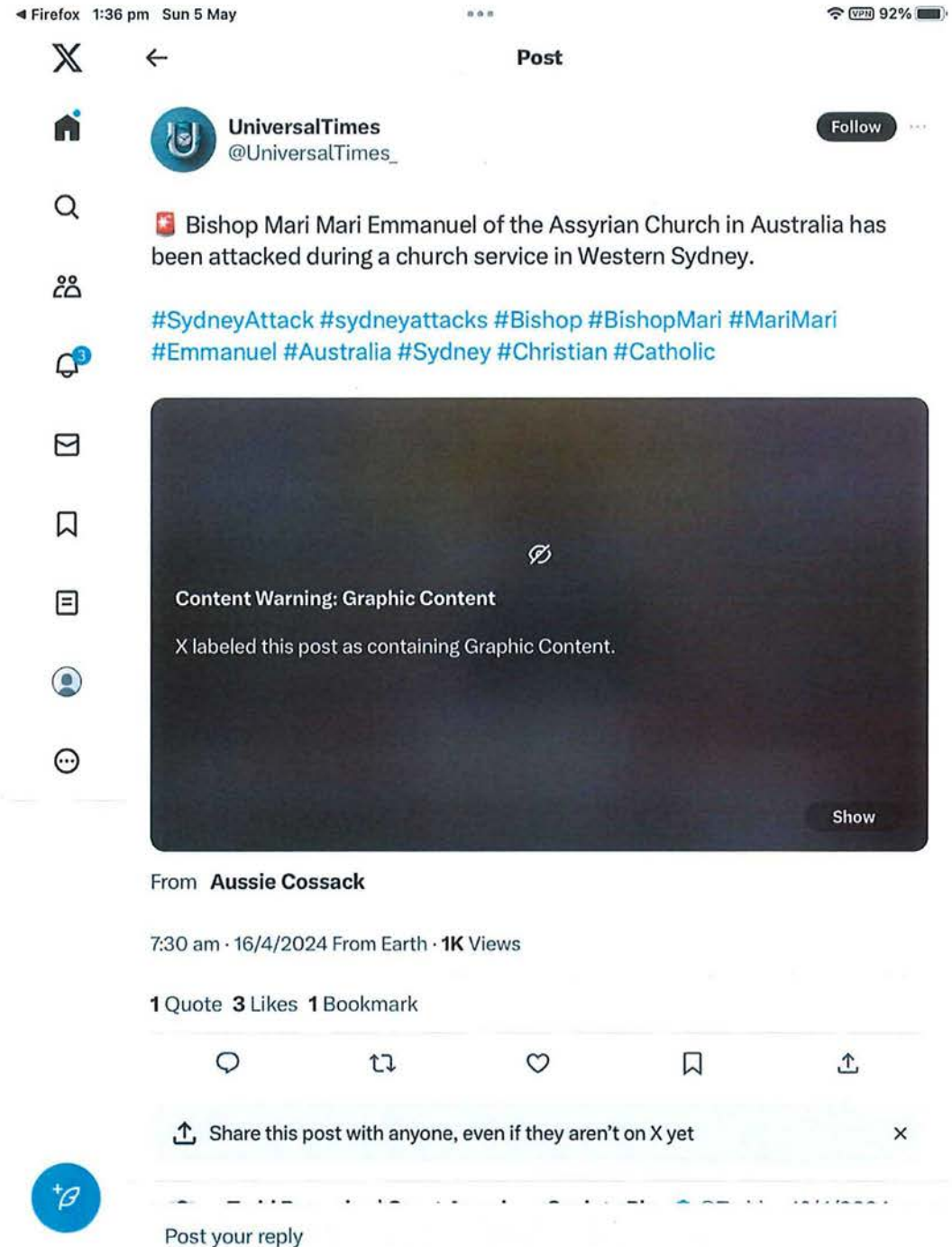


Image 10 of Annexure TAD-38

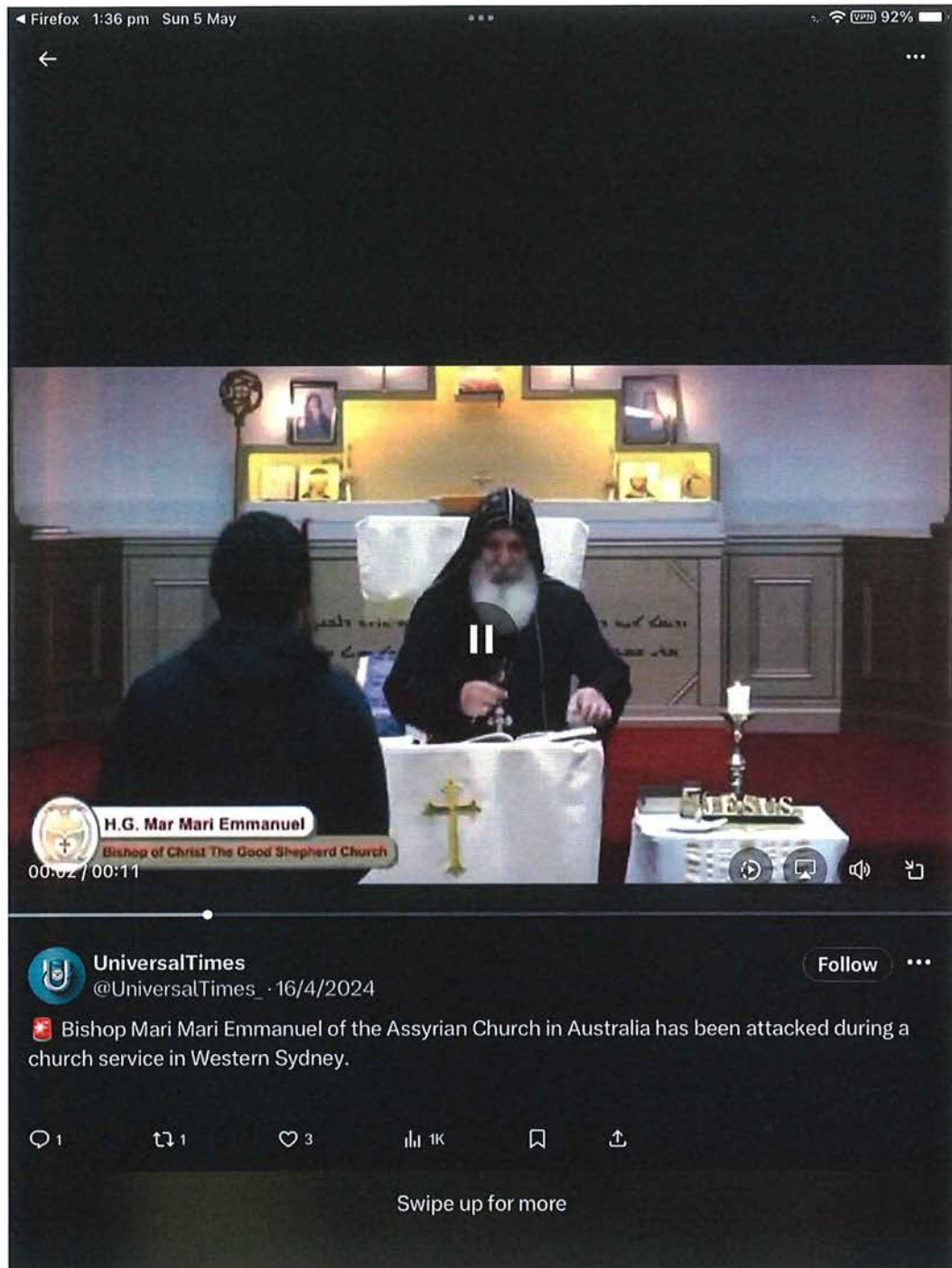













Image 11 of Annexure TAD-38


Firefox 1:42 pm Sun 5 May VPN 91%

X **Post**


        

 **Andre Nuta** 
@andre_nuta Follow

Christian Bishop Mar Mari Emmanuel was stabbed multiple times in suburb of Sydney during livestream of his service. The Bishop is a big free speech advocate who calls out the media lies and is an ardent supporter of President Trump and will recover fully.









Content Warning: Graphic Content
X labeled this post as containing Graphic Content. Show

From **VISION** 

1:25 am · 16/4/2024 From Earth · **421** Views

1 Repost 3 Bookmarks

 Share this post with anyone, even if they aren't on X yet ×


 Post your reply

Image 12 of Annexure TAD-38



Image 13 of Annexure TAD-38

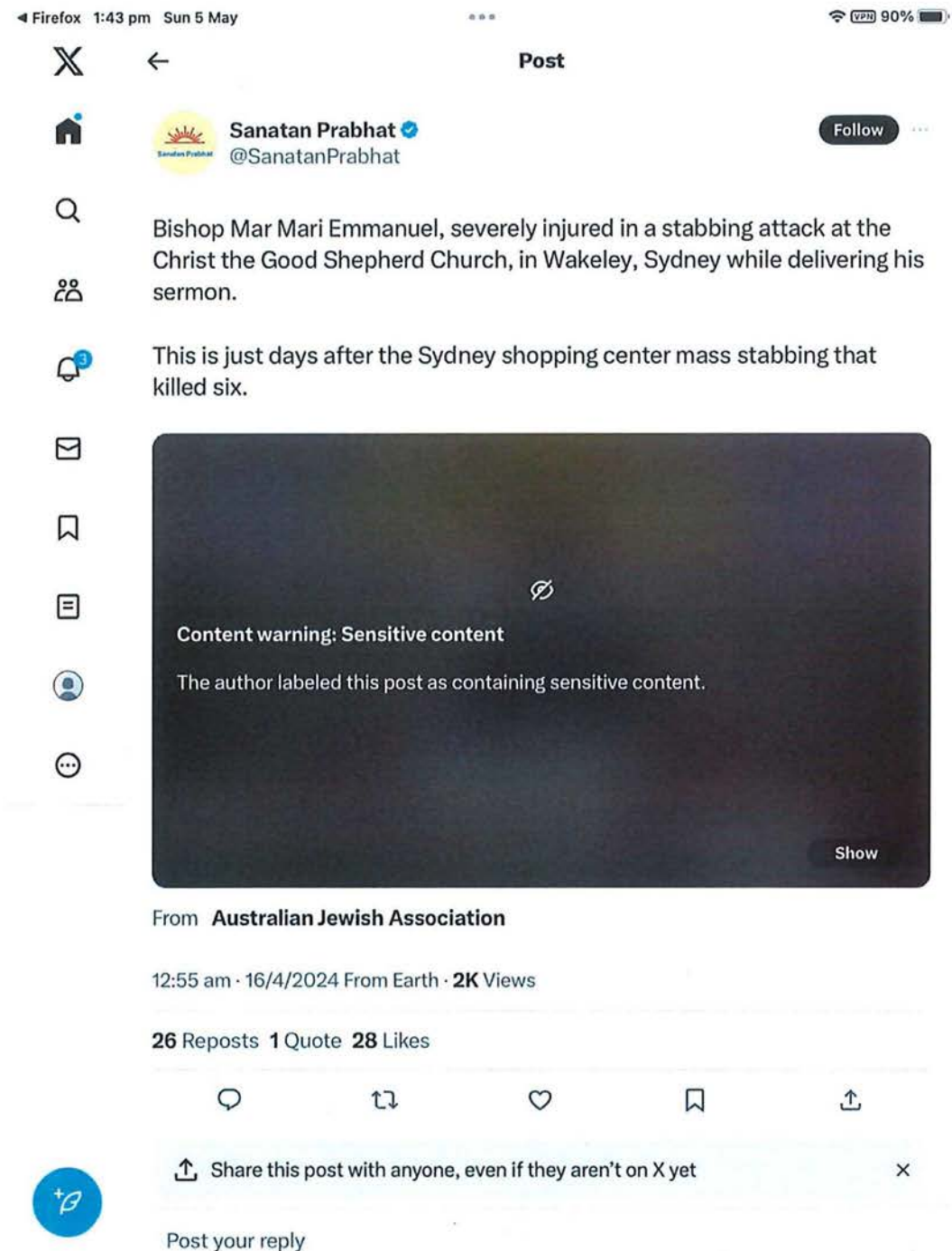


Image 14 of Annexure TAD-38

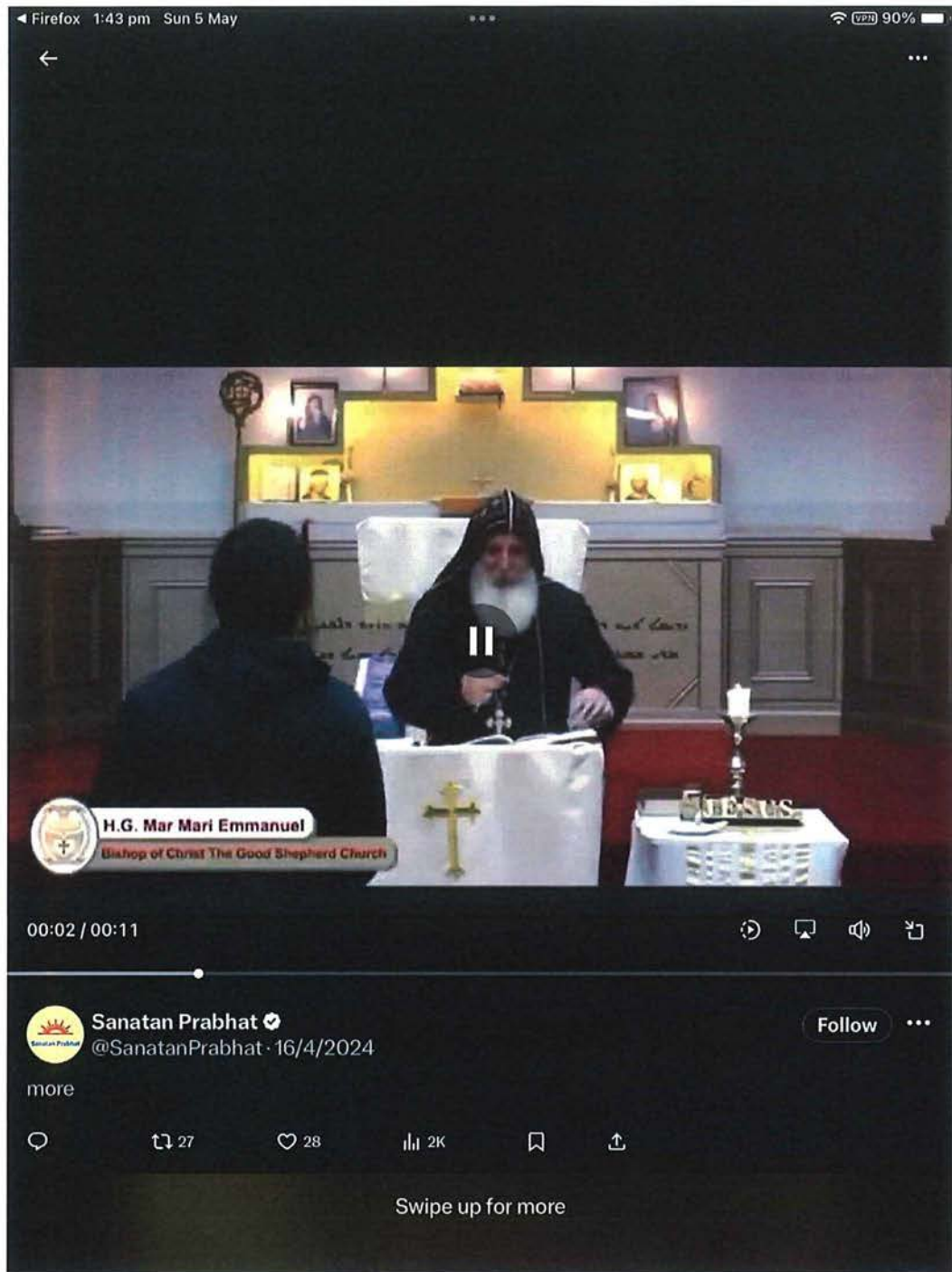













Image 15 of Annexure TAD-38

Firefox 1:44 pm Sun 5 May 90%

Post


        

 **Vivid.** 
@VividProwess Follow

Bishop Mari Emmanuel was brutally stabbed in Sydney, Australia.

The demon behind this heinous act screamed 'allah akbar', obviously proud of his despicable actions.






It's clear who the culprit is, and justice will be served.



Content warning: Sensitive content
The author labeled this post as containing sensitive content.
Show

From **Aussie Cossack**

12:47 am · 16/4/2024 From Earth · **33K** Views

91 Reposts **18** Quotes **281** Likes **47** Bookmarks

 Share this post with anyone, even if they aren't on X yet ×


 Post your reply

Image 16 of Annexure TAD-38

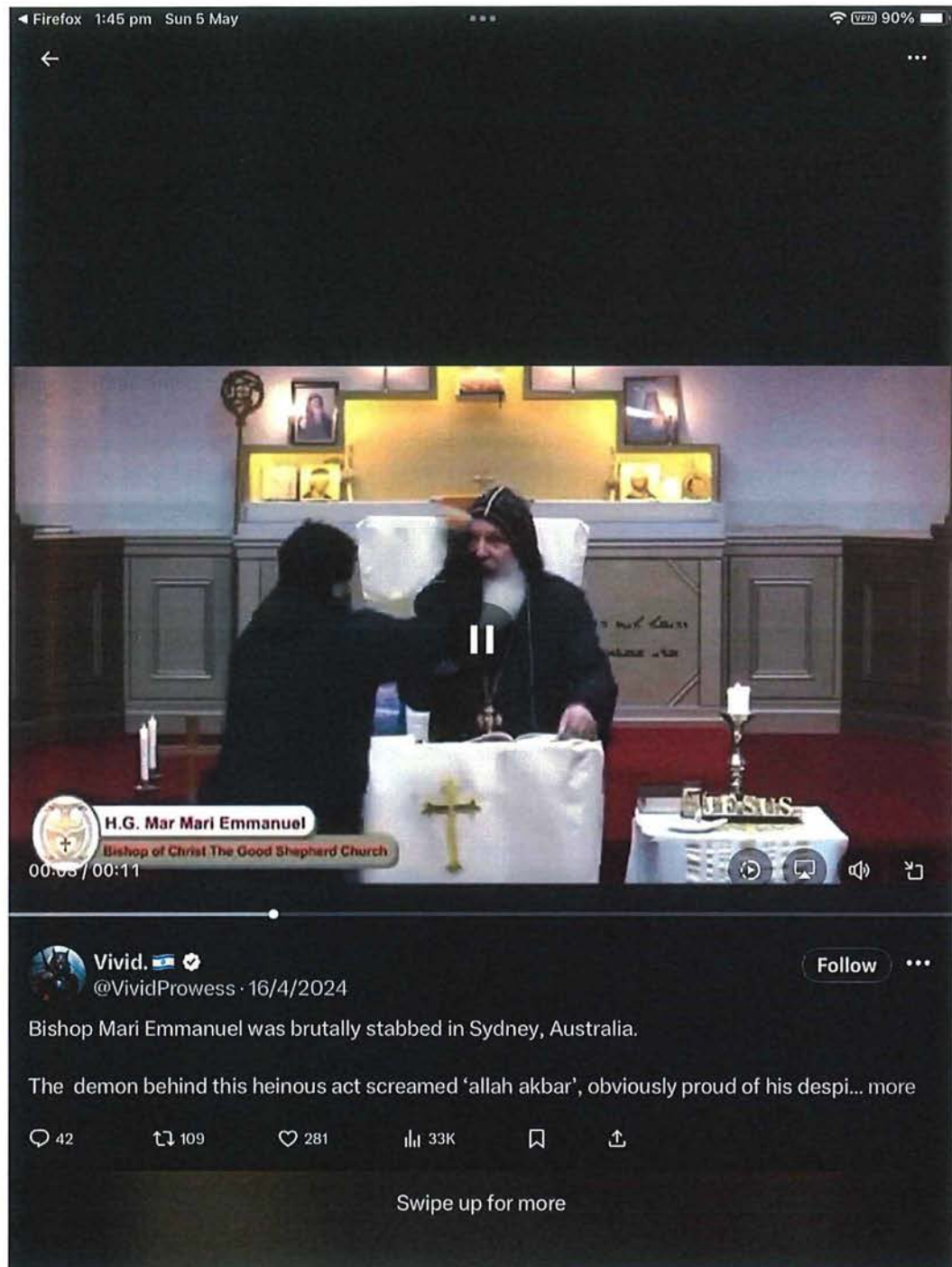


Image 17 of Annexure TAD-38

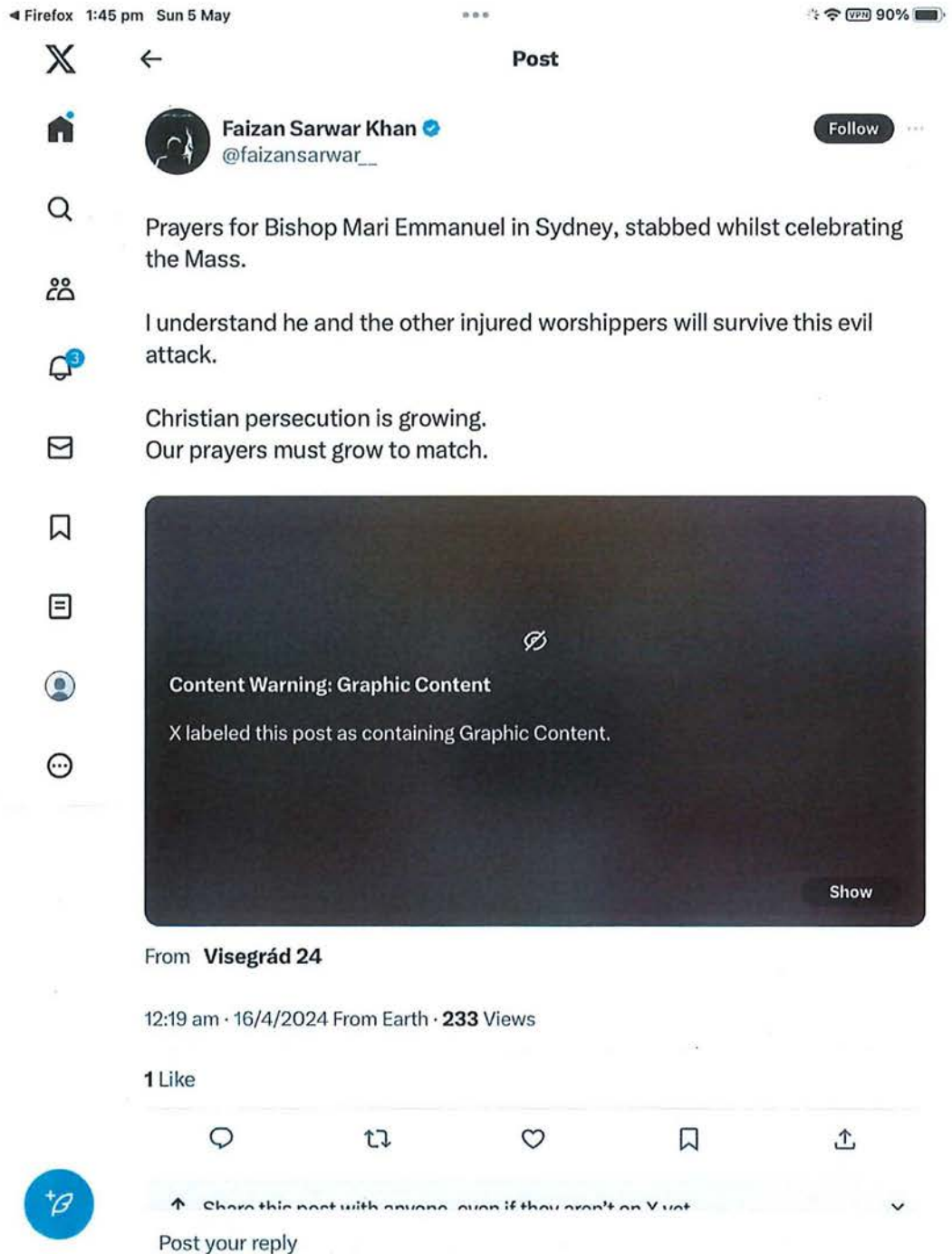


Image 18 of Annexure TAD-38

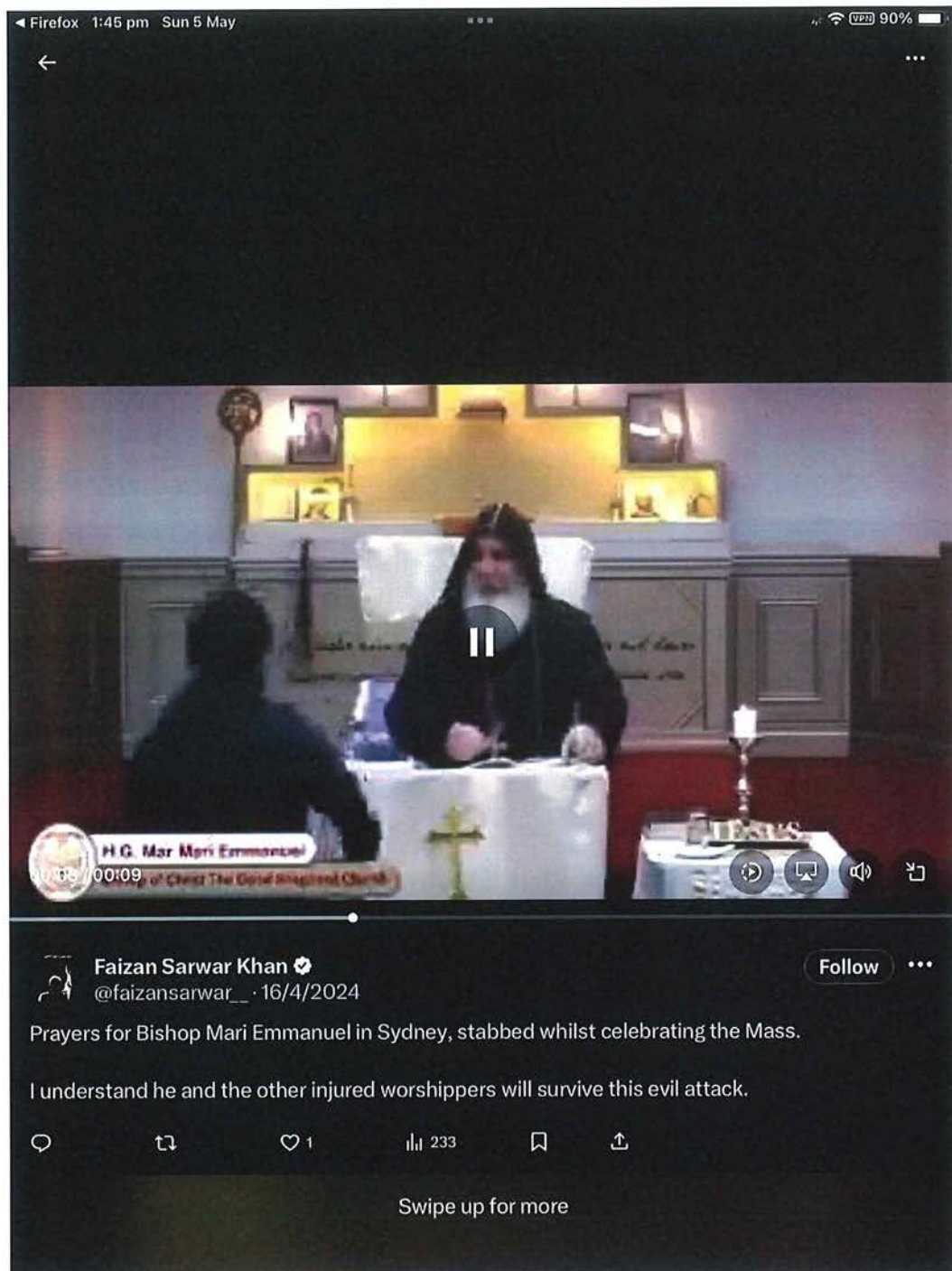


Image 19 of Annexure TAD-38

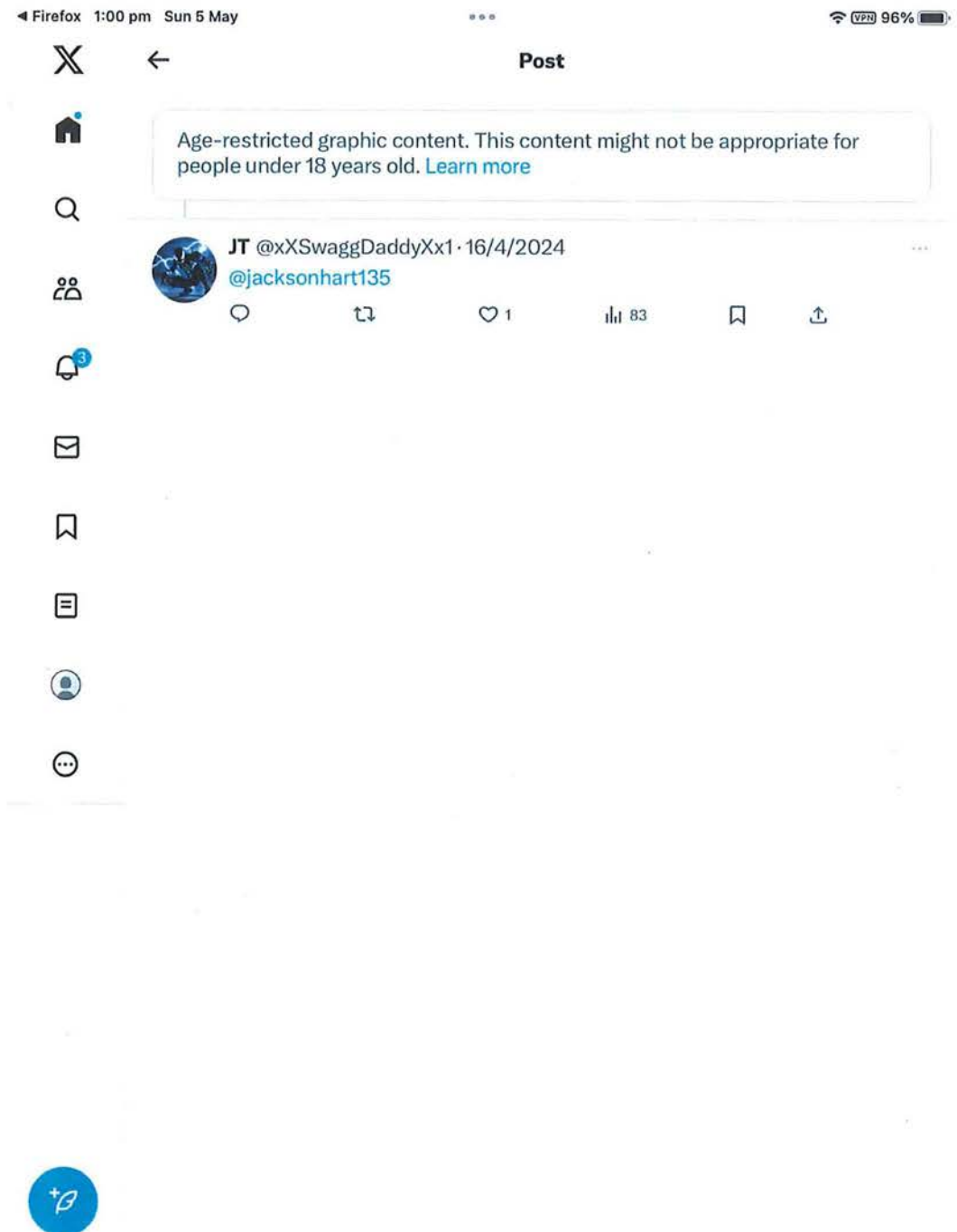


Image 20 of Annexure TAD-38

Firefox 1:11 pm Sun 5 May VPN 95%

Post

Age-restricted adult content. This content might not be appropriate for people under 18 years old. [Learn more](#)

Åby1kenåby @aby1kenaby · 15/4/2024
Borde du inte radera den har tweeten? x.com/DABooooomB/stat... x.com/DABooooomB/stat...

Age-restricted adult content. This content might not be appropriate for people under 18 years old. [Learn more](#)

4 20 17K

Aja baja 🙌 @DABooooomB · 15/4/2024
Nej varför då? det står klart och tydligt i tråden tweet 2-3 jag antar att du inte har läst det 🤔

3 25 8.4K

[Show replies](#)

Weszo 🇧🇪 @WeszoK · 16/4/2024
Det där är den kända ortodoxa prästen som var på PBD podcast nyligen. En fin god man. Hoppas han överlevt.

1 1 32 6.1K

Aris @cellisten · 16/4/2024
Så synd. Hoppas att det gick bra. Han är bland få religiösa jag gillar.

1 1 193

Dino 🦖 @dinmammasmutti · 15/4/2024
Gillar den där filuren. Någon som vet hur det gick med honom?

2 3 971

arzo @95Arzo · 15/4/2024
Finns det något annat än brutal islamisk terrorism? 🤔🤔

3 24 6.1K

OneStepAhead 🇧🇪 @OneStepAhead777 · 16/4/2024

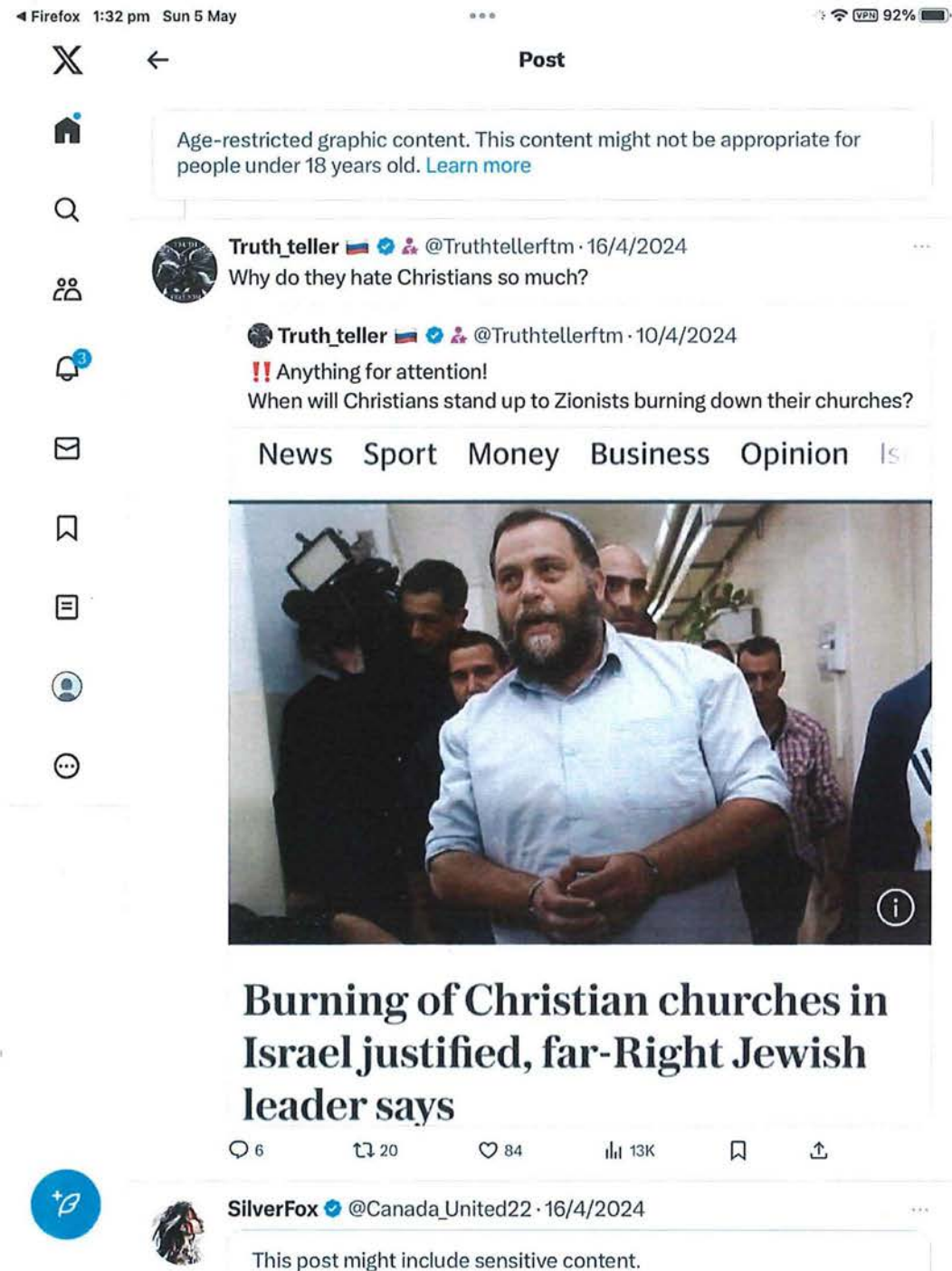
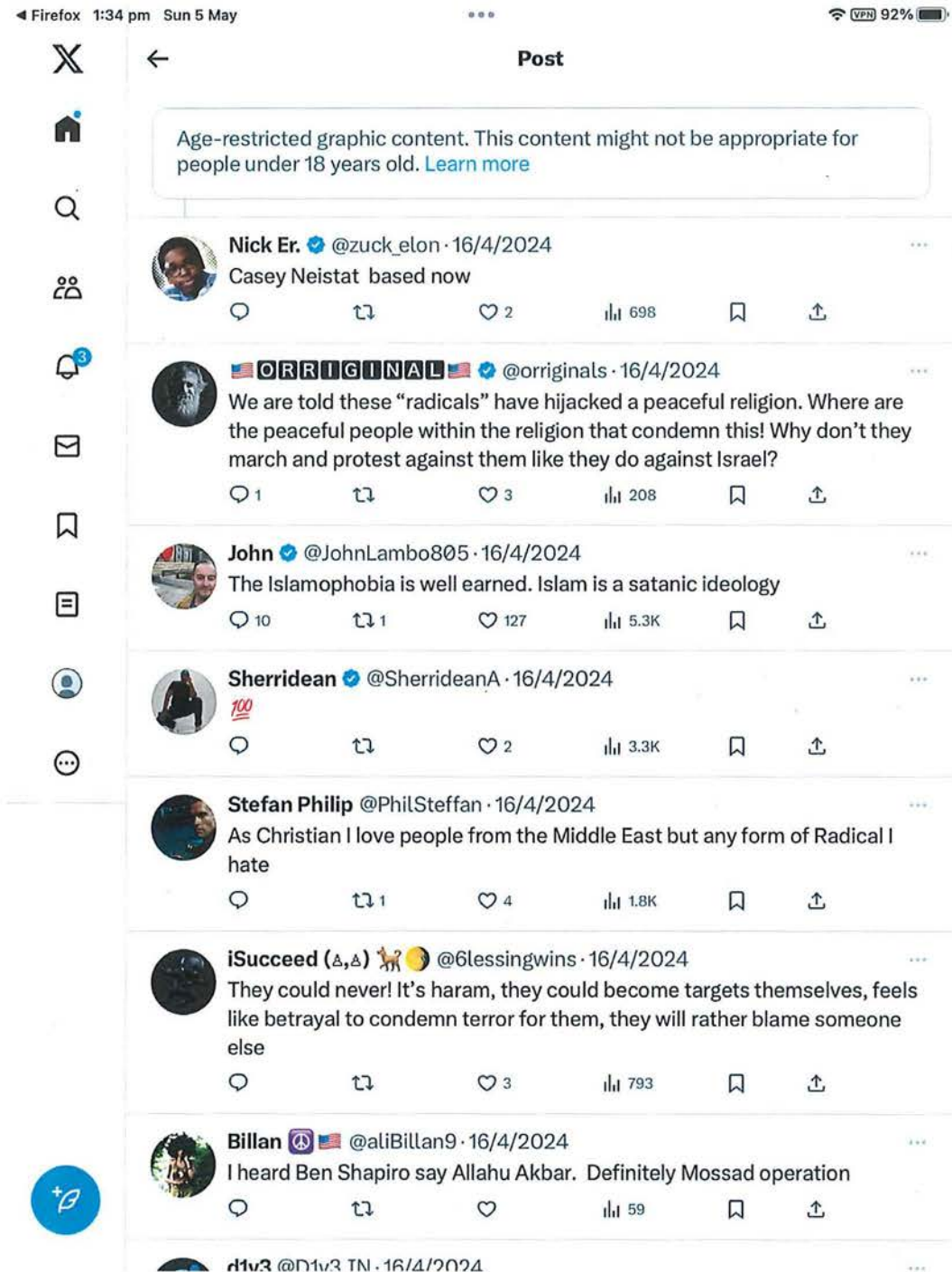


Image 22 of Annexure TAD-38



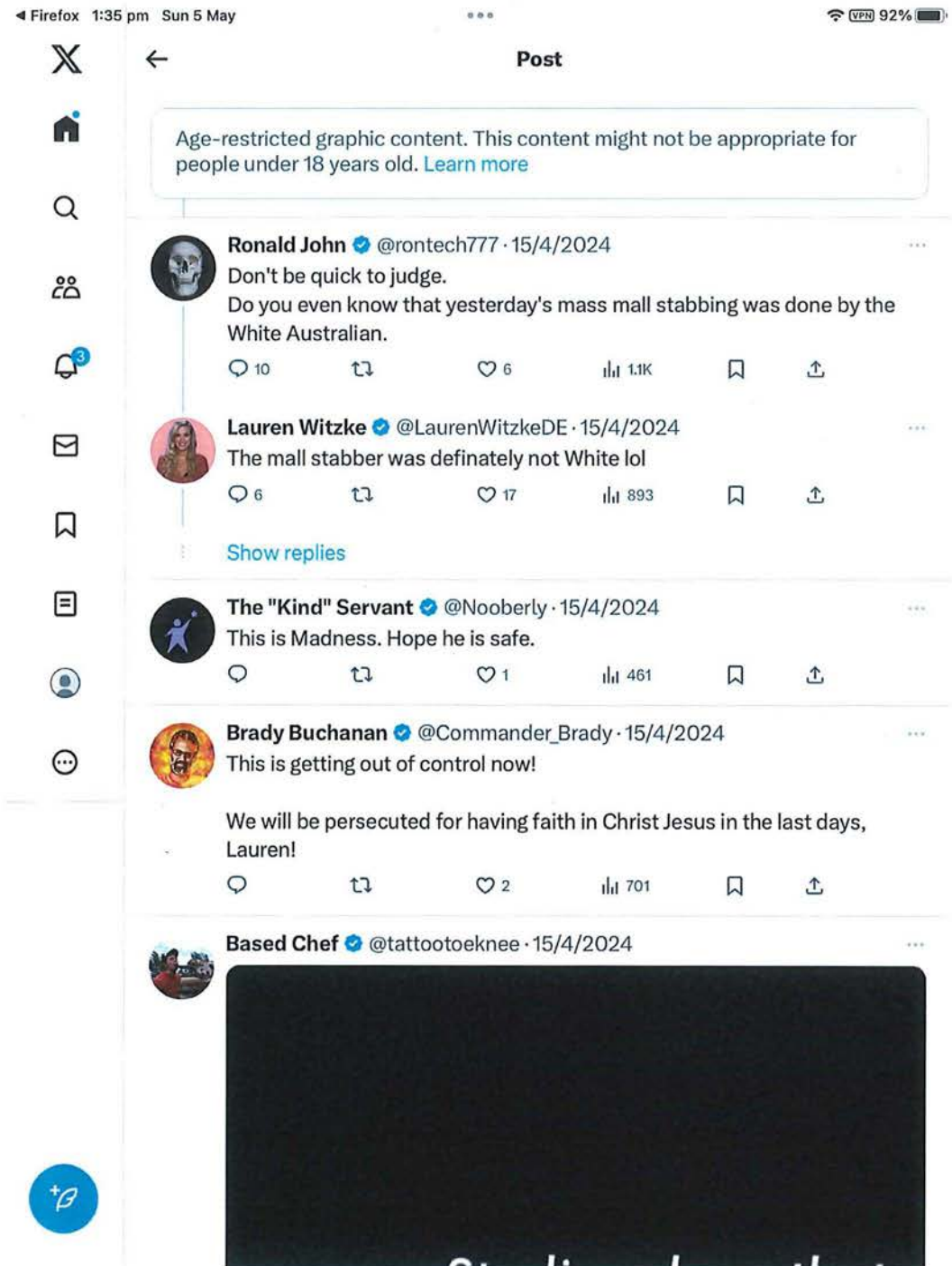


Image 24 of Annexure TAD-38

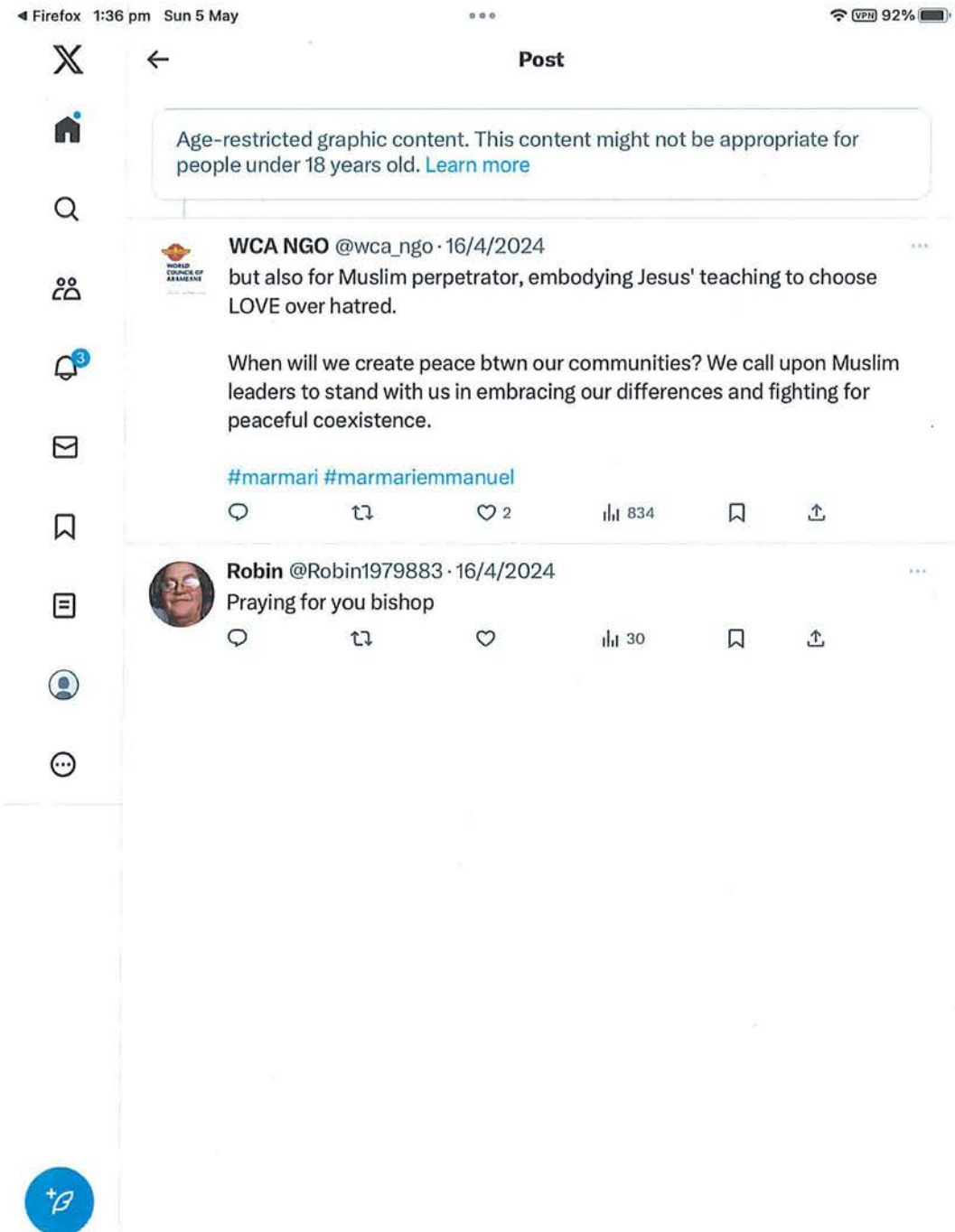
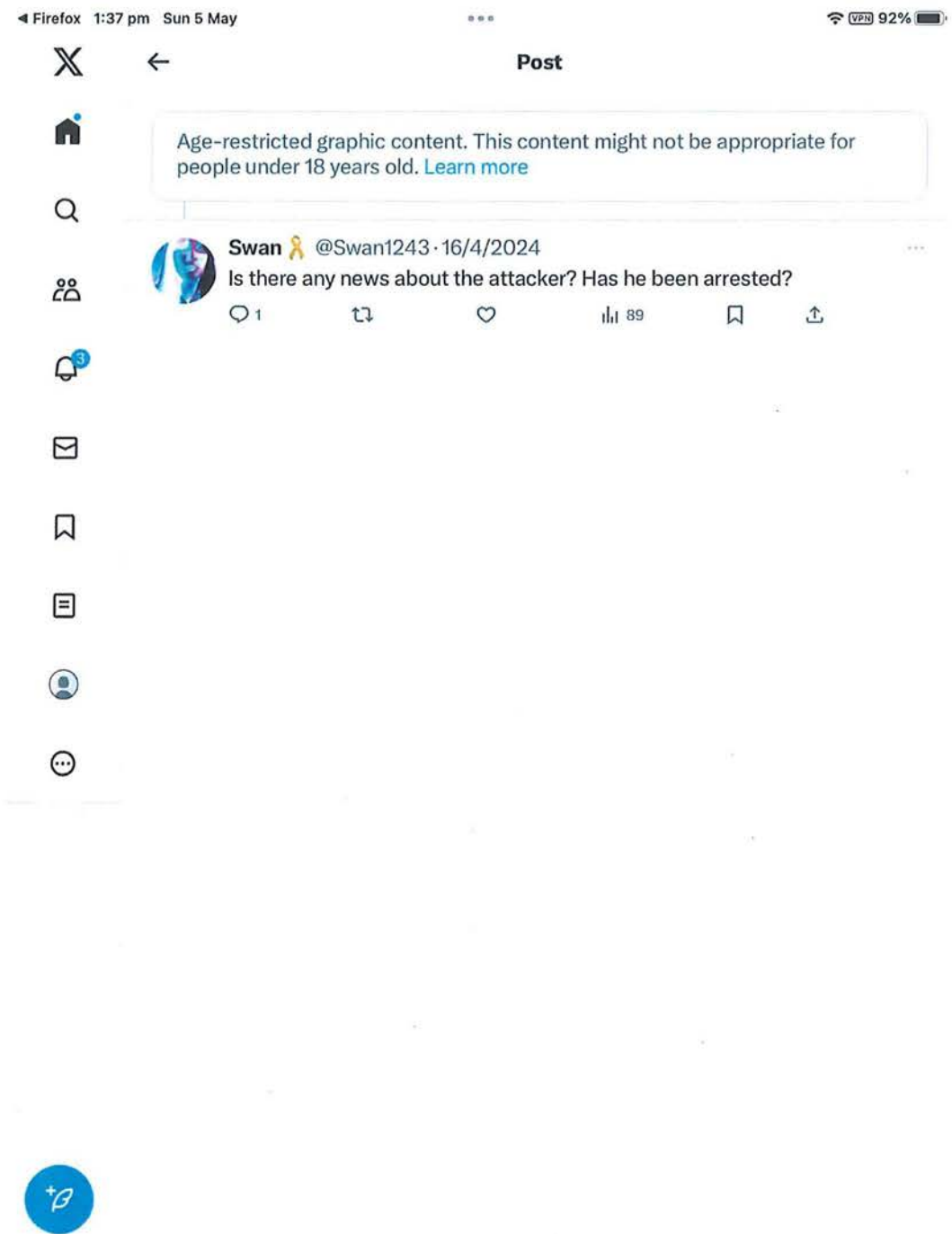


Image 25 of Annexure TAD-38





Post



Age-restricted graphic content. This content might not be appropriate for people under 18 years old. [Learn more](#)



DR. Kek @Thekeksociety · 16/4/2024

DO YOU
THINK

THE ASSASSINATION ATTEMPT
MADE ON

BISHOP MAR MARI EMMANUEL

WAS AN ATTEMPT TO SILENCE HIM FOR SPEAKING AGAINST

THE DEEP STATE?

Yes

88%

No

12%

2,758 votes · Final results

24

39

67

25K



Dave W. Palmer, CD @Blue22Dave · 16/4/2024

WHAT IS THE STATUS OF THIS?

How severe were the Bishop's wounds??

FINALLY this international news appears on CTV MSM!

[x.com/thekeksociety/...](#) [x.com/Thekeksociety/...](#)

Age-restricted graphic content. This content might not be appropriate for people under 18 years old. [Learn more](#)

1

8

21

10K



Maria @mariawelter6 · 16/4/2024

This guy is amazing. He tells the truth!

Has anyone heard an update on his condition?

I wouldn't doubt if it was a hit. Christians are quietly being killed,
everywhere. 😞

4

8

86

11K



Image 27 of Annexure TAD-38

Firefox 1:40 pm Sun 5 May

Post

Age-restricted graphic content. This content might not be appropriate for people under 18 years old. [Learn more](#)

EverluvenUSA @everluvenusa · 16/4/2024
Coordinated attacks imo, acts of war. These are not protesters.

cate warren @Gemma1Warren · 16/4/2024
Liar! Are you in Australia? No, stop peddling misinformation.

Name @realCatStan · 16/4/2024
Nobody says Allahu Akbar

Someone says "stop stop" in Arabic

Also, it's conceivable that the bishop would say Allahu Akbar because it means "God is Great" in his actual language

James Taplin #FreeAssange @jamestaplin · 16/4/2024
I watched and listened to the video and could not confirm your statement. That has not been reported in Australian media as far as I am aware.

LFA @Ms_politician · 16/4/2024
He is a Zionist and the bishop is a pro Palestine. Don't spread hate upon a religion! There's so much hate everywhere.

Linda Hodson @Legabug · 16/4/2024

amazinglmg @Jfeesfriend · 16/4/2024
blame everything on muslims, noted

Image 28 of Annexure TAD-38

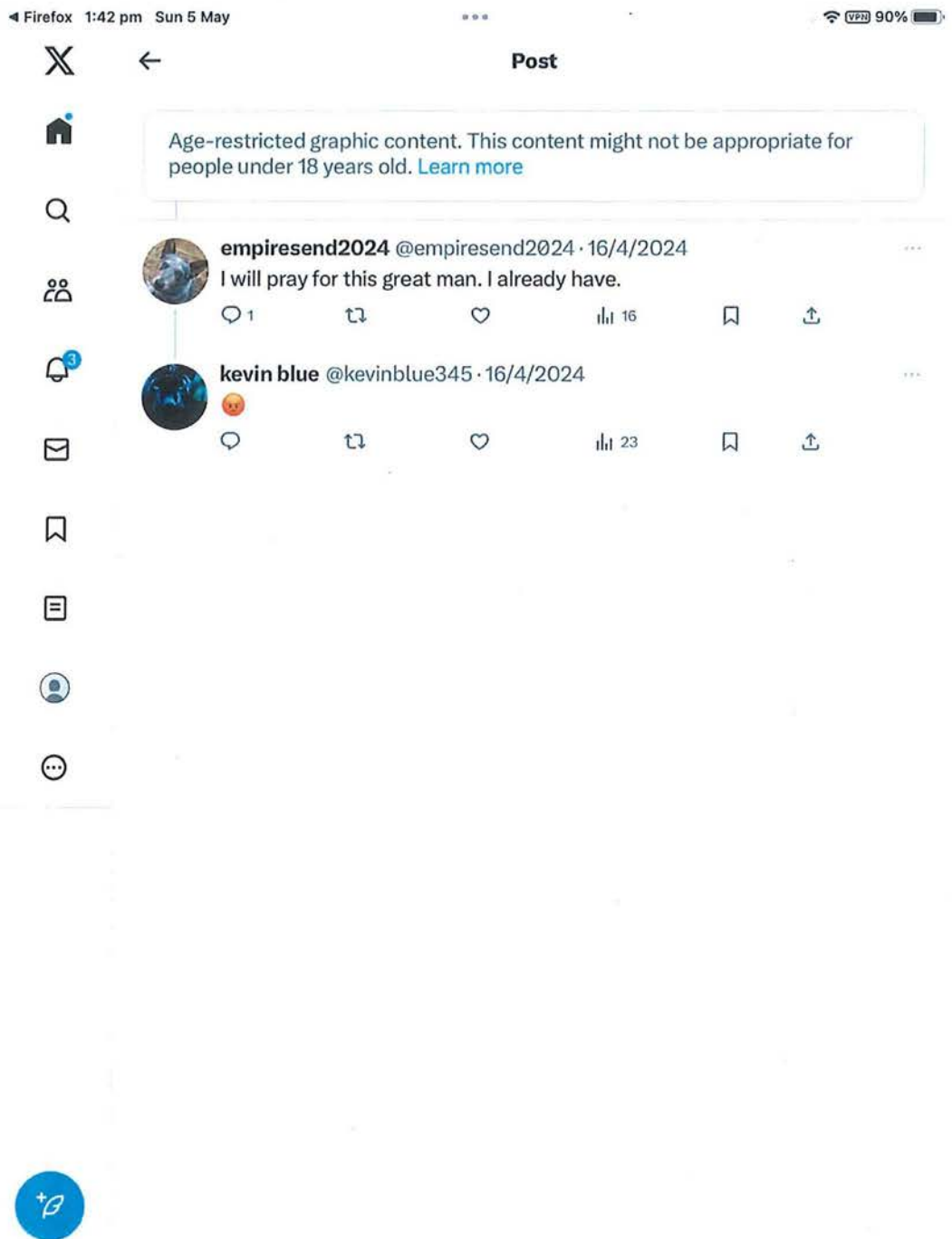
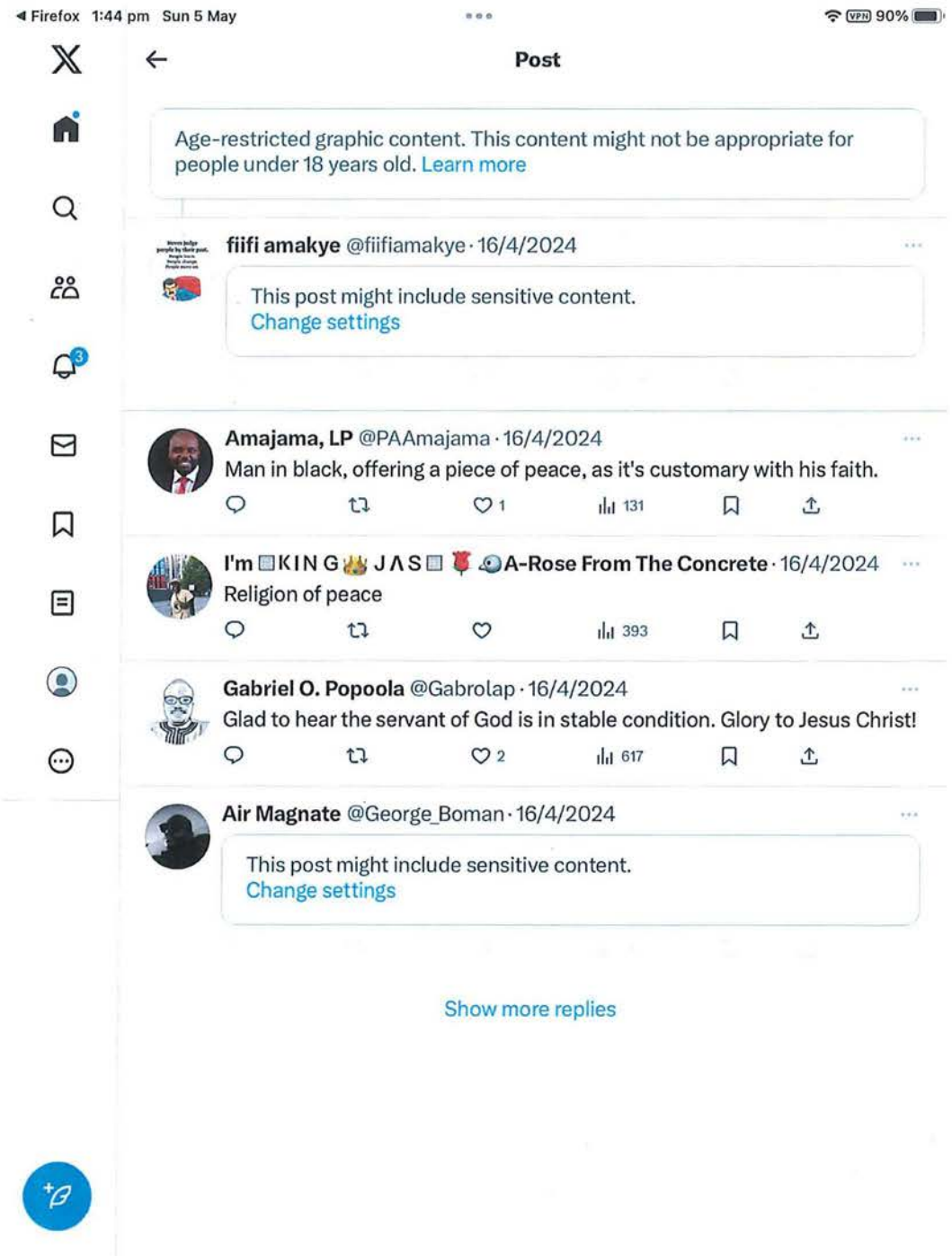


Image 29 of Annexure TAD-38



ANNEXURE TAD-39

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NSW
DIVISION: GENERAL

NO NSD 474 OF 2024

ESAFETY COMMISSIONER

Applicant

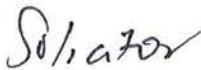
X CORP

Respondent

The following 17 pages is the annexure marked TAD-39 referred to in the affidavit of
Toby Allan Dagg made on 6 May 2024 before me:



.....
Signature



.....
Qualification

Filed on behalf of the Applicant, eSafety Commissioner
Prepared by: Matthew Garey
AGS lawyer within the meaning of s 55I of the *Judiciary Act 1903*

Address for Service:
The Australian Government Solicitor,
Level 10, 60 Martin Place, Sydney, NSW 2000
Matthew.Garey@ags.gov.au

File ref: 24003626

Telephone: 02 9581 7625
Lawyer's Email:
Matthew.Garey@ags.gov.au
Facsimile: 02 6169 3054

Image 1 of Annexure TAD-39

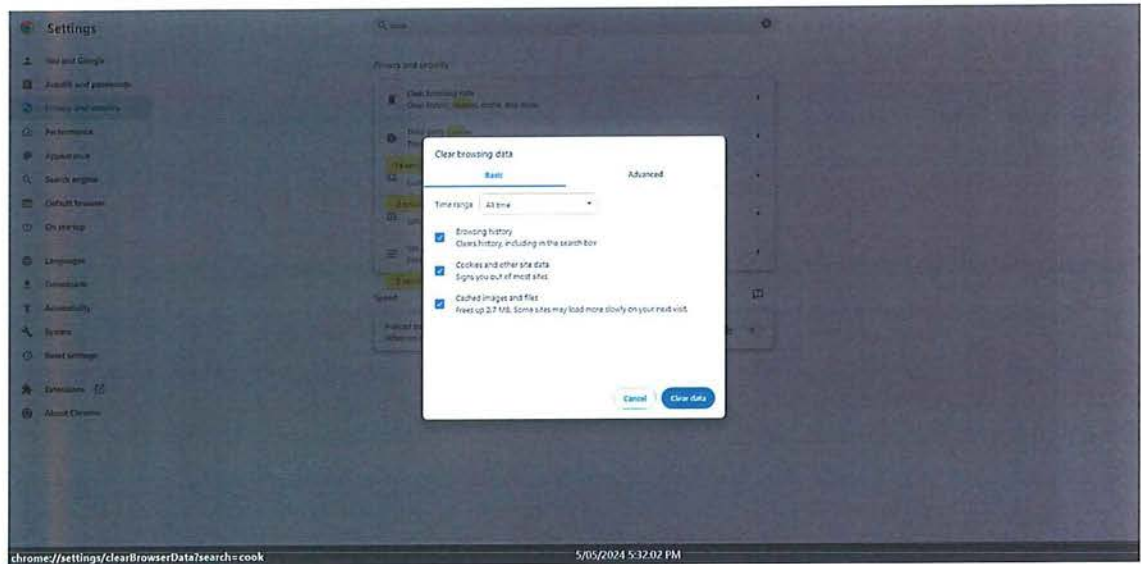


Image 2 of Annexure TAD-39

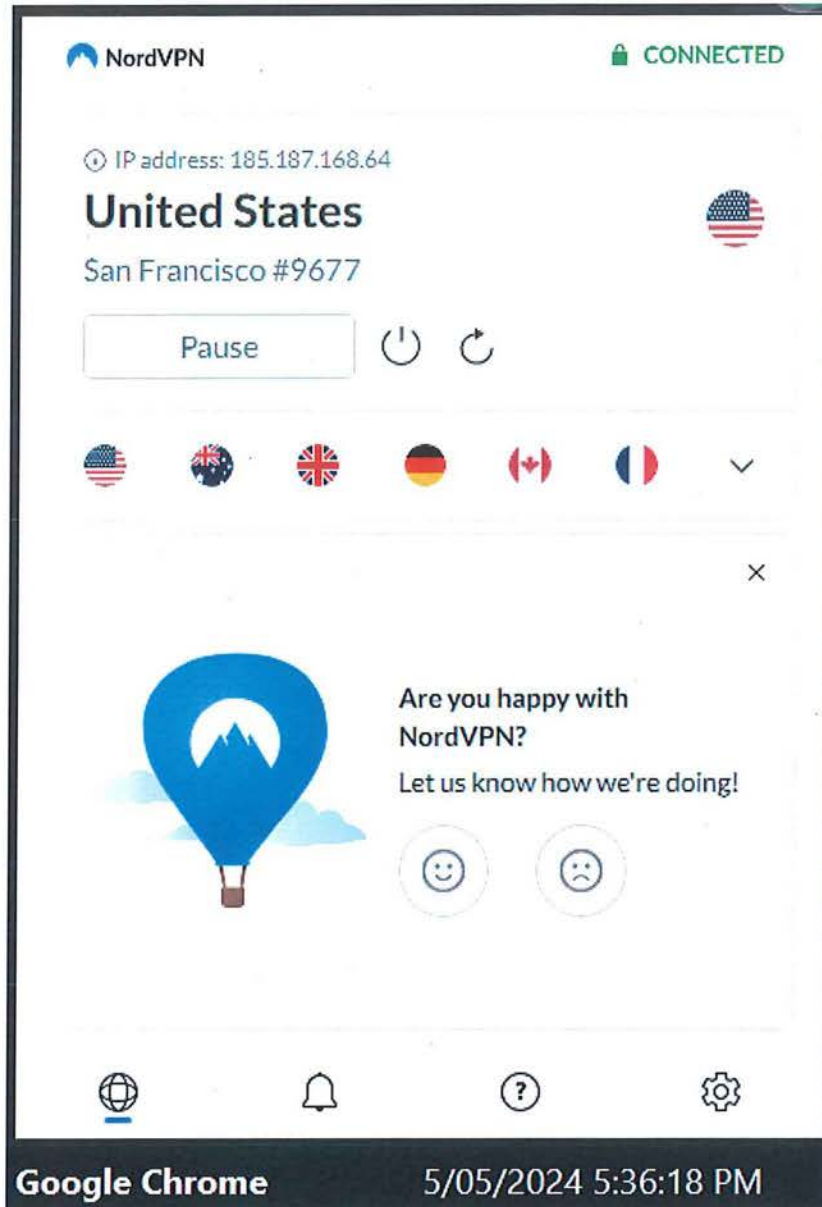


Image 3 of Annexure TAD-39

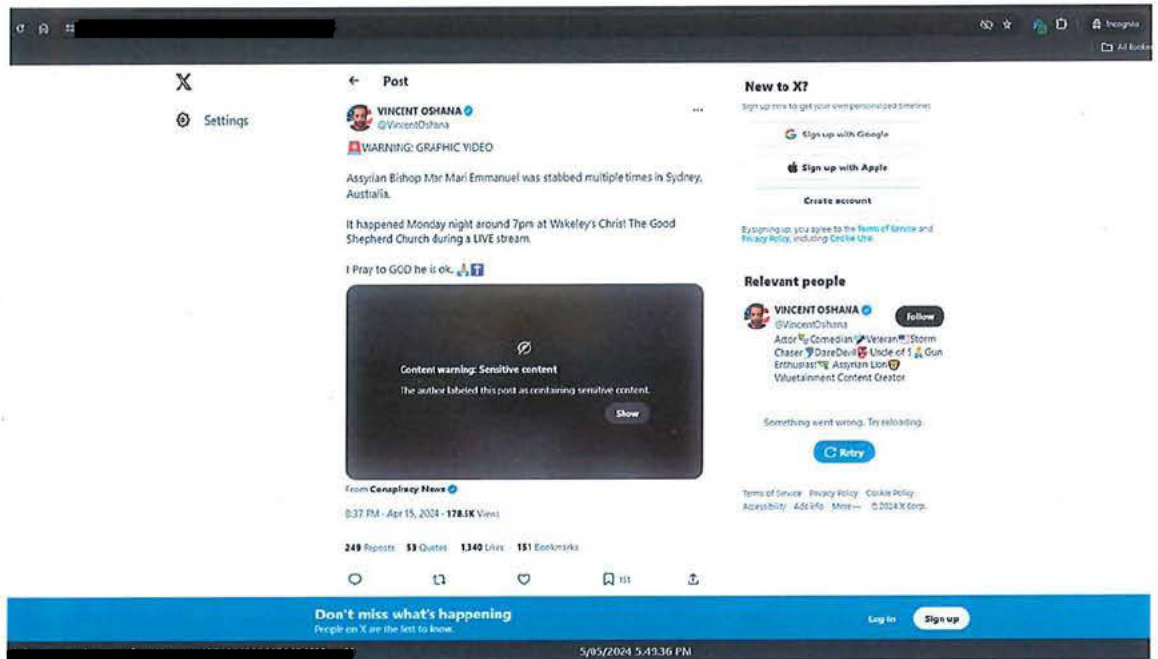


Image 4 of Annexure TAD-39

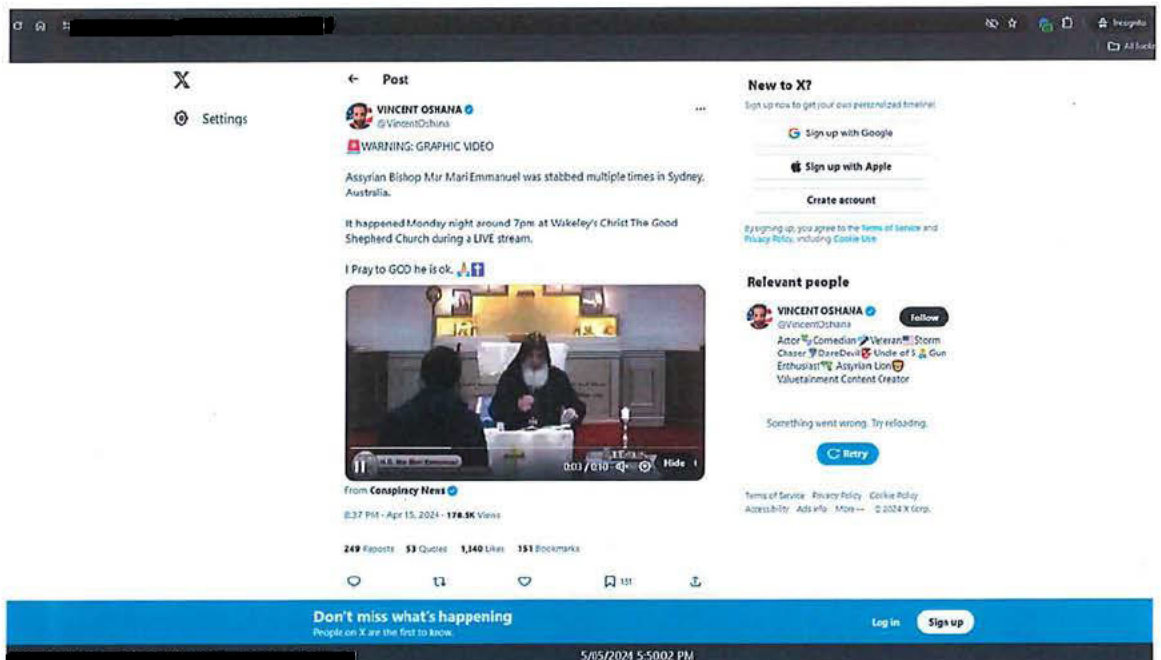


Image 5 of Annexure TAD-39

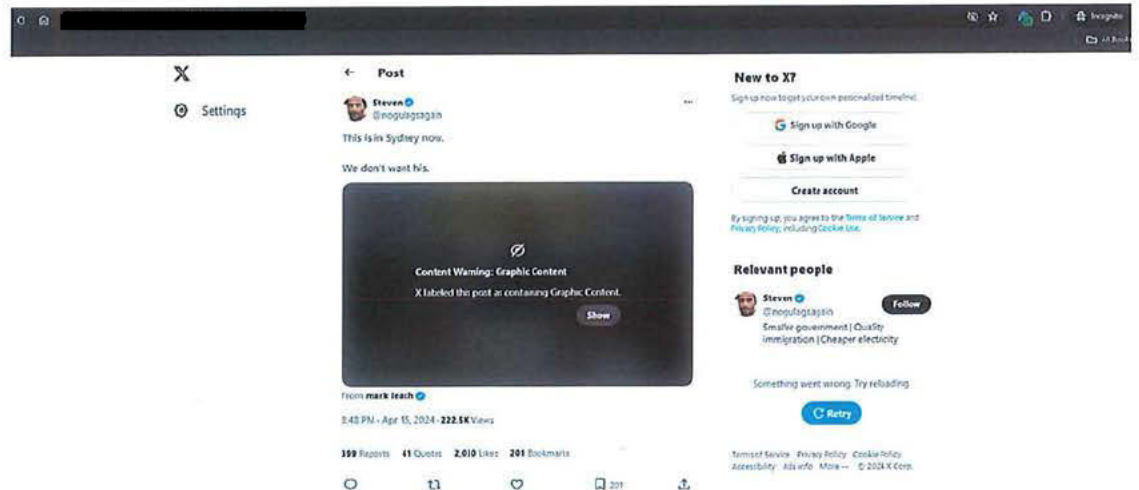


Image 6 of Annexure TAD-39



Image 7 of Annexure TAD-39

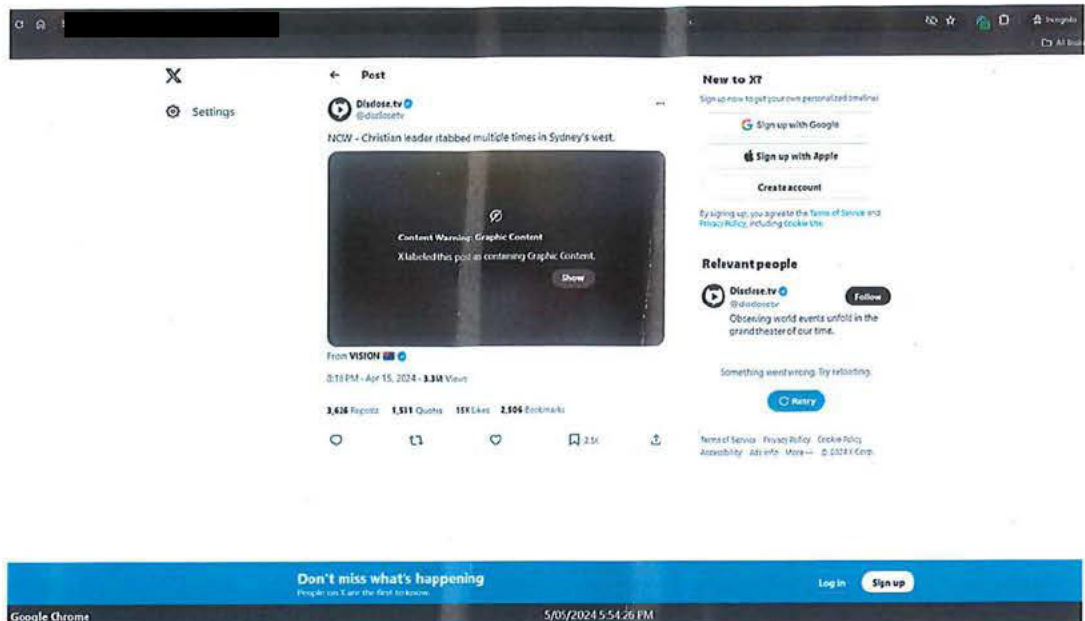


Image 8 of Annexure TAD-39

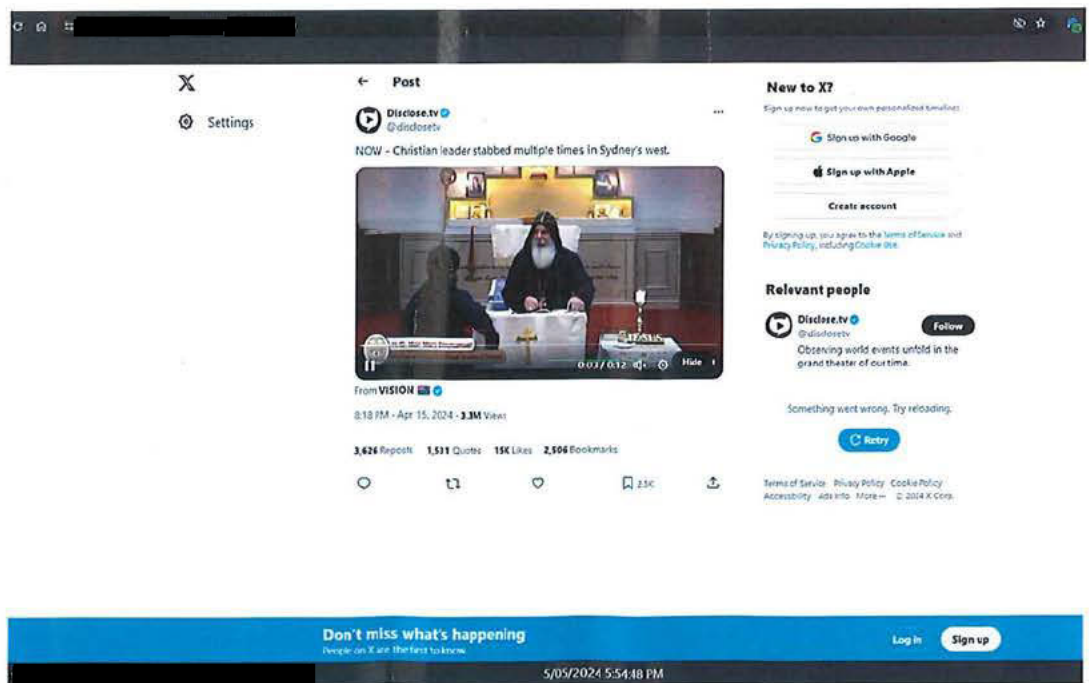


Image 9 of Annexure TAD-39

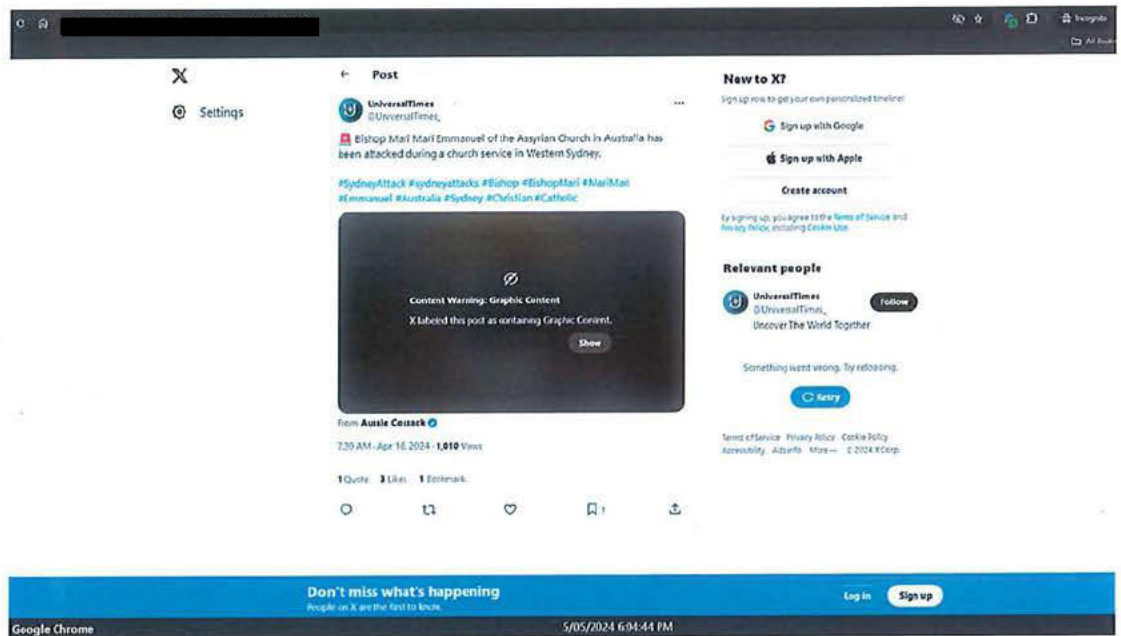


Image 10 of Annexure TAD-39

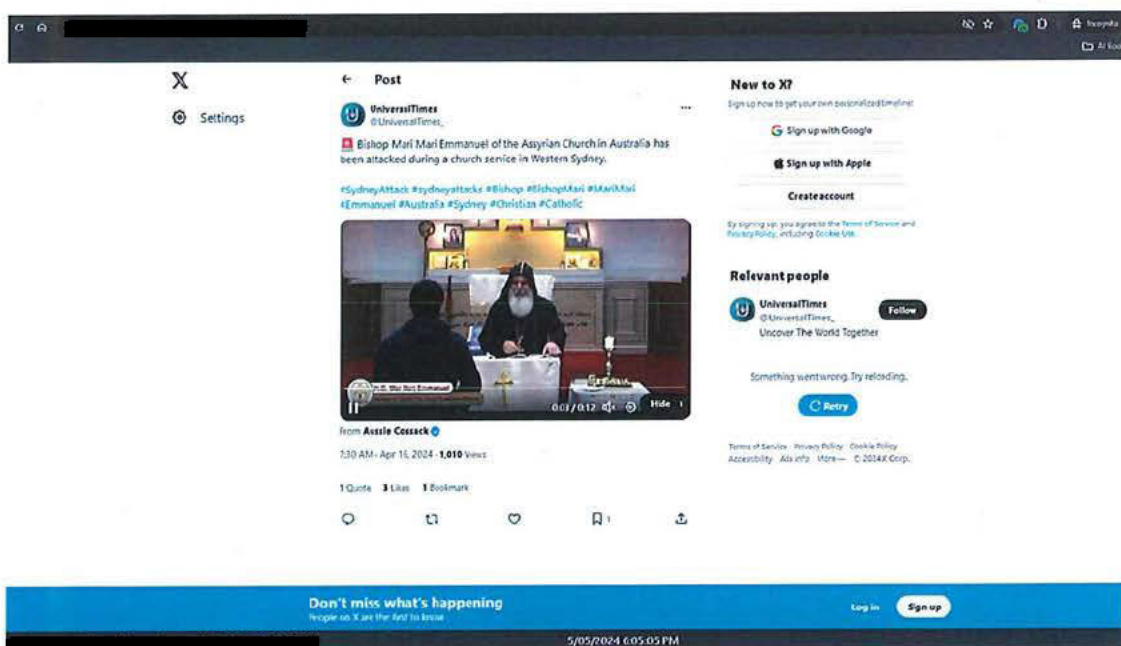


Image 11 of Annexure TAD-39

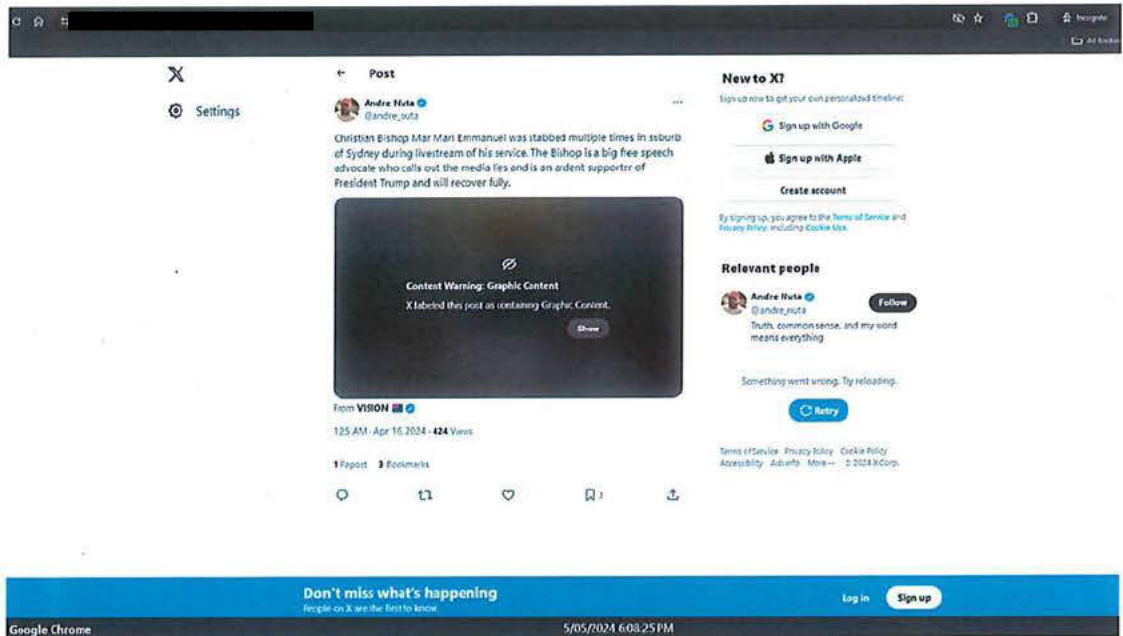


Image 12 of Annexure TAD-39

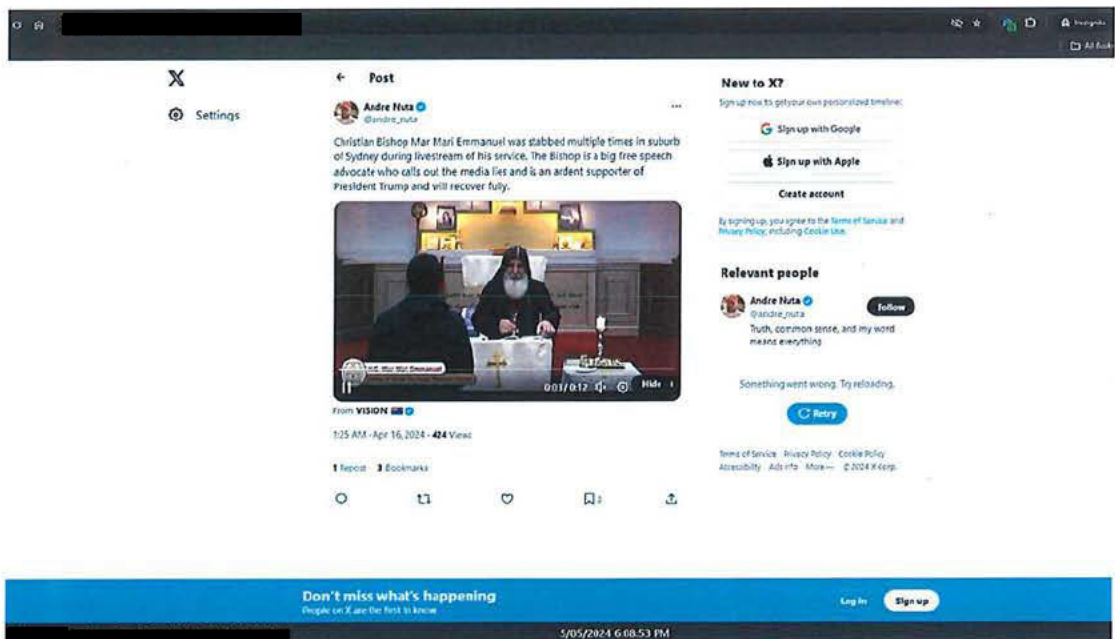


Image 13 of Annexure TAD-39

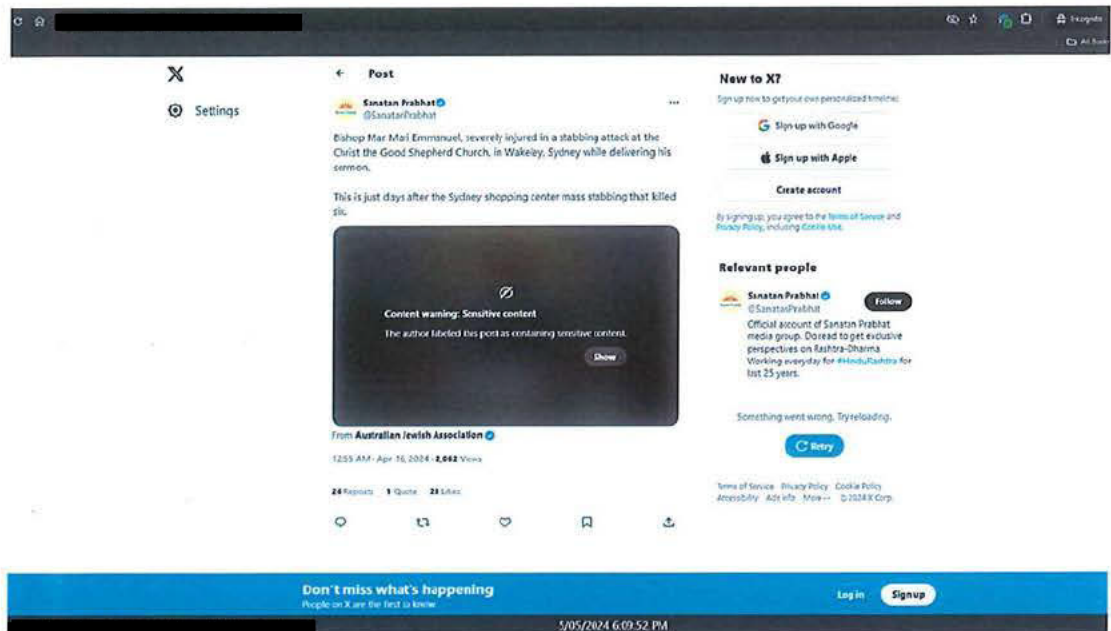


Image 14 of Annexure TAD-39

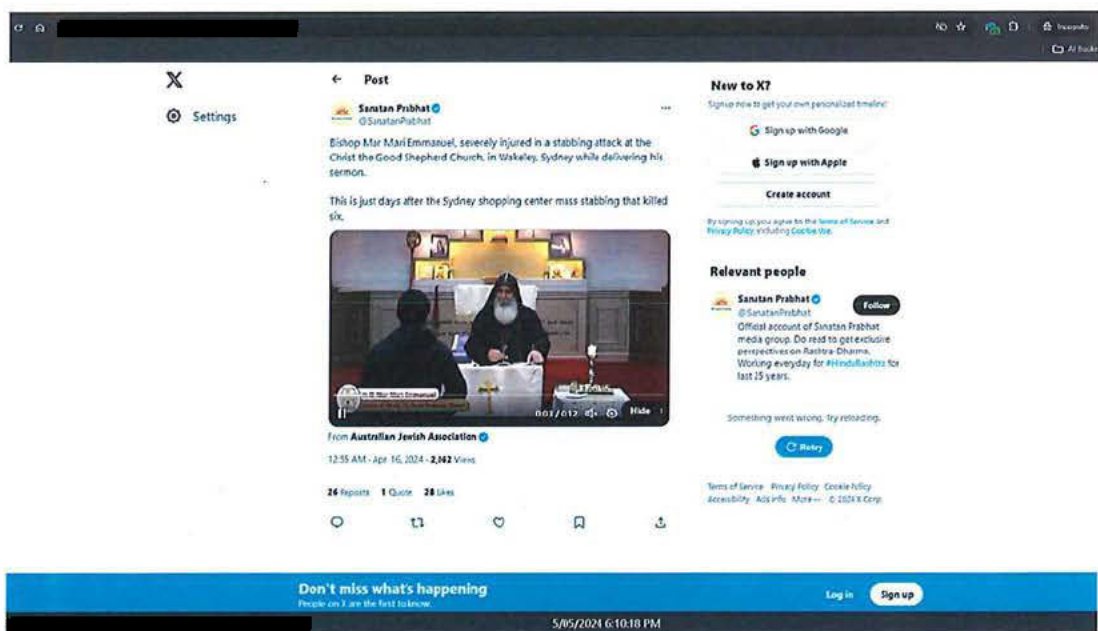


Image 15 of Annexure TAD-39

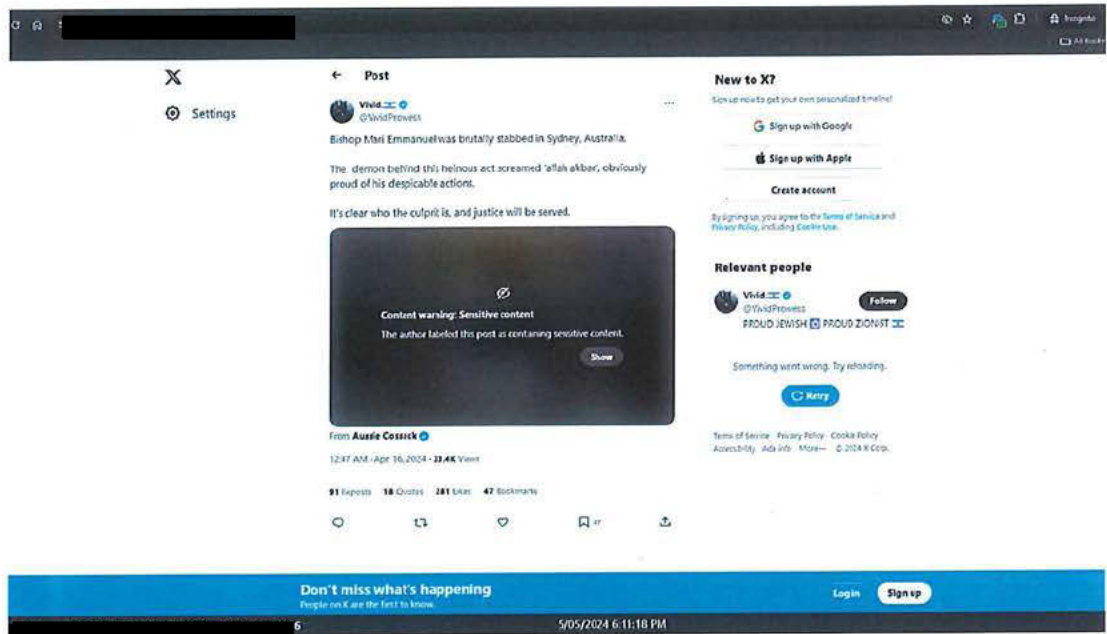


Image 16 of Annexure TAD-39

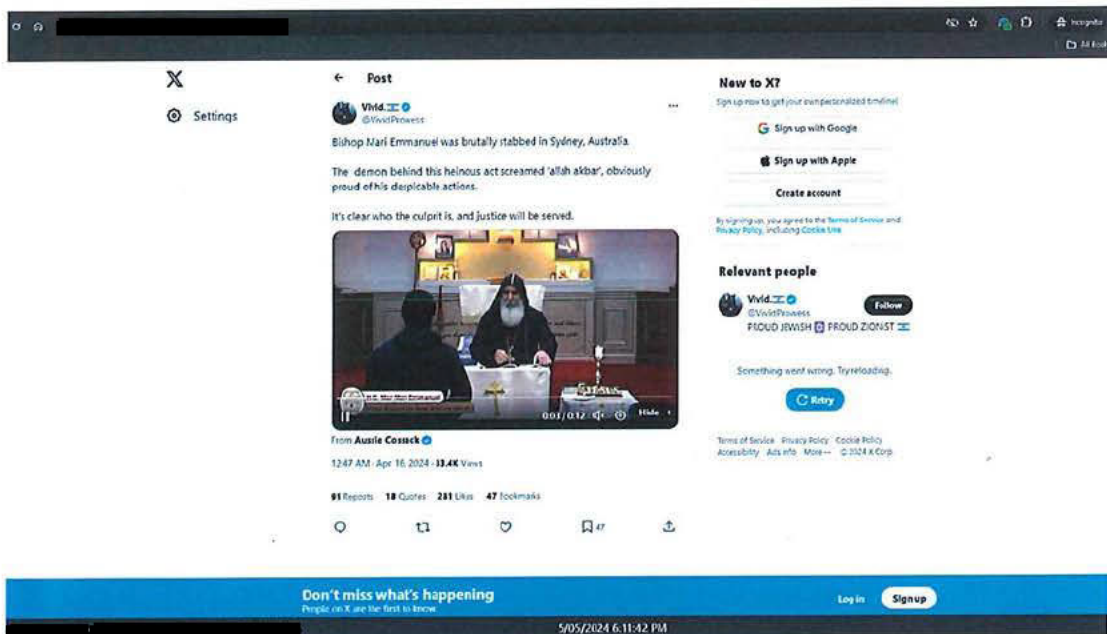


Image 17 of Annexure TAD-39

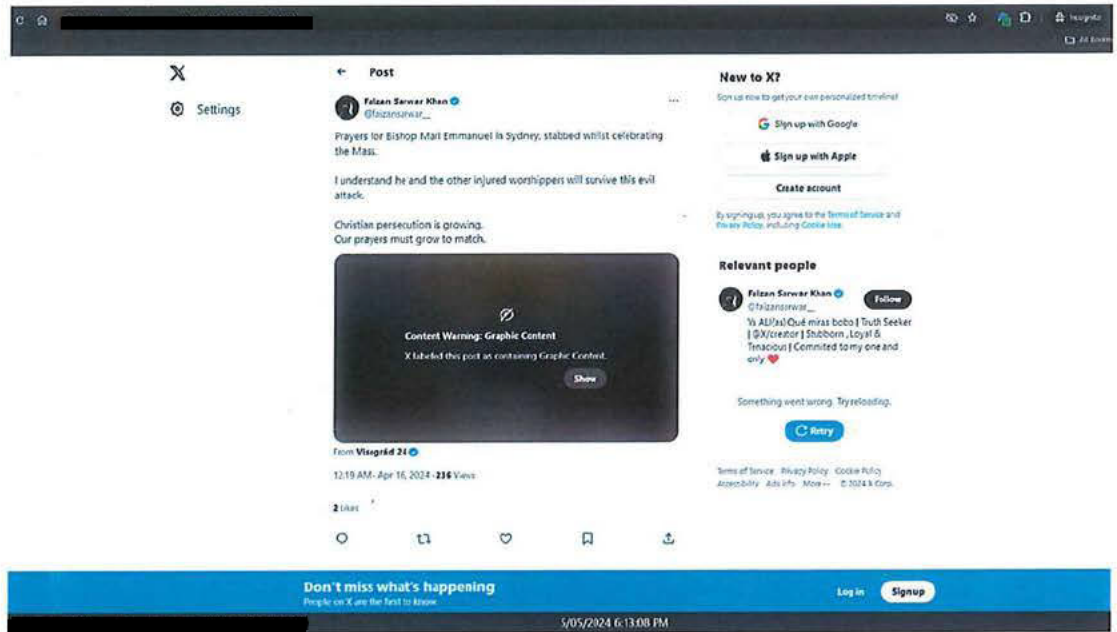


Image 18 of Annexure TAD-39

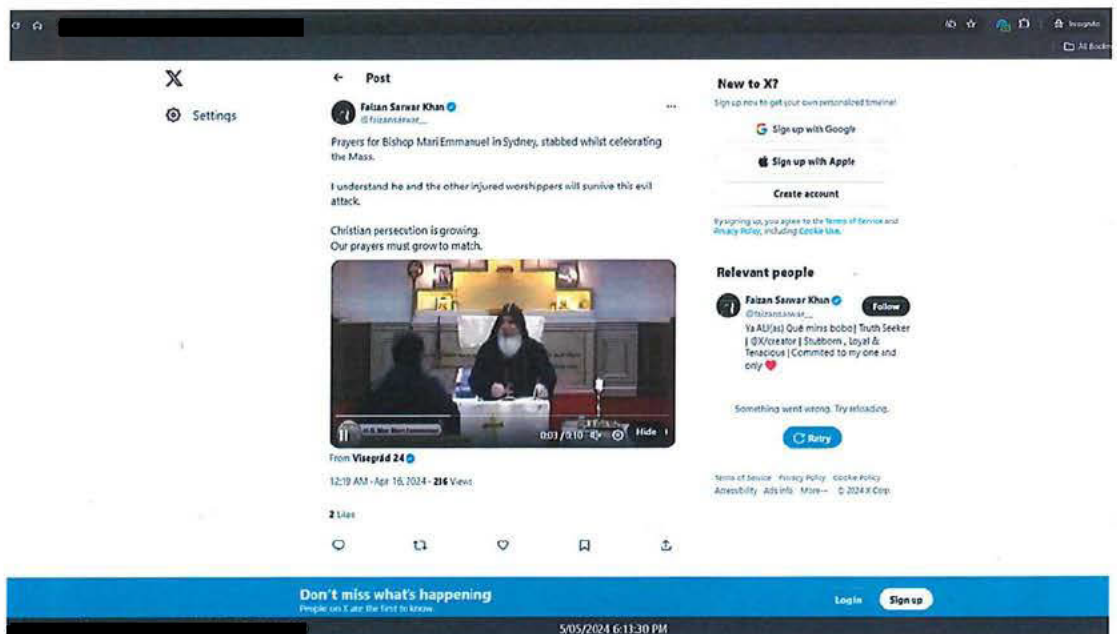


Image 19 of Annexure TAD-39

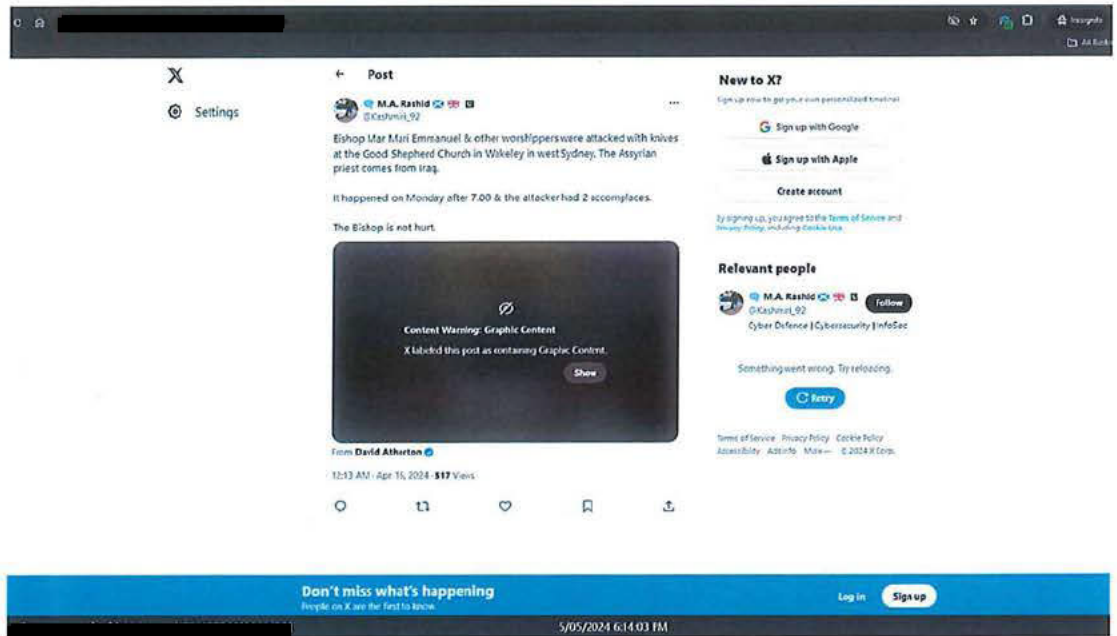


Image 20 of Annexure TAD-39

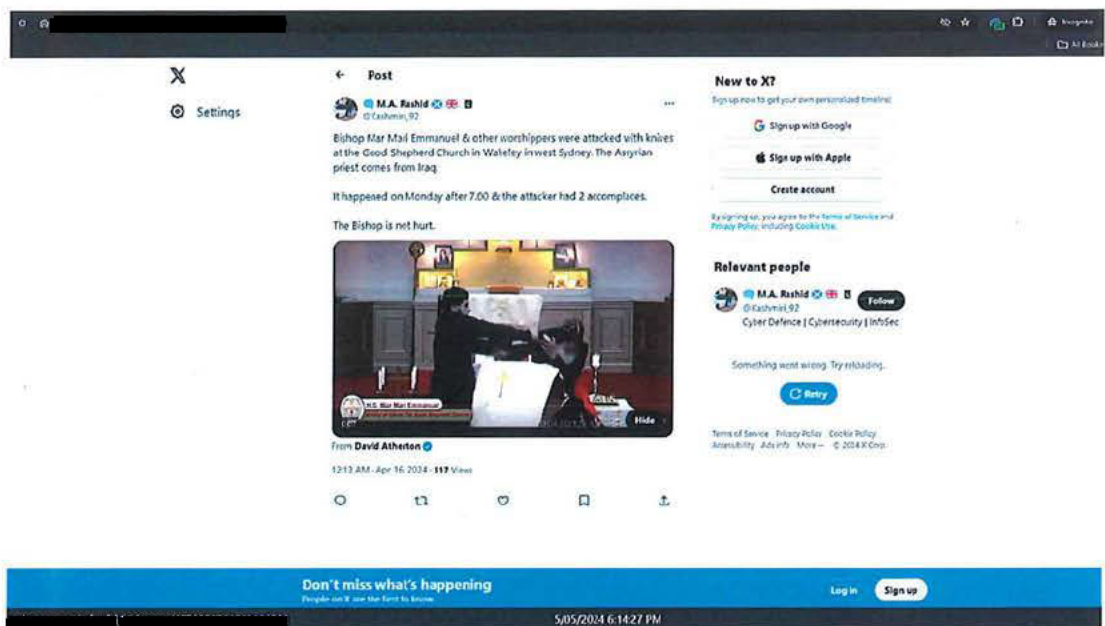


Image 21 of Annexure TAD-39

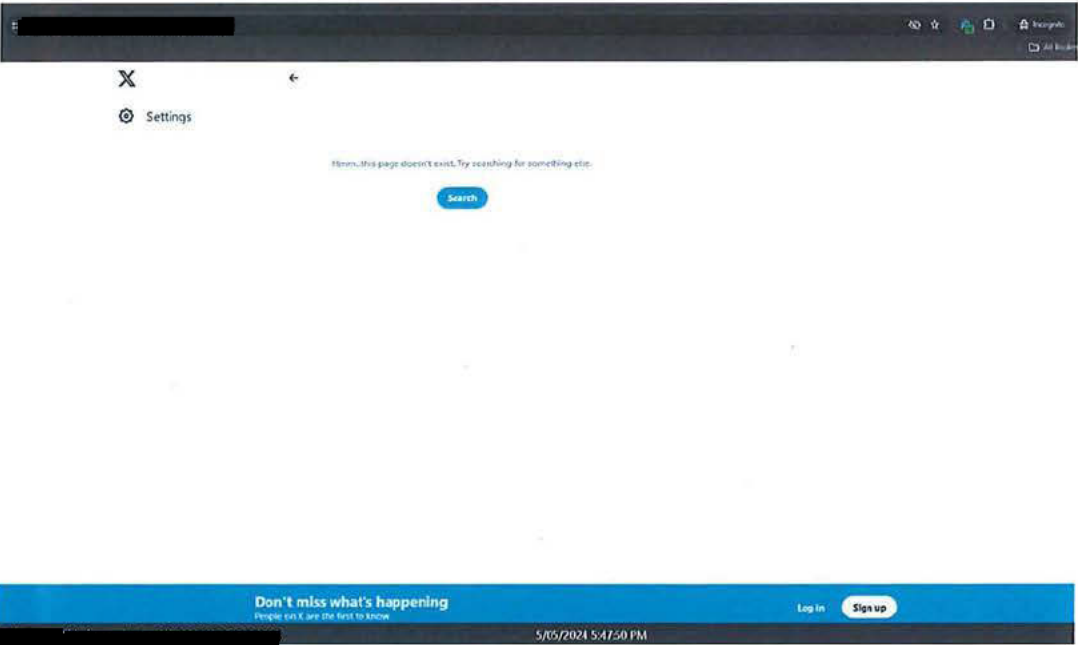


Image 22 of Annexure TAD-39

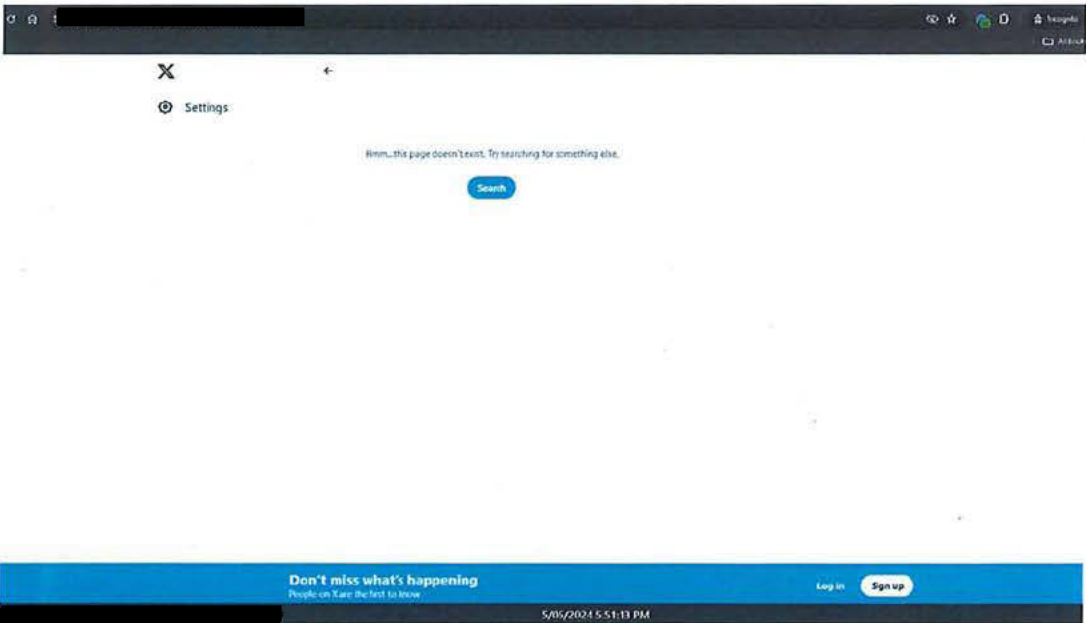


Image 23 of Annexure TAD-39

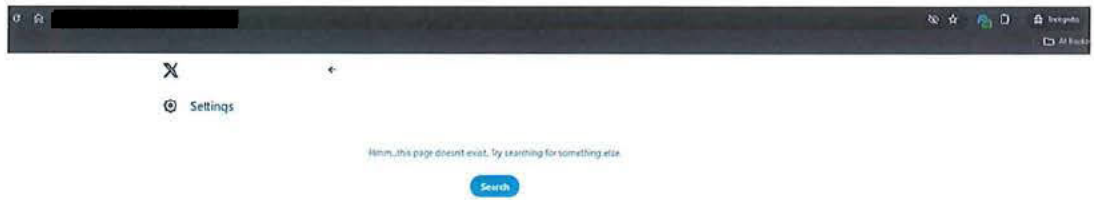


Image 24 of Annexure TAD-39

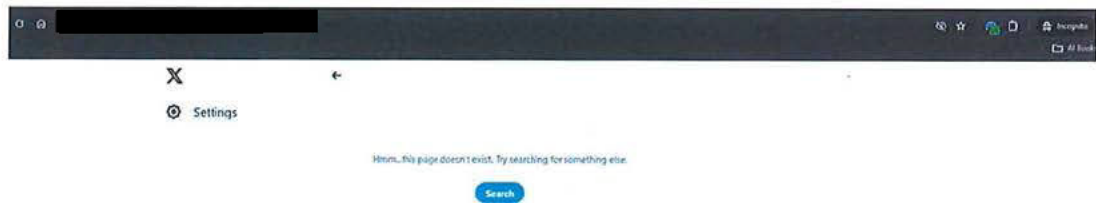


Image 25 of Annexure TAD-39

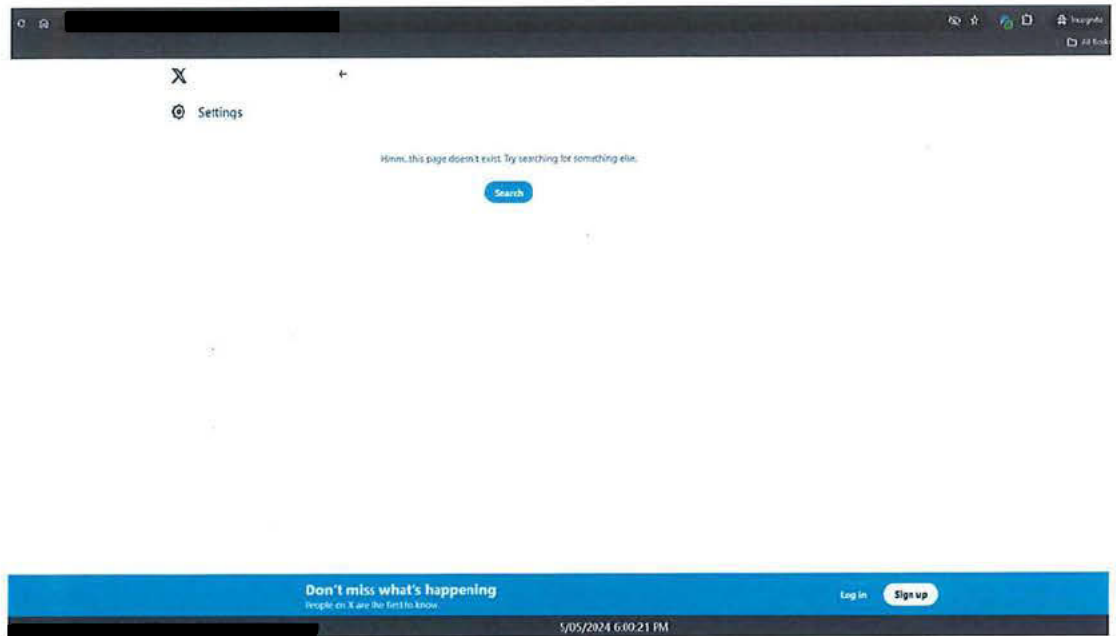


Image 26 of Annexure TAD-39

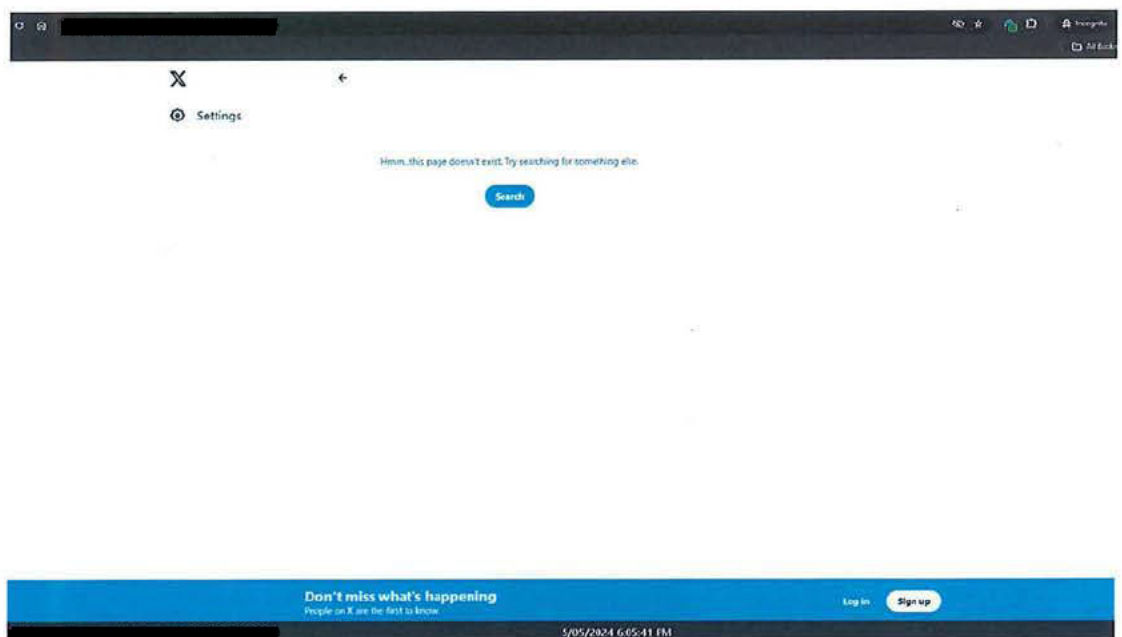


Image 27 of Annexure TAD-39

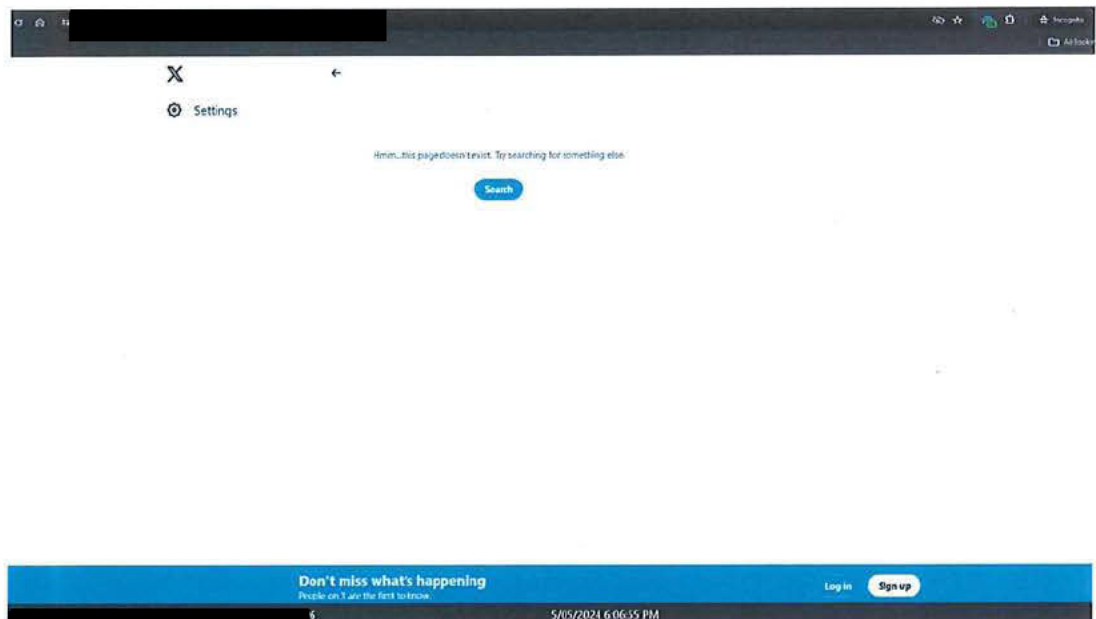


Image 28 of Annexure TAD-39

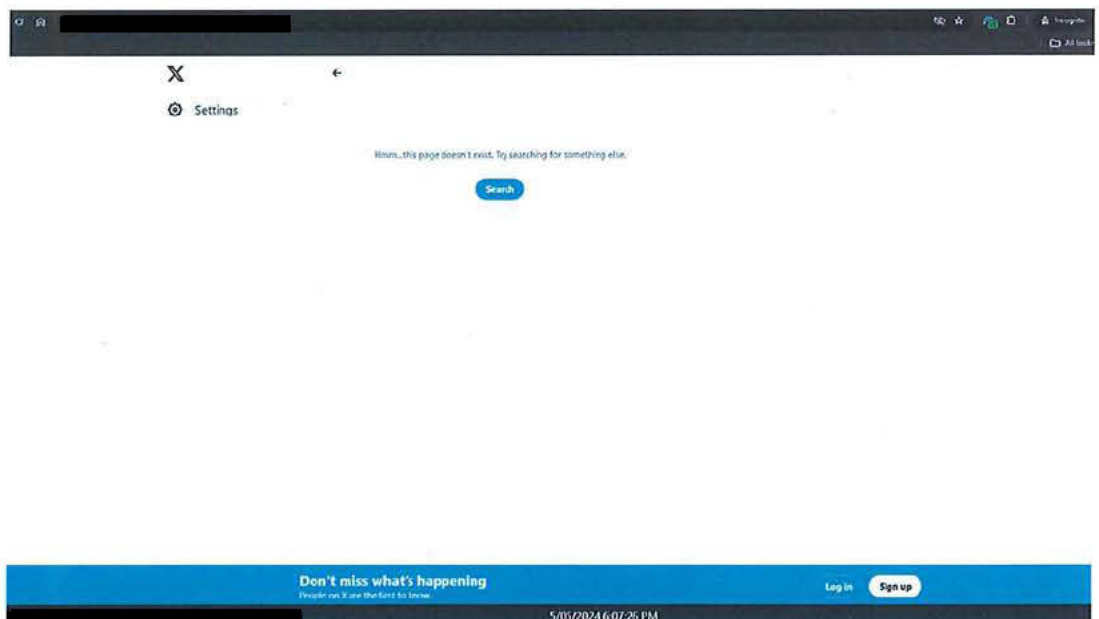


Image 29 of Annexure TAD-39

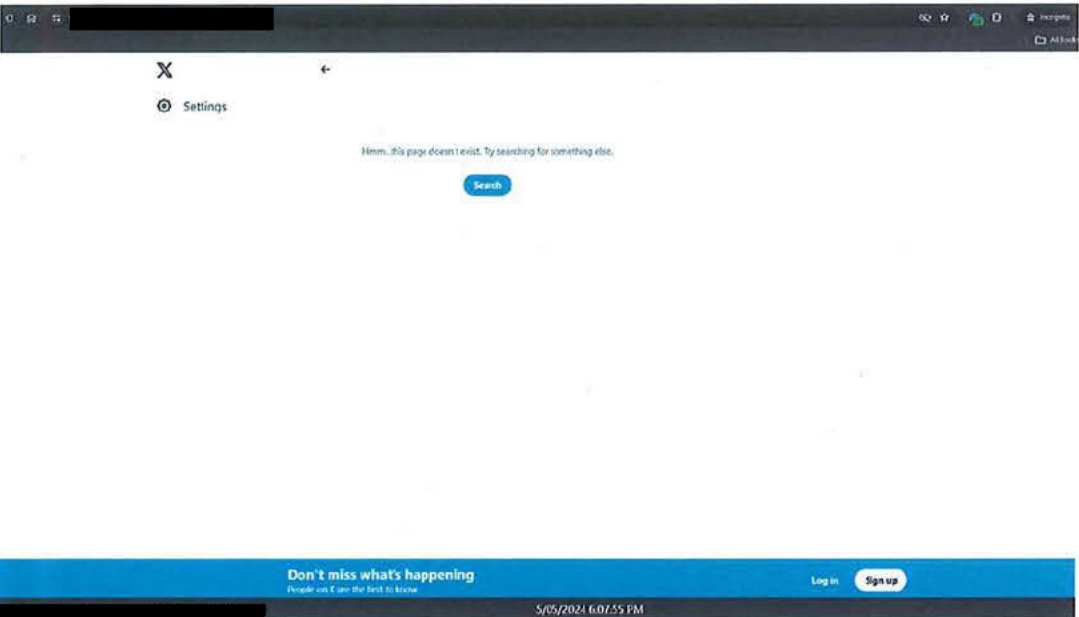


Image 30 of Annexure TAD-39

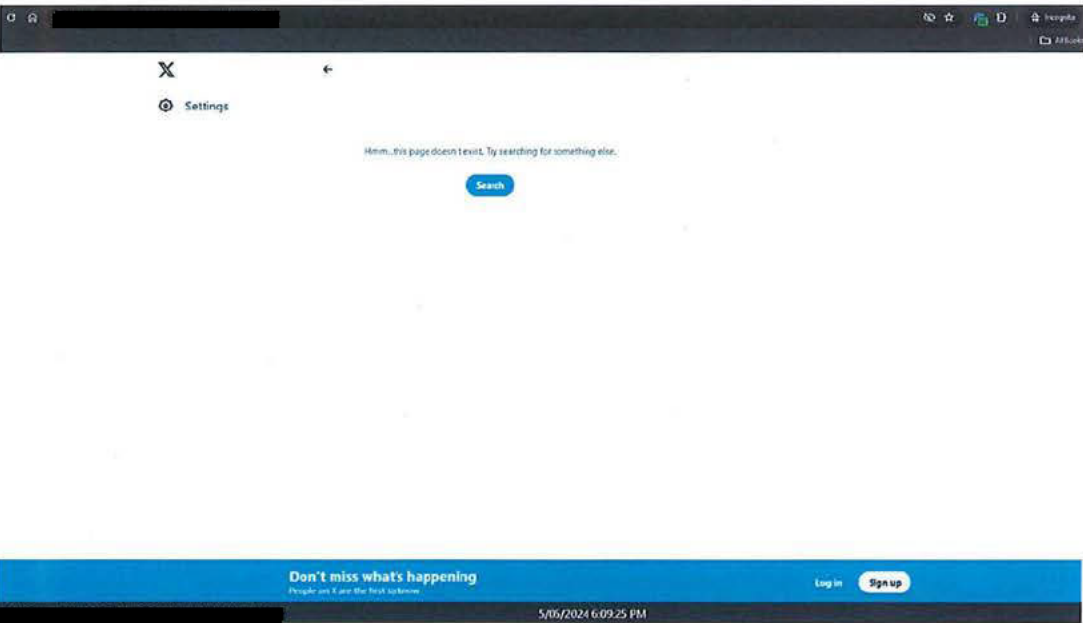
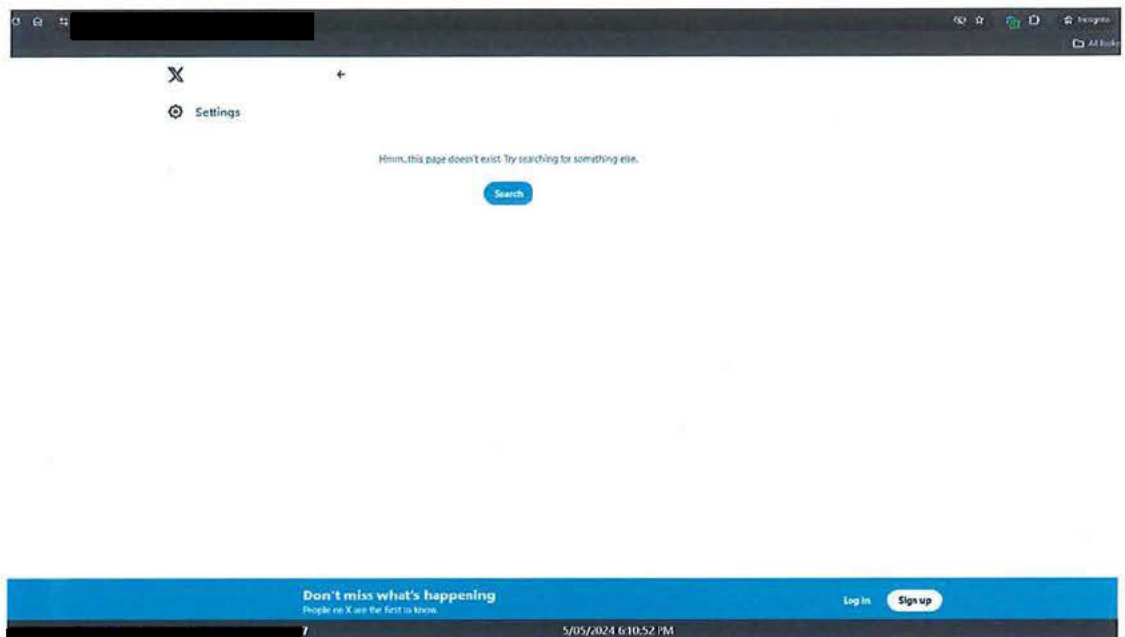


Image 31 of Annexure TAD-39



ANNEXURE TAD-40

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NSW
DIVISION: GENERAL

NO NSD 474 OF 2024

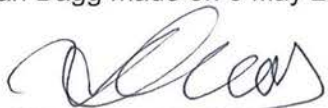
ESAFETY COMMISSIONER

Applicant

X CORP

Respondent

The following 22 pages is the annexure marked TAD-40 referred to in the affidavit of
Toby Allan Dagg made on 6 May 2024 before me:



.....
Signature



.....
Qualification

Filed on behalf of the Applicant, eSafety Commissioner
Prepared by: Matthew Garey
AGS lawyer within the meaning of s 55I of the *Judiciary Act 1903*

Address for Service:
The Australian Government Solicitor,
Level 10, 60 Martin Place, Sydney, NSW 2000
Matthew.Garey@ags.gov.au

File ref: 24003626

Telephone: 02 9581 7625
Lawyer's Email:
Matthew.Garey@ags.gov.au
Facsimile: 02 6169 3054

Image 1 of Annexure TAD-40

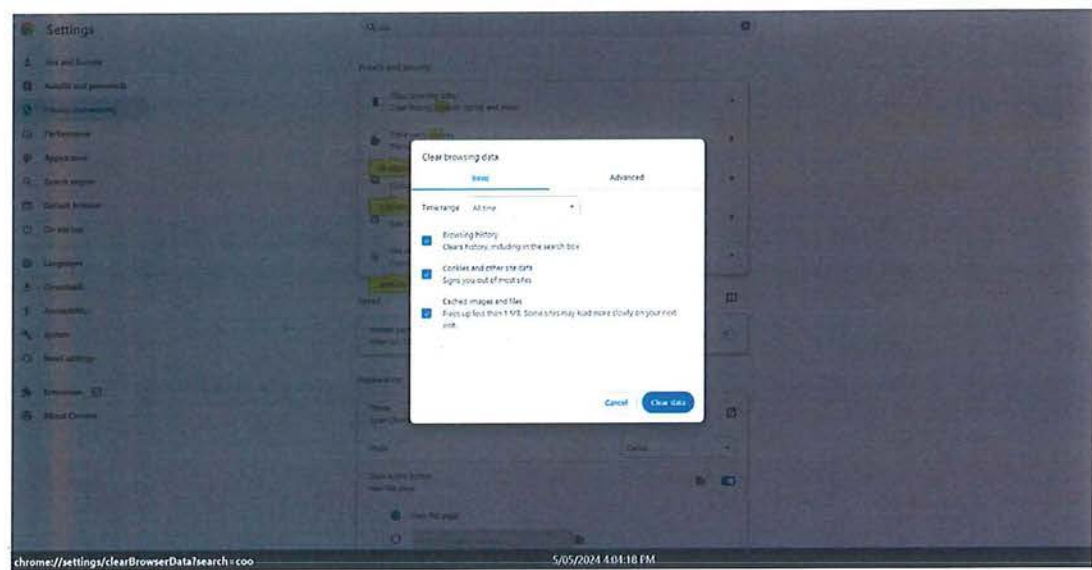


Image 2 of Annexure TAD-40

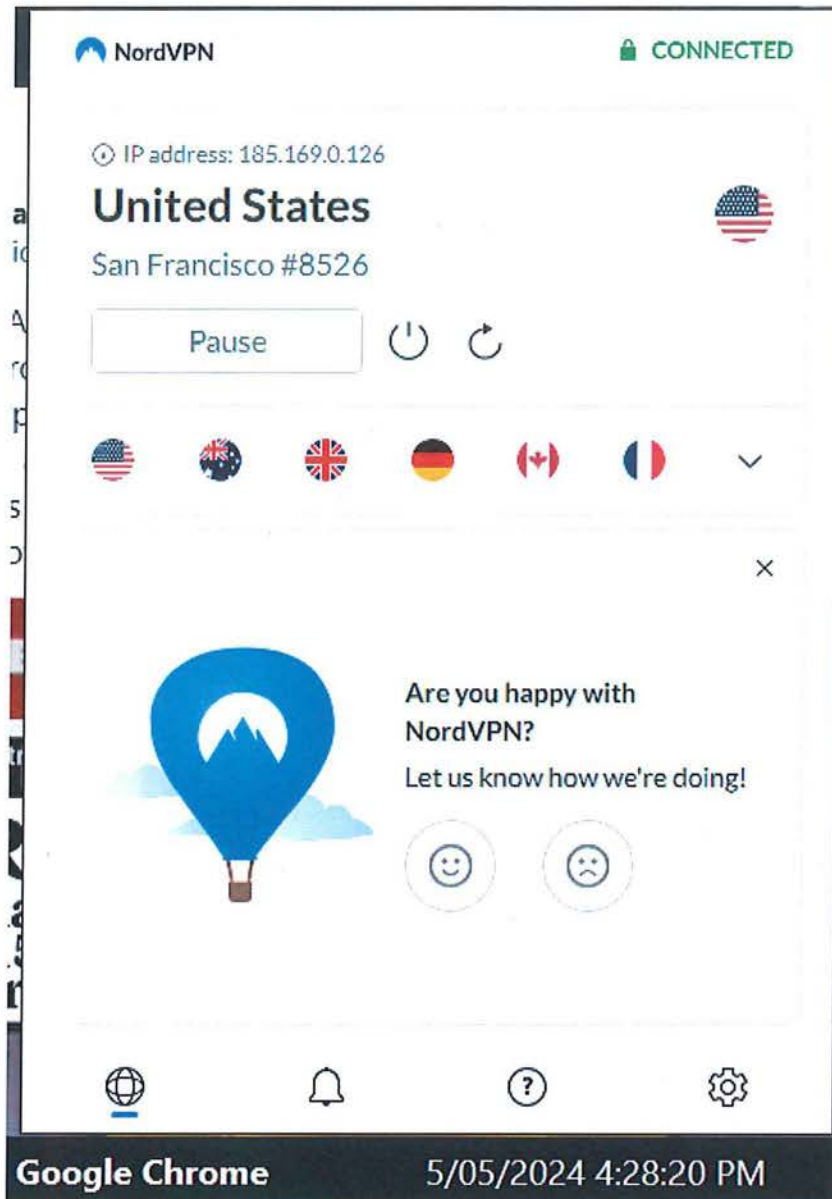


Image 3 of Annexure TAD-40

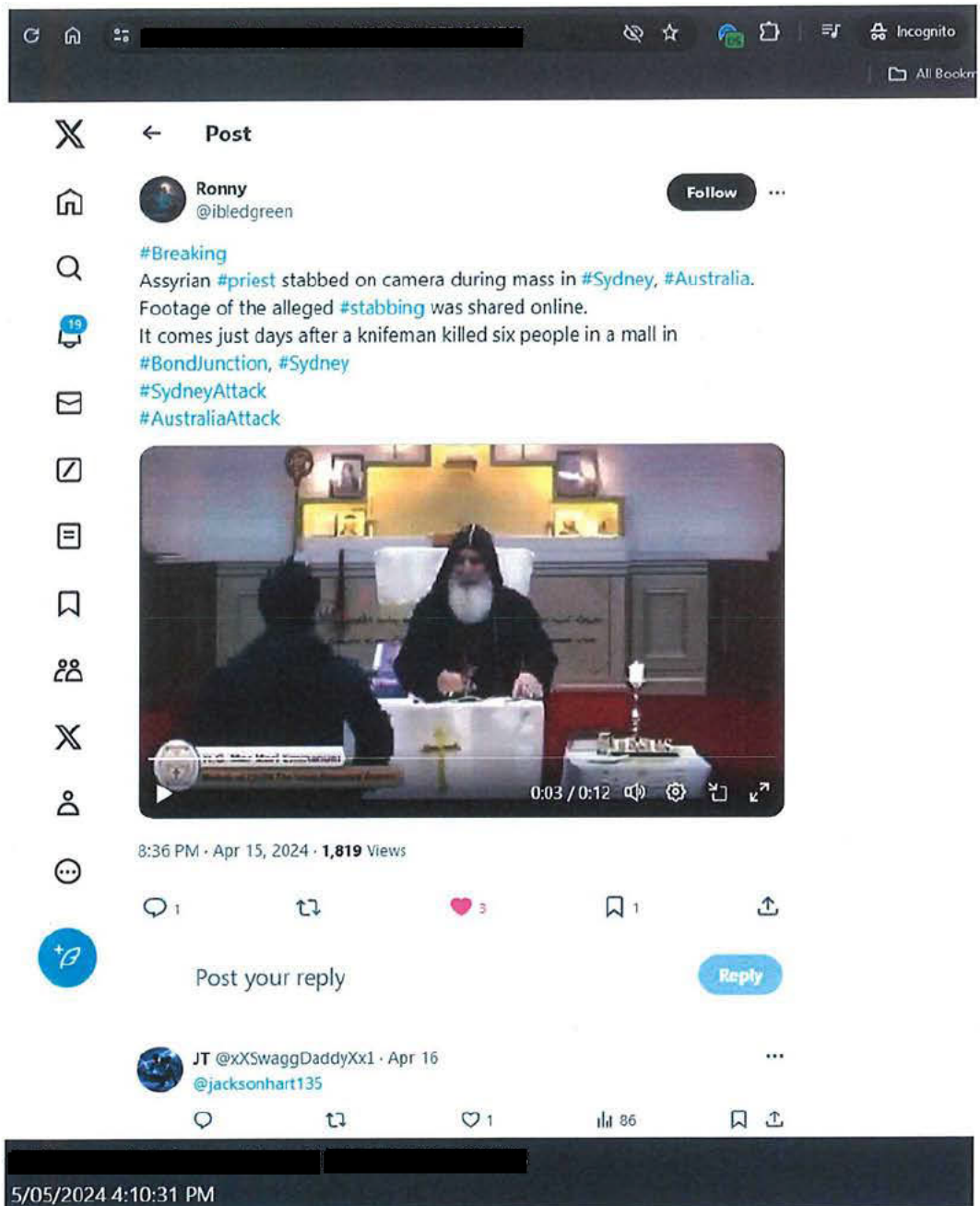


Image 4 of Annexure TAD-40

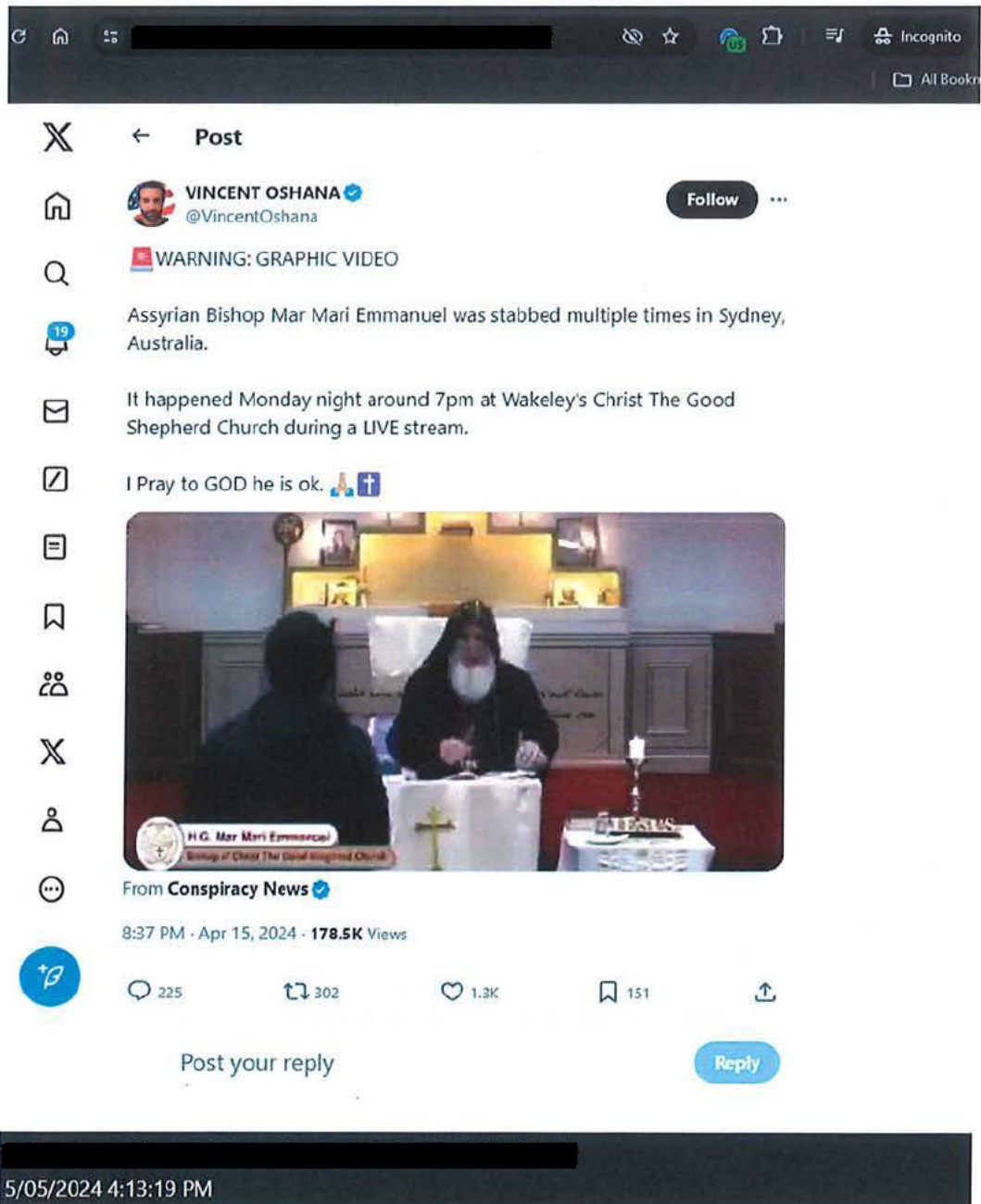


Image 5 of Annexure TAD-40

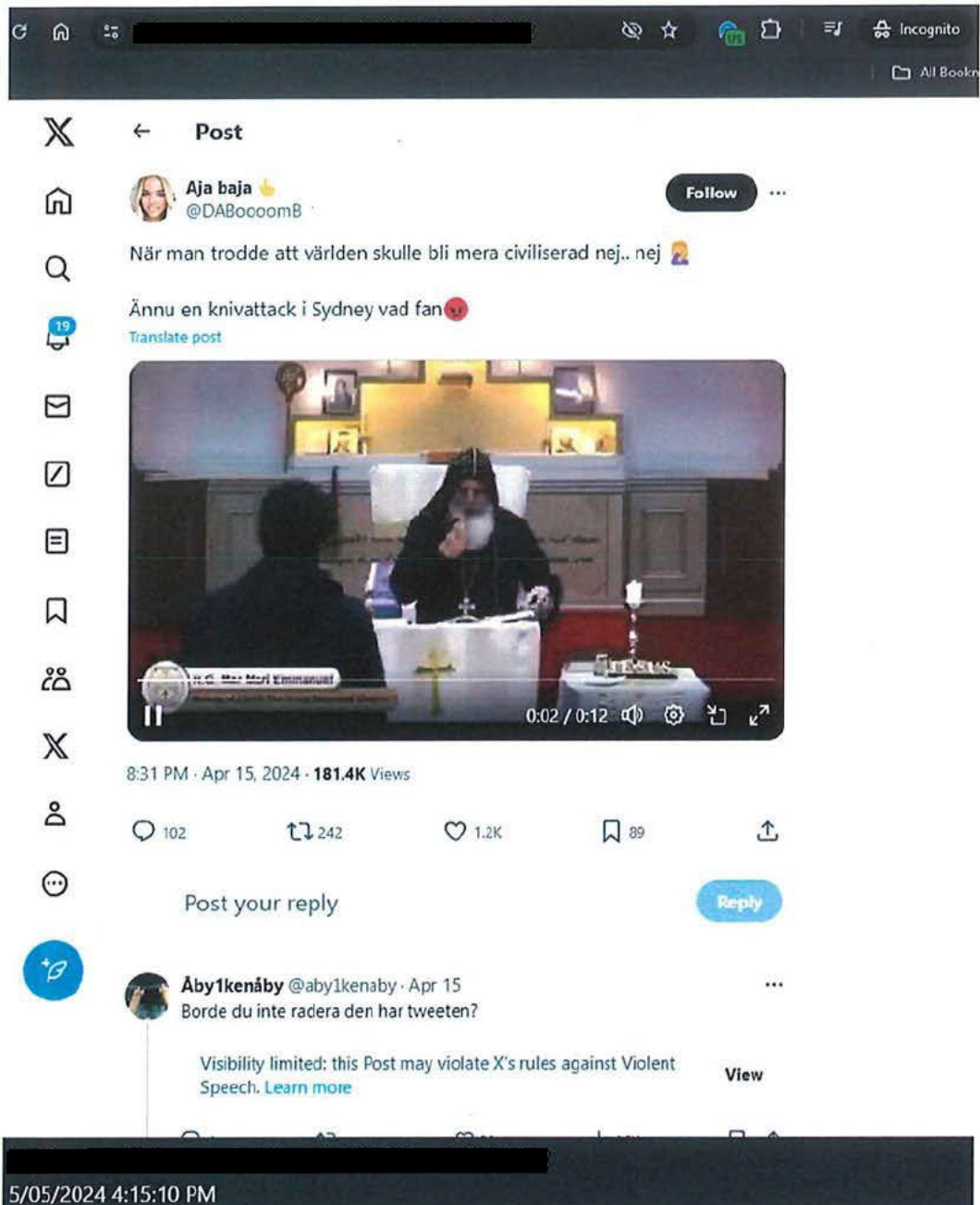


Image 6 of Annexure TAD-40

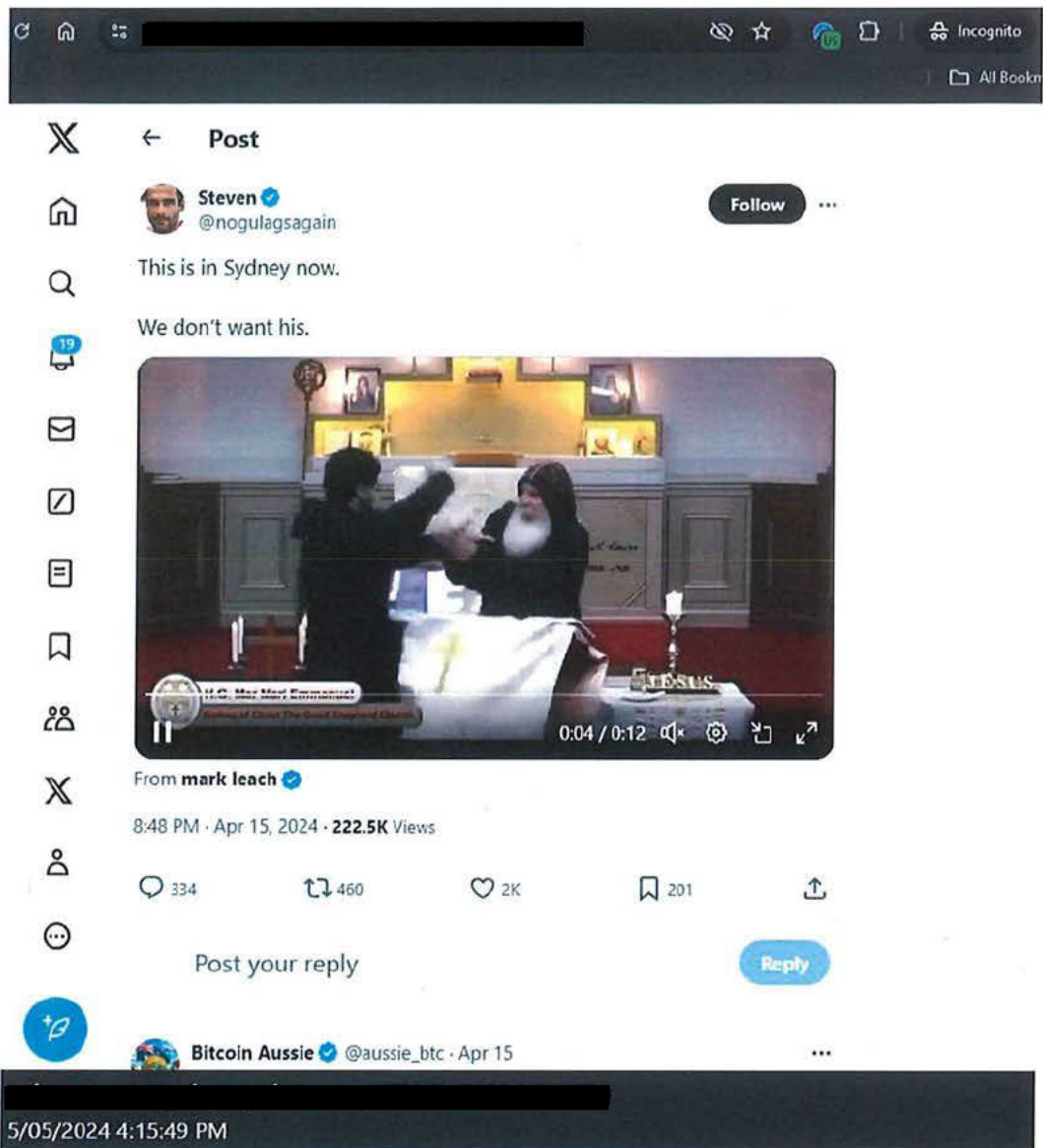


Image 7 of Annexure TAD-40

Incognito


All Book

Post

Disclose.tv @disclosetv

Subscribe

NOW - Christian leader stabbed multiple times in Sydney's west.



H.G. Mar Mari Emmanuel
Bishop of Christ The Good Shepherd Church

0:08

From VISION

8:18 PM · Apr 15, 2024 · 3.3M Views

1.4K 5.1K 15K 2.5K

Post your reply

Reply

Disclose.tv @disclosetv · Apr 15

UPDATE - Four people stabbed at Christ The Good Shepherd Church in a western Sydney suburb. Major police operation underway.

47 329 2.3K 209K

5/05/2024 4:16:24 PM

Image 8 of Annexure TAD-40

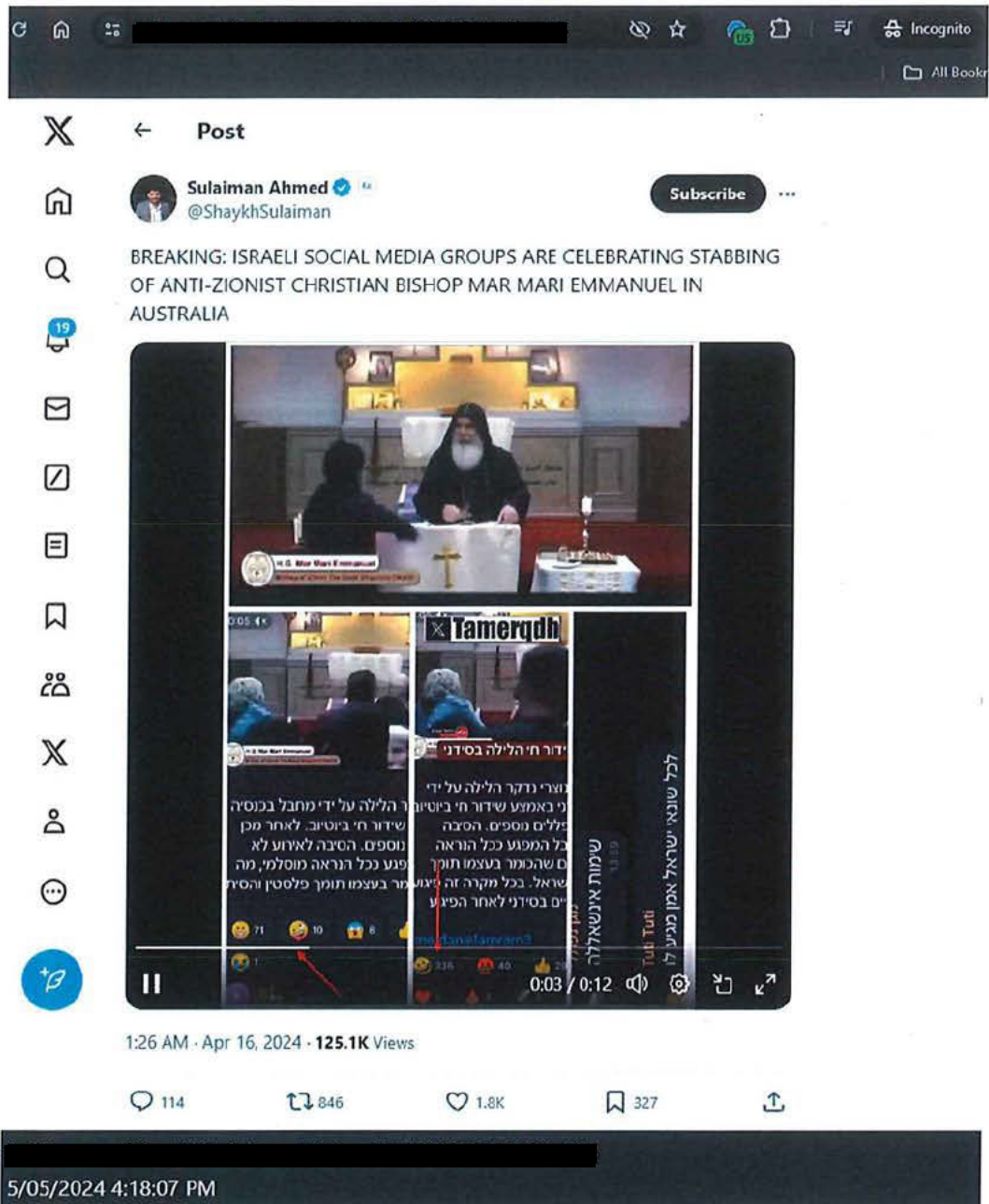


Image 9 of Annexure TAD-40

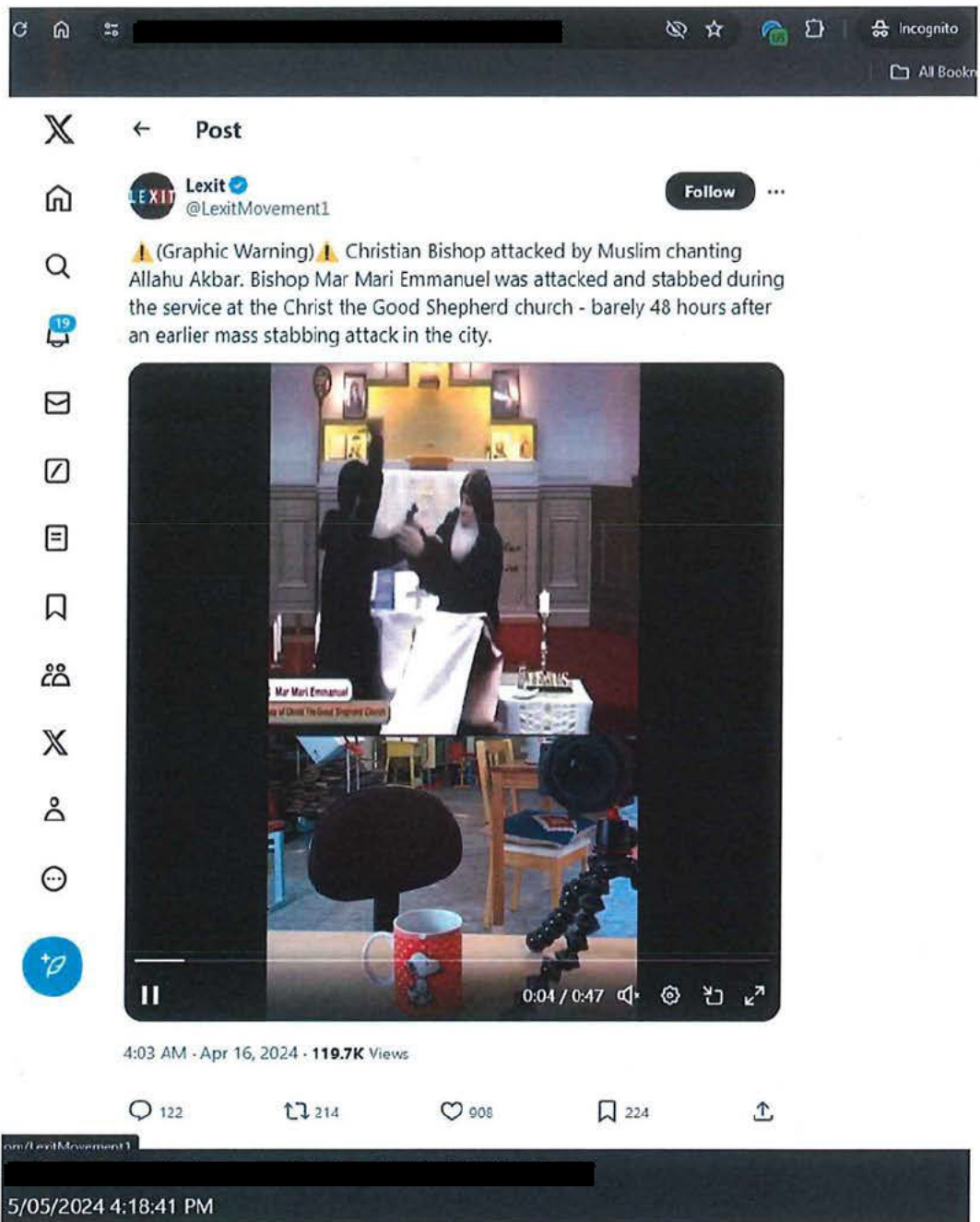


Image 10 of Annexure TAD-40

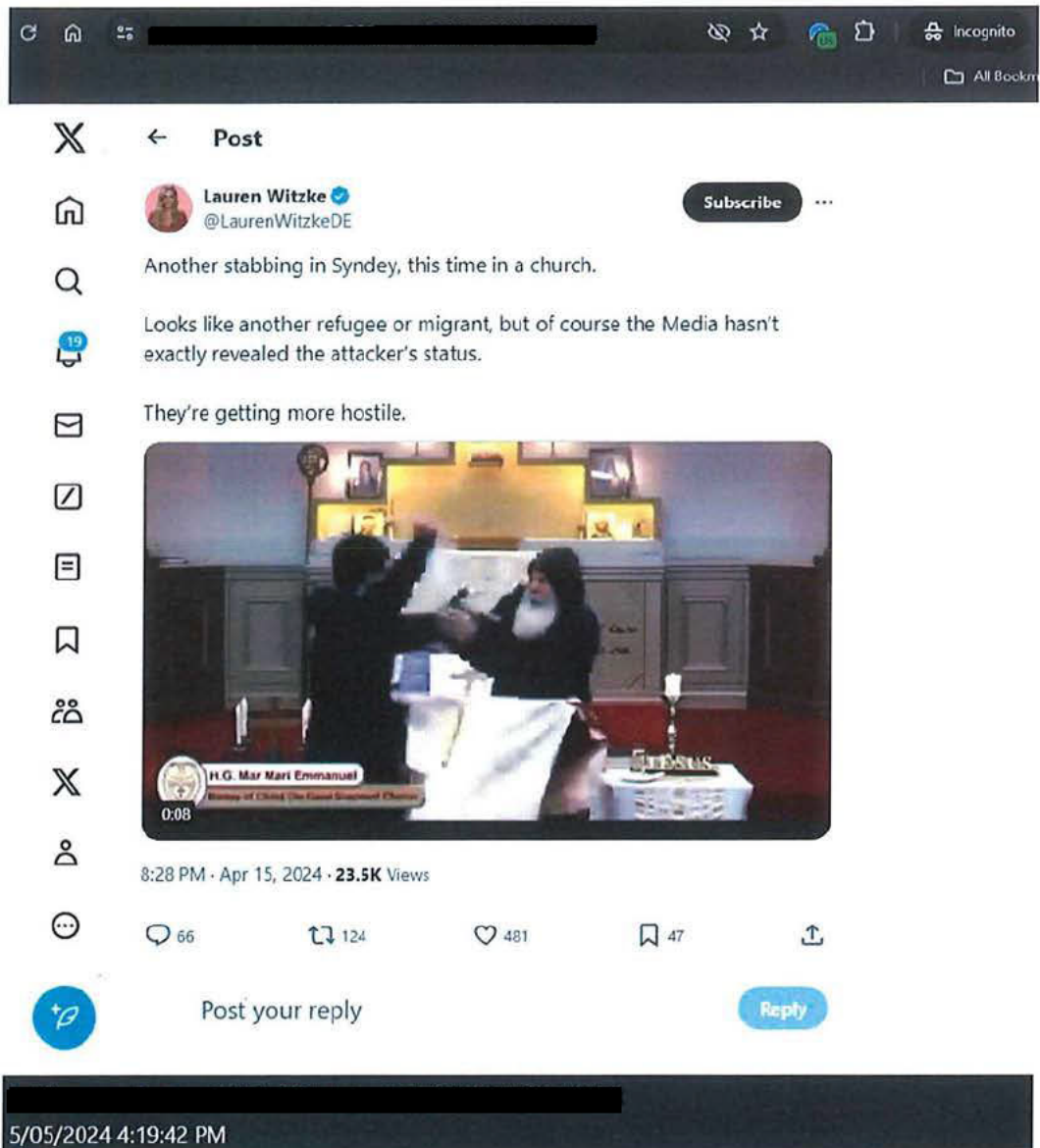


Image 11 of Annexure TAD-40

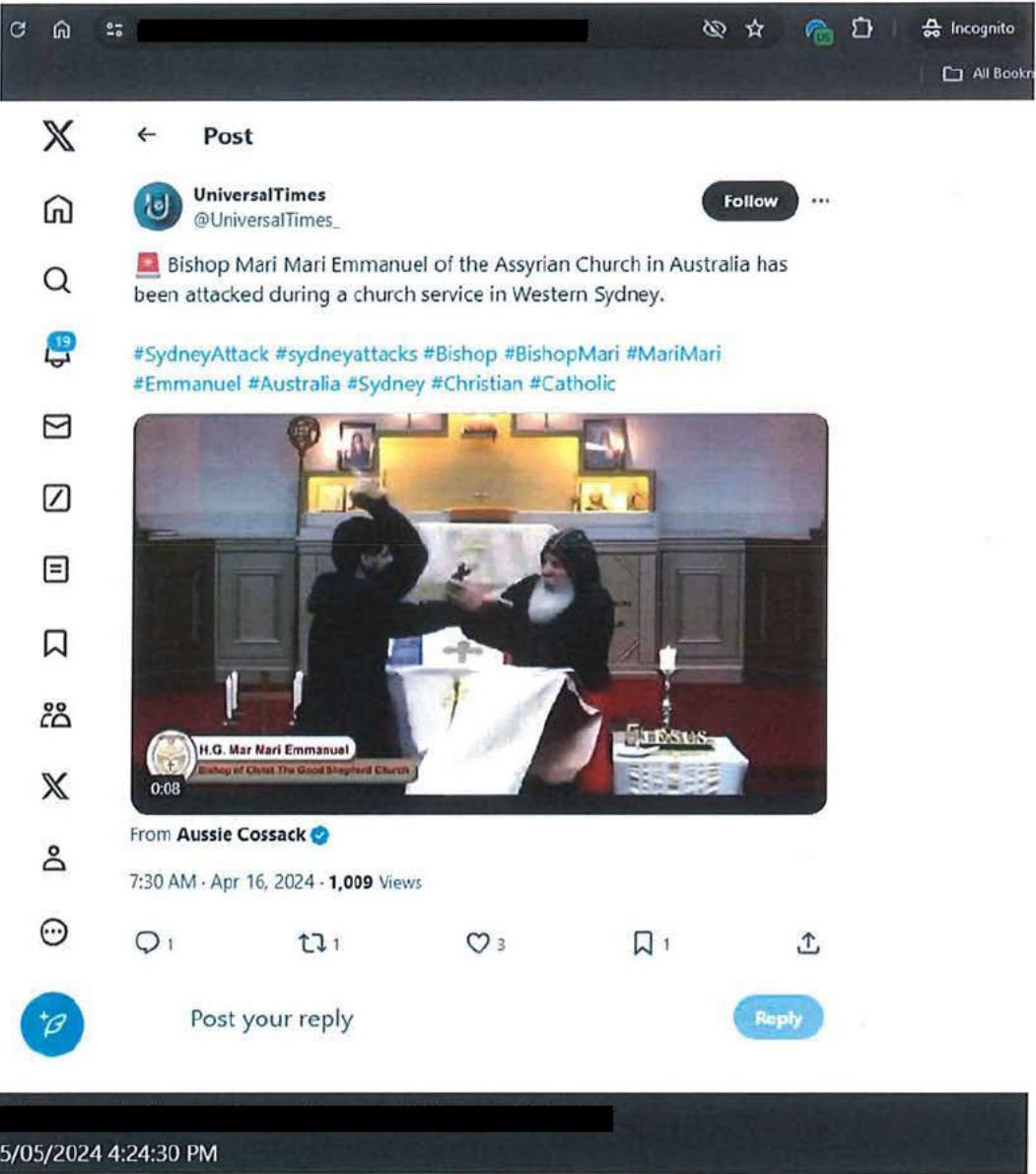


Image 12 of Annexure TAD-40

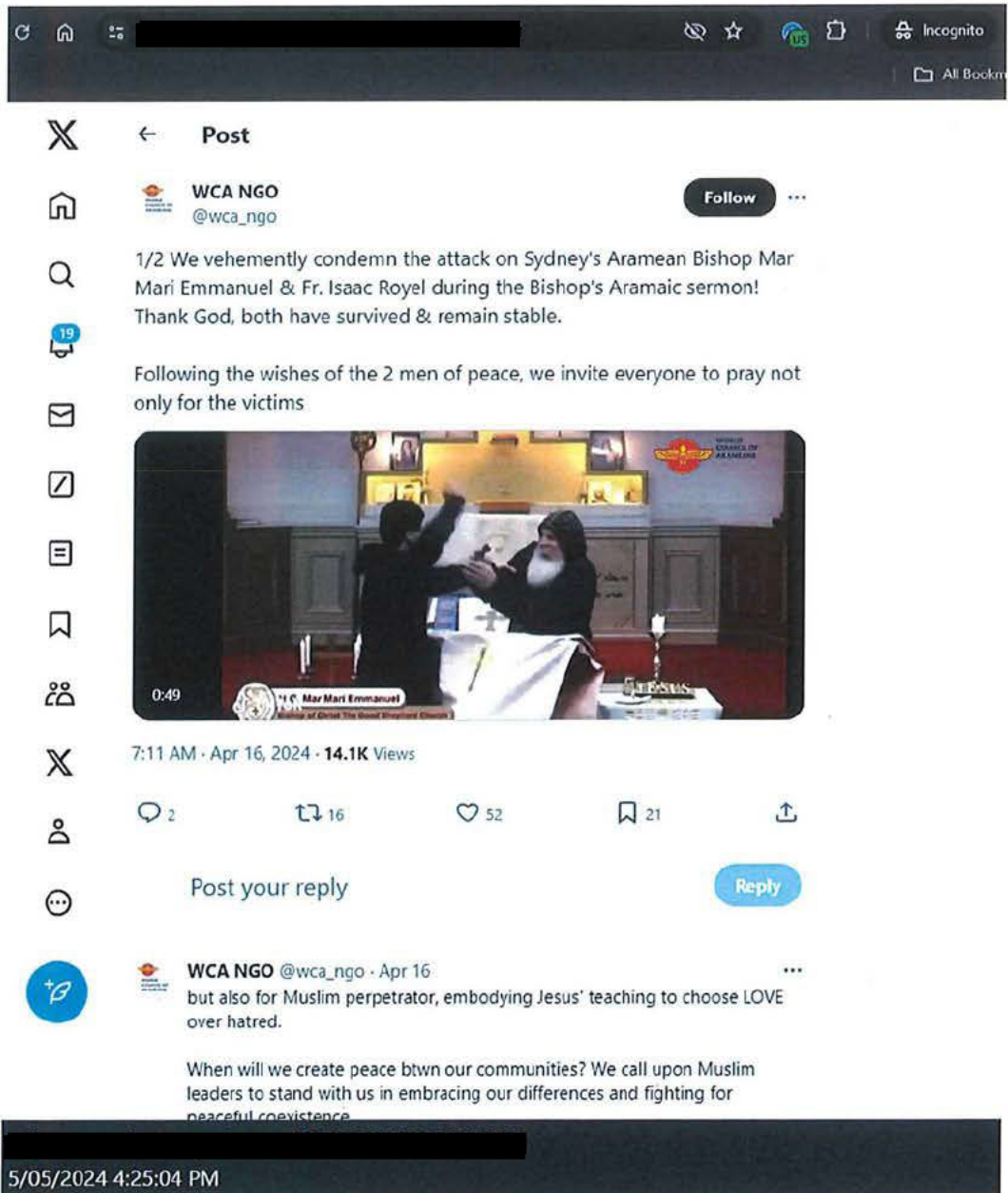


Image 13 of Annexure TAD-40



← Post



Americas Tribune 
@AmericasTribune

Follow ...

MUSLIM ATTACKS CHRISTIAN PREACHER!

#Christians around the world are outraged by 15 year old Muslim who #attacked popular #Christian teacher #Bishop Mar Mari Emmanuel as he was speaking at his #church in #Sydney #Australia. God was on the side of the Bishop, as the knife "malfunctioned" in the hand of #Muslim attacker. #God was protecting him.



6:57 AM · Apr 16, 2024 · 1,408 Views

5/05/2024 4:27:00 PM

Image 14 of Annexure TAD-40

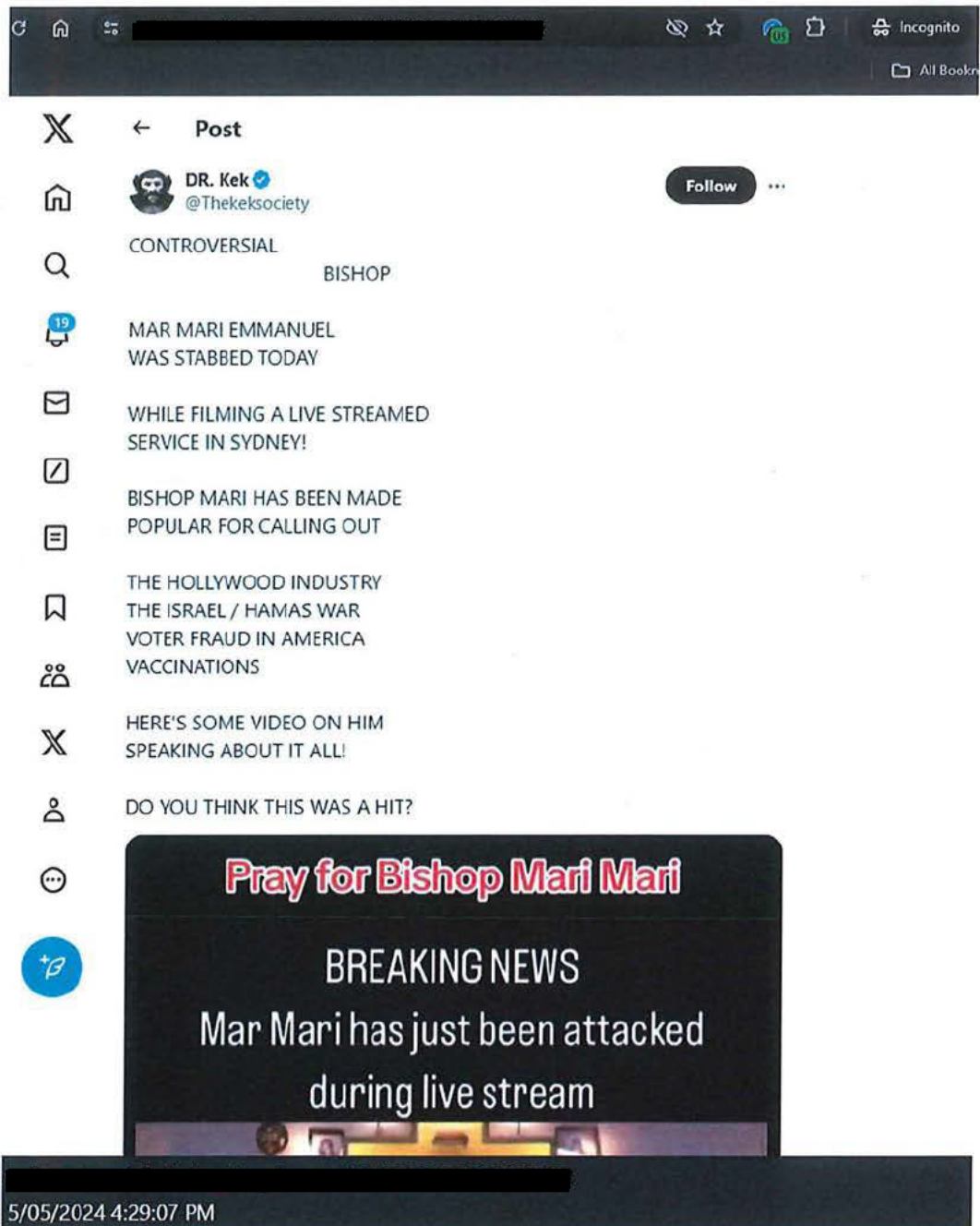


Image 15 of Annexure TAD-40

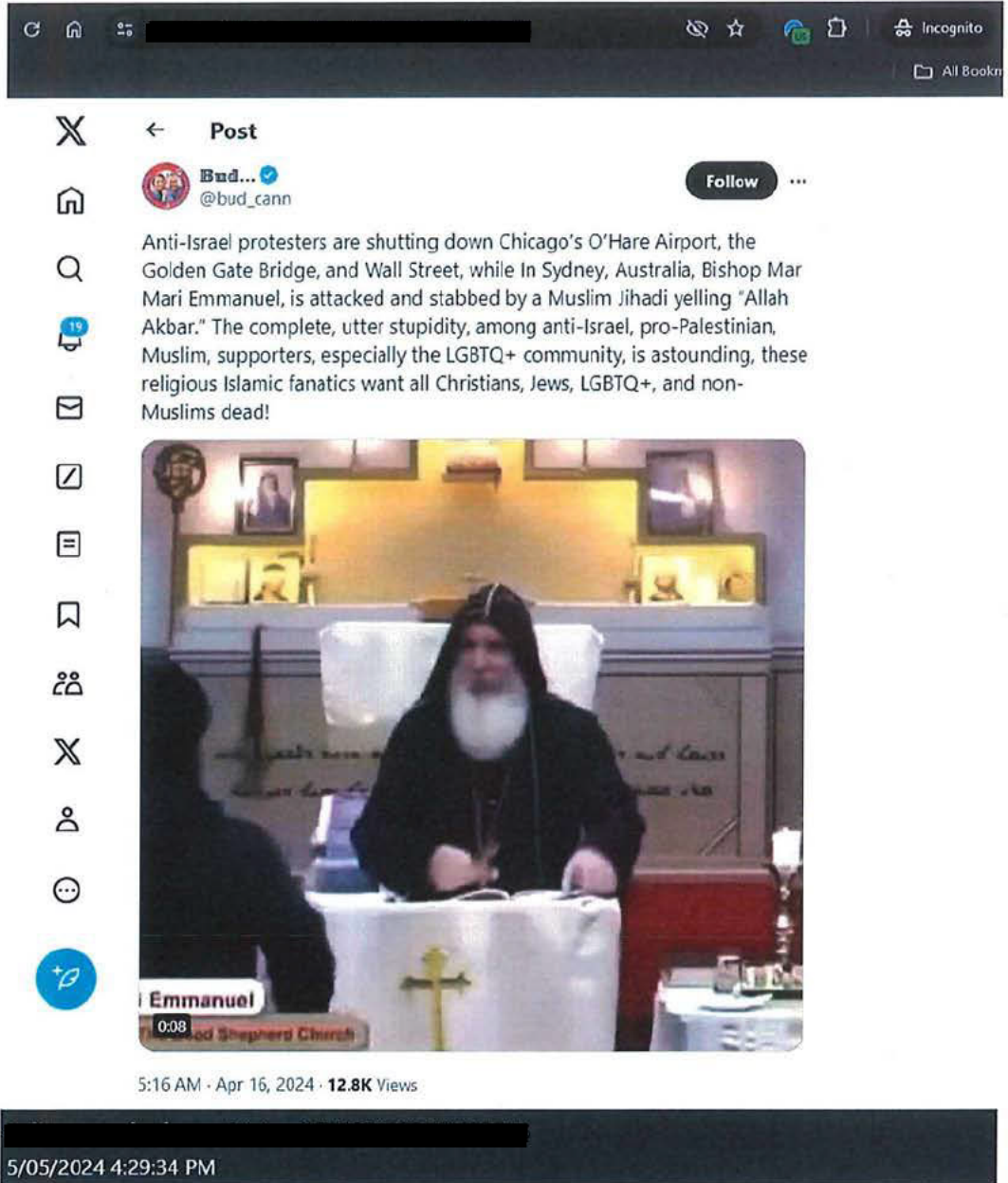


Image 16 of Annexure TAD-40

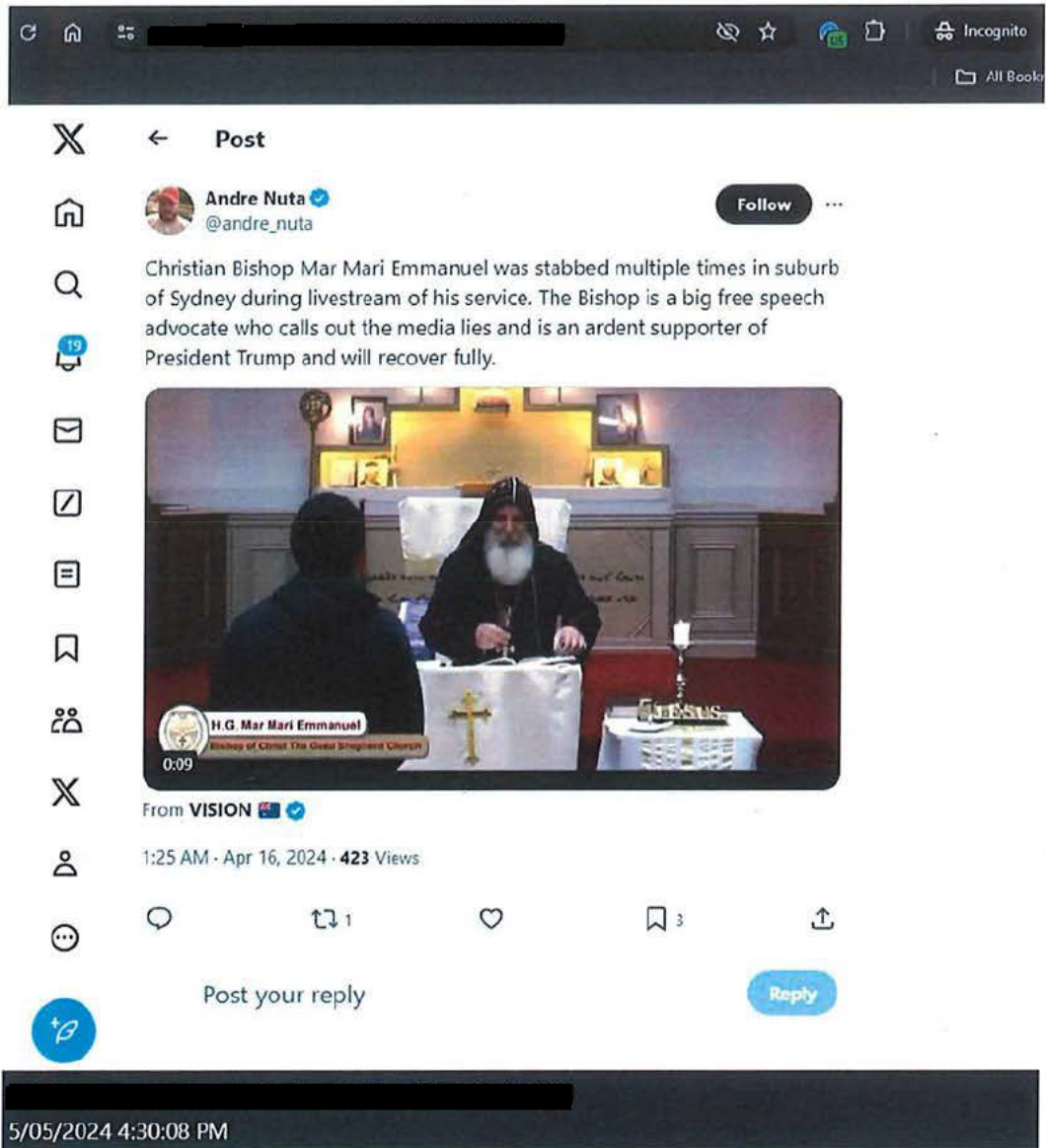


Image 17 of Annexure TAD-40

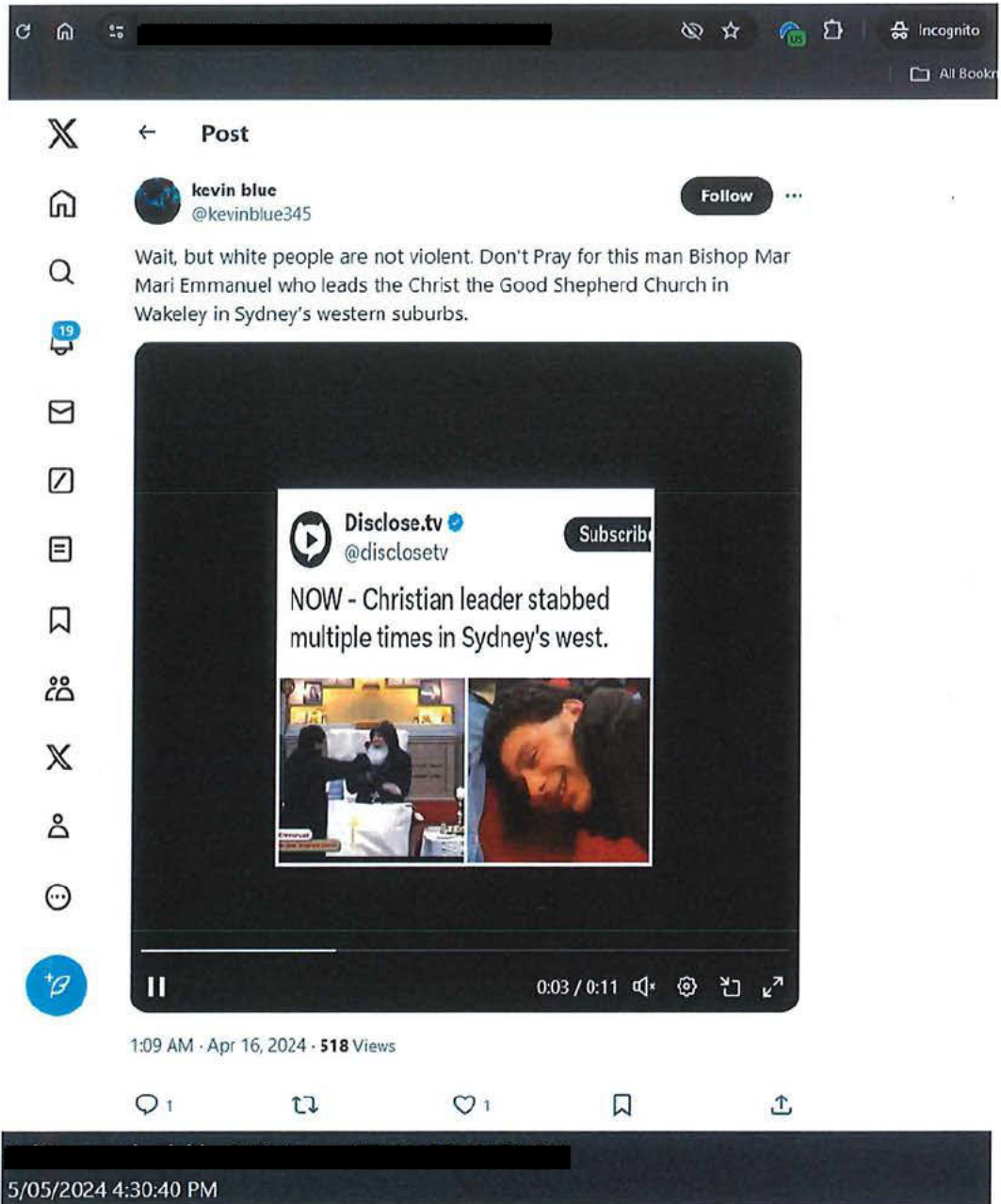


Image 18 of Annexure TAD-40

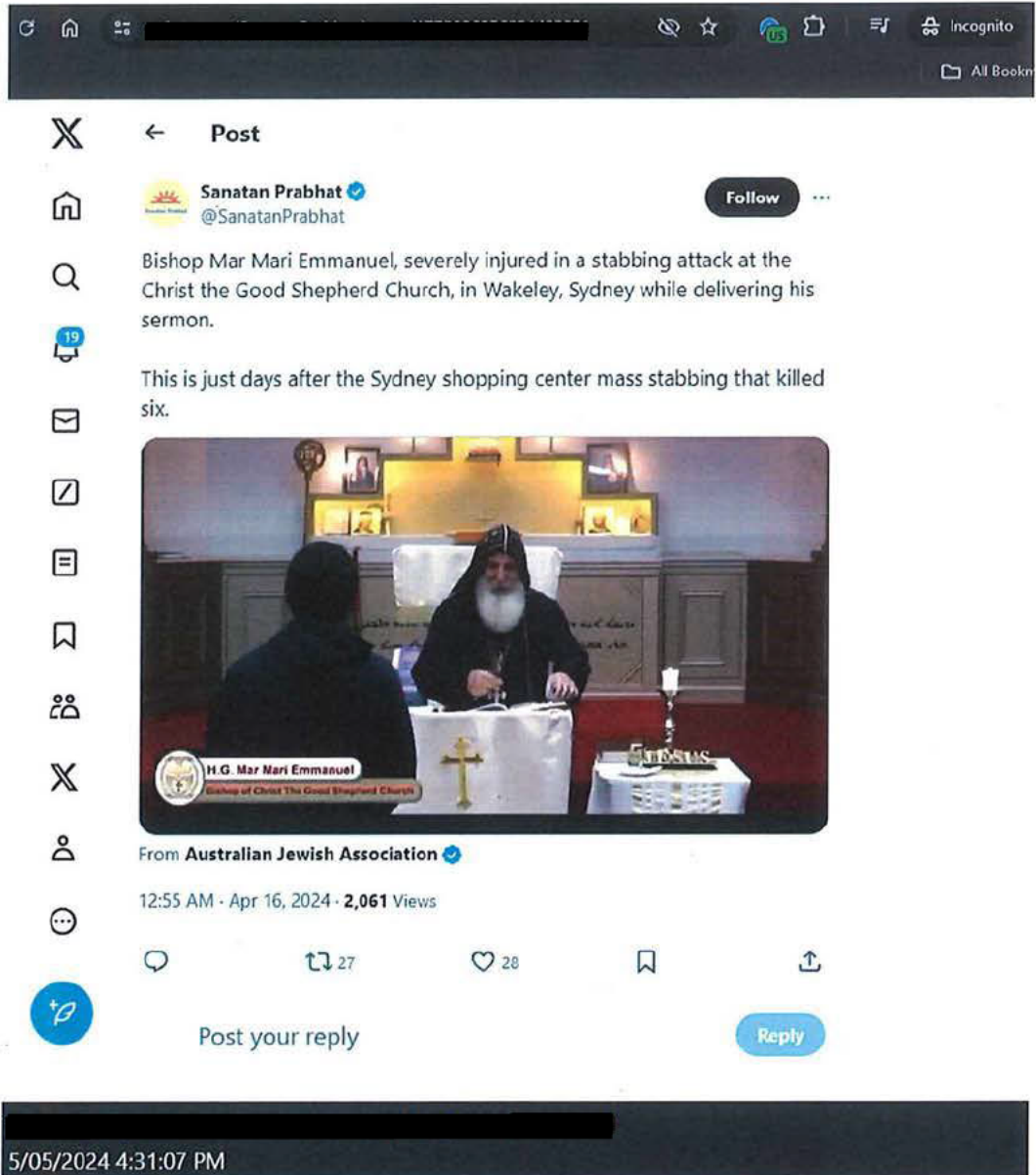


Image 19 of Annexure TAD-40

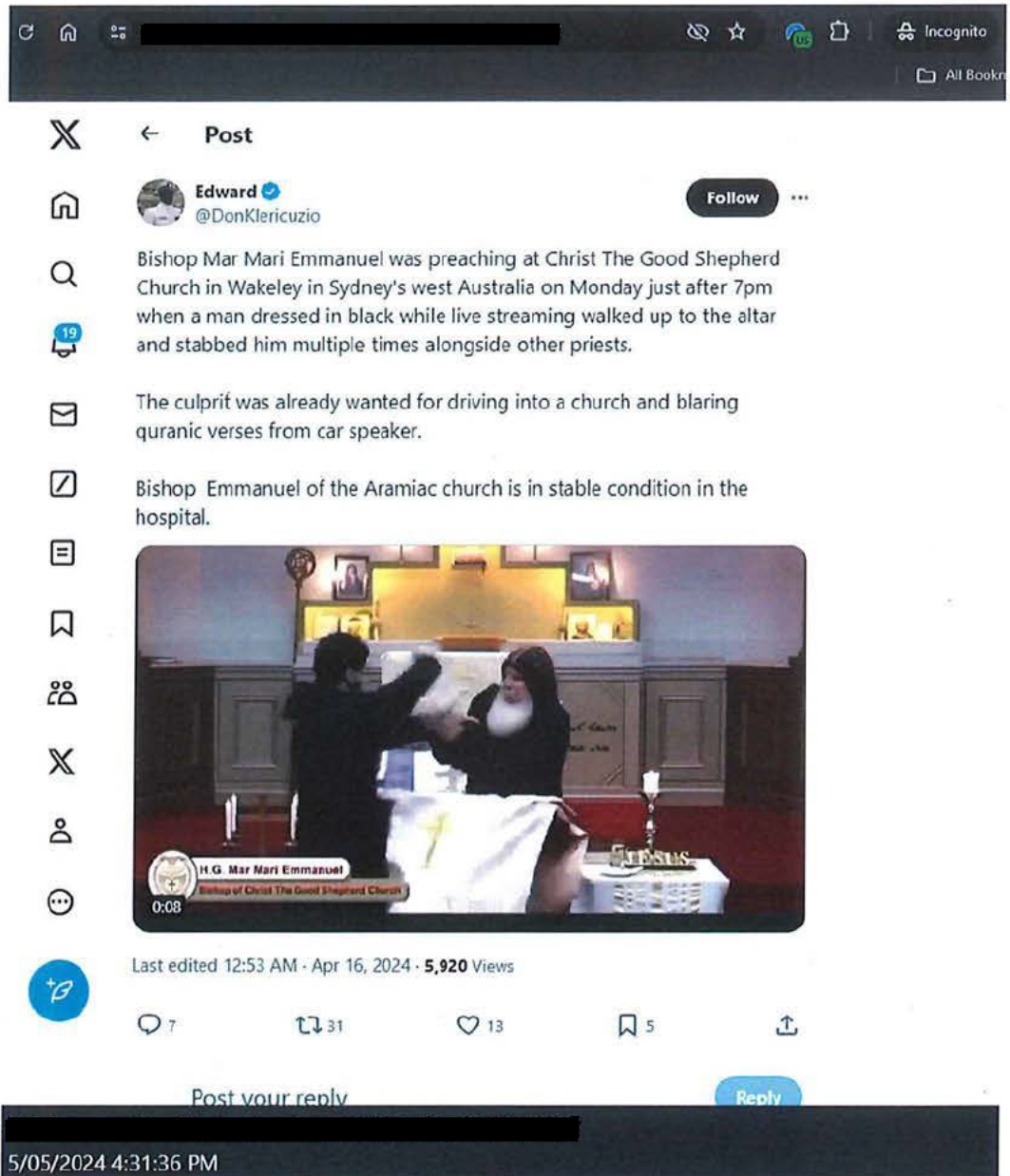


Image 20 of Annexure TAD-40

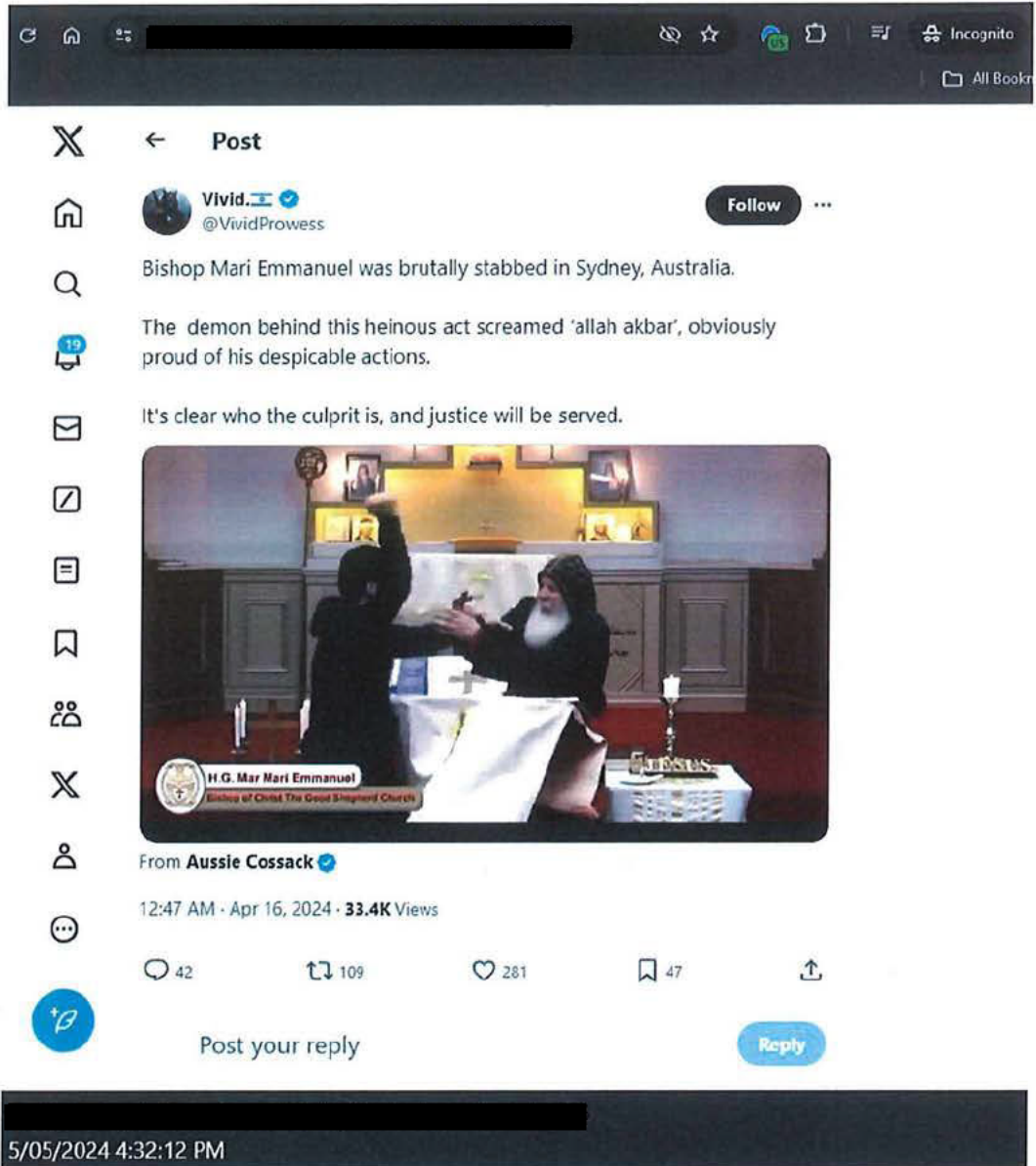


Image 21 of Annexure TAD-40

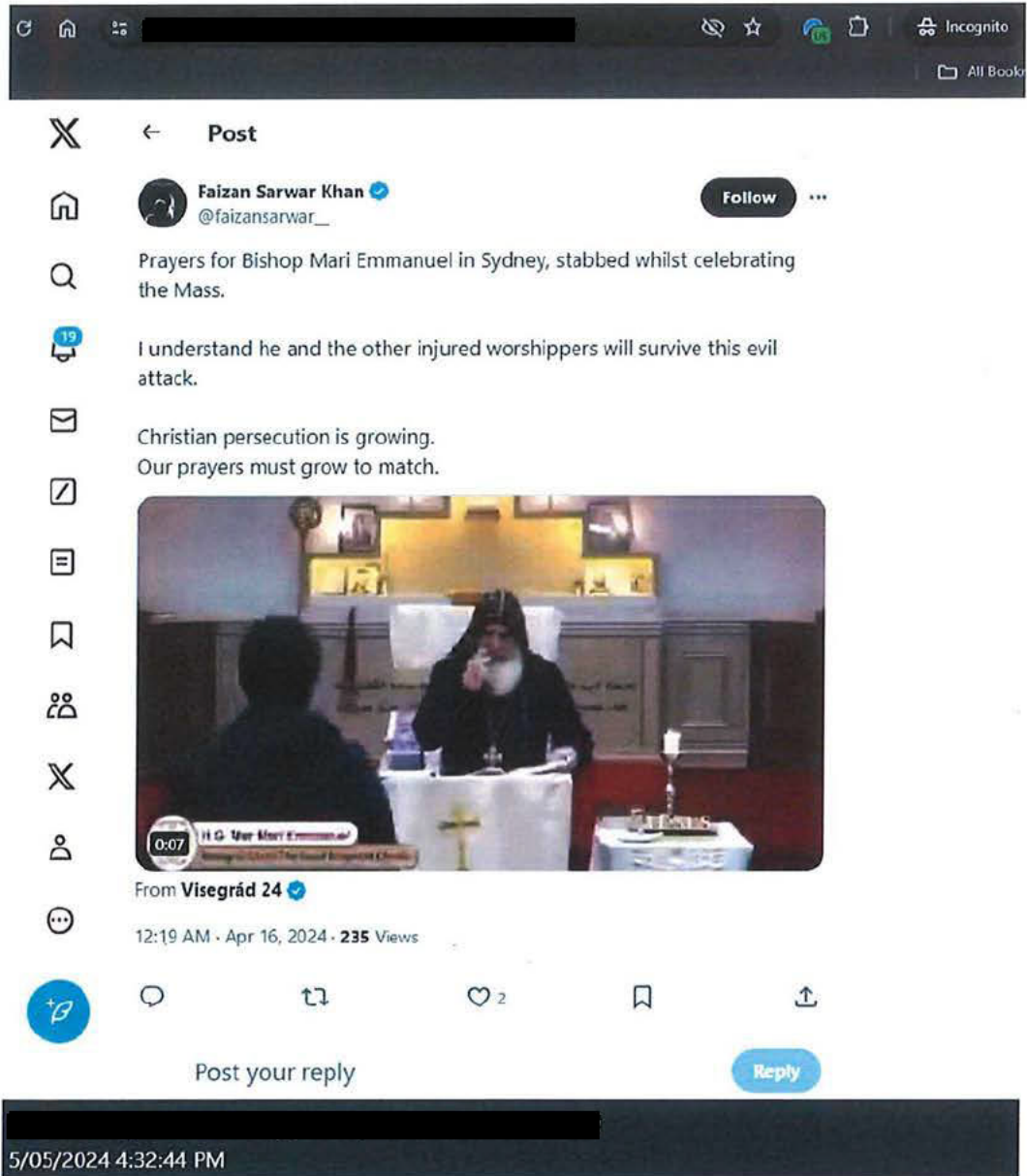


Image 22 of Annexure TAD-40

Incognito

All Bookmarks

Post


M.A. Rashid @Kashmiri_92

Follow

Bishop Mar Mari Emmanuel & other worshippers were attacked with knives at the Good Shepherd Church in Wakeley in west Sydney. The Assyrian priest comes from Iraq.

It happened on Monday after 7.00 & the attacker had 2 accomplices.

The Bishop is not hurt.



From David Atherton

12:13 AM · Apr 16, 2024 · 516 Views

Post your reply

Reply

5/05/2024 4:33:08 PM

ANNEXURE TAD-41

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NSW
DIVISION: GENERAL

NO NSD 474 OF 2024


ESAFETY COMMISSIONER

Applicant

X CORP

Respondent

The following 6 pages is the annexure marked TAD-41 referred to in the affidavit of
Toby Allan Dagg made on 6 May 2024 before me:



.....
Signature



.....
Qualification

Filed on behalf of the Applicant, eSafety Commissioner
Prepared by: Matthew Garey
AGS lawyer within the meaning of s 55I of the *Judiciary Act 1903*

Address for Service:
The Australian Government Solicitor,
Level 10, 60 Martin Place, Sydney, NSW 2000
Matthew.Garey@ags.gov.au

File ref: 24003626

Telephone: 02 9581 7625
Lawyer's Email:
Matthew.Garey@ags.gov.au
Facsimile: 02 6169 3054

2024 VPN Trends, Statistics, and Consumer Opinions

As consumers become increasingly protective of their online data, VPNs have surged in popularity, and 10 million more people may adopt VPNs this year.

All of our content is written by humans, not robots. [Learn More \(/editorial-guidelines/#written-by-humans\)](#)

By [Brett Cruz](https://www.security.org/author/brett-cruz/) (<https://www.security.org/author/brett-cruz/>) on Jan 23, 2024

In a world defined by cybercrimes and intrusive data practices, Americans are increasingly drawn to the security and privacy of [VPNs](/vpn/) (</vpn/>).

The American virtual private network (VPN) market has expanded rapidly in recent years, shifting from a niche tool used [primarily by businesses](/vpn/best/business/) (</vpn/best/business/>), enthusiasts, and power users to a household product that nearly all Americans are at least familiar with.

For the [last four years](/resources/vpn-consumer-report-annual/2023/) (</resources/vpn-consumer-report-annual/2023/>), the research team at Security.org has conducted a broad study of nearly 1,000 Americans to learn how VPN awareness, preferences, and perception are changing. Our latest annual VPN market report reflects continued growth in the general public's understanding and use of the technology, with adoption today driven by personal use as corporate networks rely less on the technology.

Here are a few key insights from this year's report:

- VPNs have continued to grow in use and recognition: 95% of adults are now familiar with the technology, and 46% use VPNs. This means as many as 105 million Americans have VPNs today.
- The most popular VPNs were [NordVPN](/vpn/nordvpn/) (</vpn/nordvpn/>), [Proton VPN](/vpn/protonvpn/) (</vpn/protonvpn/>), and Google One VPN, which has surged in popularity since Google began offering it free with cloud storage subscriptions and Pixel 7 phones last year.
- About half of all users rely on VPNs for work or business applications, and an equal number use them on personal devices.
- Nearly 40% of users rely on VPNs to prevent tracking from search engines or social media sites. As many as 10 million American adults could begin using VPNs in 2024, underscoring the growing recognition of the significance of online privacy.
- Despite the risks, about 43% of users have free VPNs, which can jeopardize data security.

Table of Contents

- [Privacy, Security, and Streaming: Personal Users Drive VPN Market Growth](#)
- [Most Popular VPNs in 2024](#)
- [Perceptions of Cost and Convenience Limit VPN Adoption](#)
- [2024 Outlook: Market Primed for Growth as Consumers Prioritize Privacy](#)
- [Our Data](#)

Privacy, Security, and Streaming: Personal Users Drive VPN Market Growth

IP-based VPNs have been around since the 1990s (<https://nordvpn.com/blog/history-of-vpn/>). Companies needed a way to access their internal network from outside the office without risking the exposure of their files on the broader internet. Today, VPNs are very frequently used by individuals on their personal devices. The rapid growth we noticed in VPN use, as seen in our study and analysis of thousands of consumer insights, is due primarily to a more informed consumer market in recent years.

Ninety-five percent of American adults are now familiar with VPNs, and most correctly defined them as software services that allow users to establish a secure and encrypted connection over the internet to ensure data privacy and security. In 2020, only 72 percent of respondents had this familiarity, an impressive jump in public awareness in just three years.

That greater awareness has translated to greater adoption. Today, 46 percent of people in our study, which could represent over 100 million American adults, now use a VPN. This is a significant jump from 39 percent of respondents just last year.

VPN providers have expanded their offerings to cater to this growing market of knowledgeable personal users. They've increased security and user anonymity with features like antimalware services built into VPNs. Some providers have rolled out multi-hop, which routes traffic through [multiple VPN tunnels \(/vpn/split-tunneling/\)](/vpn/split-tunneling/). Killswitch, a standard option on most VPNs, cuts the internet connection if the VPN connection is lost.

To improve the surfing experience, features like "stealth mode" can now hide the fact that a VPN is being used at all, enabling a smoother experience on sites that don't like them. Built-in ad-blockers reduce both tracking and intrusive ads.

Top reasons for VPN use, by year	2021	2022	2023
For general privacy	54%	50%	63%
For general security	55%	55%	54%
Job requirement	38%	34%	39%
To prevent tracking by search engines or social media (e.g. Google, Facebook)	18%	17%	39%
To use public Wi-Fi more securely	34%	24%	36%

Top reasons for VPN use, by year	2021	2022	2023
To hide your internet activity from your ISP	23%	23%	35%
For access to international/non-local media content not available in your country	19%	22%	28%
For greater security when online shopping	24%	20%	25%
Torrenting	13%	12%	21%
For work in activism/journalism/whistle-blowing/research	3%	5%	4%

Personal users are drawn primarily to the privacy, security, and greater access VPNs provide.

There were a few key shifts in the primary motivations for using VPNs in the past year, with a new focus on enhanced privacy and anonymity. We observed a substantial increase in the number of users who rely on VPNs to avoid search engine or social media tracking year over year. Additionally, there was a significant uptick in users depending on VPNs to conceal their online activities from their internet service provider (ISP) compared to the previous year.

Accessing non-local media, such as region-specific streaming content or content banned within a country, is another popular reason many turn to VPNs. There was also a substantial increase in respondents saying they use the technology to torrent or download (generally) pirated media.

Most Popular VPNs in 2024

VPN preferences don't just vary by age: knowledgeable and casual users have very different approaches to their choice of VPN. More familiar users are likelier to elect paid services from companies emphasizing privacy and security, such as Nord and Proton. The third most popular service, VPN by Google One, attracted a significantly higher percentage of low-familiarity users.

What VPN do you use?	Percent of users
NordVPN	27%
Proton VPN	13%
Google One VPN	9%
ExpressVPN	8%
Private Internet Access	7%
Brave VPN	7%
Norton Secure VPN	6%
Mozilla VPN	5%
Surfshark	5%
CyberGhost	4%

What VPN do you use?	Percent of users
Mullvad VPN	4%
Windscribe	3%
IPVanish	3%
Atlas VPN	3%
Other VPNs	21%

Far and away the most popular VPN among personal users in our study was NordVPN. NordVPN delivers privacy through features such as an automatic kill switch and Double VPN, which doubles the VPN encryption for extra privacy. NordVPN has also kept its promise not to keep IP addresses and VPN usage logs, which could improve trust among its users.

Proton VPN was also popular among users in our study. Though many use it for personal reasons, the service is excellent for business applications. It topped our ranking in upload speed, which is essential for remote workers.

43 percent of users pay nothing for their VPNs

Generally, using a VPN costs between \$5 to \$10 a month. About half of all VPN users in our study paid this amount for their services. Since our last analysis, the use of free VPNs has mostly stayed the same. This year, just over 43 percent of personal VPN users relied on free software.

How much does your VPN cost per month?	Percentage of personal VPN users
\$0; I use a free VPN	43%
Less than \$5 per month	25%
\$5 – \$10 per month	24%
More than \$10 per month	8%

We don't typically recommend free VPN services, as they may limit devices, data, servers, or log-on time. These free services may also harvest personal data in exchange for service or adversely affect your online experience. Remember: when the service is free, you are often the product.

Around 62 percent of free VPN users have had issues with their service. Slow internet speed was the most common problem, which can happen since some VPN providers have limited servers, leading to overcrowding and reduced performance. Bandwidth limitations, ad-supported models consuming extra resources, lower-quality infrastructure, and P2P restrictions can all contribute to slower connections.

You indicated that you use a free VPN. When using your free VPN, have you experienced any of the following? Select all that apply.	Percentage of free VPN users
Slow internet speed	36%
Difficulty using streaming services	19%
Difficulty accessing websites	19%
Limited server locations	19%
Frequent disconnections or interruptions	12%
Bugs (software issues)	8%

You indicated that you use a free VPN. When using your free VPN, have you experienced any of the following? Select all that apply.

	Percentage of free VPN users
Viruses or malware attempts	6%
Invasive advertisements	4%
Battery life problems	4%
Identity theft or privacy concerns	3%
Poor customer support	3%
No issues	38%

While slow internet speeds are inconvenient, other more sinister issues can arise with free VPN use. Six percent of users reported viruses or malware attempts. Free VPNs can introduce viruses or malware through malicious software bundling, where additional unwanted programs or harmful elements are included with the VPN software. Additionally, since some rely on ads for revenue, free VPNs can expose users to potentially malicious ads containing malware or phishing links.

Perceptions of Cost and Convenience Limit VPN Adoption

Today, about 54 percent of adults in our study did not use VPNs. Given their utility, we wanted to understand why. The main reason people don't use VPNs is that many people feel they don't need them. Cost emerged as the second-most common deterrent, as VPNs were deemed too expensive by 27 percent of holdouts.

Why don't you use a VPN? Select ALL that apply.	Percentage of non-users
I don't need one	52%
Too expensive	27%
Too much trouble to set up	20%
I don't see the benefit	13%
I don't trust their privacy	9%
I don't trust their security	8%
Sites block them	5%
I don't know enough about them	4%
Other reasons	5%

Additionally, 20 percent found VPNs to be too complex to set up. For people who are not very tech-savvy, choosing, installing, and connecting to VPNs on their devices could seem intimidating. A smaller percentage, approximately 10 percent, harbored concerns about the privacy and security of VPNs.

2024 Outlook: Market Primed for Growth as Consumers Prioritize Privacy

In the current landscape, where approximately five percent of individuals not currently using a VPN are contemplating adoption within the next year, the continued importance of VPNs is evident. As many as 10 million American adults could enter the market in 2024, underscoring the growing recognition of the significance of online privacy. In an era where data

breaches and privacy concerns are rising, VPNs offer a crucial layer of protection.

The sustained relevance of VPNs is due to their low cost, tangible benefits to privacy and security, and ease of setup, which providers should continue to emphasize to win over new customers. As awareness reaches a saturation point and the desire for online privacy remains high, VPNs are poised to play an integral role in safeguarding digital identities and ensuring secure internet experiences for a broader user base.

Our Data

In December 2023, researchers at Security.org conducted their fourth annual study on VPN usage. 998 adults residing in the U.S. participated in the study, and were representative of the U.S. population based on ethnicity, age, and gender. The online platform used to gather data for this study doesn't allow users to access it using a VPN, which may have resulted in underreporting the number of people using VPNs.

	Company	Research	
(https://www.security.org/)	About Us (/about-us/)	Our Research (/resources/)	(https://www.youtube.com/watch?v=Sem)
Privacy Policy (/privacy-policy/)	Contact Us (/contact-us/)	Deals & Promotions (/deals/)	
Terms & Conditions (/terms-and-conditions/)	Careers (/careers/)	Password Strength Checker (/how-secure-is-my-password/)	
Accessibility (/accessibility/)		Password Generator (/password-generator/)	
Do Not Sell/Share My Personal Information (https://compliance.security.org/doNotSell.php?ReferenceURL=security.org)		What's My Security Score? (/security-score/)	
Limit the Use of My Sensitive Personal Information (https://compliance.security.org/doNotSell.php?ReferenceURL=security.org)			
© Copyright 1995 - 2024 Security.org a Centerfield Media Company			

ANNEXURE TAD-42

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NSW
DIVISION: GENERAL

NO NSD 474 OF 2024

ESAFETY COMMISSIONER

Applicant

X CORP

Respondent

The following 27 pages is the annexure marked TAD-42 referred to in the affidavit of
Toby Allan Dagg made on 6 May 2024 before me:



.....
Signature



.....
Qualification

Filed on behalf of the Applicant, eSafety Commissioner
Prepared by: Matthew Garey
AGS lawyer within the meaning of s 55I of the *Judiciary Act 1903*

Address for Service:
The Australian Government Solicitor,
Level 10, 60 Martin Place, Sydney, NSW 2000
Matthew.Garey@ags.gov.au

File ref: 24003626

Telephone: 02 9581 7625
Lawyer's Email:
Matthew.Garey@ags.gov.au
Facsimile: 02 6169 3054

by Use
by OS/Device
by Country
Guides
Compare providers
Reviews

got the biggest VPN market share?

re a commission when you buy using links on our site.

VPN Market Report 2024: Who's got the biggest market share?

REBECCA MOODY - HEAD OF DATA RESEARCH

Updated: February 9, 2021



comparitech

VPN research done properly

Who's got the biggest VPN market share?



Digital privacy is becoming a mainstream issue, and many governments around the world censor the web. For those who want open access to the web without being tracked by corporations and authorities, VPNs offer a way to enjoy internet freedom and privacy.

But which is the most popular [VPN](#)?

Which VPN has the greatest market share?

To find out, we looked at a number of factors, including how much each VPN has been searched for in Google, how "trendy" each VPN is, how big a social following each VPN has, how many website visits they're

Latest guides

[How to Uninstall Intego VirusBarrier – Step-by-Step Guide for your Mac](#)

April 30, 2024 / by Craig McCart

[How to Uninstall Comodo on PC and Mac](#)

April 30, 2024 / by Craig McCart

[How to Uninstall Sophos on PC and Mac](#)

April 30, 2024 / by Craig McCart

[How to Uninstall Emsisoft on PC and Mac – Removal Guide](#)

April 27, 2024 / by Craig McCart

[How to Uninstall Panda on PC and Mac – Trouble-Free](#)

getting, and how many downloads and reviews they're getting on the App Store and Google Play.

Alternatively, if you'd like to know which VPNs are top of the list based on merit (rather than popularity), view our guide on the [best VPN services here](#).

Which VPN has had the highest number of searches?

First, we'll take a look at the monthly search volumes for the main keywords of each VPN provider. For example, NordVPN is "nordvpn" and "nord vpn," ExpressVPN is "expressvpn" and "express vpn," Hotspot Shield is "hotspot shield" and "hotspot shield vpn," and so on.

The provider that receives the highest search volume will win this category as it suggests more people are searching for this VPN online.

Here are the top 20:

of Monthly Global Web Searches

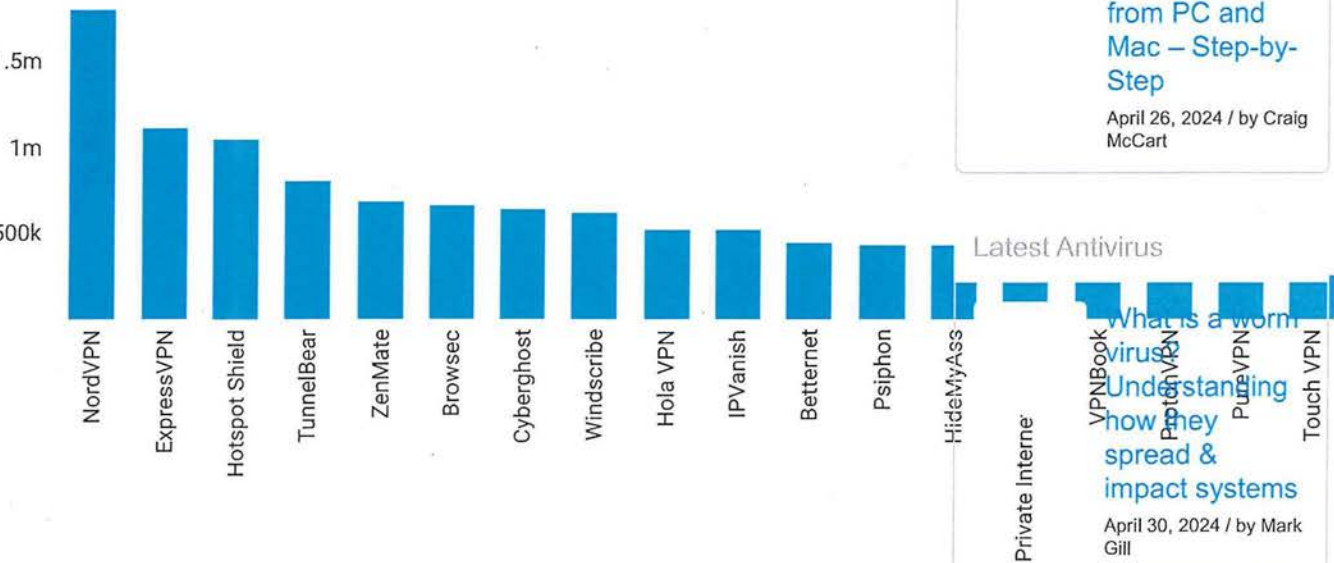


Chart: Comparitech • Source: Ahrefs • Get the data • Created with Datawrapper

Removal Process

April 27, 2024 / by Craig McCart

How to Uninstall ESET on PC and Mac

April 27, 2024 / by Craig McCart

How to Uninstall PC Matic on PC and Mac – Comprehensive Guide

April 26, 2024 / by Craig McCart

How to Uninstall HitmanPro – Complete Removal Instructions

April 26, 2024 / by Craig McCart

How to Uninstall Avira – Step-by-Step Guide for Windows & Mac

April 26, 2024 / by Craig McCart

How to Uninstall AVG from PC and Mac – Step-by-Step

April 26, 2024 / by Craig McCart

How to Uninstall AVG from PC and Mac – Step-by-Step

April 30, 2024 / by Mark Gill

How to uninstall VIPRE – A step-by-step guide

So, the monthly search term winner is...

NordVPN.

With almost 1.8 million searches per month, NordVPN is the most-searched VPN on Google. ExpressVPN comes second with 1.1 million, closely followed by Hotspot Shield with 1.04 million.

Which VPN is trending?

The above shows us how popular each VPN service is at this moment in time. But things can soon change, which is why we examined which VPN providers have been trending over a longer period of time.

April 30, 2024 / by Craig McCart

[How to protect yourself from email threatware – Prevention strategies](#)

April 26, 2024 / by Mark Gill

[Malware, Ransomware, Spyware: What's the difference and why you should care](#)

April 12, 2024 / by Mark Gill

[Best Antivirus for Linux in 2024](#)

March 18, 2024 / by Craig McCart

Out of the top 20 VPNs we've analyzed, the 5 with the most interest over the last year (from January to December 2019) are [NordVPN](#), [ExpressVPN](#), Hotspot Shield, Turbo VPN, and [Psiphon](#).

We can see that NordVPN has, on average, been the most popular. The number of searches increases from August with a particular peak in October (which coincides with [NordVPN's news of a data center breach](#)).

[Hotspot Shield](#) also enjoyed peaks in April, May, and June.

Latest App Studies

[1 in 4 Apple App Store kids' apps breach Children's Online Privacy Protection Act \(COPPA\) rules](#)

June 21, 2023 / by Rebecca Moody

[Nearly 1 in 4 children's Google Play Apps breach the ICO's age-appropriate design code](#)

February 17, 2023 / by Rebecca Moody

[7 Best App Store Optimization Platforms](#)

July 14, 2022 / by Amakiri Welekwe

[Over 1 in 4 children's Google Play](#)

However, the largest peak is perhaps most surprising as it belongs to Turbo VPN. Turbo VPN ranked 19th in our monthly search list but moved up to fifth in 2019's trending list. The peak itself occurred in May 2019 and far exceeds any of the others. Unlike NordVPN's peak, which can be attributed to its news-related data breach, nothing seems to stand out for Turbo VPN. Therefore, the peak is likely due to an increase in demand, i.e. because of a good review, increased advertising, etc.

So, the most trendy VPN is...

NordVPN. And this is despite the peaks caused by the data breach. Even though more people searched for NordVPN at the time of the announcement, it doesn't distort the overall figures or trend.

Which VPN provider has the biggest social following?

How big a social following VPN providers have on Facebook and Twitter is a great way to see how popular they are. How many people are wanting to interact and hear more about our top 20 VPNs?

VPN	Facebook	Twitter	Total
Hotspot Shield	4,138,763	95,059	4,233,822
Private Internet Access	1,023,163	148,338	1,171,501
TunnelBear	75,509	200,164	275,673
NordVPN	114,963	45,317	160,280
Turbo VPN	131,716	44	131,760
Psiphon	93,893	17,733	111,626
PureVPN	101,335	1,248	102,583
ExpressVPN	54,196	27,084	81,280

[Apps breach Children's Online Privacy Protection Act \(COPPA\) rules](#)

June 22, 2021 / by Paul Bischoff

[Stalkerware app use by country](#)

June 1, 2021 / by Paul Bischoff

Latest Cloud and Online Backup

[Best free backup apps for Android in 2024: Effortless data backup](#)

October 21, 2021 / by Ray Walsh

[The Best Secure File Sharing Tools & Software for Business in 2024](#)

October 21, 2019 / by Tim Keary

[Rapidshare is discontinued, try these alternatives](#)

February 4, 2019 / by Aimee O'Driscoll

[The Best Edge Services Providers](#)

October 15, 2018 / by Stephen Cooper

[The best apps to encrypt your files before uploading to the cloud](#)

October 11, 2018 / by Paul Bischoff

Latest Crypto

VPN	Facebook	Twitter	Total
ZenMate	66,156	7,898	74,054
HideMyAss	56,111	16,461	72,572
ProtonVPN	10,325	49,851	60,176
CyberGhost	41,298	13,948	55,246
Windscribe	5,250	48,120	53,370
VPNBook	31,327	14,672	45,999
IPVanish	29,815	13,314	43,129
Hola VPN	26,801	4,233	31,034
VyprVPN	13,729	10,624	24,353
Betternet	N/A	10,337	10,337
Browsec	4,898	N/A	4,898
Touch VPN	853	259	1,112

[Worldwide crypto & NFT rug pulls and scams tracker](#)

August 3, 2022 / by Rebecca Moody

[What bitcoin is and how to buy it and use it](#)

October 14, 2021 / by Mark Gill

[Bitcoin and Crypto Hacking: Fraud, theft, and security statistics](#)

May 6, 2021 / by Aimee O'Driscoll

[Bitcoin Price History – the value of 1 BTC over time](#)

April 19, 2021 / by Rebecca Moody

[How Do People Feel About Cryptocurrencies?](#)

July 31, 2019 / by Paul Bischoff

With an overall social audience of 4.2 million, the hands-down winner of this category is...

Hotspot Shield, which has a huge social following on Facebook with 4.1 million likes.

In second place is [Private Internet Access](#) thanks to its large Facebook following of 1 million people. And we should also mention [Tunnelbear's](#) impressive Twitter following of more than 200,000 followers.

Which VPN provider gets the most visitors to its website?

Using SimilarWeb, we compared the number of website visits for each provider over the last six months of 2019.

Latest Crypto Popular Posts

[How to buy and pay with bitcoin anonymously](#)

April 18, 2018 / by Aimee O'Driscoll

[What is Bitcoin mining and how can you do it?](#)

March 7, 2018 / by Aimee O'Driscoll

[15 best bitcoin wallets for 2024 \(that are safe and easy to use\)](#)

February 25, 2018 / by Aimee O'Driscoll

VPN	Total Visits (July 2019)	Total Visits (August 2019)	Total Visits (September 2019)	Total Visits (October 2019)
ExpressVPN	24,500,000	24,600,000	24,500,000	30,500,000
NordVPN	11,600,000	12,100,000	11,900,000	10,900,000
Hola VPN	3,450,000	3,600,000	3,450,000	3,500,000
HideMyAss	2,700,000	2,750,000	2,800,000	3,150,000
Windscribe	2,800,000	290,000	2,650,000	3,150,000
IPVanish	2,850,000	3,150,000	2,500,000	2,450,000
CyberGhost	2,350,000	2,350,000	2,200,000	2,250,000
ProtonVPN	2,000,000	2,250,000	2,150,000	2,150,000
TunnelBear	2,100,000	2,300,000	2,050,000	1,950,000
Hotspot Shield	2,000,000	1,950,000	1,800,000	1,950,000
Private Internet Access	1,800,000	1,800,000	1,700,000	1,750,000
PureVPN	1,450,000	1,350,000	1,400,000	1,700,000
Touch VPN	1,450,000	1,550,000	1,550,000	1,800,000
ZenMate	1,550,000	1,150,000	950,000	1,150,000
VPNBook	1,350,000	1,250,000	1,100,000	1,350,000
Betternet	1,000,000	940,000	1,000,000	1,200,000
VyprVPN	860,000	750,000	740,000	730,000
Browsec	1,050,000	400,000	350,000	360,000
Psiphon	490,000	460,000	470,000	410,000
Turbo VPN	180,000	260,000	200,000	140,000



Enjoying 172.7 million visitors in the past 6 months, the winner is...

Latest Cryptocurrency Studies

[Does the price of Bitcoin impact ransomware attacks and ransoms?](#)

October 17, 2022 / by Rebecca Moody

[Worldwide NFT heists tracker](#)

July 26, 2022 / by Rebecca Moody

[Worldwide cryptocurrency heists tracker \(updated daily\)](#)

June 28, 2019 / by Theo Tsihitas

Latest Cybercrime Studies

[The average UK government employee receives 2,246 malicious emails per year](#)

April 20, 2022 / by Paul Bischoff

[Cybercrime victims lose an estimated \\$714 billion annually](#)

August 11, 2021 / by Paul Bischoff

[Cybersecurity rankings by country: Which countries have the worst \(and best\) cybersecurity?](#)

February 6, 2019 / by Paul Bischoff

Latest Cybersecurity Employment Studies

[2022 US Cybersecurity](#)

140

ExpressVPN. With nearly 87 percent more visitors than second-place NordVPN, ExpressVPN's visitor numbers far exceed any of the other VPN providers. And as we can see, there was some increase toward the end of the year, especially in December when visitor numbers increased by 31 percent on the previous month.

Which VPN provider has had the most downloads?

Unfortunately, Apple doesn't reveal the number of downloads an app has had in its store so only approximate estimates are available. However, we can see how many reviews each app has received and the overall rating it has been given. Likewise, we can get a rough idea of the number of downloads in Google Play and the rating for the Android apps.

VPN	# of Google Play Downloads	# of Google Play Reviews	Google Play Rating	Apple Store Reviews	Apple Store Rating
NordVPN	10 million +	191,490	4.5	21,000	4.5
Hotspot Shield	100 million +	1,410,800	4.1	6,900	4.2
TunnelBear	10 million +	208,780	4.4	13,000	4.4
Browsec	1 million +	33,466	4.5	489	4.6
ZenMate	1 million +	67,682	3.8	133	3.3
ExpressVPN	10 million +	117,719	4.1	17,000	4.5
Windscribe	1 million +	16,583	4.4	792	4.6
CyberGhost	10 million +	85,554	4.2	6,200	4.3
Hola VPN	50 million +	1,165,563	4.5	271	2.5
IPVanish	1 million +	7,917	4.1	7,000	4.2
Psiphon	50 million +	459,059	4.3	277	3.8

Salary & Employment Study – which state has the best prospects?

April 5, 2021 / by Paul Bischoff

2024 US Network Administrator Salary & Employment Study – How Much Does a Network Admin Make by State?

June 25, 2019 / by Rebecca Moody

Latest Data Breaches Studies

US manufacturing & utility businesses leaked nearly 88 million records in 302 data breaches in 2023

January 26, 2023 / by Paul Bischoff

Medical breaches accounted for 422.7 million leaked records from 5,478 data breaches

August 18, 2022 / by Paul Bischoff

Financial data breaches accounted for 232 million leaked records across 2,260 data breaches

July 21, 2022 / by Paul Bischoff

The rise of two-factor authentication: Key statistics

VPN	# of Google Play Downloads	# of Google Play Reviews	Google Play Rating	Apple Store Reviews	Apple Store Rating
Betternet	50 million +	1,054,562	4.3	16,000	4.4
HideMyAss	1 million +	29,240	4.5	2,700	4.4
VPNBook	10000+	330	4	N/A	N/A
Private Internet Access	1 million +	20,474	3.8	3,200	4.6
Touch VPN	10 million +	654,588	4.5	668	4.4
PureVPN	1 million +	24,825	3.4	202	3.5
ProtonVPN	100000+	1,116	4.1	122	3.9
Turbo VPN	100 million +	3,492,392	4.6	4,900	4.6
VyprVPN	1 million +	46,995	3.9	1,000	4.3

[from 2020 to 2024](#)

July 18, 2022 / by Craig McCart

[The State of Data Breaches in the US: Report and Statistics 2020](#)

August 17, 2021 / by Paul Bischoff

Latest Data Privacy Management

[The Best Sensitive Data Scanners](#)

November 30, 2023 / by Amakiri Welekwe

[The Best Audit Trail Tools](#)

November 29, 2023 / by Amakiri Welekwe

[The Best Phishing Awareness Training Tools](#)

November 29, 2023 / by Amakiri Welekwe

[The Best Ransomware Training Tools](#)

November 29, 2023 / by Amakiri Welekwe

[The Best Privacy Training Tools for Employees](#)

November 29, 2023 / by Amakiri Welekwe

Latest Data Recovery Software

[The Best Data Loss Prevention Software Tools](#)

April 18, 2019 / by Stephen Cooper

Based on **Google Play** figures, the app with the most downloads and the highest number of reviews on Google Play is Turbo VPN. With almost 3.5 million reviews and an overall rating of 4.6 stars *and* over 100 million downloads, Turbo VPN is by far the most popular VPN when it comes to Android devices.

Second-place Hotspot Shield has less than half the number of reviews and an overall rating of 4.1 but the same approximate number of downloads. This would suggest that even though a similar number of people have downloaded these two VPNs, Turbo VPN is more popular with users.

Hola VPN, Psiphon, and Betternet also enjoy a large number of downloads (over 50 million) and similar ratings (4.3 or 4.5 stars).

But if we look at the **Apple App Store's** ratings, there is quite a different picture.

NordVPN has the most ratings with 21,000 at 4.5 stars, followed by ExpressVPN with 17,000 at 4.5 stars and Betternet with 16,000 at 4.4 stars. Turbo VPN has less than half the reviews (4,900) but does enjoy an overall rating of 4.6 stars.

Overall, Turbo VPN would appear to be the most popular across the two platforms but NordVPN and ExpressVPN are clear favorites for Apple users.

Which VPNs dominate the market?

Within each of the above categories, we had some clear winners.

For monthly searches, NordVPN wins by a good margin. It was also the most "trendy" VPN according to Google Trends from throughout 2019. But when it came to social followings, NordVPN dropped in the rankings and was replaced with the likes of Hotspot Shield and Private Internet Access. It also lost out to ExpressVPN when it came to website visits.

Finally, NordVPN and ExpressVPN appear the most popular choice for Apple users, but Turbo VPN stormed ahead as the clear favorite for Android Users (and was another VPN with clear peaks in interest on Google Trends).

Overall, then, NordVPN and ExpressVPN continue to hold a large share of the market but they are sharing this with the likes of Turbo VPN and Hotspot Shield, which also have huge followings. Out of these four, Turbo VPN is the only free service.

Latest Identity Theft Protection

[Common Facebook Marketplace scams and how to avoid them](#)

June 27, 2023 / by Ray Walsh

[IDX Identity vs LifeLock: Full comparison for identity theft protection](#)

June 18, 2022 / by Kyle Schurman

[LifeLock vs Experian: Which is best?](#)

May 9, 2022 / by Kyle Schurman

[Complete ID vs LifeLock: Which identity protection service is right for you?](#)

May 9, 2022 / by Kyle Schurman

[Identity Guard vs LifeLock: Which is best?](#)

April 27, 2022 / by Kyle Schurman

Latest Information Security

[What are fake apps? How to identify and avoid fake apps](#)

April 5, 2024 / by Ray Walsh

[How secure is Signal?](#)

March 9, 2024 / by Marc Dahan

[Is Telegram safe and secure?](#)

Methodology

of monthly searches

We used Ahrefs to find the total monthly searches for each VPN, using the top 20 of these for the basis of our report. The figures are derived from Ahrefs' own database and are based on the number of times each keyword has been searched globally on Google.

Trends

We used Google Trends to see which of the VPNs were trending most on Google over the past year. We compared each of the top 20 against one another to find the top 5.

Google Trends works by taking the total number of searches for a keyword and how these change with geography and time. This gives you the "interest over time" graph which shows how keyword search volumes change within a certain period. We used the entire year of 2019 and worldwide searches.

Website Visits

SimilarWeb has a number of data sources and uses all of its aggregated data to create algorithms that offer estimated figures for things like the number of website visits.

Opera VPN and Avast VPN were omitted from the study due to their parent companies offering more than one service. Due to this, it wouldn't be fair to compare their website visits, social followings, etc. to companies only offering VPNs.

Roundup - best VPNs for

March 9, 2024 / by Marc Dahan

[How do I get my CompTIA Security+ certification?](#)

March 3, 2024 / by Mark Gill

[How difficult is the Security+ certification?](#)

March 2, 2024 / by Mark Gill

Latest Internet providers

[How to clear your cookies in Chrome, Firefox, Edge, Safari or Opera](#)

February 21, 2019 / by Chris Stobing

Latest Internet Studies

[What internet activity would you be willing to cut down on to save energy?](#)

November 8, 2021 / by Rebecca Moody

[The rising tide of child abuse content on social media](#)

February 19, 2021 / by Paul Bischoff










[Internet Censorship 2024: A Map of Internet Censorship and Restrictions](#)

January 15, 2020 / by Paul Bischoff

[Which government censors the tech giants the most?](#)

Our
Score

Our Verdict

1.  **NordVPN®**  4.5/5 Best VPN for changing Netflix region [Get NordVPN »](#)
2.  **Surfshark®**  4.5/5 Best budget option [Get Surfshark »](#)
3.  **ExpressVPN**  4.5/5 Highly versatile [Get ExpressVPN »](#)
4.  **CyberGhost**  4/5 Easy to use [Get CyberGhost »](#)
5. **IPVANISH VPN**  3/5 Unlimited devices [Get IPVanish »](#)

PRIVACY ALERT: Websites you visit can find out who you are

The following information is available to any site you visit:



Your IP Address:
155.190.54.35



Your Location:
Sydney, New South Wales, Australia



Your Internet Provider:
Cisco OpenDNS, LLC

Latest IPTV

[Is Facebook profiting from illegal streaming?](#)

June 11, 2019 / by Sam Cook

[How to set up IPTV on Perfect Player](#)

January 31, 2019 / by Tom Blackstone

[Kodi Solutions IPTV: Your gateway to low-cost global TV channels in 2024](#)

September 24, 2018 / by Tom Blackstone

[Area 51 IPTV: What is Area 51 IPTV and should you use it?](#)

September 23, 2018 / by Tom Blackstone

[Terrarium TV shut down: Use these top 10 Terrarium TV alternatives](#)

September 18, 2018 / by Sam Cook

Latest Kodi

[Kodi in steep decline after introduction of anti-piracy steps](#)

February 28, 2022 / by Sam Cook

[Can You Watch Tyson vs Jones on Kodi?](#)

August 13, 2020 / by Sam Cook

This information can be used to target ads and monitor your internet usage.

Using a VPN will hide these details and protect your privacy.

We recommend using [NordVPN - #1 of 72 VPNs](#) in our tests. It offers outstanding privacy features and is currently available at a discounted rate.

[Visit NordVPN](#)

[How to install the PBS Kids Kodi addon](#)

September 25, 2019 / by Ian Garland

[How to watch AEW – All Out Free on Kodi with a VPN](#)

August 30, 2019 / by William Elcock

[How to watch the US Tennis Open 2021 on Kodi – free livestream](#)

August 16, 2019 / by William Elcock

Latest Kodi Popular Posts

[Can you watch Bellator MMA live on Kodi?](#)

June 21, 2019 / by Sam Cook

[How to watch the 2022 French Open on Kodi](#)

May 21, 2019 / by Sam Cook

[How to watch the NCAA Frozen Four 2021 on Kodi](#)

April 10, 2019 / by Sam Cook

[How to watch the 2024 NCAA Final Four and Championship game on Kodi](#)

April 5, 2019 / by Sam Cook

[30+ Best Kodi Addons working in 2024 \(of 130+ tested\)](#)

March 15, 2019 / by Ian Garland

Latest Net Admin

[The Best Log Parsing Tools](#)

April 24, 2024 / by Scott Pickard

[The Best Tools for IoT Software Monitoring](#)

April 24, 2024 / by Scott Pickard

[The Best Service Request Management Software](#)

April 24, 2024 / by Stephen Cooper

[The Best E-commerce Fraud Prevention Software](#)

April 22, 2024 / by Amakiri Welekwe

[The Best Tools to Monitor the Health of HAProxy](#)

April 22, 2024 / by Liku Zelleke

Latest Net Admin Popular Posts

[The Best Free TFTP Servers for Windows, Linux and Mac](#)

February 28, 2019 / by Jon Watson

[The Best SFTP and FTPS Servers Reviewed 2024](#)

February 27, 2019 / by Jon Watson

[The Best NetFlow Analyzers & Collector Tools for 2024](#)

January 23, 2019 / by
John Kimball

[The Best
Bandwidth
Monitoring
Tools to
Analyze
Network Traffic
Usage](#)

December 21, 2018 / by
John Kimball

Latest News

[Virginia Union
University
notifying people
of data breach
following cyber
attack in
February 2023](#)

May 2, 2024 / by
Rebecca Moody

[OE Federal
Credit Union
confirms data
breach that
compromised
SSNs, credit
and debit cards](#)

May 1, 2024 / by Paul
Bischoff

[The
Philadelphia
Inquirer notifies
25,000+ people
of data breach
that leaked
financial,
personal info](#)

April 30, 2024 / by Paul
Bischoff

[Ransomware
gang claims
cyber attack on
New York
Legislative Bill
Drafting
Commission](#)

April 29, 2024 / by Paul
Bischoff

[Software
company
DATAIR](#)

[notifying people of LockBit ransomware attack in December 2022 that stole data and demanded \\$250K](#)

April 29, 2024 / by Rebecca Moody

Latest Password Managers

[Best password managers for iPhone in 2024](#)

March 21, 2023 / by Mark Gill

[Best password managers for Android in 2024](#)

March 16, 2023 / by Mark Gill

[Best password managers for Mac in 2024](#)

March 7, 2023 / by Mark Gill

[Best password managers for Windows in 2024](#)

February 28, 2023 / by Mark Gill

Latest Plex

[Watch your Plex library in Kodi with the Plex Kodi addon](#)

December 24, 2017 / by Aaron Phillips

[How to set up Plex on Chromecast and get the most out of it](#)

December 7, 2017 / by Aaron Phillips

[Plex vs Kodi: Which streaming software is right for you?](#)

November 1, 2017 / by Aaron Phillips

[Installing and using the Fire TV Plex app](#)

October 31, 2017 / by Aaron Phillips

[The best Plex plugins: 25 of our favorites \(Updated\)](#)

September 20, 2017 / by Aaron Phillips

Latest Plex Popular Posts

[How to get started streaming with Plex media server](#)

September 20, 2017 / by Aaron Phillips

[Selectively routing Plex through your VPN](#)

September 20, 2017 / by Aaron Phillips

Popular Posts

[The Best VPNs for Netflix in 2024 – Unblock US Netflix and more](#)

January 5, 2019 / by Paul Bischoff

[Best VPNs for Torrenting Safely and Privately in 2024](#)

January 1, 2019 / by Paul Bischoff

[Die besten und schlechtesten](#)

[VPNs für Torrent-Dateien und P2P- Filesharing 2018](#)

September 25, 2018 /
by Paul Bischoff

[How to make your own free VPN with Amazon Web Services](#)

May 15, 2018 / by Paul
Bischoff

[A beginner's guide to online censorship](#)

August 26, 2017 / by
Paul Bischoff

Latest Privacy Studies

[Digital IDs: 50 countries ranked by digital ID requirements and use](#)

January 29, 2024 / by
Rebecca Moody

[Where in the world is your child's data safe? 50 countries ranked on their child data protection legislation](#)

May 25, 2022 / by Paul
Bischoff

[Direct-to- Consumer DNA Testing: How protected is the genetic data you're submitting to these websites?](#)

March 1, 2022 / by
Rebecca Moody

[Which country has the most- watched](#)

[workers in the world?](#)

April 27, 2021 / by Paul Bischoff

[Encryption laws: Which governments place the heaviest restrictions on encryption?](#)

October 20, 2020 / by Paul Bischoff

Latest Ransomware Studies

[Nearly 1 in 5 ransomware attacks led to a lawsuit in 2023](#)

April 26, 2024 / by Rebecca Moody

[Ransomware attacks on the education sector have cost the world economy over \\$53 billion in downtime alone](#)

September 15, 2023 / by Rebecca Moody

[Ransomware attacks on the manufacturing industry cost the world economy \\$46bn in downtime alone](#)

July 31, 2023 / by Rebecca Moody

[Ransomware attacks on the finance sector have cost the world economy \\$32.3bn in downtime alone](#)

July 5, 2023 / by Rebecca Moody

[Ransomware attacks on food,](#)

beverage, and
agriculture
organizations
have cost the
world economy
\$1.36bn in
downtime alone

June 5, 2023 / by
Rebecca Moody

Latest Scams Studies

Over 114,000
Americans lost
more than \$8
billion to
investment
scams in 2023

April 27, 2022 / by Paul
Bischoff

Ofcom's new
measures could
save UK
consumers from
115m scam
calls and £9.6m
in fraud losses

October 26, 2021 / by
Paul Bischoff

The State of
Spam in the
US: Report and
Statistics

October 5, 2021 / by
Rebecca Moody

The State of
Phishing in the
US: Report and
Statistics 2021

July 27, 2021 / by Paul
Bischoff

The State of
Robocalls in the
US: Report and
Statistics 2020

July 19, 2021 / by Paul
Bischoff

Latest Sports Streaming

How to watch
Day of
Reckoning

[\(boxing\) live online](#)

December 21, 2023 / by Mark Gill

[How to watch the Caribbean Premier League from anywhere](#)

December 6, 2023 / by Mark Gill

[How to watch the Premier League for free on Amazon Prime](#)

December 6, 2023 / by Ian Garland

[How to watch Power Slap from anywhere](#)

November 23, 2023 / by Ray Walsh

[How to watch the DP World Tour Championship 2023 online](#)

November 6, 2023 / by Mark Gill

Latest Sports Streaming Popular Posts

[How to watch Spain vs. Germany \(World Cup 2022\) online from anywhere](#)

November 25, 2022 / by Craig McCart

[How to watch England vs. United States \(World Cup 2022\) online from anywhere](#)

November 23, 2022 / by Craig McCart

[How to watch United States vs. Wales \(World Cup](#)

[2022\) online from anywhere](#)

November 19, 2022 / by Craig McCart

[How to watch Gervonta Davis vs Leo Santa Cruz live online](#)

October 20, 2020 / by Sam Cook

[How to watch Vasiliy Lomachenko vs Teofimo Lopez live online](#)

October 16, 2020 / by Sam Cook

Latest Streaming Studies

[Which countries have the most Christmas movie fans?](#)

December 8, 2021 / by Rebecca Moody

[The most popular Netflix Original series by country](#)

July 7, 2021 / by Rebecca Moody

[Celebrate July 4 with the most popular patriotic movies by state](#)

June 29, 2021 / by Rebecca Moody

[Screen Time Statistics: Average Screen Time by Country](#)

June 8, 2021 / by Rebecca Moody

[What is the world watching on Netflix?](#)

April 6, 2021 / by Rebecca Moody

Latest Studies

Surveillance camera statistics: which football fans are the most watched in the world?

September 4, 2023 / by Rebecca Moody

Which of the top 50 UK cities have the most Hikvision and Dahua camera networks?

June 8, 2023 / by Rebecca Moody

NDAA-prohibited cameras: Which countries and cities have the most Hikvision and Dahua camera networks?

April 19, 2023 / by Rebecca Moody

Ransomware attacks on US manufacturing and utility businesses cost \$5.53bn in 2022

March 3, 2023 / by Paul Bischoff

On average, healthcare organizations lose \$900,000 per day to downtime from ransomware attacks

November 14, 2022 / by Paul Bischoff

Latest Surveillance Studies

The top 50 most surveilled colleges in the United States

March 29, 2022 / by Paul Bischoff

[Government Social Media Spying Powers: 50 countries ranked on social media surveillance](#)

January 19, 2022 / by Paul Bischoff

[China now lets citizens opt out of private face recognition. Does your country?](#)

August 12, 2021 / by Paul Bischoff

[Facial recognition technology \(FRT\): Which countries use it? \[100 analyzed\]](#)

June 8, 2021 / by Paul Bischoff

[CCTV surveillance in the most populated cities in the United States](#)

February 3, 2021 / by Paul Bischoff

Latest TV Streaming

[How to watch Everything Everywhere All at Once online](#)

January 18, 2024 / by Mark Gill

[How to watch Masters of the Air online from anywhere](#)

January 17, 2024 / by Ian Garland

[How to Watch The Ted TV](#)

Series (Season 1) Online

January 8, 2024 / by Ian Garland

How to stream Berlin season one online from anywhere

January 1, 2024 / by Ian Garland

How to watch The Grinch on Netflix

December 21, 2023 / by Ian Garland

Latest TV Streaming Popular Posts

How to Watch Floyd Mayweather vs John Gotti III from anywhere

June 9, 2023 / by Craig McCart

How to watch Love Island online from abroad (stream it free)

May 30, 2019 / by Ian Garland

How to watch Game of Thrones Season 8 free online

April 14, 2019 / by Sam Cook

How to watch Super Bowl 58 (LVIII) free online anywhere in the world

February 2, 2019 / by Sam Cook

Latest Utilities

Best free YouTube

[downloader apps](#)

January 13, 2024 / by Ian Garland

[10 Best Video Compressors for Windows and Mac in 2024](#)

September 9, 2023 / by Paul Bischoff

[Best video downloaders for Windows 10 in 2024](#)

August 1, 2022 / by Aimee O'Driscoll

[6 Best PC tune up software: How to tune up your PC](#)

March 22, 2021 / by Aimee O'Driscoll

[How to convert YouTube to MP3](#)

February 18, 2021 / by Aimee O'Driscoll

Latest VPN & Privacy

[iOS Malware Stats and Facts for 2024](#)

April 26, 2024 / by Ray Walsh

[Best Omegle alternatives for having fun live chats in 2024](#)

April 24, 2024 / by Ray Walsh

[VPN Jurisdiction: Where's the best place for a VPN to be based?](#)

April 22, 2024 / by Ray Walsh

[MPLS vs. VPN – What are the](#)

[differences?](#)

April 22, 2024 / by Marc Dahan

[What do Google's cookie changes mean for privacy?](#)

April 19, 2024 / by Justin Schamotta

Latest VPN Studies

[VPN demand rises around key Roe v. Wade dates](#)

July 6, 2022 / by Rebecca Moody

[Study shows you can save 85% on car rental by altering your booking location](#)

May 30, 2022 / by Paul Bischoff

[Study: How the most popular free VPNs use your data](#)

January 16, 2019 / by Paul Bischoff

Comments

Leave a Reply

Comment

Name *

Leave Comment

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)



- [Home](#)[Blog](#)[Our Authors](#)[Privacy policy](#)[Cookies Policy](#)[Terms of use](#)[Disclosure](#)
- [About Comparitech](#)[Contact Us](#)[Accessibility](#)

© 2024 Comparitech Limited. All rights reserved.
Comparitech.com is owned and operated by Comparitech Limited, a registered company in England and Wales (Company No. 09962280), Suite 3 Falcon Court Business Centre, College Road, Maidstone, Kent, ME15 6TF, United Kingdom. Telephone +44(0)333 577 0163

ANNEXURE TAD-43

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NSW
DIVISION: GENERAL

NO NSD 474 OF 2024

ESAFETY COMMISSIONER

Applicant

X CORP

Respondent

The following 44 pages is the annexure marked TAD-43 referred to in the affidavit of
Toby Allan Dagg made on 6 May 2024 before me:



.....
Signature



.....
Qualification

Filed on behalf of the Applicant, eSafety Commissioner
Prepared by: Matthew Garey
AGS lawyer within the meaning of s 55I of the *Judiciary Act 1903*

Address for Service:
The Australian Government Solicitor,
Level 10, 60 Martin Place, Sydney, NSW 2000
Matthew.Garey@ags.gov.au

File ref: 24003626

Telephone: 02 9581 7625
Lawyer's Email:
Matthew.Garey@ags.gov.au
Facsimile: 02 6169 3054

Search

English

VPN

Antivirus

Online backup

Streaming

Blog

About Us

Why Use Reviews

Why OS/DeviceBy OS/Device

Why CountryGuides

Guides Compare providers

Reviews

We receive a commission when you buy using links on our site.

Australia for fast streaming

We've rounded up the best VPN services for Australia. We've looked at VPNs with fast speeds and top privacy features and those that work with popular Australian and International streaming services.

Writer

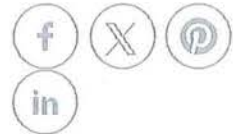
Paul Bischoff

Tech Writer, Privacy

Advocate and VPN Expert

Reviewed by: **Ian Garland** - Streaming, Kodi and VPN Expert @IanGarland_

Updated: April 30, 2024



Are you tired of not being able to access streaming services in Australia or while abroad? A Virtual Private Network (VPN) could be your answer. With VPN usage on the rise within the country and among Australians traveling abroad, choosing a reliable service that meets your needs is crucial. An Australian VPN is your go-to solution whether you're looking to **access**

May's Top VPN Discounts

Editor's Choice

Up to 74%



NordVPN OFF + 3
FREE mo
[Get Deal >](#)

85% OFF 2



Surfshark yr plan
[Get Deal >](#)



ExpressVPN Save 49%
[Get Deal >](#)

[How we test VPNs](#)

WHAT'S IN THIS ARTICLE?

Aussie TV from anywhere or safeguard your online privacy on unsecured public Wi-Fi networks.

We understand the importance of thorough testing and extensive research. That's why we've taken the time to evaluate various VPN providers to bring you an in-depth analysis of the top options available in Australia.

Protecting your online activities from prying eyes, such as your ISP and hackers, is just one aspect we'll explore. We'll also dive into the best VPNs for bypassing content restrictions and streaming blocked material while abroad.

Without further ado, let's dive into the details of each VPN. However, if you're eager to see our top Australian recommendations right away, here they are:

Best VPNs for Australia:

1. [NordVPN](#) : **The best VPN for Australia.** Best in class on security, with thousands of very fast, secure VPN servers to choose from. Works great with streaming sites like Netflix and includes a 30-day money-back guarantee. Readers' #1 choice three years running

TIP

In our testing we found that the [cheapest NordVPN plan](#) (Standard) works perfectly for Australia.

2. [Surfshark](#): Best budget option for Australia. This quick and easy-to-use VPN allows any number of connections and unblocks a huge range of services.
3. [ExpressVPN](#): Servers in 94 countries, all optimized for speed. Offers a wide range of

[Best VPNs for Australia – Our hands-on review](#)

[Best VPNs for Australia Criteria](#)

[How to use a VPN for Australia \(first-person guide\)](#)

[Why you need a VPN in Australia](#)

[How we found the best Australia VPN: Our testing methodology](#)

[Some VPNs to avoid in Australia](#)

[VPN Australia FAQ](#)

security features and strong unblocking abilities in Australia.

4. **CyberGhost**: One of the fastest Australian VPNs. Easy-to-use option with blazing fast servers and the ability to unblock Netflix and other streaming sites.
5. **PrivateVPN**: Highly secure, no logs VPN. Fast speeds. Works particularly well with Netflix Australia. Port forwarding and split tunneling for torrenting.
6. **IPVanish**: Plenty of fast server locations to choose from in Australia, a strict no logs policy, and torrent-friendly thanks to its speeds.
7. **PureVPN**: Quick and capable service that works with plenty of Australian streaming platforms. has a high connection limit, doesn't keep logs, and delivers very high speeds.
8. **ProtonVPN**: Tried and tested VPN with a great track record on security. Highly customisable, with automatic ad-blocking and a proven no logs policy.

Get NordVPN - the #1 VPN for Australia

Help our VPN research by answering one question

What is most important to you when choosing a VPN?

Let us know...



Send Feedback

WANT TO TRY THE TOP VPN RISK FREE?

NordVPN is offering a fully-featured risk-free 30-day trial [if you sign up at this page](#). You can use the VPN rated #1 for Australia, free from any limits

or restrictions, for a month. As such, it's perfect for using Australian services while abroad on vacation.

There are no hidden terms—just contact support within 30 days if you decide NordVPN isn't right for you and you'll get a full refund. [Start your NordVPN trial here.](#)

A VPN, or virtual private network, encrypts a device's internet traffic and routes it through an intermediary server in a location of the user's choosing. This can allow Australians to access blocked content that's geo-locked in their own country. It can also provide a private tunnel through which P2P filesharing applications can be used.

The VPNs in this list also have servers with [Australian IP addresses](#) so you can connect to your favorite Aussie TV when abroad in addition to accessing geo-locked content (like US Netflix or BBC) from inside Australia.

Best VPNs for Australia – Our hands-on review

We've compared the most important features for the top VPNs here. Prefer to read the in-depth reviews? [Start with NordVPN – our #1 choice for Australia.](#)

	TEST WINNER NORDVPN	Surfshark	ExpressVPN
Website	NordVPN.com	Surfshark.com	ExpressVPN.com

Ranking for Australia		1	2	
Australian servers	190+ servers	90+ servers	4	
Avg Speed (Mbps)	100+ Mbps	100+ Mbps	100+	
Simultaneous Connections	10	Unlimited		
Devices Supported	Windows, MacOS, iOS, Android, Linux	Windows, MacOS, iOS, Android, Linux, Amazon Fire TV, Apple TV	Windows, MacOS, iOS, Android, Linux, Smart TVs, Routers	
Best deal (per month)	\$3.09 <u>Up to 74% off + 3 months FREE</u>	\$2.19 <u>Save 86% on a 2 year Starter plan + 3 months free</u>	\$6.67 <u>SAVE: 49% + 3 months free</u>	

Best VPNs for Australia Criteria

You may find choosing a VPN a little difficult with so many options available. However, not all are worth your time and money. To make your decision that little bit quicker and easier, we sought out VPNs that fulfill the following criteria:

- Servers in countries worldwide (including Australia)
- Fast, unthrottled connections for streaming lag-free
- The ability to bypass geo-blocks on platforms like Netflix
- Secures your internet traffic with high-end encryption
- Protects privacy by not keeping any identifying logs

- Live chat and email support are available 24 hours a day
- Allows a minimum of five simultaneous connections (unlimited is preferred)
- Good value for money with a fair money-back guarantee

Best Australian VPNs in 2024

Based on these criteria we've compiled a list of the top VPN service providers for Australia:

1. NordVPN



APPS AVAILABLE:



Website: www.NordVPN.com

Money-back guarantee: 30 DAYS

NordVPN is one of the fastest Australian VPNs. It operates servers in over 100 countries, with multiple locations in the Asia-Pacific region, meaning you have plenty of choice when it comes to Australian servers. This VPN excels at [unblocking geo-restricted services](#) and can bypass the Netflix proxy firewall in the US and Australia. It also works very well with Amazon Prime Video and BBC iPlayer.

This VPN doesn't keep zero logs and is based in Panama, where it isn't subject to data retention laws. NordVPN puts your privacy first with AES 256-bit encryption, protection from DNS leaks, and a [kill switch feature](#). You can even connect to specialty servers

such as MultiHop and Onion Over VPN for an additional layer of security. Need help? 24/7 support is available via live chat and email.

Secure up to six devices simultaneously with NordVPN's apps for Windows, Mac, Linux, Android, iOS, and Amazon Fire TV. Browser extensions can be downloaded for Chrome, Firefox, and Edge. NordVPN supports a variety of routers with manual configuration.

Want to know more about NordVPN and why it's one of our favorite VPNs? Read our [NordVPN vs ExpressVPN](#) article, that breaks down how it stacks up against another market-leader.

NordVPN speed test data

NordVPN

[Website](#)

[NordVPN.com](#)

[Average Connection Speed - North America \(USA\)](#)

354 Mbps

[Average Connection Speed - Europe \(UK\)](#)

262 Mbps

[Average Connection Speed - Asia \(Hong Kong\)](#)

284 Mbps

Best deal (per month)

\$3.09 [Up to 74% off + 3 months FREE](#)

Pros:

Cons:

- + Top VPN contender for Australia
- Desktop app takes some getting used to
- + Unblocks foreign Netflix libraries and streams at good speeds
- + No compromises on privacy and security features
- + Purpose specific servers available (streaming, torrenting, P2P etc.)
- + Australian servers give access to Aussie content abroad

Our score:

comparitech ★★★★★

4.5 out of 5

BEST VPN FOR AUSTRALIA: [NordVPN is our #1 choice.](#) Comes packed with security features and a zero-logs policy. Unblocks most major streaming platforms abroad. Excellent connection speeds. Includes a risk-free 30-day money-back guarantee.

Read our full [review of NordVPN](#).

NordVPN Coupon

Up to 74% off + 3 months FREE

GET DEAL >

Discount applied automatically

2. Surfshark



APPS AVAILABLE:



PC



Mac



iOS



Android



Linux

Website:

www.Surfshark.com**Money-back guarantee: 30
DAYS**

Surfshark is a VPN provider that's great for unblocking region-locked content like Netflix, Hulu, Amazon Prime Video, and BBC iPlayer. It's an ideal choice for families as it allows you to have **unlimited simultaneous connections** under a single account. That makes it a great budget option to share with trusted friends and family. Surfshark also makes our list of the fastest VPNs available.

Surfshark allows P2P file-sharing on all server locations and keeps no logs of your online activity. It also offers strong 256-bit AES encryption and DNS leak protection. You can also find an automatic kill switch that prevents unprotected traffic from leaving your device if the VPN secure connection drops. If that's not enough, Surfshark also offers **MultiHop servers**. Live chat support is available 24/7.

Surfshark can be Used via its apps for Windows, Mac, Android, iOS, Linux, and Amazon Fire TV. Furthermore, Chrome and Firefox browser extensions are available. Surfshark can also be manually installed on compatible routers.

Surfshark speed test data

Surfshark

Website

[Surfshark.com](https://surfshark.com)

Average Connection Speed - North America (USA)

521 Mbps

Average Connection Speed - Europe (UK)

702 Mbps

Average Connection Speed - Asia (Hong Kong)

561 Mbps

Best deal (per month)

\$2.19 [Save 86% on a 2 year Starter plan + 3 months free](#)

Pros:

- + Generally solid speeds
- + Fantastic set of security features
- + Great at unblocking popular streaming platforms like Netflix, Hulu, and BBC iPlayer
- + Allows torrenting and P2P file-sharing
- + Unlimited simultaneous connections

Cons:

- Global server network is smaller than most other VPNs
- Some features require a subscription to Surfshark One

Our score:

comparitech ★★★★★

4.5 out of 5

BEST BUDGET OPTION: [An inexpensive way to unblock sites](#) and torrent safely across all of your devices. In fact, this fast, no-logs VPN even comes with a 30-day money-back guarantee.

Read our full [Surfshark review](#).

Surfshark Coupon

Save 86% on a 2 year Starter plan + 3 months free

GET DEAL >

Discount applied automatically

[3. ExpressVPN](#)



APPS AVAILABLE:



PC



Mac

iOS iOS



Android



Linux

Website:

www.ExpressVPN.com

Money-back guarantee: 30 DAYS

[ExpressVPN](#) operates more than 3,000 servers worldwide across 94 countries, including Australia. Torrenting is allowed on all servers. This VPN service has consistently performed well in our unblocking and speed tests, so it's a good option for streaming content. It can unblock both the US and Australian Netflix catalogs, and when you do stream, you can expect it to be lag-free thanks to unlimited bandwidth.

It's worth knowing that ExpressVPN provides excellent customer support 24 hours a day. This VPN is based in the British Virgin Islands and isn't subject to user data retention laws. Besides, it doesn't keep any user-identifying logs. Security features 256-bit AES encryption, a kill switch, and DNS leak protection. You can use ExpressVPN to connect up to five devices at the same time.

ExpressVPN has apps for desktop (Windows, Mac, and Linux) and mobile (Android and iOS). It also has an app for Amazon Fire TV. Multiple [browser extensions](#), including Chrome and Firefox, are offered. ExpressVPN even provides custom router firmware.

ExpressVPN speed test data

ExpressVPN

Website

[ExpressVPN.com](https://expressvpn.com)

Average Connection Speed - North America (USA)

319 Mbps

Average Connection Speed - Europe (UK)

303 Mbps

Average Connection Speed - Asia (Hong Kong)

278 Mbps

Best deal (per month)

\$6.67 [SAVE: 49% + 3 months free](#)

Pros:

Cons:

- + Exceptional for Australian use and accessing Australian content while abroad
- + Fast servers are great for high-quality streaming and downloading
- + Gets around torrent tracker sites blocks without compromising privacy
- + Apps have sound digital security and privacy features
- Not as configurable as some power users would like
- Doesn't come cheap, use a coupon for discounts

Our score:

comparitech ★★★★★

4.5 out of 5

HIGHLY VERSATILE: [ExpressVPN is a great choice.](#)

It's speedy, hard to beat on privacy and digital security features, and able to unblock platforms like Netflix abroad. There's even a 30-day no-quibbles money-back guarantee.

Read our full [ExpressVPN Review](#).

ExpressVPN Coupon

SAVE: 49% + 3 months free

GET DEAL >

Coupon applied automatically

4. CyberGhost



APPS AVAILABLE:



PC



Mac



iOS



Android



Linux

Website:

www.Cyberghost.com**Money-back guarantee: 45
DAYS**

CyberGhost operates a vast network of more than 10,000 servers, including 200+ in Australia and over 1,300 in the US. It focuses heavily on unblocking streaming services like Netflix and Amazon Prime Video. It's also popular with torrenters due to its very fast server speeds and strong security offering. With a single CyberGhost account, you can connect up to seven devices simultaneously.

You can expect strong privacy protection with CyberGhost, which doesn't log user activity or record IP addresses. All data is secured with 256-bit AES encryption, DNS leak protection, and an automatic kill switch feature. If you're on Windows, you'll benefit from CyberGhost's Windows security suite, which **includes an antivirus**. Live chat and email support can be contacted around the clock.

CyberGhost provides apps for Windows, Mac, Android, iOS, **Linux**, and Amazon Fire TV. You can also manually configure a connection with compatible Wi-Fi routers.

CyberGhost speed test data

CyberGhost

Website

[Cyberghost.com](https://www.cyberghost.com)

Average Connection Speed - North America (USA)

449 Mbps

Average Connection Speed - Europe (UK)

269 Mbps

Average Connection Speed - Asia (Hong Kong)

167 Mbps

Best deal (per month)

\$2.19 [SAVE 83% on the 2 year plan + 2 months free!](#)

Pros:

- + Operates servers in Australia, great for accessing local content while abroad
- + Beginners find their apps easy to set up and use.
- + We were impressed by their server speeds during testing
- + Solid privacy and security features enabled by default

Cons:

- Lack of configuration options will frustrate power users
- No dedicated apps for routers

Our score:

comparitech ★★★★★

4.5 out of 5

GOOD VALUE OPTION: [CyberGhost is easy to use.](#)

Achieves fast and reliable internet access with a good range of servers. Great privacy with zero logs, DNS leak protection and an automatic kill switch. Works well with most popular streaming platforms. 45-day money-back guarantee.

Read our full [CyberGhost VPN review](#).

CyberGhost Coupon

SAVE 83% on the 2 year plan + 2 months free!

GET DEAL >

Discount applied automatically

5. PrivateVPN



APPS AVAILABLE:



PC



Mac



iOS



Android



Linux

Website:

www.PrivateVPN.com

Money-back guarantee: 30 DAYS

[PrivateVPN](#) is a service based in Sweden that was launched with the backing of activists who support consumer rights to torrent privately. Although it has a

relatively small server network, its servers are spread across 60 countries. Furthermore, this VPN is highly capable of unblocking popular streaming services, such as Netflix or HBO Max. Speeds are more than fast enough for streaming, and there's no **bandwidth throttling**.

True to its name, PrivateVPN has a watertight no-logs policy. It also offers 256-bit AES encryption, a kill switch, DNS leak protection, port forwarding, and obfuscation. With a single account, you can install it on up to 5 devices simultaneously. Live chat and email support are available, and if you need it, there's even free remote help and installation.

You can connect to PrivateVPN servers via the apps for Windows, Mac, Android, iOS, and Amazon Fire TV. To use PrivateVPN with Linux or a Wi-Fi router, you'll need to follow manual setup instructions.

PrivateVPN speed test data

PrivateVPN

Website

[PrivateVPN.com](https://privatevpn.com)

Average Connection Speed - North America (USA)

94 Mbps

Average Connection Speed - Europe (UK)

57 Mbps

Average Connection Speed - Asia (Hong Kong)

62 Mbps

Best deal (per month)

\$2.00 [Save 85% on a one year plan + 24-months free](#)



Pros:

- + Allows torrenting throughout
- + Servers in 63 countries
- + Solid no logs policy
- + AES encryption, killswitch, and port forwarding features
- + Excellent speeds

Cons:

- Fewer servers in each country than our other recommendations

Our score:

[comparitech](#) ★★★★★

4.5 out of 5

STRONG ON PRIVACY: [Based in Sweden.](#) Secure bare metal servers. No logs policy. Servers located in 63+ countries. Allows torrenting. Has a Kill-switch,

DNS leak protection, and obfuscation. Perfect for streaming Netflix or accessing restricted websites. 30-day money-back guarantee.

Read our full [PrivateVPN review](#).

PrivateVPN Coupon

Save 85% on a one year plan + 24-months free

GET DEAL >

Discount applied automatically

6. IPVanish

IPVANISH
VPN

APPS AVAILABLE:



PC



Mac

iOS iOS



Android



Linux

Website: www.IPVanish.com

**Money-back guarantee: 30
DAYS**

[IPVanish](#) has implemented the WireGuard protocol and owns all of its own physical servers. This has resulted in some of the fastest download speeds available from any VPN. It operates more than 2,000 servers in 75+ locations. Furthermore, it has over 70 servers in Australia and New Zealand. You can use IPVanish to securely access the likes of Netflix US and even Australian streaming services such as [Stan](#).

With IPVanish, you can connect an unlimited number of devices at the same time. A subscription also

includes 24-hour access to live chat and email support. This is a highly secure service thanks to its 256-bit AES encryption and no-logs policy. Note that security also includes protection from DNS leaks and a kill switch.

IPVanish offers Windows, Mac, Android, iOS, and Amazon Fire TV apps. However, browser extensions aren't available. While IPVanish supports Linux and select routers, manual setup is required.

IPVanish speed test data

IPVanish

Website

[IPVanish.com](#)

Average Connection Speed - North America (USA)

277 Mbps

Average Connection Speed - Europe (UK)

237 Mbps

Average Connection Speed - Asia (Hong Kong)

352 Mbps

Best deal (per month)

\$2.99[SAVE 76% on the 2 yr plan](#)

Pros:

- + Own and operate server locations in Australia
- + Impressive speeds and reliable secure

Cons:

- Can't signup with Bitcoin
- Apps don't work in China

connections

- + Torrenting is allowed and they keep no internet traffic logs
- + Secure unlimited devices

Our score:

comparitech ★★★★★

4 out of 5

NO CONNECTION LIMIT: [IPVanish has a large network of servers](#). Generally solid for torrenters, Kodi users, and folks who need the highest standard of privacy, but look elsewhere if you want to unblock Netflix. 30-day money-back guarantee.

Read our full [IPVanish review](#).

IPVanish Coupon

SAVE 76% on the 2 yr plan

GET DEAL >

Discount applied automatically

7. PureVPN



APPS AVAILABLE:

Website: www.PureVPN.com



PC



Mac

iOS iOS

 Android**Money-back guarantee: 31
DAYS** Linux

PureVPN has one of the larger networks we've seen, with roughly 6,000 servers spread across 65 countries including Australia. These appear to be remarkably well-optimized, resulting in average speeds of nearly 400 Mbps in our most recent testing. In other words, you shouldn't have any performance issues regardless of whether you're streaming 7plus, playing online games, or downloading large files. The generous connection limit is a huge bonus too.

Let's talk about security. PureVPN keeps your activities hidden using industry-standard encryption. It also prevents DNS and IPv6 leaks, plus there's a kill switch that ensures you never browse unprotected. This service follows a strict no-logs policy and undergoes regular audits to prove it. Unfortunately, the tracker-blocker only works if you choose one of the more expensive subscription plans and support staff take quite a while to respond via live chat. All the same, this is a VPN that's well worth trying out.

PureVPN has its own apps for Android, iOS, Windows, and MacOS. There's also a GUI for Linux users and manual setup instructions just in case you'd like to install this VPN on a router.

PureVPN speed test data

PureVPN

Website[PureVPN.com](https://purevpn.com)

Avg Speed (US)

628 Mbps

Avg Speed (UK)

324 Mbps

Avg Speed (Asia)

246 Mbps

Best deal (per month)\$2.11 [Up to 82% off the 2-yr standard plan + free months](#)**Pros:**

- + Excels at going undetected
- + Good blend of speed and security
- + Can secure up to 10 devices simultaneously

Cons:

- Limited split tunneling support
- Could offer more advanced functionality

Our score:

comparitech ★★★★★

4 out of 5

FAST AUSSIE SERVERS: [PureVPN makes it easy to get a high-speed](#), low-latency connection in Australia. Works well with most streaming platforms and includes all of the tools you'll need to browse safely. Better still, all plans come with a 31-day money-back guarantee.

Why not read our complete [PureVPN review](#)?

PureVPN Coupon

**Up to 82% off the 2-yr standard plan +
free months**

GET DEAL >

Discount applied automatically

8. ProtonVPN



APPS AVAILABLE:



PC



Mac



iOS



Android



Linux

Website:

www.protonvpn.com

**Money-back guarantee: 30
DAYS**

ProtonVPN is another service with plenty to offer users in Australia. It has minimal impact on your connection speeds (averaging 330 Mbps in our latest tests), blocks ads automatically, and can help you access stubborn streaming platforms like Netflix, 10play, and Bing from abroad. What's more, it permits up to 10 simultaneous connections and provides 24/7 assistance over live chat. There's even a limited free plan, so you can try it out before you commit.

This service has everything you'll need to browse the web safely, including [256-bit encryption](#), [a kill switch](#), and [leak protection](#). There are even special Secure Core servers stored in underground data centers for maximum protection. Experienced users will find a lot to like here, from port forwarding functionality to [split tunneling](#), but more importantly, ProtonVPN follows a

zero-logs policy. We know this for a fact, too, since it's been independently audited.

ProtonVPN apps are available for iOS, MacOS, Windows, Linux, and Android. It's also possible to manually configure this service to work with most router firmware.

ProtonVPN speed test data

ProtonVPN

Website

protonvpn.com

Average Connection Speed - North America (USA)

390 Mbps

Average Connection Speed - Europe (UK)

306 Mbps

Average Connection Speed - Asia (Hong Kong)

295 Mbps

Best deal (per month)

\$3.59 [Up to 64% off a 2-year plan](#)

Pros:

- + Large network of fast servers
- + Novice-friendly but highly-secure
- + Makes it as easy as possible to get help

Cons:

- Not the cheapest, even for long-term subscribers
- We'd like to know more about how the VPN Accelerator works

Our score:

comparitech ★★★★★

4 out of 5

READY FOR ANYTHING: [ProtonVPN is a privacy-first service](#) that's just as comfortable streaming Australian TV as it is torrenting. Paid plans come with a generous connection limit, access to ultra-fast servers, and a 30-day money-back guarantee.

Still have questions? Find answers in our comprehensive [ProtonVPN review](#).

ProtonVPN Coupon

Up to 64% off a 2-year plan

GET DEAL >

Coupon applied automatically

How to use a VPN for Australia (first-person guide)

Looking to improve your online privacy? I've created a newcomer-friendly guide that'll walk you through using a VPN step-by-step:

1. The hardest part of using a VPN is actually deciding which service to choose! I've used [ExpressVPN](#) in the screenshots below, but after extensively testing all of the providers mentioned above, I can assure you that they're all high-quality VPNs that work in a similar way, even if certain options are in different places or are called slightly different things

2. Begin by logging into your VPN app. Most providers use an email and password combination, but ExpressVPN asks you to log into the website and paste an activation code into the app or have a login link sent to your email

The image displays two side-by-side screenshots of the ExpressVPN login interface. Both windows have a blue header with the ExpressVPN logo and title bar. The left window is titled 'Please enter your activation code' and includes a sub-header: 'You can find your activation code on your dashboard when you sign in to your ExpressVPN account.' Below this is a text input field with the placeholder 'e.g. EAR4EAZRXBKAJDTKCCUD'. At the bottom of the left window are three buttons: a green 'Continue' button, a white 'Sign In with Email Sign-In Link' button, and a small 'Need help? New to ExpressVPN?' link. The right window is titled 'Enter your ExpressVPN account email:' and features an email input field. Below the input field are two buttons: a green 'Email My Sign-In Link' button and a white 'Sign In with Activation Code' button. At the bottom of the right window is a small 'Need help? New to ExpressVPN?' link.

ExpressVPN's activation code expires periodically, meaning even if your credentials are stolen, attackers won't be able to use your account for long.

3. Generally speaking, the closer your chosen server is, the more reliable your connection will be. That's why we'll be choosing one of our VPN's Australian servers. These are also the servers you'd use if you wanted to keep streaming Australian TV while traveling in other countries



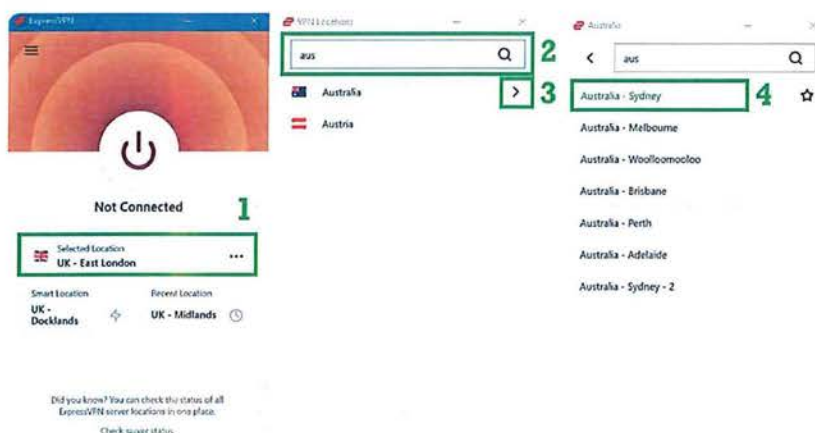
Geoblocked

Access is not available in your area.

[Why can't I create a Nine Account?.](#)

These errors often prevent travelers from staying caught up on their favorite shows. In my experience, though, services like ExpressVPN, Surfshark, and NordVPN make it very easy for you to regain access

4. I clicked on ExpressVPN's **Selected Location** button to open up the full server list. I've always found scrolling through dozens of countries to be tiresome, so I used the search bar at the top of the screen to find Australia instead
5. Next, I hit the arrow icon on the right to see all of the different server locations in Australia. In my judgment, those in major cities tend to be better for streaming, which is why I picked one in Sydney. If you're just looking for the added security a VPN offers, any of these locations would be fine



ExpressVPN has more than half a dozen Australian server locations. NordVPN and Surfshark aren't too far behind, with five each

6. In a moment or two, ExpressVPN's quick-connect button will turn green to let you know that you're connected. This cue will look a little different for every provider, but in most cases, it'll be reasonably obvious
7. You should now be able to browse the web without worrying about who might be watching. Additionally, Australia-only websites that previously displayed errors like *"Geoblocked – Access is not available in your area"* or *"Oops, something went wrong... Please try again later"* should now be accessible
8. If you're still having problems, don't panic. Years of testing VPNs have taught me that most issues can be resolved by clearing your cookies, opening the website in a private tab, or trying a different server in the same country
9. None of those tips worked? In that case, I'd recommend contacting your VPN's customer support team. All of the services mentioned above offer free live chat (accessible from the support sections of their respective websites). This is by far the fastest way to get help – whenever I've used live chat, I've gotten a response in seconds.

Why you need a VPN in Australia

When it comes to digital privacy and online freedom in Australia, several concerns make using a VPN almost essential. Here's why:

1. **5-Eyes Alliance Membership:** Australia is a key member of the [5-Eyes intelligence-sharing alliance](#). This alliance involves countries sharing surveillance data amongst themselves. You can encrypt your online activities using a VPN, making it difficult for any entity to monitor or log your data.

2. **Government Surveillance:** The Surveillance Legislation Amendment (Identify and Disrupt) bill, introduced in September 2021, grants Australian law enforcement the authority to access and alter data on your devices. A VPN can provide an added layer of security, ensuring your data remains private and out of reach.
3. **ISP Monitoring and Restrictions:** Australian [Internet Service Providers \(ISPs\)](#) are known to monitor user data. They can also throttle bandwidth or block access to P2P networks and websites. With a VPN, you can bypass these restrictions, ensuring unrestricted access to the internet and safeguarding your online activities from prying eyes.
4. **Cybersecurity Concerns:** [Cyberattacks](#) are a global concern, and Australia is no exception. Whether it's hackers trying to [steal personal information](#) or malware attempting to infiltrate devices, the risks are real. A VPN offers robust encryption, making it challenging for cyber criminals to intercept or decipher your data.
5. **Data Retention by Telecommunication Firms:** Australian laws mandate telecommunication companies to retain user data for up to two years. This data can include call logs, text messages, and more. VPNs encrypt your online activities, and many also come with anti-tracking features. This ensures that third parties, including telecommunication firms, cannot easily access or use your personal information, safeguarding you from unsolicited communications.

In conclusion, while Australia offers numerous attractions and opportunities, it's crucial to prioritize your digital privacy and security. A VPN is a protective

shield, ensuring you can enjoy the digital world without compromising your data and freedom.

How we found the best Australia VPN: Our testing methodology

Below, we go into a little more detail regarding the key criteria and our methodology for testing Australian VPNs.

- **Servers:** All major VPNs have servers covering dozens of countries, including the [US](#), [UK](#), [Canada](#), and of course, Australia. In the case of the VPNs listed in this post, thousands of servers are available in most cases. As such, you shouldn't have any trouble bypassing restrictions or finding a fast connection. Some of the VPNs even have suggested servers for specific activities, like streaming, gaming, and torrenting.
- **Speeds:** Some VPNs are simply too slow, particularly for more bandwidth-intensive activities such as streaming and torrenting. We conduct speed tests across servers in multiple locations of each VPN. That way, we can find the [fastest VPNs](#) on the market, all of which include unlimited bandwidth. It's worth noting that all VPNs will have [some impact on speed](#).
- **Unblocking:** Copyright and even government censorship means that many websites and services aren't available everywhere. Some VPNs struggle with this but the best VPNs consistently find ways around blocks. We make sure this is the case by regularly testing them with the likes of [BBC iPlayer](#), [Skype](#), and [Twitter](#).
- **Security:** At a minimum, we look for the VPNs we recommend to provide 256-bit AES encryption, protection from DNS leaks, and a kill switch.

However, many of the best VPNs for Australia offer extras such as Double VPN servers, a password manager, or an ad-blocker. As such, you'll enjoy more comprehensive protection.

- **Privacy:** A VPN should encrypt your data and change your IP address so you can browse anonymously. Some fail to provide a sufficient level of encryption while others may keep logs by which you can be identified or even log and sell your browsing data. We've looked at [140 VPN logging policies](#) so we could find the very best.
- **Ease of use:** Beginner-friendly apps can make all the difference as to whether you enjoy using a VPN. Having tested dozens of VPN apps for ourselves, we know which are the quickest to set up and the easiest to navigate. Better still, all offer 24-hour live chat and email support should you have any trouble.
- **Value:** Despite offering all of the above, the best VPNs for Australia remain affordable, particularly if you commit to a long-term subscription. Furthermore, all come with money-back guarantees of at least 30 days. To save even more, be sure to take advantage of our VPN discount coupons as we often have exclusive offers.
- **Compatibility:** The best VPNs for Australia need to work on the most popular devices and platforms. We test each provider on PC, Mac, iOS, and Android and expect a seamless experience. We also look at whether a VPN works with home routers, and streaming devices such as [Nvidia](#) and [Kodi](#). We consider how many simultaneous device connections are supported before recommending a VPN.

Our [VPN testing methodology](#) goes into even greater detail about how we analyze VPNs. It's with this hands-on approach that we can offer the most accurate and up-to-date information available.

Some VPNs to avoid in Australia

One of the biggest motivations for using a VPN is to increase your online security and the privacy of your digital footprint while online. Unfortunately, not all VPNs do this, and some can even inhibit or reduce your privacy.

Hola

Israel-based Hola isn't a traditional VPN in which customers connect to a network of centralized servers owned by the VPN company. Instead, Hola users connect to each other, using other internet users' idle bandwidth as part of a large peer-to-peer network. Obviously, this comes with some pretty big security and legal concerns. Users could use each other's internet access for illegal activity, for example. In 2015, Hola used its user's computers to create a botnet and perform a massive distributed denial-of-service (DDoS) attack. The abuse of customers' trust happened entirely without their knowledge.

HideMyAss

In 2011, a LulzSec hacker was arrested for his involvement in an attack on the Sony Pictures website. Cody Kretsinger used HideMyAss VPN to conceal his online identity, but the company complied with a court order to hand over evidence that led to his arrest. This occurred despite the company's pledge not to keep any logs of user activity. HMA says it does not log the

contents of its users' internet traffic, but it keeps detailed metadata logs that include users' real IP addresses, enough to charge Kretsinger with a crime.

Now that the UK has passed the Snooper's Charter, which requires service providers to maintain detailed logs of what their users do online, UK-based HideMyAss seems like the last service any privacy-conscious person would want to sign up for.

Recommended articles: [The Best VPN Services of 2024](#)

VPN Australia FAQ

Why you should avoid free VPNs?

It might be tempting to use a free VPN instead of a paid one, but we strongly advise against it. With very few exceptions, free VPNs are either incredibly limited or invade your privacy to mine personal data, which is then sold off to third-party advertisers.

Free VPNs often have data caps, bandwidth limits, and even queues. Server selection is limited. Some will inject advertisements into your browser and use tracking cookies to monitor your behavior. This actually reduces your privacy and defeats the purpose of a VPN.

If you insist on using a free VPN, make sure to read through the company's privacy policy. Ensure they use strong encryption standards and have no-logs policies. However, we recommend you opt for the stronger security, unlimited bandwidth and access to geo-locked

content that can only be offered by a paid VPN provider.

Is using a VPN in Australia legal?

Yes, using a VPN in Australia is perfectly legal. That doesn't make you immune to the law, however. Using a VPN to hide illegal activity is still illegal.

Using a VPN to bypass region-locked services might break those services' terms of service. These are not laws, however, and are generally not enforced with punitive action. You can find out more about VPN laws in our guide to where [VPNs are legal](#).

Will a VPN help avoid Australia's data retention law?

A VPN provides a great many privacy protections that we think everyone should take advantage of. This is especially true in Australia where a 2017 report found that in the previous 12 months, cybercrime rates had [increased by 15% to 47,000 incidents](#). However, within the specific context of Australia's 2015 data retention law, they won't do much good.

Google is full of articles claiming that a [VPN will prevent ISPs](#) from gathering metadata, but unfortunately that is not true. A VPN hides the contents of your internet traffic and your location from the outside world, but you still have to rely on your ISP's network to get there. Strictly speaking a VPN cannot prevent an ISP from logging your geolocation, device details, and traffic volume.

We've explained this in greater detail in our article on the [Australian data retention law](#). There you can also find other means of avoiding the [data retention policies](#).

See also: [Australia Freedom House report](#)

Is torrenting illegal in Australia?

Torrenting copyrighted material is a crime in Australia, but there is little enforcement. It's rare for copyright holders to successfully sue ISPs for torrenters' identities, whom they can then request remuneration from using a practice called speculative invoicing.

However, there have been attempts to crack down on torrenting with mixed success. A ["three-strikes" rule](#) in which ISPs would notify torrenters on behalf of copyright holders was canned in 2016 due to disputes over implementation costs.

In 2016, a federal court in Australia ordered ISPs to block BitTorrent tracker sites including ThePirateBay, Torrentz, TorrentHound, IsoHunt and SolarMovie. This has [proven to be somewhat effective](#) as visits from Australia to these sites have [dropped by 53%](#). This doesn't take into account VPN users — the sites can still be accessed with any of the VPNs we listed above.

In 2017, another [59 pirate sites were added](#) to the list of blocked sites, bringing the total to more than 160.

In late November 2018, the Australian Parliament passed the Copyright Amendment to the Copyright Act. This amendment forces ISPs to block proxy servers and mirror sites—duplicates of censored torrent sites that show up after the original site is blocked—without

the need for multiple court orders. Second, the new law will force search engines like Google to remove or demote links to infringing sites, as well as their proxies and mirrors.

Comparitech does not condone or encourage piracy. Please stick to legal torrents.

Is using a VPN in Australia to access U.S. Netflix legal?

No, it is not against the law to access US Netflix from Australia with a VPN.

However, using a VPN to access another country's video streaming library is against Netflix's terms of use, which state:

“You may view Netflix content primarily within the country in which you have established your account and only in geographic locations where we offer our service and have licensed such content. The content that may be available to watch will vary by geographic location and will change from time to time.”

Netflix enforces this rule by blocking connections from most VPN providers, but it does not penalize users who attempt to watch through a VPN. We've not witnessed Netflix banning, suspending, or taking legal action against VPN users beyond simply blocking streams.

What are the best Australia streaming TV channels?

Here are some streaming services in Australia you can access from Australia:

- Netflix Australia
- 10Play (Network 10)
- Kayo (live sports)
- Stan
- Amazon Prime Video
- Foxtel Now
- CBS 10 All Access
- Hayu (reality TV)
- BINGE
- Apple TV+
- Disney+

Which cities in Australia do NordVPN have servers?

NordVPN operates servers in Adelaide, Brisbane, Melbourne, Perth, and Sydney.

Which VPN is best for watching Aussie rules footy?

The cheapest way to watch Australian Rules Football (a.k.a. Aussie rules footy) online is [Kayo](#), a sports streaming service in Australia. NordVPN has plenty of servers in Australia that can unblock Kayo. Prices for Kayo start at AU\$25 per month for streaming on two devices.

You can also check out [WatchAFL.com](https://www.watchafl.com) to stream AFL Premiership games from abroad, but it's more expensive with monthly subscriptions starting at US\$33 per month. If you're outside of Australia, you won't need a VPN, but viewers in Australia will need to connect to a VPN in another country to use WatchAFL.com.

It would probably be cheaper to subscribe to NordVPN and Kayo than to just pay for WatchAFL.com.

Can I watch British TV in Australia?

Yes! By connecting to a VPN server in the UK using one of the recommended services above, you can access BBC iPlayer, All 4, ITV, Sky Go, and much more British content.

How do I get American Netflix on my smart TV in Australia?

Smart TVs typically don't support VPNs. So there are a few alternatives:

- Install the VPN on your wi-fi router, or purchase a pre-configured VPN router. ExpressVPN is our favorite option for this thanks to its custom VPN firmware. Any device you connect to the router will use the VPN.
- Use a laptop or phone as a VPN-enabled wi-fi hotspot. By connecting your phone or laptop to the VPN, then tethering your smart TV to that device, you can route your TV's internet connection through the VPN. More on [how to set up VPN-protected wi-fi hotspots from a laptop](#) here.

- Use a smart DNS proxy. Although they don't support VPNs, many smart TVs do allow customers to set custom DNS servers. For example, ExpressVPN gives all subscribers access to its MediaStreamer DNS service. This doesn't have all the protections of a VPN, but it does unblock Netflix and other streaming services.

Is Australia part of the Five Eyes alliance?

Yes. The Five Eyes (FVEY) is an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States. The alliance has been operational since at least 1946. Australia became a member of FVEY in 1956 along with New Zealand.

Which Australian cities can a VPN give me an IP address from?

The Australian cities a VPN can provide IP addresses for will depend on the server locations available with the provider you choose. Generally, most VPNs with servers in Australia can provide an IP address for Sydney, Melbourne, or Brisbane – although this will vary for each provider.

Can you be tracked if you use a VPN in Australia?

It's possible to be tracked even if you use a VPN. This is the case whether you're in Australia or any other

country. However, **using a VPN makes it more difficult for you to be tracked.**

The idea behind a VPN is that in connecting to a server, your internet traffic is encrypted. You can then browse anonymously as a result. Of course, you can only be sure of this with quality paid VPN providers such as the best VPNs for Australia. [Free VPNs](#), for example, may not properly encrypt your data and may keep logs of your activity, compromising your identity.

It's also worth noting that your ISP can see you're using a VPN. It can only see the VPN IP address in question and the amount of traffic traveling to and from your device — not your online activity. As such, if authorities were to contact your ISP and request this information, they too would know you're using a VPN. They could request logs from the VPN provider but, as long as you're using a no-logs service, there should be no identifying logs for the VPN to provide.

Which shows can I watch on Australian Netflix?

Netflix Australia offers viewers a great selection of movies and TV shows, with some exclusives only available in selected regions. Some of the most popular picks include the following:







- You season 1-4
- Selling Sunset
- Byron Baes
- The Deep
- Wild Croc Territory
- Raising the Bar

Will all of these VPNs give me an Australian IP address?

Yes, all the VPNs on our list have servers in Australia, meaning they can provide you with an Australian IP address. Connecting to an Australian server allows you to access Australian content, bypass geo-restrictions, and maintain a local online presence.

Many of our VPN picks have multiple server locations across the globe, including Australia, which ensures that you can easily obtain an Australian IP address. This can be particularly useful for expats, travelers, or anyone wanting to access Australian websites, streaming services, or other online content that might be restricted to Australian residents. Always ensure the VPN you choose has servers in Australia to guarantee a seamless online experience while accessing Australian content.

Roundup - best VPNs for Australia

	Our Score	Our Verdict
1.  NordVPN®	 4.5/5	Best VPN for changing Netflix region Get NordVPN »
2.  Surfshark®	 4.5/5	Best budget option Get Surfshark »
3.  ExpressVPN	 4.5/5	Highly versatile Get ExpressVPN »

4.  **CyberGhost**  4/5 [Get CyberGhost »](#)
Easy to use

5. **IPVANISH**  3/5 [Get IPVanish »](#)
Unlimited devices

PRIVACY ALERT: Websites you visit can find out who you are

The following information is available to any site you visit:



Your IP Address:

155.190.54.35



Your Location:

**Sydney, New South Wales,
Australia**



Your Internet Provider:

Cisco OpenDNS, LLC

This information can be used to target ads and monitor your internet usage.

Using a VPN will hide these details and protect your privacy.

We recommend using [NordVPN - #1 of 72 VPNs](#) in our tests. It offers outstanding privacy features and is currently available at a discounted rate.

[Visit NordVPN](#)

Comments

Leave a Reply

Comment

Name *

Leave Comment

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)



- [Home](#)[Blog](#)[Our Authors](#)[Privacy policy](#)[Cookies Policy](#)[Terms of use](#)[Disclosure](#)
- [About Comparitech](#)[Contact Us](#)[Accessibility](#)

© 2024 Comparitech Limited. All rights reserved.
Comparitech.com is owned and operated by Comparitech Limited, a registered company in England and Wales (Company No. 09962280), Suite 3 Falcon Court Business Centre, College Road, Maidstone, Kent, ME15 6TF, United Kingdom. Telephone +44(0)333 577 0163

ANNEXURE TAD-44

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NSW
DIVISION: GENERAL

NO NSD 474 OF 2024

ESAFETY COMMISSIONER

Applicant

X CORP

Respondent

The following 16 pages is the annexure marked TAD-44 referred to in the affidavit of Toby Allan Dagg made on 6 May 2024 before me:



.....
Signature



.....
Qualification

Filed on behalf of the Applicant, eSafety Commissioner
Prepared by: Matthew Garey
AGS lawyer within the meaning of s 55I of the *Judiciary Act 1903*

Address for Service:
The Australian Government Solicitor,
Level 10, 60 Martin Place, Sydney, NSW 2000
Matthew.Garey@ags.gov.au

File ref: 24003626

Telephone: 02 9581 7625
Lawyer's Email:
Matthew.Garey@ags.gov.au
Facsimile: 02 6169 3054

Why Use VPNs? Reviews
Why OS/Device? By OS/Device
Why Country? Guides
Guides Compare providers
Reviews

We receive a commission when you buy using links on our site.

How to bypass geo-blocking with a VPN and spoof your location

Looking to get around geo-blocking and spoof your location? We explain how to bypass online censorship and access region-locked services like Netflix and BBC iPlayer from anywhere using a VPN.

IAN GARLAND - STREAMING, KODI AND VPN EXPERT
@IanGarland_ Updated: March 15, 2024



Isn't it frustrating when you're blocked because of your location from accessing your favorite streaming shows, thrilling sports events, immersive gaming experiences, or exciting gambling platforms? You're not alone. Most premier online platforms have region-locked content, leaving many globally-minded users in the cold. Worse still, countries like China have intensified the digital divide by placing extensive restrictions on universally popular platforms.

May's Top VPN Discounts

Editor's Choice

NordVPN®

Up to 74% OFF + 3 FREE months
[Get Deal >](#)

85% OFF 2 yr plan

Surfshark®

[Get Deal >](#)

Save 49%

ExpressVPN

[Get Deal >](#)

[How we test VPNs](#)

WHAT'S IN THIS ARTICLE?

[How to avoid geo-blocking with a VPN](#)

But what if we told you there's a proven, secure way to this geo-restricted content?

We've found the powerful tool of a Virtual Private Network (VPN) through exhaustive research and rigorous testing. VPNs reroute your online footprint through international servers, seamlessly **replacing your original IP address** (a key factor in geo-location) with a new, region-specific one. This tricks most platforms into believing you're in a 'permitted' location.

But there's more. With rising concerns about online surveillance, **VPNs are also your armor against prying eyes**. They encrypt your digital activities, ensuring they remain invisible to employers, governments, and your ISP. This is particularly helpful if you're in a country with strict internet censorship.

How to avoid geo-blocking with a VPN

With the right VPN, it's easy to access region-locked services abroad. Just follow the steps below.

Here's how to get around geo-blocking using a VPN:

1. Start by signing up for a suitable VPN. We particularly recommend [NordVPN](#), but [Surfshark](#) and [ExpressVPN](#) are two versatile, high-performance alternatives.
2. Download and install the VPN app, taking care to get the right version for your device.
3. Connect to one of your VPN's servers in the appropriate country. For example, you'll need to use a British server to unblock BBC iPlayer or a US one for Hulu.
4. Log in to your chosen service and play previously geo-blocked content. In most cases, it should start

[How does geo-blocking work?](#)

[When might I encounter geo-blocking?](#)

[How can websites and services tell which country I'm in?](#)

[Can I bypass China's Great Firewall with a VPN?](#)

[Can I beat geo-blocking with a free VPN or proxy?](#)

[Why isn't my VPN unblocking a particular service?](#)

[What services can I access abroad with a VPN?](#)

[Can I bypass VPN blocks to watch US shows?](#)

[What VPN allows me to watch Hotstar India?](#)

[Is it legal to bypass geo-blocking?](#)

[Our Methodology: Choosing the right VPN to get around geo-blocking](#)

[How to remove geo-blocking FAQs](#)

immediately, but if not, clear your browser's cache and cookies, then refresh the page.

If you continue to experience issues, it's worth contacting your VPN's support team directly to see if there's a particular server you should use.

TIP

In our testing we found that the [cheapest NordVPN plan](#) (Standard) works perfectly for beating geo blocking.

WANT TO TRY THE TOP VPN RISK FREE?

NordVPN is offering a fully-featured risk-free 30-day trial [if you sign up at this page](#). You can use the VPN rated #1 for unblocking stubborn services with no restrictions for a month. This is ideal if you want to binge your favorite show or are going on a short trip abroad.

There are no hidden terms—just tell support within 30 days if you decide NordVPN isn't right for you and you'll get a full refund. [Start your NordVPN trial here](#).

How does geo-blocking work?

Geo-blocking works by restricting access to internet content based on the user's geographical location. In a geoblocking scheme, the user's location is determined using internet geo-location techniques, such as checking the user's IP address against a blocklist or allowlist. GPS location data can also be used on mobile devices.

Geo-blocking can also be implemented via various technologies, including internet addresses, credit card numbers, and other electronic identification means. It enables rights holders and intermediaries (such as Netflix) to segment the internet into different markets, provide access to different content based on copyright contracts, charge different prices, or offer different services to consumers.

When might I encounter geo-blocking?

There are two main situations in which you might experience geo-blocking. One is when you try to use a service like Netflix, BBC iPlayer, or ESPN abroad. Some streaming platforms have **different content libraries** for different regions, while others are completely inaccessible from outside of their required countries. Sling TV, for instance, prevents you from even viewing its website abroad, saying *"We're sorry. Sling TV is only available in the US."*

This is because streaming services usually only have the right to show their content in specific countries. Other types of sites geo-restrict their content, too. For example, betting websites typically only serve people located in specific countries.

Another situation in which you may encounter geo-blocking is when trying to access content that's restricted, banned, or against the law in your current location. This doesn't necessarily mean that you're up to no good; some countries just have different values, leading them to block things like gambling, dating, and social media sites.

Depending on where you are in the world, you might find that you can't even use services that could be

considered essential, like WhatsApp, Skype, or FaceTime. All three of these and more are blocked in countries like China and the [UAE](#), which can make it difficult to communicate with friends and family back home.

How can websites and services tell which country I'm in?

Most of the time, services rely entirely on the user's [real IP address](#) to tell where they are in the world. However, more advanced platforms often employ additional verification measures. They could cross-reference your IP address with GPS location data if you're using a mobile device, for instance, or check your IP address against a list of known VPN servers.

Sometimes, it isn't even the website you're trying to access that blocks the connection—it's the government. For instance, China's Great Firewall has an expansive list of blocked websites and monitors domestic traffic for specific keywords and recognizable VPN traffic patterns to determine whether you're trying to access a blocked website.

Can I bypass China's Great Firewall with a VPN?

It's especially difficult, although not impossible, to bypass regional restrictions in China. You can't just install a VPN and start browsing, though, as the government has tried exceptionally hard to block all access to privacy-focused services, including VPN websites. As a result, there are only a few [VPNs that reliably work in China](#).

If you're planning a trip to China (or any country that restricts access to VPNs), you'll have to download and install the VPN beforehand. We'd also recommend making a note of any mirror sites your VPN might operate and instructions on how to manually configure the service. This information should be kept in a password-protected file and saved locally on your device since countries with strict online censorship tend to block access to cloud storage platforms.

Not sure if a particular website is blocked in China? You can check before arriving by entering a URL into our [Great Firewall tool](#). Remember: the Great Firewall is updated all the time, so even if a site is accessible right now, it might not be when you get to China.

Can I beat geo-blocking with a free VPN or proxy?

Free VPNs tend to struggle when it comes to unblocking services. They often have smaller networks than their paid rivals so it's easier for platforms to blacklist all of their IP addresses, and with fewer resources, it's more difficult to find a workaround whenever new VPN-detection features are introduced. Free proxies have similar performance issues and to make matters worse, they only protect your browser traffic, meaning anything you do in an app will still be visible.

These services usually have huge numbers of users, so you'll almost certainly experience slow speeds. Even if a free VPN or proxy unblocks your chosen service, you'll likely have to contend with long buffering times and laggy playback.

Free VPN services have a poor record when it comes to privacy. A survey of more than 280 free VPN apps discovered that almost 40% contained malware and **over 80%** leaked personal information over IPv6.

Worst of all, nearly one in five used no encryption whatsoever, meaning their users were no safer than when browsing the web normally. We've even seen major players in this space use shady business tactics, such as when Hola was caught selling its users' bandwidth to facilitate a botnet.

Why isn't my VPN unblocking a particular service?

Some platforms have stricter geo-blocking than others. For instance, a local TV live stream likely won't have advanced geo-restriction and VPN-detection features built in. However, Netflix, an international network worth billions of dollars, absolutely does. This is why some users encounter errors like "**You seem to be using an unblocker or proxy**" when accessing geo-blocked services with a VPN.

Even if you see an error, your VPN may be actually capable of unblocking your chosen service.

Sometimes, you'll find that not every server works, so trying a different server is often all it takes. If you're having problems, you can ask your VPN's support team for help directly. The best providers offer 24/7 live chat, so you can often be up and running in a matter of minutes.

What services can I access abroad with a VPN?

With the right VPN, you can access a huge variety of geo-blocked sites and services from anywhere in the world. Below, we've listed some of the types of geo-restricted content you can unblock:

- TV streaming sites ([Netflix](#), Hulu, [BBC iPlayer](#), [Amazon Prime Video](#))
- Sports streaming sites ([ESPN](#), [beIN Sports](#), Sportsnet)
- Social media (Facebook, Twitter, Instagram)
- Gambling and gaming sites (Bet365, SkyBet, Steam)
- Messaging services (WhatsApp, [Telegram](#))
- Dating services (Tinder, Match, PlentyOfFish)
- News websites (NYTimes, Washington Post, The Guardian)
- Privacy websites (NordVPN, Comparitech, OpenVPN)

Can I bypass VPN blocks to watch US shows?

If you're an American traveling abroad, you may find yourself unable to stream your favorite [US TV shows](#). Luckily, despite most streaming platforms cracking down on VPNs, there are still a few providers that excel at beating regional restrictions. Note that while many VPNs prioritize the ability to access US streaming services, they usually also work with platforms from the UK, Canada, Australia, and other countries, at least to some extent.

What VPN allows me to watch Hotstar India?

There are actually quite a few VPNs that work with [Hotstar India](#) (also known as Disney+ Hotstar). These

include [NordVPN](#), [Surfshark](#), and [ExpressVPN](#), but in our experience, most major providers with Indian servers have worked. If you're having trouble using this service, we'd encourage you to contact your VPN's support team and ask if there's a specific server that can unblock Disney+ Hotstar.

Is it legal to bypass geo-blocking?

Most countries don't specifically have laws against using a VPN to access geo-restricted content. After all, VPNs are legitimate privacy tools used by millions of people every day; criminalizing everyone who inadvertently tried to watch TV while connected would be madness.

It's worth noting that using a VPN is against most streaming platforms' terms of service. Still, even if a service detects that you're connected (which isn't guaranteed), there are no real consequences. You'll usually just be asked to disconnect, rather than banned.

Disclaimer: While we've researched this topic extensively, we are not legal experts and cannot account for every country's laws. As such, nothing we've said above should be considered legal advice.

Our Methodology: Choosing the right VPN to get around geo-blocking

Unfortunately, you can't just use the first VPN you stumble across if you're looking to access geo-blocked services securely. First off, there's no guarantee that your provider will be fast or secure enough. Further, geo-blocked platforms have gotten very good at

identifying VPN traffic, so most services won't work. Here are some of the main qualities a suitable VPN should have:

- **An expansive network:** The more countries there are to choose from, the wider the range of platforms you can (theoretically) access. We also look for VPNs with lots of servers in high-traffic areas like [the US](#), since this helps prevent network congestion during peak times.
- **Quick and reliable speeds:** Your VPN could be the best at bypassing geo-restrictions, but if it's too slow, it's useless. Our team regularly tests providers to see [which VPNs are fastest](#), and crucially, we look at consistency as well. This way, there's as little trial and error as possible.
- **Versatility:** We prefer VPNs that work with lots of services. If a provider is blocked by popular platforms like Netflix, Hulu, HBO Max, or Disney Plus, we probably won't recommend it. Additionally, our top VPNs must allow [torrenting](#), since there's really no easy way to do so safely otherwise.
- **Powerful security tools:** 256-bit encryption, leak protection, a [kill switch](#), and a [no-logs policy](#) are non-negotiable. These provide a solid level of protection against snoopers, but we welcome any additional tools that may be included.
- **A seamless user experience:** The best VPNs make it as easy to get connected as possible. Ideally, they'd offer multi-platform support, 24/7 live chat, and well-designed apps. Some even include task-specific servers while others have scrapped connection limits altogether.

This isn't everything we look for in our top VPNs; to find out more, read our full [VPN testing methodology](#)

[post](#).

How to remove geo-blocking FAQs

Will TOR help unblock geo restricted content?

Yes, changing your location with Tor is as simple as editing a single file. However, the Tor network is particularly slow, which means it's not exactly ideal for data-intensive tasks like streaming.

Instead, we recommend trying out a VPN. Plenty of these pride themselves on their ability to fly under the radar, and the top providers have been in an arms race to prove that they're the fastest lately. Setup is easier, too, and you can use a VPN on just about any device, whereas Tor is predominantly focused on desktop systems.

Should I buy a VPN for just geoblocking?

That really depends on how badly you want to access the content.

Here's the thing about VPNs: they can actually help you in lots of other ways as well. For instance, their encryption keeps your activities hidden from your service provider and stops public hotspot owners from seeing what you get up to (or blocking you from certain sites).

Because your IP address changes when you connect, hackers can't use it to pin down your location or ISP. This makes a VPN extremely helpful when torrenting,

playing online games, or blogging in a country with strict online surveillance.

Why does Netflix use geoblocking to maintain different libraries?

Netflix doesn't have the right to broadcast titles in every country around the world. Instead, it will buy the rights to show a specific TV show in select regions. Naturally, if it broadcasts these shows in countries not covered by the agreement, it could end up in hot water, which is why the service has tried so hard to block VPN users in recent years.

The problem is that this approach prevents users from streaming their usual content while traveling.

Moreover, regional Netflix libraries are not equal.

American subscribers, for instance, normally have access to [almost 6,000 titles](#), but if they decide to visit Croatia, their Netflix library will shrink to roughly half that.

How can I watch a geo-blocked video?

A VPN is the most effective way to bypass geo-blocking. It works by rerouting your internet traffic through a secure third-party server located in a different country, giving you an IP address corresponding to the server's location. This change of IP address allows you to access content that you aren't usually allowed to access.

Is geo-fencing the same as geo-blocking?

No. Geo-blocking prevents an individual from accessing a website or content based on their geographical location. [Geo-fencing](#), on the other hand, uses technology to create a virtual geographic boundary around a specific area. Once someone crosses into that area, they are then able to access certain content or blocked websites.

How are proxies and VPNs different?

While you can [hide your IP address](#) by using either a proxy or a VPN, **the main difference is that only a VPN encrypts your internet traffic**. As such, a VPN better protects your privacy and makes it harder for you to be tracked by your ISP or the government. Furthermore, a VPN sends all of your traffic through the VPN server (if you're using an app as opposed to a [browser extension](#)), while a proxy typically only routes the traffic of your browser or a specific app.











Is there geo-blocking within the EU?

Yes, geo-blocking within the EU does exist. Geo-blocking is a form of territorial discrimination whereby customers from certain countries are blocked from accessing online content or services based on their geographical location. This can take various forms, such as preventing access to websites, applications, or other digital services and restricting the sale of goods and services within the European Union (EU).

Geo-blocking is used to protect copyright applied by right holders to prevent access in specific Member States.

See also: [IP address blockers – the best free and paid services](#)

Roundup - best VPNs for beating geo blocking

	Our Score	Our Verdict
1.  NordVPN®	 4.5/5	Best VPN for changing Netflix region Get NordVPN »
2.  Surfshark®	 4.5/5	Best budget option Get Surfshark »
3.  ExpressVPN	 4.5/5	Highly versatile Get ExpressVPN »
4.  CyberGhost	 4/5	Easy to use Get CyberGhost »
5.  IPVANISH VPN	 3/5	Unlimited devices Get IPVanish »

PRIVACY ALERT: Websites you visit can find out who you are

The following information is available to any site you visit:

 Your IP Address:
155.190.54.35

Your Location:



**Sydney, New South Wales,
Australia**



**Your Internet Provider:
Cisco OpenDNS, LLC**

**This information can be used to target ads and
monitor your internet usage.**

Using a VPN will hide these details and protect your
privacy.

We recommend using [NordVPN - #1 of 72 VPNs](#) in
our tests. It offers outstanding privacy features and is
currently available at a discounted rate.

[Visit NordVPN](#)

Comments

Leave a Reply

Comment

Name *

Leave Comment

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)



- [Home](#)[Blog](#)[Our Authors](#)[Privacy policy](#)[Cookies Policy](#)[Terms of use](#)[Disclosure](#)[About Comparitech](#)[Contact Us](#)[Accessibility](#)

© 2024 Comparitech Limited. All rights reserved.
Comparitech.com is owned and operated by Comparitech Limited, a registered company in England and Wales (Company No. 09962280), Suite 3 Falcon Court Business Centre, College Road, Maidstone, Kent, ME15 6TF, United Kingdom. Telephone +44(0)333 577 0163