Social Media Apps

OFFICIAL

Please note, that all these apps and sites are legal and use of them does not indicate criminality or extremism. This briefing document is intended as a guide to different social media apps, and to raise awareness of how they have been or can be potentially misused for terrorist and extremist purposes.

TWITTER
https://about.twitter.com/

What is it: A hugely popular social media application that allows users to send and receive short posts called 'tweets', that can include pictures, videos and links which can then be commented upon and shared. Users can 'follow' other users of their choice to regularly see their tweets and timeline activity.
Who uses it: Millions of users daily, including high profile public figures such as the Queen and the US President**.**
Why they use it: To connect people and allow them to share their thoughts with a huge worldwide user base of potential followers**.**
Potential for misuse: Due to the large audience, the platform may be desirable to extremists to post content or links on and has been used for this purpose in the past. Twitter advocates removal of content that violates its rules[1] and has a public-interest exception were it will hide a tweet behind a warning.

GAB
https://gab.com/

What is it: A social network that champions free speech, individual liberty, and the free flow of information online. Similar to Twitter and Reddit, individuals can post messages and comment upon them.
Who uses it: Open to everyone who values free speech, however it has been largely linked to those with an extreme right-wing ideology and has been described as a social media haven for extremists, who find themselves unwelcome on Facebook and Twitter[2]
Why they use it: A lack of censorship is fundamental to the site.
Potential for misuse: Due to the above, Gab has been used to promote and encourage extremist behaviour. The Pittsburgh synagogue shooter posted his intentions on this app prior to the attack in which 11 people died[2.] In 2019, members of the terrorist group Sonnerkrieg Division, called for the assassination of Prince Harry on this app[3]

INSTAGRAM
https://www.instagram.com/

What is it: A photo and video social networking service, that allows users to create profiles, upload photos, create 'stories' and apply filters, tags, and hashtags for others to browse and follow themes of interest.
Who uses it: Hugely popular with all generations, many celebrity users, businesses, and organisations. Bloggers and influencers use it to promote their 'personal brands'.
Why they use it: Easy to network, follow individuals and themes of interest, useful for businesses to expand their reach and following.
Potential for misuse: Users can set their profiles to private so only approved followers can see the content, which is posted, this maybe a desirable function for those wanting to post extremist content. Reports of ISIL propaganda and the terrorist attack on the Mosque in New Zealand was identified to be present on this site[4]. Instagram advocates the removal of such content when they become aware of it.

DISCORD
https://discordapp.com/

What is it: A specialist chat and video platform established for the gaming community that allows users to set up chat groups and servers.
Who uses it: Very popular in recent times with over 250 million users. Users should be over 13 years, although this is not verified on sign up.
Why they use it: Discord provides free voice and massaging chat via virtual "servers" with a high level of security, privacy, and anonymity.
Potential for misuse: Discord has had problems with hostile behaviour and abuse within chats, with some servers being "raided" by other communities and flooded with controversial topics. In 2017 it was found that Discord had been used to plan and organize the "Unite the Right" rally in the US[5]. Discord have made steps to try and address these issues of potential misuse and have sought to remove several neo-Nazi and alt-right servers.

Wire
https://wire.com/en/

What is it: Wire is an encrypted communication and collaboration app, allowing messaging, file-sharing, video and voice calls, group calling and video conferences.
Who uses it: The app can be for personal user, or they promote use for businesses, large-scale organisations, and crisis collaboration (Wire Pro, Wire Enterprise & Wire Red)
Why they use it: Security and privacy, the app utilises end-to-end encryption and users can register using just an email address.
Potential for misuse: Similarly, to the other encrypted platforms there is potential for extremists to share content via Wire without risk of detection.

MINDS
https://www.minds.com/

What is it: A free open source social network application that values free speech and user privacy, the website urges users to "Take back control of your social media". The site uses cryptocurrency to pay users to produce content which can then be redeemed for enhanced features.
Who uses it: Those that believe Facebook and other sites take liberties with their users' personal information.
Why they use it: Content is less regulated and moderated making it easy to publish their own content of views.
Potential for misuse: Due to the lack of censorship, it has been described as a haven for the Right-Wing community. Several White Supremacist sites linked to the terrorist groups Atomwaffen Division and Feuerkrieg Division have been banned from the site for inciting violence[6]

REDDIT
https://www.reddit.com/

What is it: A social media site which allows registered members submit content to the site such as links, text posts, and images, which are then voted up or down by other members. Posts are organized into user-created boards called "subreddits", which cover a variety of topics
Who uses it: Millions of users, in particular Reddit's format is attractive to niche fan communities and interest groups.
Why they use it: The website generally lets moderators on individual subreddits make editorial decisions about what content to allow.
Potential for misuse: Due to the above, extremist propaganda and ideology has the potential to be promoted amongst associated sub-reddits. Indeed, Left and Right-Wing extremist groups have been banned from the site only to reappear under different names[7].

NIMBUZZ
http://www.nimbuzz.com/en/

What is it: An instant messaging and voice over the internet provider (similar to Skype)**.**
Who uses it: The app is currently offline however when it was up and running it had 150 million users in 200 countries. It is not clear why it went offline but there are plans to 'relaunch soon' (message has been on their Facebook page since August 2019, with no change June 2020) as Nimbuzz Kuraakani**.**
Why they use it: On launch in the early 2000's Nimbuzz was one of the only messengers compatible with older Java-based phones. It also offers discounted call rates to overseas numbers.
Potential for Misuse: While there is potential for extremists to use this app it is currently offline

FACEBOOK
https://facebook.com/

What is it: A long-established social media platform where users create a profile or groups with a brief biography and interact with 'friends'. Allows for posting of text, photos, videos, and live stories which friends can 'like' and comment upon**,** as well as online shopping and selling.
Who uses it: Very widespread but tends to be an older user base.
Why they use it: Facebook is very popular, comprehensive, and well- established. Messenger also allows for end to end encrypted messaging and free video and voice calls.
Potential for misuse: Users can set their profiles to private so only approved friends can see posts; this may be a desirable function for those wanting to post extremist content. Group pages can be set up to allow people of a similar interest to discus and post content.

Social Media Apps

Please note, that all these apps and sites are legal and use of them does not indicate criminality or extremism. This briefing document is intended as a guide to different social media apps, and to raise awareness of how they have been or can be potentially misused for terrorist and extremist purposes.

TELEGRAM
https://telegram.org/

What is it: An instant messaging company run by the two Russian brothers who also own VK. It is an encrypted, cloud based communications app that can be used to send text messages and multimedia such as pictures and videos. Users can send to individuals or group chats and have unique usernames.
Who uses it: Those who believe in the ethos of the site and believe strongly in free speech resulting in extreme content.
Why they use it: The ability to promote their views with very low levels of censorship.
Potential for misuse: The Christchurch shooting video[8] and copycat one in Halle Germany during 2019[9] were also available to view. In 2015 ISIS were very active on this site, supported with a defence of free speech[10]

SNAPCHAT
https://www.snapchat.com/

What is it: A very popular multi-media messaging app that allows pictures and videos to be sent between users and for 'stories' to be uploaded for friends or the entire platform to see. This app also contains a location feature which allows the users to see where friends are located, and also different multi-media stories all over the world.
Who uses it: Very popular with young users, particular teenagers, though it has been somewhat overshadowed by TikTok (see below).
Why they use it: Short messages or videos can be sent that disappear after a few seconds (decided by the sender). Such ephemeral messaging provides an element of privacy.
Potential for misuse: the use of videos and ephemeral messaging was popular with Al Qaida promoting their cause[11].

YOUTUBE
https://www.youtube.com/

What is it: The world's largest video chatting website that allows users to upload and view videos for entertainment or education. Users can subscribe to their favourite channels which then fill their feed with the latest relevant content.
Who uses it: After BBC 1 and ITV, YouTube is the next most popular channel watched by British adults[12]
Why they use: The huge and ever expanding content means that there is a video for almost any search term. The breadth of content means that for many people YouTube is a strong compliment to, or total replacement for conventional TV.
Potential for misuse: Due to the volume of content YouTube is challenging to moderate, for instance videos of the Christchurch shooting appeared here before being taken down by administrators[13]

KIK MESSENGER
https://www.kik.com/

What is it: A Canadian instant messaging app for phones that allows the sending of text, pictures, and videos and group chats.
Who uses it: Very popular with teenagers.
Why they use it: Anonymity is paramount with users able to register without a phone number or a valid email.
Potential for misuse: While the app is anonymous the communication is not encrypted, and the system does log the users IP address. As such while abuse is possible Kik represents a less secure platform than some other apps

TAMTAM MESSENGER
No official website

What is it: A new Russian based instant messaging app that allows the sending of text photos and videos.
Who uses it: A relatively new app that is similar to other messaging apps such as Telegram, and provides a substitute for it whilst the Russian authorities are cracking down on Telegram[14]
Why they use it: It is new, and the user base continues to rise.
Potential for misuse: ISIS used this application to claim responsibility for the London Bridge attack in June 2017 with 8 deaths plus the 3 terrorists[15]

BCM MESSENGER
No official website

What is it: New, highly secure instant messaging application, "by hackers for hackers"- according to their Twitter page[16]
Who uses it: Those who are concerned with anonymity.
Why they use it: No phone or email link to the user. Uses the same block chain encryption that is used by the bitcoin cryptocurrency.
Potential for misuse: ISIS alleged to be using it to distribute videos after being banned from the Telegram app[17]

WHATSAPP
https://www.whatsapp.com/

What is it: An instant messaging service now owned by Facebook that allows user to send text, voice notes, photos, and videos to other people or within a group chat. The app also allows for video chat.
Who uses it: Large user base, this is the world's most popular messaging service.
Why they use it: Privacy is very important, and all messages are end to end encrypted.
Potential for misuse: The November 2015 Paris attacks were discussed on this platform prior to the event, as were the 2017 Westminster bridge attacks in London**,** causing the then Home Secretary Amber Rudd to call for police and security service access to these encrypted emails (Though see "Security Apps" below)[18]

ZERONET
https://zeronet.io/

What is it: Marketed as a 'peer to peer' decentralised network, i.e. there is no central controlling moderator just that which exists between individuals using the site. The website promotes it as providing a platform for 'un-censorable content' generated by the users.
Who uses it: Those looking for security and anonymity and who are attracted to the concept of a decentralised network.
Why they use it: It takes the security of its users very seriously, including cryptography associated with the bitcoin cryptocurrency and the BitTorrent' network.
Potential for misuse: Islamic State has experimented with using this application due to its security and lack of censorship[19].

ROCKETCHAT
https://rocket.chat/

What is it: An instant messaging application from 2018. It is open source meaning it is free to all to download from the internet.
Who uses it: Aimed at the business community and other groups.
Why they use it: Being open source means that it can be customised to suit a particular customers' needs
Potential for misuse: Rocket chat was used by ISIS before they moved onto TamTam[20]

Social Media Apps

Please note, that all these apps and sites are legal and use of them does not indicate criminality or extremism. This briefing document is intended as a guide to different social media apps, and to raise awareness of how they have been or can be potentially misused for terrorist and extremist purposes.

MASTODON
https://joinmastodon.org/

What is it: A self-hosted social networking service that allows users to create their own networks
Who uses it: Those interested in this type of social networking structuring.
Why they use it: It represents a different and more flexible way of social networking.
Potential for misuse: The Mastodon service was linked to GAB for a brief period before they moved to distance themselves from the Right-wing platform[21]

STEEMIT
https://steemit.com/

What is it: A blogging and social media app based around the use of cryptocurrency and the decentralisation of wealth. The app rewards users with cryptocurrency for producing blogging content.
Who uses it: Those who view the decentralisation of wealth and power as a goal in and of itself.
Why they use it: Security is paramount through the use of block chain encryption, and interaction with others' content raises its profile and therefore value in bitcoin currency.
Potential for misuse: While there is potential for use in raising cryptocurrency, there is no known association with extremism or terrorism at this time.

ZOOM
https://zoom.us/

What is it: An American video communications technology company that provides video teleconferencing and online chat.
Who uses it: This application has become hugely popular since the advent of the covid-19 lockdown.
Why they use it: Provides video connectivity of friends and family groups and education for children which has become very important in lockdown. Passwords and group identification provide strong security.
Potential for misuse: 'Zoom bombing' is the term given to the process of hacking into other peoples' meetings that have not been properly secured and posting extreme and/or offensive content. The resulting responses have then been shared on YouTube and other platforms[22].

TIKTOK
https://www.tiktok.com/

What is it: A hugely popular Chinese based social video sharing app that allows for the uploading, viewing, and commenting on short videos between 3 and 15 seconds.
Who uses it: Extremely popular, but especially with those under 25.
Why they use it: Seen as a fun app, particularly during lockdown.
Potential for misuse: Islamic state militants posted short propaganda videos including corpses being carried through the streets either within other videos or as stand-alone videos[23]. The US-based Boogaloo group have posted material on TikTok[24]

4CHAN
http://www.4chan.org/

What is it: An anonymous image board social media website. Divided into "boards" on various subjects. Threads within a board move up a ranking relative to the number of replies and move down over time.
Who uses it: Hugely popular with tens of millions of users monthly. The "Politically incorrect" board in particular is popular with Right-Wing users espousing violence, misogyny, racism, and Anti-Semitism.
Why they use it: Anonymity is the main reason, users are not able to create accounts and identifying themselves is a bannable offence.
Potential for misuse: The anonymity is open to abuse and there have been numerous instances of extremist material being uploaded and celebrated. Both the Toronto van attack which killed 11[25] and the Umpqua Community College Shooting[26] were discussed on the site prior to being carried out. The site does record IP addresses of posters, so anonymity is not completely guaranteed.

8KUN (8CHAN)
No official website

What is it: An anonymous image board social media website. Threads on any subject can be posted similar to 4Chan.
Who uses it: 8kun was created in 2013 in response to perceived censorship online. Popular with those with extreme Right-Wing views and those banned from 4chan.
Why they use it: Anonymity allows for extreme views to flourish.
Potential for misuse: Messages boards promoting child abuse led to it being blacklisted from google searches. The message boards have been found to promote mass shootings and the manifestos of the perpetrators prior to the events – links were posted to the Christchurch[27] live streaming on Facebook, being applauded and widely shared from this site. The El Paso Walmart shooting manifesto was uploaded to this site hours before the massacre occurred[28]

VK
https://vk.com/

What is it: One of the largest social media networking sites in Russia, run by the brothers who also host the Telegram app. Social media and social networking service, similar in scope to Facebook. Allows for both public and private messaging.
Who uses it: Mainly Russian language speakers, but globally ranked second only to Facebook. As of August 2018, had over 500M accounts and 97M monthly active users?
Why they use it: Available in multiple languages throughout the former Soviet Union.
Potential for misuse: Quoted as a place where terrorists go to spread their message when they have been removed from other sites[29].Few laws surrounding copyright and the storage of IPs as a Russian company.

KAG.SOCIAL
https://kag.social/

What is it: A niche social media group with the "Keep America Great" campaign for the 2020 US election, being the successor of "Make America Great Again" and Donald Trump.
Who uses it: Social media for the right wing of US politics and those supporting the ideals of Donald Trump.
Why they use it: Support network for the US presidential campaign.
Potential for misuse: None specific to this service, this app has no known association with extremism or terrorism.

HOUSEPARTY
https://houseparty.com/

What is it: A video chatting service, new in 2019 that enables registered users to video chat and join each other's 'house parties'. Users are notified when someone is 'in the house'.
Who uses it: Very popular since the outbreak of the current pandemic
Why they use it: Very easy to use, without the security steps that are required by others such as Zoom.
Potential for misuse: None specific to this service, this app has no known association with extremism or terrorism.

Social Media Apps

OFFICIAL

Please note, that all these apps and sites are legal and use of them does not indicate criminality or extremism. This briefing document is intended as a guide to different social media apps, and to raise awareness of how they have been or can be potentially misused for terrorist and extremist purposes.

VIBER
https://www.viber.com/en/

What is it: A popular instant messaging app that allows the use of text photos and videos and calls.
Who uses it: Popular worldwide with those concerned with privacy.
Why they use it: End to end encryption of messages, and self-destruct features for messages, similar to that of snapchat.
Potential for misuse: Many of these sites have potential for use by terrorists because of the their levels of security and factors such as self destructive messaging which has obvious attractions. ISIS using it as they move onto less popular platforms to more widely spread their message[30].

SKYPE
https://www.skype.com/en/

What is it: One of the earlier free applications that provides video chat, voice calls and instant messaging. This can be accessed between computers, phones, tablets, smart watches and Xbox One etc.
Who uses it: In March 2020 Skype was used by over 40 million people on a daily basis due to the Covid- 19 outbreak. Skype for business is widely used by companies.
Why they use it: Skype is a long-running and easily accessible communications app.
Potential for misuse: Sudesh AMMAN who carried out the Streatham terror attack 2020, was sharing bomb making literature via Skype messenger[31]

PALTALK
https://www.paltalk.com/

What is it: A video chat service that allows users to form groups for video chats and text, it is similar to several other messaging/chat apps.
Who uses it: The app is said to have over 100 million users as of 2015.
Why they use it: Users can host text chat rooms with potentially thousands of users and video chats of up to fifteen.
Potential for misuse: it is quoted as a place where terrorists can go to disseminate material and further their cause due to its relative anonymity[32]. However in 2013 Paltalk was targeted by the US National Security agency, who allegedly siphoned data from the system.[33]

TWITCH
https://www.twitch.tv/

What is it: A video live streaming service owned by Amazon that allows users to livestream their own video games or watch others, often used for instructional gaming and recreation.
Who uses it: The gaming community and professional 'e-sports' as well as conventional sports for live game streaming.
Why they use it: Live streaming is very popular and allows the watching of sports not available on other platforms.
Potential for misuse: As streams are broadcast live it can be challenging to moderate them as any takedowns need to be near instantaneous to be effective. Live streaming of the Christchurch massacre was shown on this platform within a little used gaming section under misleading titles to hide its content before being removed by the site[34]

QQ
https://im.qq.com/

What is it: A Chinese instant messaging and social media service, also known as TencentQQ. The full range of social media services including microblogging and online games.
Who uses it: TencentQQ holds the Guinness world record for the highest number of simultaneous users of over 200 million.
Why they use it: Used in over 80 countries and has a built in translator
Potential for misuse: Use of QQ is tracked and shared with Chinese authorities and QQ likely censors material which is 'politically sensitive' to the government of China. [39]

SIGNAL
https://signal.org/en/

What is it: An instant messaging service that allows the sending of pictures and videos, with an emphasis on security.
Who uses it: Edward Snowden (the US Whistle blower) had repeatedly endorsed it and the European Commission recommended that their staff switch to it this year.
Why they use it: Advanced end to end encryption, and no messages are stored on the servers.
Potential for misuse: None specific to this service, though it is heavily encrypted. This app has no known association with extremism or terrorism.

THREEMA
https://threema.ch/en

What is it: An instant messaging service that enables the sending of texts, pictures, and videos. Threema is an independent Swiss company hosting its own servers in Switzerland for 'Seriously secure messaging'.
Who uses it: Those who demand high security and anonymity.
Why they use it: Users can create an identity which does not require an email or a phone number.
Potential for misuse: Pictures of the dead from the Islamic State attack in Bangladesh that killed 29 people in July 2016 were shared during the attack[35] and the attack was discussed prior to the event[36]

WECHAT
https://www.wechat.com/en/

What is it: A Chinese instant messaging and social media site owned by Tencent. The app can link in with other networks such as TencentQQ and Facebook and has a huge range of options having been compared favourably to WhatsApp.
Who uses it: One billion monthly active users
Why they use it: Wechat is China's largest social media app, alternatives are frequently blocked in China.
Potential for misuse: Use of WeChat is tracked and shared with Chinese authorities[37] and censors material which is 'politically sensitive' to the government of China.[38]

Tumblr
https://www.tumblr.com

What is it: tumblr is a micro-blogging and social media site, allowing users to post text and multimedia content to a short blog. It also incorporates messaging and group text chat.
Who uses it: tumblr hosts millions of blogs and is reported in pop culture as having something of a progressive userbase[40]
Why they use it: tumblr is popular with special interest groups and fan communities to share content. tumblr blogs can link to Twitter and Facebook, automatically updating when the blog does.
Potential for misuse: None specific to this service, this app has no known association with extremism or terrorism. The site has been criticised for allowing users to stifle discourse and there have been instances of raiding and bullying from tumblr users[41]

Social Media Apps

Please note, that all these apps and sites are legal and use of them does not indicate criminality or extremism. This briefing document is intended as a guide to different social media apps, and to raise awareness of how they have been or can be potentially misused for terrorist and extremist purposes.

ProtonMail

https://protonmail.com/

What is it: Secure email service.

Who uses it: Scottish Dawn[42]

Why they use it: Uses end-to-end encryption and client-side encryption, two-factor authentication, allows users to have 50 aliases/addresses[43]. ProtonMail has mentioned in recent media Mr. Robot[44] (2015 & 2017) and Knives Out[45] (2019), bringing light to the service and potentially widening it's userbase. Servers are located in Switzerland, making all user data protected by Swiss privacy laws[46].

Potential for misuse: No personal information is required to create an account. They do not store any IP logs[46]. End-to-end encryption means that ProtonMail cannot provide public bodies with a user's data, messages, or passwords.

Tutanota

https://tutanota.com/

What is it: Secure email service that offers end-to-end encryption and two-factor-authentication.

Who uses it: Scottish Dawn[42] [47]

Why they use it: The end-to-end encryption means that neither public bodies nor the company themselves can access or view content shared within the software. Only the device the content is shared on and the device it is shared to can view the content.

Potential for misuse: No personal information or phone numbers are required to make an account. Offers the world's first end-to-end encrypted calendar (*zero-knowledge calendar*[48]) which encrypts all data including attendees and notifications, potentially allowing extremist groups to plan and organise events with the security of end-to-end encryption.

Wickr

https://wickr.com/

What is it: Instant messenger application. Allows users to send end-to-end encrypted and content-expiring messages, including photos, videos, and file attachments. Allows users to send secure links, revoke messages; has screen shot detection[49].

Who uses it: Used by a variety of people including celebrities. Promoted by celebrity Iggy Azalea, potentially boosting its userbase[47] and has become popular with drug dealers[51]

Why they use it: Wickr saves no information to a server and no data on its users[50].

Potential for misuse: Used by drug dealers[51] because of the anonymity and end-to-end encryption. Messages can be set to automatically destruct after a set amount of time, making it unviewable to anyone[47].

BitChute

https://www.bitchute.com/

What is it? A video hosting service, similar to YouTube, that accommodates far-right content. It was created in 2017 in England by Ray Vahey[53]. It was created in response to You tube's content rules regarding hateful content. BitChute allows its users to monetise their content by letting them link their PayPal and cryptocurrency processors[54].

Who uses it? Predominantly used by the Right Wing

Why do they use it? BitChute describes itself as a "free speech" website[55]. It has become a "major platform for neo-Nazi videos, racism, violence, conspiracy theories and […] terrorist propaganda[55].

Potential for misuse: BitChute not only allows but encourages its Far Right userbase. BitChute's official Facebook account boasted hosting Tommy Robinson, co-founder of EDL, on their platform[55]. Independent research conducted by *Hope Not Hate* found numerous videos supporting terrorist groups, including ISIL, NA, AQ, etc[54].

Odysee

https://odysee.com/

What is it: A **v**ideo hosting site.

Who uses it: Far-right and extremists

Why they use it: Allows content that would otherwise be removed from other streaming services, such as YouTube. Odysee's approach to content moderation has been described as "no censorship, no deplatforming, no matter what users say"[56]

Potential for misuse: Content on the site is not moderated, allowing individuals with extremist ideologies to spread their rhetoric to a wider audience.

Dlive

https://dlive.tv/

What is it: Video live streaming service. Allows for donations and subscriptions to content creators.

Who uses it: Popular among White Nationalists, conspiracy theorists and neo-Nazis[57]

Why they use it: Dlive has a lax enforcement of prohibited content guidelines.

Potential for misuse: Little to no moderation of content allows content creators with extremist ideologies to say and do as they please with no consequences. Dlive has been used to promote Far Right ideologies. Dlive was used to livestream the storming of the US Capitol on 06/01/2021, with one streamer earning more than $2000 in donations from viewers [57].

Social media apps

Please note, that all these apps and sites are legal and use of them does not indicate criminality or extremism. This briefing document is intended as a guide to different social media apps, and to raise awareness of how they have been or can be potentially misused for terrorist and extremist purposes.

Element
https://element.io/

What is it: Element is an End to End encrypted messaging app with unlimited voice and video. It is built on Matrix, which is an open network for secure, decentralised communication, connecting 42m+ users over 80k+ deployments. You are able to file share securely with encrypted data[58].

Who uses it: It is now estimated that over 42 million individuals, companies and government use this app to protect their communication[59]. Like all apps and messaging platforms, Element is widely used by the general population as well as business services. As yet, it is unclear if extremist or politically motivated individuals/groups specifically use Element to communicate/spread awareness of their ideology.

Why is it used: The app promotes itself as being different from other messaging and collaboration apps due to it operating on Matrix, an open network for secure messaging and decentralised communication. It allows self-hosting to give users maximum ownership and control of their data and messages. It also allows for users to search for other users with criteria such as names, email addresses or usernames using the full matrix e.g., @billywhite:matrix.org or send an invite link. Users can also create a new room (or a group chat) or explore public rooms[60].

Potential for misuse: CTPNE Internet Intelligence Investigations noted that last year, the app was suspended from the Google Play Store, potentially due to some abusive content that was easily accessible. These issues have been resolved and the app is available to download from the Google store. Element Android is an open source project and is hosted by GitHub[61].

GETTR
https://www.gettr.com/onboarding

What is it: GETTR appears to be a social media platform and microblogging website. It was officially launched on 04/07/2021 and it's user interface and features have been described as very similar to those of Twitter[62] . It's official site advertises itself to be the 'marketplace of ideas' and goes on to describes GETTR as a brand new social media platform founded on the principles of free speech, independent thought and rejecting political censorship and "cancel culture." [63] *Comment: Cancel culture is a prevailing ideation forming in America that describes the act of ''cancelling" one out, usually a public figure, due to their unpopular, even offensive, views or opinions on a given topic or event. They may then be subject to polarisation, or boycotting, from the public on social media and be revoked from their cultural cachet. So much so, that it may affect their careers or public sway.*

Who uses it: Open source research would suggest that the site is primarily used by American conservatives, perhaps due to the founder, Jason Miller, being a former Donald Trump aide. It does not appear that the site is used as a main platform by any one group, however due to its association with freedom of speech and –pro-Trump; foundation, it could be suggested that the site may host individuals promoting far right political opinions, views and/or values.

Why is it used: The social media site has been described as having a striking similarity with Twitter. It may, therefore, be easier for those who are familiar with navigating Twitter as they find the familiarity comforting when using Gettr. As described above, the site also promotes the use of free-speech and promises not to 'cancel' people out should they wish to share their opinions or political views.

Potential for misuse: Whilst no discernible groups have been identified as using the site as a main platform, tech companies such as TechCrunch+ have described the site as being 'pro-Trump' and 'a mess [64] as it was thought that hackers were quick to scrape sensitive personal information of its users including birthdays, names and email addresses, as well as creating 'fake' accounts. Others list internet trolls flooding the site with pornography and the brief hacking of high-profile accounts. Some journalists have observed the prevalence of extreme content on the platform, including racism, antisemitism, and terrorist propaganda[65].

Security Apps

This page is intended as a guide to common online security tools, either for personal use or to raise awareness when dealing with the public. It is not a substitute for security advice.

- Password Lockers and End to End encryption are common for ordinary users and are relatively ordinary security practices.
- VPN's and TOR are less common.

With the possible exceptions of Password Managers these items could be abused for criminal purposes, i.e., concealing criminal activity. This does not necessarily mean their usage is primarily, or even predominantly, criminal and each case should be examined in context.

Password Managers

https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

What are they? A password manager stores your passwords in an encrypted file, generally backed up to a cloud storage service such as Dropbox, OneDrive, or Google Drive. They usually work across all your devices. The manager can be opened by a single password, or via a fingerprint or facial recognition.

What Problem do they Solve? Online services require dozens of accounts, and no one can memorize hundreds of strong passwords. Users often use the same password for each one. Users can also forget accounts they only use infrequently, having to reset their password over and over.
Outdated advice to "change our passwords regularly" isn't likely to help, if someone gets your password they generally use it right away.

Why use One? A password manager removes reliance on memory, you can generate hundreds of very strong passwords and input them automatically. No more coming back to an online store after two years and needing a password reset. Secondly it ensures your passwords are all unique and impossible to guess.

What do They Cost? Password managers are relatively inexpensive and basic models can be found for free. There is a potential cost if you forget the password to unlock the manager itself, you'd then need to reset all your passwords and start over.
Of the tools discussed here a Password Managers are relatively obscure but provide great security benefits. By themselves they increase security significantly.

End to End Encryption

What is it? End to End encryption is a means of sending messages without eavesdroppers being able to read them. Sending data unencrypted is the equivalent of sending a postcard, anyone can read it if they know how to look. Encrypted data is the equivalent of sending your message in code.

What Problem Does it Solve? Internet data can be intercepted, but financial and valuable data needs to be sent safely online. If this kind of encryption did not exist the internet would be useless for jobs such as online banking, shopping, and sending personal information.
Generally speaking, there is no such thing as a 'backdoor' into encrypted data, something is either encrypted or it isn't. Having a 'backdoor' would be the equivalent of locking your doors but opening your windows. It is mathematically impossible to have a 'backdoor' in encryption which police can access and criminals cannot.

Why use it? You probably already do without realizing, almost every website uses end to end encryption in its basic operation (Anything with https in the URL uses this). Businesses like shops, banks and social media generally use this technology in the background. If you are sending information which you would not wish to be made public you should check you are on a secure platform.

What does it Cost? End to End Encryption is almost everywhere, common apps such as WhatsApp, Facebook Messenger and Discord use it. Generally speaking, there is no cost and it is essentially standard practice. Storage can also be encrypted, again this is typically something that can be done by free apps or which is integrated into devices as standard. The internet as we know it would not function without end to end encryption.

Virtual Private Networks (VPN)

What is it? A VPN uses End to End encryption (See above) to connect your device to another computer and send web traffic through it. This means, in theory, that your data cannot be intercepted.

What Problem do they Solve? Internet providers can typically see and monitor unsecured internet traffic (Typically just the first part of the URL) that flows through them. VPN's privatise this traffic and hide your usage.

Why use One? In the past numerous exploits have been used to compromise internet security, for instance man in the middle type attacks could intercept data on public wifi. VPNs were intended to prevent this, keeping data private, however these exploits have since been patched. VPN's can also make it look like you are in another country, this is typically advertised as a means to bypass region locking and this is likely the main utility of VPN's.
Updates to modern internet security have addressed many of the security issues VPN's were originally intended to deal with. Furthermore, a VPN potentially represents a single point of failure with all data being routed through a single place. With security loopholes having been closed and several VPN providers having recently been acquired by large companies with inconsistent track records their use is now somewhat questionable in general.

What do They Cost? While there are free options these tend to be very limited. Paid options can become expensive so whether a VPN is worthwhile depends on the user.
By their nature VPN's are somewhat slower than a standard connection. Ordinary browsing and streaming is usually fine; but intense usage such as gaming, high definition streaming or live video can be obstructed.

The Onion Router (TOR) Browser

What is it? TOR is an anonymous browser that encrypts your internet traffic and routes it through a global network of other computers. It uses layers of end to end encryption (See above) so that the intermediate computers don't know what they're sending.

What Problem does it Solve? TOR attempts to remove identifying information from your connection and makes it more difficult to trace activity to you. This is intended to protect the privacy of users.

Why use it? TOR can be used to send data and browse anonymously, making it attractive to activists, journalists or whistle-blowers wishing to remain anonymous.
It can also connect to 'Darknet' sites, which cannot be reached by ordinary browsers. This aspect of TOR is frequently used to distribute illegal content. While TOR itself is legal to use it can access illegal content ordinary browsers can't reach.

What does it Cost? TOR itself is free to use. However, as TOR sends data through several intermediaries it is much slower than a standard connection. Browsing and streaming will be slow, intense usage such as gaming, high definition streaming or live video may fail altogether.

Unless the data you are sending and receiving is extremely sensitive there is little reason to use TOR.

Social Media Apps

References

1. https://help.twitter.com/en/rules-and-policies/violent-groups
2. https://www.washingtonpost.com/technology/2018/10/28/how-gab-became-white-supremacist-sanctuary-before-it-was-linked-pittsburgh-suspect/
3. https://www.independent.co.uk/news/uk/crime/neo-nazi-trial-terror-prince-harry-michal-szewczuk-oskar-dunn-koczorowski-a8963396.html
4. https://www.telegraph.co.uk/news/2019/05/11/isil-extremists-using-instagram-promote-jihad-incite-support/
5. https://www.nytimes.com/2017/08/15/technology/discord-chat-app-alt-right.html
6. https://www.vice.com/en_ca/article/wjvp8y/minds-the-anti-facebook-has-no-idea-what-to-do-about-all-the-neo-nazis
7. https://www.splcenter.org/hatewatch/2018/04/19/day-trope-white-nationalist-memes-thrive-reddits-rthedonald
8. https://www.chicagotribune.com/nation-world/ct-mosque-killer-white-supremacy-20190315-story.html
9. https://www.chicagotribune.com/nation-world/ct-mosque-killer-white-supremacy-20190315-story.html
10. https://www.wired.co.uk/article/isis-telegram-security
11. The New Arab, 19/09/2017 ONLINE
12. https://inews.co.uk/culture/television/watching-actual-tv-is-still-vastly-more-popular-than-streaming-or-youtube-ofcom-says-323573
13. https://www.chicagotribune.com/nation-world/ct-mosque-killer-white-supremacy-20190315-story.html
14. https://theprint.in/tech/tamtam-is-new-isis-favourite-after-leaving-telegram-london-bridge-attack-was-claimed-here/328728/
15. https://theprint.in/tech/tamtam-is-new-isis-favourite-after-leaving-telegram-london-bridge-attack-was-claimed-here/328728/
16. https://twitter.com/bcm_social?lang=en
17. Fearn, M., 16/12/2019 Decrypt ONLINE
18. https://www.theguardian.com/technology/2017/mar/26/intelligence-services-access-whatsapp-amber-rudd-westminster-attack-encrypted-messaging
19. Europol Conference Paper, King, P., 09/04/2019
20. https://theprint.in/tech/tamtam-is-new-isis-favourite-after-leaving-telegram-london-bridge-attack-was-claimed-here/328728/
21. https://www.vice.com/en_us/article/mb8y3x/the-nazi-free-alternative-to-twitter-is-now-home-to-the-biggest-far-right-social-network
22. Nguyen, N 02/04/2020 The Wall St Journal online.
23. Hannah Boland, 22/10/2019 The Telegraph online
24. https://www.bbc.com/news/technology-53269361
25. https://www.latimes.com/local/lanow/la-me-ln-elliot-rodger-incel-20180426-story.html
26. https://www.ibtimes.co.uk/oregon-shooting-did-4chan-trolls-incite-chris-harper-mercer-massacre-umpqua-community-college-1522163
27. New York Times, 14/03/2019 ONLINE
28. BBC News 05/08/2019 ONLINE
29. Nikita Malik 18/10/2018 Forbes .com online
30. Rita KATZ, 01/09/2019 Wired.com online
31. David Mercer, 07/02/2020 Sky News online
32. https://www.forbes.com/sites/nikitamalik/2018/10/18/where-do-terrorists-go-when-they-are-kicked-off-social-media-platforms/#2bc228143e9c
33. https://eu.usatoday.com/story/news/2013/06/06/nsa-surveillance-internet-companies/2398345/
34. Bagchi, I. 06/07/2016, The Times of India online
35. 06/07/2016 BBC news online
36. Marshall, C. 27/05/2019 Polygon ONLINE
37. https://www.wired.com/story/inside-chinas-massive-surveillance-operation/
38. https://qz.com/960948/what-happens-when-you-try-to-send-politically-sensitive-messages-on-wechat/
39. https://web.archive.org/web/20130316125952/http://surveillance.rsf.org/en/china/
40. https://psmag.com/social-justice/how-tumblr-taught-social-justice-to-a-generation-of-teenagers
41. https://www.vice.com/en/article/3da838/an-attempted-suicide-forced-a-tumblr-community-to-open-its-eyes-about-bullying
42. https://theferret.scot/revealed-neo-nazi-terrorists-are-behind-scotlands-newest-far-right-group/
43. https://protonmail.com/pricing
44. https://protonmail.com/blog/protonmail-mr-robot-secure-email/
45. https://twitter.com/protonmail/status/1204465589579898885?lang=en
46. https://www.echosec.net/blog/what-is-vk-and-why-should-you-care
47. https://www.dailymail.co.uk/news/article-9529545/Neo-Nazi-British-police-officer-jailed-four-years-four-months.html
48. https://tutanota.com/blog/posts/most-secure-email-service
49. https://wickr.com/security/
50. https://www.theguardian.com/australia-news/australia-news-blog/2015/mar/02/wickr-the-secret-messaging-app-of-the-party-unfaithful
51. https://www.verdict.co.uk/what-is-wickr/
52. https://support.wickr.com/hc/en-us/articles/115004958907-Does-Wickr-cooperate-with-the-government-or-law-enforcement-
53. https://en.wikipedia.org/wiki/BitChute#
54. https://www.bellingcat.com/news/uk-and-europe/2021/02/24/the-websites-sustaining-britains-far-right-influencers/
55. https://www.independent.co.uk/news/uk/home-news/bitchute-far-right-youtube-neo-nazi-terrorism-videos-a9632981.html
56. https://en.wikipedia.org/wiki/LBRY
57. https://en.wikipedia.org/wiki/DLive
58. CTPNE Internet Intelligence Investigations Report, New App: ELEMENT, 16/02/2022
59. https://element.io
60. CTPNE Internet Intelligence Investigations Report, New App: ELEMENT, 16/02/2022
61. CTPNE Internet Intelligence Investigations Report, New App: ELEMENT, 16/02/2022
62. https://en.Wikipedia.org/wiki/Gettr

Glossary

Blockchain - is a type of database that stores data in 'clocks' that are then chained together. As new data comes in, it is entered into a new block. Once a block is filled with data, it is chained onto the previous block, making the data chained together in chronological order. Blockchain is commonly used as a ledger for transactions. It can be openly shared in a peer to peer manner amongst users to create an unchangeable record of transactions. Each transaction generates a randomised number which is then time stamped and linked to the previous transaction. Once new data is entered, it cannot be erased making Blockchain very secure. If someone were to attempt to alter a blockchain, all other copies of the blockchain would cross-reference with one another, they would notice that the altered one did not match and it would cast it out as illegitimate. Blockchain is the record-keeping technology behind the Bitcoin network.

Bitcoin - is a virtual currency which is managed using blockchains. All transactions are thus transparent to all and very secure.

Cryptocurrency – Virtual currency which can be used to transfer value anonymously, transactions are typically stored in a public blockchain (See above).

Cloud Based - Remote servers are used upon demand via the internet to access information rather than storing it on a local server hard drive.

References

63. https://www.gettr.com/onboarding
64. https://techcrunch.com
65. https://en.Wikipedia.org/wiki/Gettr

Glossary