Written evidence submitted by Yoti (COR0154)

1. This evidence is provided on behalf of an organisation, Yoti.

2. Yoti owns and operates a free digital identity app and wider online identity platform that allows organisations to verify who people are, online and in person. This could be using the Yoti app, which allows individuals to share verified information about themselves on a granular basis or it could be using Yoti's 'embedded' services which allow organisations to add an identity verification flow into their website or app. It could also be using Yoti's authentication algorithms such as facial recognition, liveness detection and age estimation.

3. Yoti has a team of over 250 based in London, with offices in Bangalore, Los Angeles, Melbourne and Vancouver. There have been over 7 million installs of the Yoti app globally, following our launch in November 2017. Similarly, over 300 million checks have been conducted using the Yoti age estimation algorithm since February 2019.

4. Yoti holds the ISO 27001 certification and continues to be audited every year. Further, in November 2019 Yoti was certified to SOC 2 Type 2 for its technical and organisational security controls by a top four auditing company. The SOC 2 standard is an internationally recognised security standard. Yoti also holds the Age Verification Certificate of Compliance, issued by the BBFC. Yoti is certified to the publicly available specification PAS:1296 Age Checking.

Evidence

5. Yoti is providing evidence in regard of the following three areas:
   a. child abuse and exploitation;
   b. revenge pornography;
   c. fraud and scams.

6. Yoti wishes to demonstrate to the Committee the steps that are currently being taken to preclude the commission of the above online harms and impress upon the Committee the need for these steps to be adopted more broadly by online platforms.

Child abuse and exploitation (age verification, verified profiles, parental consent)

7. Yoti has developed a number of solutions which are being used to prevent child abuse and exploitation. Three are worth considering in detail:
   a. age verification;
   b. verified profiles
   c. parental consent.

Age verification

8. Yoti has developed an age estimation algorithm. It has been designed to be anonymous, with data privacy and security as primary considerations. The user

simply presents their face in front of the camera and once the age estimate is performed, the captured facial image is deleted.

9. As stated in the *Online Harms White Paper*, "*Yoti, a digital identity provider, is partnering with the Yubo social network to use machine learning age estimation to detect whether website users are in the right age band for their platform – an important step in helping safeguard children online*."[1]

10. Yoti has also provided its age estimation to a law enforcement agency to estimate age of victim/perpetrator. Yoti's age estimation was used in a BBC documentary to highlight that underage people were selling indecent images on major platforms. A competent regulator could perform this action as a method of auditing online platforms that are thought to be failing to uphold their terms of service or failing to prevent safeguarding issues.

11. In addition, a foreign government department responsible for youth protection has recently approved Yoti's approaches for age estimation and age verification for its domestic adult content market. Further detail regarding this will be available soon.

12. In order to be as transparent as possible, Yoti has published a white paper, explaining the approach and detailing the levels of accuracy, as well as noting how accuracy has improved over time.[2] An image and a verified age of that image is the minimum data needed to develop age-estimation technology. This is obtained by Yoti with consent during the onboarding process for the Yoti app.

13. Further, Yoti invites scrutiny from a wide number of academic, regulators and civil society organisations. For example, through the various organisations Yoti engages with including techUK, the Digital Policy Alliance, and the Age Verification Providers Association. Yoti has also undertaken an Accuracy of Algorithm Review with Dr Allison Gardner. She works on the IEEE P7000 Global Initiative on the Ethics of Autonomous and Intelligent Systems and specifically P7003 on algorithmic bias, providing a framework for Algorithmic Impact Assessments. Yoti's approach has also been reviewed by the Center for Democracy and Technology.

Verified profiles

14. Online platforms can use Yoti solutions to let their users verify their profiles, thereby increasing trust and safety in their community. Verified profiles can dissuade bad actors from using a platform, as it increases the likelihood that they will be caught after committing a malicious act.

15. Amongst others, the social media platform, Yubo, the online classifieds website, Freeads and the large online dating platform, TrulyMadly, use Yoti for verified profiles.

[1] *Online Harms White Paper*, page 78.

[2] https://www.yoti.com/blog/yoti-age-scan-whitepaper/

16. Businesses can choose which specific verified identity details to request from their users via Yoti, for example photo and date of birth. Users then have to give their permission to share these.

17. The verification can be optional, relying on users' choice, or mandated, for example when a profile was blocked as a cautionary step while waiting for the user to confirm their age or identity.

Parental consent

18. Yoti can help platforms obtain consent from a parent or guardian when this is required for a child to use online services. Through the use of Yoti's age estimation solution, platforms can reliably check that the person about to give consent is old enough to be a parent. This provides a pragmatic approach that greatly improves on self-declaratory, tickbox approaches, without sacrificing user experience and onboarding rates.

19. Additionally, Yoti identity verification and e-signature solutions can also be used to verify parents' details, and can be, in certain scenarios, a relevant alternative to the above age-estimation approach. The relying party can select different options for the responsible adult to provide consent. The adult can provide an electronic signature tied to a verified age. Alternatively, the adult can add an electronic signature, which is not tied to their digital identity.

Revenge pornography

20. The non-consensual sharing of intimate images, known colloquially as 'revenge pornography' is a societal and legal problem. Yoti recognises that there are technological methods which can be used to address the non-consensual sharing of images. Consequently, Yoti has partnered with the NSPCC and Internet Watch Foundation to create a tool that helps young people report sexual online images of themselves, and have them removed.

21. The tool is privacy-preserving. It uses Yoti's free app and once an individual's details have been verified, Yoti encrypts them and store them safely in their phone. From this point, only the user holds the key to access or use their data. Yoti can't see any personal details.

22. As stated by the NSPCC, "*Working with Yoti has helped us to address a major hurdle we have in validating young people's age online*."[3]

23. A detailed description of how the tool works can be found on Yoti's website.[4]

Fraud and scams

[3] https://www.yoti.com/blog/helping-under-18s-anonymously-report-their-sexting-images/

[4] Ibid.

24. Although identity fraud isn't a specific offence, it often serves as the catalyst for other offences. With the need to prove elements of one's identity remotely, there come increased opportunities for fraud to be undertaken.

25. For example, BEIS and Companies House have given consideration to the need for more effective identity verification on the Companies House website, making use of digital identity for that purpose.

26. Yoti considers that a digital option can both streamline the process verification and offer the required security, robustness and level of data responsibility. There are now cost effective, privacy-preserving options that enable individuals to verify their identity using a robust digital identity platform. On these platforms, verification is done swiftly and securely.

27. In Yoti's view, there are three additional methods that online platforms could consider to provide greater certainty to their users and mitigate the risk of fraud and scams occurring.

28. First, the use of electronic signatures, augmented with a biometric feature. Using an electronic signature, which has been augmented with a biometric feature such as a facial biometric template, it is possible for an individual to prove who they are, and for online platforms to receive high assurance of the identity of the individual providing the signature.

29. Secondly, the use of verifiable attributes. Verifiable attributes are an attestation from a reputable body that an individual has a claim to something. For example, NHS staff are able to add a verifiable attribute of the fact of their employment to their Yoti.[5] Verifiable attributes could be used to ensure that an individual is a representative of the organisation they claim to be.

30. Finally, multi-factor authentication. Multi-factor authentication provides an additional layer of certainty that an identity verification is genuine. There are different ways in which multi-factor authentication can be undertaken. For example, the government could request that individuals complete a "biometric selfie check" before they are able to share any details with another individual or an online platform. This would create a considerable barrier where an individual is attempting to undertake identity fraud.

May 2020

[5] https://www.yoti.com/digital-id-cards/