Your response

Please refer to the sub-questions or prompts in the of our call for evidence.

Question	Your response
Question 1: Please provide a description introducing your organisation, service or interest in Online Safety.	*Is this response confidential? – N* Fujitsu is a global Information, Communication and Technology (ICT) company that has developed a range of solutions that digitally verify the age of individuals wanting to access age restricted content, products and services that are available online or on-premises. Organisations integrate our technology and solutions into their systems to introduce age controls that protect minors from harm by preventing them from accessing age restricted content, products, and services. Our technology and solutions integrate with online content and service providers enabling them to determine the level of access and entitlement an individual may have based on their age via a secure challenge/response mechanism. The system requires an individual to use their mobile phone to initially register and then verify themselves when accessing online content and services. **Registration** is quick, simple, and secure and requires an individual to download an app onto their mobile phone and then digitally scan a recognised form of photo identity. Then uses biometric matching technology to confirm the identity of the individual with the identity documents and create a secure credential that is stored on the phone. **Verification** takes less than 2 seconds and is required when an individual wants to access age restricted content and services. To verify, an individual opens the app and scans their face to biometrically confirm their identity. They then scan a challenge QR code presented by the online content and service provider and the resulting age is passed from the individual's mobile phone to the service provider and access provided, if permitted. No Personal Identifiable Information (PII) is shared with the service provider and the individual's personal information remains on the phone in a secure encrypted state. The individual remains

	anonymous to the service provider and is tracked by a unique User ID.
	The unique User ID can be used to block an individual from accessing the service providers site, should the individual contravene the sites acceptable use policies.
Question 2: Can you provide any evidence relating to the presence or quantity of illegal content on user-to-user and search services?	*Is this response confidential?* – *N* Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.
Question 3: How do you currently assess the risk of harm to individuals in the UK from illegal content presented by your service?	*Is this response confidential?* – *N* Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.
Question 4: What are your governance, accountability and decision-making structures for user and platform safety?	*Is this response confidential?* – *N* Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.
Question 5: What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements?	*Is this response confidential?* – *N* Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.
Question 6: How do your terms of service or public policy statements treat illegal content? How are these terms of service maintained and how much resource is dedicated to this?	*Is this response confidential?* – *N* Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.
Question 7: What can providers of online services do to enhance the transparency, accessibility, ease of use and users' awareness of their reporting and complaints mechanisms?	*Is this response confidential?* – *N* Technology can assist online content and service providers in taking significant steps towards protecting minors from accessing age restricted content and services and better manage and control individuals that post inappropriate content that either may be accessible to minors and/or contravene the sites acceptable use policies. Online content and service providers are responsible for the content visible on their platforms and controlling and restricting who can access it.

	It is common for online service providers to use account registration and login controls to access their site, but it is recognised that such controls can be exploited by individuals falsifying information during the account registration process to mask their identity or circumvent age controls. Further, account-based information can be exploited and shared with unknown third parties to gain access to restricted content, products, and services. Online content and service providers need to adopt methods that can verify the individual rather than solely the account. Adoption of such technology will allow service providers to: • Validate the registered owner of an account is who they claim to be • Implement robust age verification controls • Control account access to age-appropriate content, products, and services, including interactions between registered site members • Remove fake accounts By adopting methods that make the end user responsible for presenting valid credentials to verify they are who they claim to be, online content and service providers can maintain regulatory compliance, improve audit and traceability of content posted online, and allow restrictions to be enforced based on the individual accessing, viewing, and creating content rather than the account they are using.
Question 8: If your service has *reporting or flagging* mechanisms in place for illegal content, or users who post illegal content, how are these processes designed and maintained?	*Is this response confidential?* – *N* Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.
Question 9: If your service has a *complaints* mechanism in place, how are these processes designed and maintained?	*Is this response confidential?* – *N* Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.
Question 10: What action does your service take in response to *reports* or *complaints*?	*Is this response confidential?* – *N* Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 11: Could improvements be made to content moderation to deliver greater protection for users, without unduly restricting user activity? If so, what?	*Is this response confidential? – N* Fujitsu believes that improvements can be made to content moderation if better controls are implemented to verify an individual against a specific registered account that is used to access and publish content on a site. It is common for online service providers to use account registration and login controls to access their sites, but it is recognised that such controls can be exploited by individuals falsifying information during the account registration process to mask their identity or circumvent age controls. Further, account-based information can be exploited by individuals or groups to create fake accounts and post content that can be inappropriate, illegal, or contravene the sites acceptable use policy. To prevent this, site operators need to implement technology that creates a direct relation between an individual and their registered account, and that requires an individual to verify that they are who they say they are when using that account. This will enable site operators to: • Verify the individual accessing a site • Trace published content to a specific account and individual • Block site access at an individual and account level where the sites acceptable use policy has been contravened • Prevent the registration of shared and fake accounts. Therefore, if better controls are implemented to verify an individual against a specific registered account it would enable online content and service providers to better moderate content, improve user attribution for published content, and help tackle the prevalence of fake accounts that are used as a common vehicle to publish inappropriate content.
Question 12: What automated moderation systems do you have in place around illegal content?	*Is this response confidential? – N* Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.
Question 13: How do you use human moderators to identify and assess illegal content?	*Is this response confidential? – N*

	Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.
Question 14: How are sanctions or restrictions around access (including to both the service and to particular content) applied by providers of online services?	*Is this response confidential?* – *N* Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.
Question 15: In what instances is illegal content removed from your service?	*Is this response confidential?* – *N* Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.
Question 16: Do you use other tools to reduce the visibility and impact of illegal content?	*Is this response confidential?* – *N* Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.
Question 17: What other sanctions or disincentives do you employ against users who post illegal content?	*Is this response confidential?* – *N* Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.
Question 18: Are there any functionalities or design features which evidence suggests can effectively prevent harm, and could or should be deployed more widely by industry?	*Is this response confidential?* – *N* Fujitsu believes that technology can be implemented by site operators that would effectively prevent individuals accessing, viewing, or obtaining age restricted content, products, or services, and prevent minors from harm. Technology and solutions that verify an individual against a specific registered account provide site operators with greater controls than existing systems that rely on basic self-attested account registration and login controls. Technology that enables a site operator to verify the age of an individual can be used to restrict the content, products, and services that an individual is entitled to access and act against individuals that create and share content that contravenes a sites acceptable use policy, allowing site operators to block both the account and the individual, preventing the further publication of harmful content from that account. The application of technology to verify an individual can be deployed specifically for a site operator

	and/or a broader industry approach taken. Where a broader industry approach is considered, technology to digitally verify an individual could potentially be adopted and supported by a scheme operator such as PASS CO, a government backed proof of age standards scheme, to support wider national requirements for digital age verification.
Question 19: To what extent does your service encompass functionalities or features designed to mitigate the risk or impact of harm from illegal content?	*Is this response confidential? – N* Our technology and solutions integrate with online content and service providers enabling them to determine the level of access and entitlement an individual has based on their actual age. The system uses a secure challenge/response mechanism to confirm that an individual is who they say they are. The system requires an individual to use their mobile phone to initially register and then verify themselves when accessing online content and services. The individual's identity, date of birth, and a biometric match is undertaken during the initial registration process to create a secure credential and it is this information that is biometrically verified each time the individual accesses the service provider's online site. During the verification process the system shares the recorded age and a Unique Identifier for the individual with the site operator. The site operator uses the verified age provided by the system to serve content and set access entitlements for the individual's online account. The Unique Identifier is linked to the individuals online account, and should the account contravene the sites acceptable use policy it can be blocked by the site operator. The system provides many benefits that protect individuals from harm and site operators from the impact of illegal content. • Age verified access can prevent minors from accessing age-appropriate content and services • Interaction and content sharing between accounts can be controlled • Attribution of content between individuals and accounts can be monitored and controlled

	• Individuals and accounts can be blocked from accessing the site, if in breach of site policy.
	• An account cannot be shared with another individual or group
	• Restricts the use of robotic/ghost accounts used to generate automated content as an individual is required to verify account access.
Question 20: How do you support the safety and wellbeing of your users as regards illegal content?	*Is this response confidential?* – *N* Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.
Question 21: How do you mitigate any risks posed by the design of algorithms that support the function of your service (e.g. search engines, or social and content recommender systems), with reference to illegal content specifically?	*Is this response confidential?* – *N* Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.
Question 22: What age assurance and age verification technologies are available to platforms, and what is the impact and cost of using them?	*Is this response confidential?* – *N* Age Verification services vary in price, most have a license cost and per transaction verification charge. Most Age Verification service providers use SaaS based services, that are liable to unexpected downtime. Any service outage will mean that Age Verification services will be unavailable to the online content service provider requiring site operators to fall back on less robust controls or risk impacting the service provider's revenue. Our solution does not incur a per transaction cost to the service provider, allowing online content and service providers to understand their costs upfront. Our system of Age Verification does not have a SaaS component and is designed to be fault tolerant and is therefore not liable to unexpected downtime and/or temporary relaxation of controls by a service provider.
Question 23: Can you identify factors which might indicate that a service is likely to attract child users?	*Is this response confidential?* – *N* Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 24: Does your service use any age assurance or age verification tools or related technologies to verify or estimate the age of users?	*Is this response confidential?* – *N* Fujitsu provides online content and service providers with a system to age verify individuals accessing sites containing age restricted content, products, and services. Individuals that want to access sites protected by our technology are required to register prior to accessing the site(s). To register an individual needs a mobile phone, a recognised photo identity containing their date of birth, and to download the site app. The system authenticates the individual using a biometric algorithm to cross reference against their ID (to ensure they are who they say they are) and verify their age, thus removing the possibility of fake or borrowed ID's being used. The online age controls provided by the system can be embedded into an existing app or online platform. Access to the site is performed using a challenge/response mechanism. The individual uses their mobile phone to verify their identity using the biometric matching capability within the installed app and is then asked to scan a unique time sensitive QR code presented online by the site operator. On reading and validating the QR code the mobile phone securely passes the individual's age and a Unique Identifier to the site operator and access is granted with the appropriate age restrictions set. The Fujitsu age verification system does not require an individual to register with an online content and service provider to access systems protected by Fujitsu but does require the individual to have registered themselves using their mobile phone prior to accessing the site.
Question 25: If it is not possible for children to access your service, or a part of it, how do you ensure this?	*Is this response confidential?* – *N* Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

Question 26: What information do you have about the age of your users?	*Is this response confidential?* – *N* The Fujitsu age verification system requires individuals to use their mobile phone to initially register and then verify themselves with the system. To register with the system the individual is required to download an app to their mobile phone and have available a recognised Government form of photo ID containing the individual's date of birth. During the registration process the following data is captured and securely stored in an encrypted state within the app: • Name • Date of birth • Picture of the individual The data remains on the mobile device and is not externally stored or transmitted by the system. The system does not share any Personal Identifiable Information (PII) with online content and service providers and only provides a verified age and a unique user ID to the service provider during the verification process. The system validates and warrants the users age, and this confirmation is passed to the content provider's system, as a service provider would, in most instances, only want to know if a user is of the appropriate age rather than request an exact date of birth.
Question 27: For purposes of transparency, what type of information is useful/not useful? Why?	*Is this response confidential?* – *N* The Fujitsu solution is based on a system of entitlement and uses data differently depending on whether an individual is registering or verifying with the system. **Registering** Personal Identifiable Information (PII) captured during the registration process is securely stored as an encrypted credential on the individual's personal mobile device. Personal Identifiable Information is not transmitted from the phone and is not stored on an external server unless the individual has given their express permission to do so.

<table>
<tr>
<td></td>
<td>

Verifying

Verification is undertaken by the individual using their mobile phone and when complete confirms to the online service provider the individual's entitlement to access their account and/or age-related content, products, and services.

During the age verification process the Fujitsu age verification application acts as a trusted third party between both the individual and the site operator.

The age verification application uses biometric matching technology to confirm that the individual attempting to verify with the system matches the information held on the secure credential containing the identity of the registered user. If a match is found, then the system confirms to the site operator that both the individual is known, verified and confirms the age of the individual to the site operator.

The system approach minimises PII data held by the site operator and therefore reduces the risk of potentially serious data breaches.

From a user perspective the system addresses some of the legitimate concerns that an individual may have sharing details of their identity or personal data with a site operator when requiring access to age restricted content and services. The system therefore only confirms that the individual is known and verified and that their age entitlement has been verified.

This basic entitlement information enables online content and service providers to process site access requests, manage entitlement to age restricted content and services, and revoke access when required.

</td>
</tr>
<tr>
<td>

Question 28: Other than those in this document, are you aware of other measures available for mitigating risk and harm from illegal content?

</td>
<td>

Is this response confidential? – N

Not applicable – It is understood that this section is relevant to online content and service providers and has therefore been left blank.

</td>
</tr>
</table>

Please complete this form in full and return to OS-CFE@ofcom.org.uk