Ofcom | STEP 1 - UNDERSTAND ILLEGAL CONTENT | USER-TO-USER SERVICE

Your unique reference number

OSA39CQFG2T

Your potential risk factors and illegal harms

Is your service any of these types?

File-storage and file-sharing service

File storage or file-sharing services

If your service is a file-storage or file-sharing service, you should consider how it may be used by potential perpetrators to store and share illegal content. File-sharing services, in particular those that allow users to upload and share images, are used to store child sexual abuse material that can be shared through URLs that perpetrators embed on other services. Potential perpetrators can also create folders of non-consensual intimate images and instructions used to 3D-print firearms on these services which can be downloaded by others.

Associated kinds of priority illegal content

- Terrorism
- Image-based child sexual abuse material
- Intimate image abuse

How the content relates to the risk factor

Terrorism
A wide range of types of user-to-user services are known to be used by terrorist actors. Terrorist content is often identified on file-storage and file-sharing services.

Image-based child sexual abuse material
Any service can be used to distribute child sexual abuse material (CSAM). Services that have the capacity to share images or videos, post text or share hyperlinks pose particular risks. File-storage and file-sharing services, in particular those that allow

users to upload and share images through links, are considered particularly risky, facilitating the storage of large, curated collections of CSAM.

Intimate image abuse
Research indicates that intimate image abuse occurs particularly on adult (pornographic) services, social media services, and file-storage and file-sharing services.

Do child users access some or all of the service?

Yes

Child users (under-18s)

If your service has a high proportion of child users or is aimed at children, your service may be used by potential perpetrators to identify and initiate contact with children for the purposes of grooming them. Child users may also upload, post or share self-generated indecent images (indecent images that are shared often consensually between children and can be non-consensually reshared). These risks can increase for both child sexual abuse material and grooming if your service has direct messaging and/or encrypted messaging. If so, you should refer to the user communication risk factor in the Risk Profiles as children may also experience different or increased risks across other kinds of illegal harm. Gender and other protected characteristics of users on your service affects how likely they are to experience illegals harms from illegal content. You can also refer to the user groups risk factor in the Risk Profiles.

Associated kinds of priority illegal content

- Grooming (child sexual exploitation and abuse)
- Image-based child sexual abuse material
- Child sexual abuse material URLs

How the content relates to the risk factor

Grooming (child sexual exploitation and abuse)
For grooming offences, a high-risk factor in terms of user base characteristics is the age of users. Groomers who want to contact child users will be drawn to services that children access. You should consult the ‘Grooming’ chapter in our Register of Risks to understand more about how harms manifest online in respect of user base.

Image-based child sexual abuse material

Child users on a service can be a risk factor for child sexual abuse material (CSAM), as offenders may search for content uploaded by children on their personal accounts; in some cases, such content may be considered CSAM. You should consult the CSAM chapter in our Register of Risks to understand more about how harms manifest online in respect of user base.

Child sexual abuse material URLs

Child users on a service can be a risk factor for child sexual abuse material (CSAM), as offenders may search for content uploaded by children on their personal accounts; in some cases, such content may be considered CSAM. You should consult the CSAM chapter in our Register of Risks to understand more about how harms manifest online in respect of user base.

Does your service include any of these user identification functionalities?

User profiles

User profiles

In some cases, potential perpetrators may be able to use the information displayed on a profile to identify and target a specific user or group of users for illegal purposes. This is especially relevant for gendered illegal harms such as harassment or stalking, where the information can help potential perpetrators find specific individuals to target. We explain how you should consider your user base demographics at the end of this tool. For grooming (child sexual exploitation and abuse), user profile information can enable potential perpetrators to identify children to target.

Associated kinds of priority illegal content

- Grooming (child sexual exploitation and abuse)
- Hate
- Harassment, stalking, threats and abuse offences
- Sexual exploitation of adults
- Human trafficking
- Unlawful immigration

Fraud and financial services offences

Proceeds of crime

Drugs and psychoactive substances

Foreign interference offence

How the content relates to the risk factor

Grooming (child sexual exploitation and abuse)
Functionalities that allow abusers to identify and make contact with children are risk factors in the facilitation of grooming offences. User profiles, and the information that is presented on them, can be used by perpetrators to identify and target victims and survivors, thereby starting the grooming process.

Hate
Usernames on identifiable user profiles can also be used to reference hate, while the ability to edit them can allow perpetrators to avoid enforcement action by recreating terminated profiles with slight edits to the original username.

Harassment, stalking, threats and abuse offences
Several functionalities of user-to-user services can be used in specific ways to perpetuate harassment, stalking and violent threats. User profiles, and the information that is often displayed on them, can help facilitate stalking. Perpetrators can also gain unauthorised access to victims and survivors' accounts to impersonate them through their user profile.

Sexual exploitation of adults
User profiles can be used to identify individuals. Amongst other functionalities, this enables the commission of the offence of controlling a prostitute for gain.

Human trafficking
User profiles, including fake profiles used to hide the perpetrator's real identity and manipulate a victim/survivor, can be exploited by a perpetrator looking to build trust with their victim.

Unlawful immigration
In the case of both unlawful immigration and human trafficking offences, user profiles can be exploited by a perpetrator looking to build trust with their victim.

Fraud and financial services offences
The information on user profiles can also be used by fraudsters to identify potential victims, such as high net-worth individuals or those who are looking to make connections, for instance on online dating services.

Proceeds of crime
User profiles, and the information displayed on them, can be used by perpetrators to gather information surrounding a potential victim.

Drugs and psychoactive substances
Users often have to connect with potential dealers through user connections before viewing their user profiles and associated content. It is also common for suspected dealers to connect with one another, which may provide another way for users to find user profiles offering drugs for sale.

Foreign interference offence
The evidence we assessed suggests that the ability to target specific sub-groups on a service can be exploited by perpetrators of foreign interference operations, particularly where personal information is visible on user profiles. Diaspora groups may be targeted for foreign influence operations. It may be possible that the display of profile information which would enable other users to identify members of these groups (for example, information about language spoken or home town) could also increase the risks of harm to these diaspora groups.

Fake user profiles

In a different context, users can create fake user profiles that do not accurately reflect the official identity of the account holder. While this can be an important tool for protecting the identity of some users who may be targeted for their views or online activity, particularly marginalised communities, whistle-blowers, and dissenting voices, it also comes with risks. For example, our evidence indicates potential perpetrators may create fake user profiles to impersonate another entity, often with fake images and usernames. This may allow them to impersonate others as part of illegal behaviours such as fraud (impersonation or misrepresentation offences), foreign interference or to monitor, harass or humiliate victims and survivors of controlling or coercive behaviour.

Associated kinds of priority illegal content

- Grooming (child sexual exploitation and abuse)
- Harassment, stalking, threats and abuse offences
- Controlling or coercive behaviour
- Fraud and financial services offences
- Proceeds of crime

Foreign interference offence

How the content relates to the risk factor

Grooming (child sexual exploitation and abuse)
Functionalities that allow abusers to identify and make contact with children are risk factors in the facilitation of grooming offences. The ability to create fake user profiles allows perpetrators to misrepresent themselves to victims and survivors by displaying a false age, name and location.

Harassment, stalking, threats and abuse offences
Several functionalities of user-to-user services can be used in specific ways to perpetuate harassment, stalking and violent threats. Cases of harassment and stalking often involve perpetrators creating multiple and often fake user profiles to contact individuals against their will and to be omnipresent in their lives.

Controlling or coercive behaviour
Several functionalities enable monitoring practices. The most prominent are fake user profiles, which perpetrators can use to impersonate victims and survivors, as well as other individuals, to gain access to the target's account, as well as to monitor and harass victims and survivors.

Fraud and financial services offences
The ability to create fake user profiles on a user-to-user service can be used to commit or facilitate fraud. This allows fraudsters to conceal their identity and impersonate legitimate entities such as banks, insurance providers or financial advisors to add legitimacy to false claims.

Proceeds of crime
The ability to create fake user profiles can make it harder to trace money mule recruiters and individuals posting fake job opportunities on legitimate job sites.

Foreign interference offence
The ability to create fake user profiles can be exploited by perpetrators of foreign interference operations to disseminate content and to impersonate authoritative and high-profile sources.

Does your service include any of these user networking functionalities?

Users can connect with other users

User connections

User connections may be used by potential perpetrators to build networks and establish contact with users to target, you should also review the risk profile on user profiles. For terrorism and drug offences, user connections can be used by potential perpetrators to

connect with thousands of other users to widely share illegal content. Our evidence also suggests that terrorists may exploit these networks to raise funds, in particular if online payments can be made on the service. Potential perpetrators can also use connections to build online networks which can enable them to access other users indirectly; for example, to gain visibility of a target's user profile in cyberstalking offences or to serve to add legitimacy to fraudsters and their content. These connections can also be used by online groomers to appear as if they are part of a child's social network allowing them to establish contact with child users and begin communicating.

Associated kinds of priority illegal content

- Terrorism
- Grooming (child sexual exploitation and abuse)
- Harassment, stalking, threats and abuse offences
- Controlling or coercive behaviour
- Fraud and financial services offences
- Drugs and psychoactive substances
- Foreign interference offence

How the content relates to the risk factor

Terrorism
User connections allow terrorism content to be disseminated through users' networks, especially when official pages or channels are removed.

Grooming (child sexual exploitation and abuse)
Functionalities that allow abusers to identify and make contact with children are risk factors in the facilitation of grooming offences. User connections allow perpetrators to establish contact with child users who have been identified and begin communicating. The sense of trust that mutual connections can create may also be exploited by perpetrators. Perpetrators can often use network recommender systems in the form of publicly displayed connections list of children to infiltrate groups of children at speed and utilise this as a tool to blackmail and coerce children to further the sexual abuse.

Harassment, stalking, threats and abuse offences

In some cases, perpetrators can leverage the user connections functionality by connecting with second- and third-degree connections of the victim or survivor in order to access content that is otherwise not publicly available. This gives a perpetrator visibility of a target's profile without connecting with them directly. User connections also enable perpetrators to build online networks which can be leveraged to facilitate harassment and abuse. Individual perpetrators can incite their network to join the abuse of an individual.

Controlling or coercive behaviour
User connections allow users to build online networks around the perpetrators as well as the victims and survivors. These networks can extend perpetrators' ability to coerce and control victims and survivors, for example by creating an environment for public humiliation or getting contacts to join in with monitoring or harassment.

Fraud and financial services offences
Fraudsters will make use of people who have a large number of user connections to achieve their aims.

Drugs and psychoactive substances
Users often have to connect with potential dealers through user connections before viewing their user profiles and associated content. It is also common for suspected dealers to connect with one another which may provide another way for users to find user profiles offering drugs for sale.

Foreign interference offence
The use of coordinated networks on social media accounts can also be used to amplify content and spread narratives across services. The functionality of user connections is therefore a risk factor for this offence.

Does your service include any of these user communication functionalities?

None of the above

No risk factors

No risk factors identified.

Does your service allow users to post goods and services for sale?

No

No risk factors

No risk factors identified.

Does your service include any of the following functionalities that allow users to find or encounter content?

Searching for user-generated content

User-generated content searching

The ability to search for user-generated content within services may allow users to find illegal content and identify users to target on your service. For example, fraudsters may post content relating to the supply of stolen bank details or money alongside advice on how to use them to commit fraud or launder the money which can be found by other users through content searching. Often, these posts include combinations of key terms or hashtags to make it easier for users to find this kind of content. Our evidence indicates that search results on user-to-user services can include illegal content such as scams or extreme pornography, even when users are not actively searching for it.

Associated kinds of priority illegal content

- Terrorism
- Extreme pornography offence
- Fraud and financial services offences
- Proceeds of crime
- Drugs and psychoactive substances
- Firearms, knives and other weapons

How the content relates to the risk factor

Terrorism
User-generated content searching allows individuals to easily seek out terrorist content.

Extreme pornography offence
The ability to search for user-generated content on user-to-user services may help users find extreme pornography content.

Fraud and financial services offences
Searching for user-generated content can enable fraudsters or potential fraudsters to find posts offering to supply information, advice and articles such as stolen bank details which support the commission of fraud.

Proceeds of crime
Recruiters of money mules will use user-to-user services to contact potential victims easily and directly. Direct messaging can be used by recruiters to directly contact potential money mules, often using specific phrases to attract people. The functionality of user-generated content searching can also enable victims to initiate contact. Potential victims can respond to a post offering the chance to make money after searching for relevant content or seeing a misleading job opportunity.

Drugs and psychoactive substances
User-generated content searching is a popular way for users to find illicit drugs and psychoactive substances. Menus or images depicting the products for sale can be posted on services, or in closed user groups.

Firearms, knives and other weapons
The ability to post goods or services for sale enables users to sell, market and purchase firearms and weapons, while user-generated content searching can allow them to find firearms and weapons.

Hyperlinking

Hyperlinking

You should consider how hyperlinks can be used by potential perpetrators to direct users towards illegal material, including on third-party services. For example, perpetrators use hyperlinks and plain-text URL linking to share illegal images among themselves on various types of services, giving the opportunity to access and download child sexual abuse material, or direct users to marketplaces where they are able to buy and sell illegal goods such as drugs.

Associated kinds of priority illegal content

- Child sexual abuse material URLs
- Fraud and financial services offences
- Drugs and psychoactive substances
- Foreign interference offence

How the content relates to the risk factor

Child sexual abuse material URLs
Messages or posts can include hyperlinks to collections of child sexual abuse material saved on file-storage and file-sharing services. These hyperlinks can be shared with perpetrators, sometimes for a fee.

Fraud and financial services offences
The functionality of hyperlinking enables fraudsters to redirect victims to webpages outside of the original service which can then facilitate scams such as purchase scams, advance-fee scams and impersonation scams if the victim shares their personal information or have malicious programmes downloaded onto their device.

Drugs and psychoactive substances
Hyperlinking and user-generated content searching can be popular methodologies for linking users to additional illicit content.

Foreign interference offence
Services where users can more easily share this content onward, both within and across services, are a particularly risky. This is because they enable foreign influence operations to spread between services and other online spaces, thereby broadening their impact. These functionalities include re-posting and forwarding content, encrypted messaging, and mechanisms for sharing information across services, such as the use of hyperlinks.

Does your service use content or network recommender systems?

No

No risk factors

No risk factors identified.

Play Back Summary

Your answers

Is your service any of these types?

- File-storage and file-sharing service

Do child users access some or all of the service?

- Yes

Does your service include any of these user identification functionalities?

- User profiles

Does your service include any of these user networking functionalities?

- Users can connect with other users

Does your service include any of these user communication functionalities?

- None of the above

Does your service allow users to post goods and services for sale?

- No

Does your service include any of the following functionalities that allow users to find or encounter content?

- Searching for user-generated content
- Hyperlinking

Does your service use content or network recommender systems?

- No