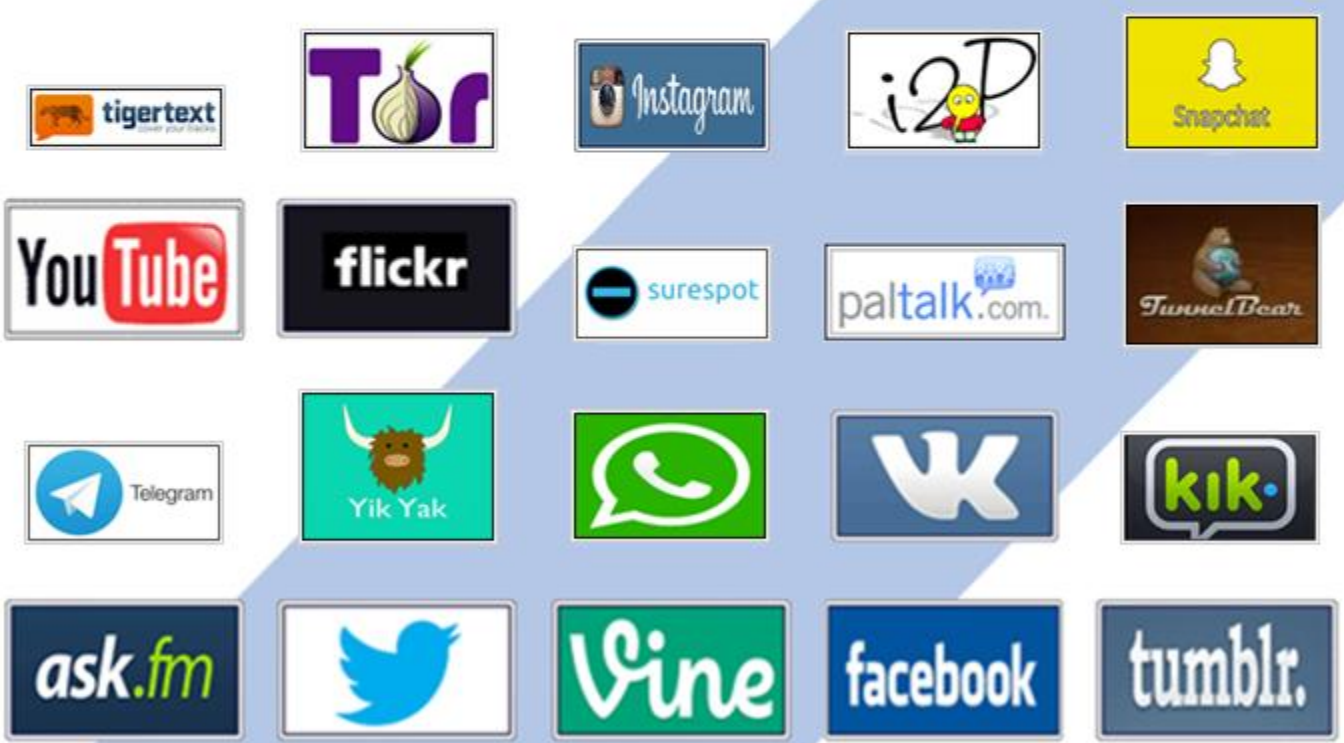
NORTH EAST
COUNTER
TERRORISM UNIT

Version 1.0

Guide to Online Applications

For Partners with a Statutory Duty for Prevent



Version Control

Version	Date	Author	Changes
1.0	27th October 2015	Josh Hopkins	Original document

Introduction

This document is intended to provide supporting information to statutory agencies with a duty towards Prevent.

This document contains an introduction to some of the more popular social media and online privacy applications; this is not an exhaustive list but is influenced by previous real-life cases. **It is important to note that <u>none</u> of the applications mentioned over the next 8 pages are illegal to access.** Gaining access is straight forward in the majority of cases; although varying levels of personal data are required to set up accounts. It is recommended that where a further understanding of any of the applications is required, readers access the respective official website where additional details can be found.

As further applications are identified they will be added to the document.

Social Media Applications: Explained

Mainstream Networking

These are the applications which contain the most content and have the best safeguarding tools; although here 'best' could mean 'more than none'. Data is stored and controlled by the companies which run the applications; personal data has to be requested by the Police but postings can be captured without applying directly to the host company.

Facebook

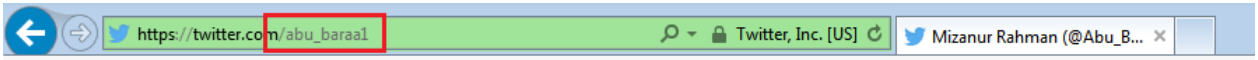
900,000,000 estimated unique monthly visitors

- Facebook is the most popular social network and generally one of the most visited websites worldwide (on many rankings it is second only to Google).
- Users have control over their account security settings, limiting who can see the information they post.
- Sign up requires a full name, date of birth and mobile number or email.
- Facebook is used by the full spectrum of extremist groups as a gateway to more secure platforms, generally such users will look to remain within the law to avoid attention.
- When reporting concerns about a user it is important to capture the account's unique ID which can be found in the page URL (as shown below). It can be very difficult to recover a post by an account with a common name like 'John Smith', as there will be 100,000s such accounts in existence.

Twitter

310,000,000 estimated unique monthly visitors

- Text (140 character limit) and media sharing platform.
- Users can privatise their accounts to control who is able to view the content.
- Sign up requires a full name and email address.
- Twitter is popular amongst members and supporters of ISIL – a 2015 study found over 46,000 such profiles.
- Twitter reacts quickly to inappropriate content by suspending or deleting accounts, however users get around this by pairing the same username with sequential numbering. I.e. 'ISILmember01' gets deleted so the user creates 'ISILmember02' and so on, thus making it easier for followers to find the new account.
- Advice for reporting concerns mirrors that for Facebook; capturing the ID from the URL (as below).



Ask fm

150,000,000 estimated unique monthly visitors

- Ask.fm is a Q&A based platform, questions can be asked anonymously but once answered by the user they can be viewed by anyone (even those without an account).
- Having been linked to a growing number of cyber-bullying cases, new safety features have been added which provide advice for users, parents and teachers.
- Ask.fm now provide a guide to law enforcement agencies wanting to request information on users.
- Sign up via Facebook, Twitter and VKontakte – or name, date of birth and email.

Social Media Applications: Explained

Mainstream Networking: Continued

Tumblr

110,000,000 estimated unique monthly visitors

- Multimedia micro-blogging platform owned by Yahoo.
- Sign up only requires an email address.
- The site offers an 'ask me anything' section in order to interact with other users, profiles can also be made private.
- English-speaking extremists based in Iraq and Syria have been observed providing advice and information on travelling to the 'Islamic State' and what to expect on arrival.
- The service has been forced to crack down on violent content, specifically relating to self-harm following the suicide of a British teenager who had a blog on the site.

VKontakte

80,000,000 estimated unique monthly visitors

- The Russian equivalent of Facebook, with many of the same features.
- Sign up requires a full name and mobile number or a Facebook account.
- Used by extremists/criminals due to the fact that data is held in Russia and therefore difficult for Western law enforcement agencies to gain access.
- User base is mainly in Russian-speaking countries so questions should be raised as to the motives of someone in this country using the site (not discounting innocent explanations).

Social Media Applications: Explained

Media Sharing

These are websites designed specifically to provide video and image sharing services, where media is uploaded to the company's servers. Generally they are used in conjunction with other social networking platforms. Content filtering can vary quite dramatically between the different sites; as a general rule the more *well-known* the site the better safeguarding measures it has in place.

YouTube

1,000,000,000 estimated unique monthly visitors

- Large volume of extremist/violent media uploaded despite YouTube's comparatively robust moderation mechanisms; content remains for a short period of time before being removed.
- Other social media sites are used to direct traffic to videos.
- Software is freely available which allows users to download content from YouTube.
- A Google Account is required to upload content and view certain flagged videos (adult content). This requires a full name, date of birth and mobile number and generates a Gmail account.

Instagram

300,000,000 estimated unique monthly visitors

- Image and short video sharing platform owned by Facebook.
- Can be synchronised with other platforms such as Tumblr and Twitter.
- The app comes with a 'direct' service which allows users to share media with other specific users (rather than anyone who happened to view their account).
- To sign up, users must download the Instagram app on an Apple or Android mobile device; they can then use the web interface (www.instagram.com).

Flickr

65,000,000 estimated unique monthly visitors

- Image and video hosting service – used to import media which can then be embedded into other websites e.g. blogs.
- Owned by Yahoo and therefore requires a Yahoo account to upload content; this requires a full name, date of birth and mobile number and generates a Yahoo email account.
- No login is required to view content, although users can control who has access to their media.
- Flickr can change the access settings for entire countries; for example German users were assigned the rights of a 'minor' in 2007.

Vine

42,000,000 estimated unique monthly visitors

- Owned by Twitter, Vine allows users to share 6-second video clips which are recorded through the app.
- Sign up requires the user to download the app on an Android, Apple or Windows device, users can also log in using a Twitter account on the web version.
- Vine states in its own terms and conditions that it does not actively monitor content, but sets out criteria for 'content boundaries'; e.g. threats, graphic content, pornography.

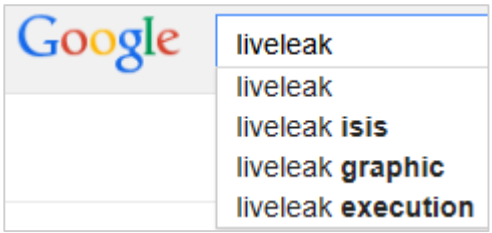
Social Media Applications: Explained

Media Sharing: Continued

LiveLeak

45,000,000 estimated unique monthly visitors

- Video streaming website known for having graphic content.



- A Google Instant (predictive) search for 'liveleak' comes up with the results to the left, demonstrating the kind of material available.
- Sign up to the site only requires an email address.
- Suggested that this site is added to 'block' lists (if not already).

Paltalk

- Video chat service that allows users to meet in large public 'rooms' (which can hold 1000s of users at once) or smaller private 'rooms' (up to 15 users).
- Content can only be viewed when the channel is 'live' – a bit like television before Sky+!
- Sign up to the full Paltalk service requires the download of a client, however a more basic version ('PaltalkExpress') is available to view on the web which requires an email address to sign up.

Ustream

- Ustream is a video streaming website, similar to Paltalk but with less facilities for 'chat' between 'hoster' (the person broadcasting) and users.
- Sign up isn't required to view publically hosted streams and users can review previous streams after their original airing.
- In order to host media, sign up is necessary which requires a Facebook account or email address.

Social Media Applications: Explained

Instant Messaging

The purpose of these apps are fairly self explanatory and are used instead of conventional SMS messaging for reasons such as avoid charges for sending messages overseas and sending information more securely (or encrypted). It is more or less common knowledge that mobile phone operators have access to SMS data *including content* and therefore the use of the service is in decline in favour of the apps mentioned in this section.

WhatsApp

800,000,000 active users

- Instant messaging app for smartphones.
- The app operates over a mobile phone's internet connection (or over Wi-Fi) and therefore users are not charged for sending SMS messages.
- Under default settings, media sent to a device through WhatsApp is automatically saved. This option can be switched off making it impossible to recover messages once deleted as content is not stored remotely by WhatsApp.

Snapchat

700,000,000 images and videos per day

- The unique feature is that messages (or 'snaps') 'self-destruct' after a specified time-frame once viewed (1-10 seconds).
- Users can send 'stories' made up to any number of individual 1-10 second clips.
- Whilst 'snaps' disappear from your device after the time window expires, a previous leak of 4.6 million people's data demonstrates that snaps <u>are</u> retrievable!

Kik Messenger

200,000,000 users

- Only an email address is required to be registered rather than being linked to a mobile number. This allows access via PC.
- Kik operates a 'law enforcement support' page which offers information about how to request user information and the circumstances this information can be released. User data can be retained for up to 90 days before deletion.
- <u>Concerns have previously been raised about the use of Kik by paedophiles</u>.

ooVoo

100,000,000 users

- Video messaging app for mobiles and PC/Mac targeted at the under-25 market.
- Aims to expand into the games console arena by making the app available on PlayStation.
- Unlike Skype, <u>all</u> calls between ooVoo users are free and hosted by the company rather than the user's device thus improving the quality.
- ooVoo do not record or store the data from communications, however the app is not encrypted and therefore third parties can gain access.
- In order to access the app an email address is required.

Social Media Applications: Explained

Instant Messaging: Continued

Tango

200,000,000 total users

- Free text and video messaging app.
- Sign up requires a Facebook account or email address/mobile number.
- The app doesn't have any particular privacy features and the company, based in America will release data to law enforcement agencies.

Telegram

15,000,000 daily users

- Developed by the founders of VKontakte but based in Germany.
- Instant messaging service for mobile and PCs. The app works with cloud technology so users can access their account from multiple devices.
- Two layers of security:
    1. Standard messaging which includes many of the common instant messaging features, where the content is encrypted between the user and central server.
    2. Secret messaging which takes place between two devices only and is encrypted from user to user (so if the server was compromised no data would be lost).
- Because multiple devices can be used to access an account, if a device is lost or seized the user (or someone with their password) can delete the account remotely.

TigerText

- Secure messaging app for Apple, Android and PC. Mainly aimed at corporations but not exclusively and can be used by individuals.
- Messages are not received by a specific device (e.g. a mobile phone) rather they remain on the company's servers and the receiver can view the content for a specified time period before it is deleted centrally.
- TigerText messages cannot be saved or forwarded.

SureSpot

- Text, image and video messaging app with end to end encryption.
- Intended for mobile devices (Apple and Android).
- The user has a password and is issued with private and public encryption keys (these can be changed at the user's request). When communicating the sender's public key in combination with the receiving party's private key will give access to the message; you only share your public key to other users.
- If a device is seized the app cannot be viewed without the password and the user can remotely delete any stored content.
- The company does not store any data and encourages uses to encrypt a 'back-up' of their SureSpot identity in cloud storage so that accounts can be recovered.

Social Media Applications: Explained

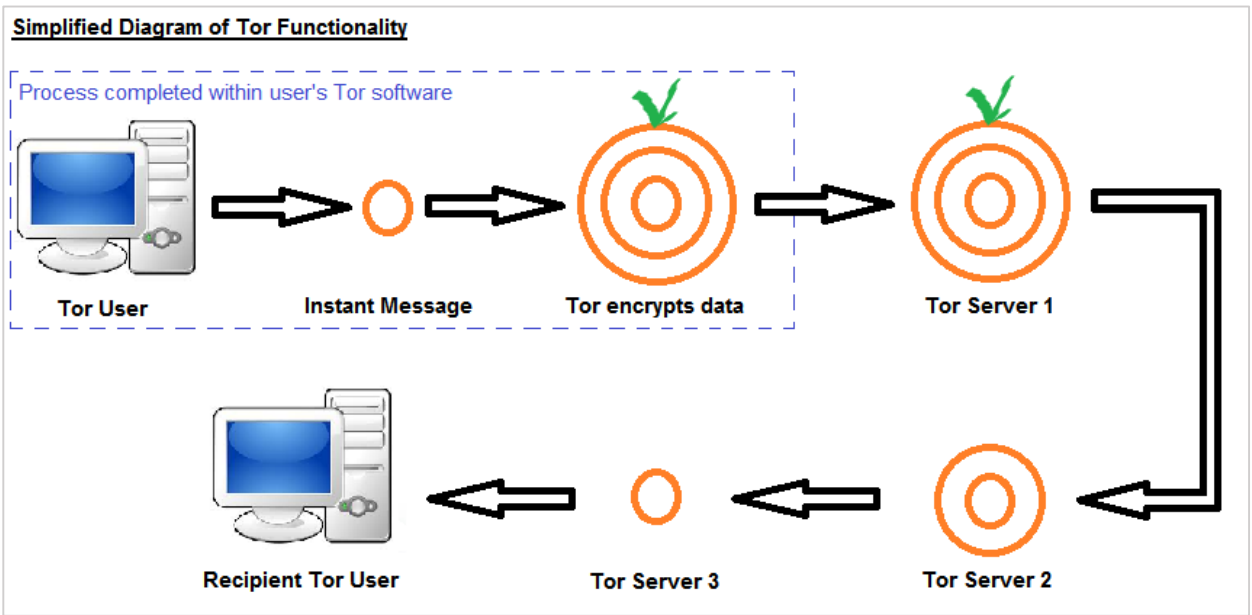
Anonymous Networks

These services provide an enhanced level of privacy which allows users to operate other apps in a more secure environment. Some services also allow the user to circumnavigate online censorship; for example allowing access to websites which have been blocked locally or nationally. These services are almost impossible to monitor; for example Edward Snowden used Tor to leak sensitive information held by the (US) National Security Agency. The threat is that extremists, along with organised crime groups encourage the use of anonymising services, in conjunction with secure messaging such as SureSpot and therefore making it extremely difficult to identify illegal behaviour online.

The Onion Router (Tor)

Upwards of 2,500,000 users

- Tor is an open source tool which provides anonymity for users online.
- Tor anonymises the transportation of data; using the onion metaphor, it encrypts data in multiple layers which is passed through volunteer servers (other Tor users) so that on each occasion a layer of the onion is 'de-crypted' until the final layer is directed to the intended destination.
- Users can chose between web browsers such as Firefox which has a Tor plugin, or for extra security can use Tor's own browser; however certain common features are disabled e.g. Adobe Flash player which is used to create and display content on many frequently used websites.



The Amnesic Incognito Live System (Tails)

- Tails is a computer operating system (like Windows or Mac OS X) which blocks all incoming/outgoing traffic not directed through the Tor network. It also contains various other secure software for email and web browsing.
- Tails can be saved onto a portable memory device, allowing the user to boot the software at start-up on any computer terminal with a CD or USB drive.
- Tails is designed to be untraceable so that when the device is removed from the computer there is no record of activity left behind. This makes public computers vulnerable and should be a consideration in schools and FE/HE institutions.

Social Media Applications: Explained

Anonymous Networks: Continued

The Invisible Internet Project (I2P)

- I2P is an open source software which provides an 'overlay' for other applications to run anonymously. A number of these apps come pre-built in I2P.
- The software is also available on Android mobile devices.
- I2P works by passing data through 'tunnels' which are connections to other I2P users. Based on security and delivery time users can define how many such 'tunnels' their data passes through before reaching the intended target.
- Unlike Tor, I2P is designed more for activities which remain within the network; to improve security there are very few 'exit points' through which to browse regular internet pages (for example).

TunnelBear

- TunnelBear is a virtual private network (VPN); in simple terms this means the internet is used to create a link between selected computers all over the world to replicate a private network - as if these computers were located in the same room and hard-wired.
- TunnelBear is available on both desktop and mobile devices.
- TunnelBear has servers in 14 different countries; this allows users to mask their IP addresses (a unique online identifier which discloses a user's location) by connecting to the internet through a server based in another country to their own, thus allowing circumvention of geographical internet censorship as well as disguising the user's location.
- VPNs can be used to bypass online content filtering, e.g. parental controls or school firewalls.

Hola!

- Hola works in a similar way to TunnelBear but rather than using servers it relies on the users themselves in a 'peer-to-peer' network.
- Hola is available on both desktop and mobile devices.
- Whilst paid users can request that their own computer is not used as a 'peer' by other others, free users have no choice; meaning they are at risk as an 'exit' point in the network and by doing so are actually allowing their own internet bandwidth to be used (this is problematic if your internet provider places a limit on your account, or charges when you exceed a certain amount of data).
- Hola has access to the browsing data of its user-base which could in theory be requested by law enforcement agencies – although there is no test of this process at present.