Ofcom feedback

Based on an in-depth discussion between IDC and Ofcom on Thursday 8th of February, here are some of the areas of concern raised by IDC, with regards to online safety act. The outcome must be that underage individuals are protected from consuming non-suitable (adult) content online. However, to achieve this goal, a user's privacy must not be compromised, nor should the end user be exposed to a great risk of cyber criminals.

We believe that while all the proposals could work for legitimate adult sites, this comes at a cost and significant overhead. It also comes at increased risk of personal identifiable data being breached by cyber criminals, attacking adult content websites. Ultimately, these actions will lead to an increase in non-legitimate sites.

Such non-legitimate (regulated) sites significantly increase the risk of exposure to cyber criminals, who will be able to use these recommendations by Ofcom to not only trick end users, but also to exploit their privacy for the purpose of ultimately identity theft and/or financial gain.

In the following sections, this document provides an overview and some evidence of why ID Crypt Global has concerns with many of the age verification methods proposed.

Open banking and Credit Card usage

While both solutions can provide confirmation that an account/card holder is over the age of 18, it does come with a number of risks – specifically with an increased risk of falling vicitim to cyber-criminals.

While both Open Banking and Credit Card implement highly secure processes and messaging, the issue is one of perception – specifically when a user visits a non-legitimate website. In such a case, the cybercriminal follows a similar approach to that of a phishing attack, however in this case, pornography is used to attract the end user.

Card fraud

Initially when adult content was accessed online, many sites insisted that age verification was completed by a user providing their card details. However, the instances of fraud taking place significantly increased.

In the same way that users are tricked to visit a website and make a purchase for good that do no arrive, her, users are tricked to an adult site that will appear to follow the online safety guidelines. The user will then provide their card details, only for funds to be debited from that card.

Though users will be able to report the crime, and the card schemes will be able to initiate charge backs, in most cases the acquiring bank is left exposed to the risk of paying the sums back to the consumer. As for the criminals, they often will only operate this way for several weeks – closing the site down just as the number of charge back investigations start to arrive.

It is worth noting that now that card acquiring organisations require little to no collateral, and that funds are paid into the account the next day, this type of fraud is becoming increasingly attractive to cyber criminals.

[See card fraud numbers based on false websites]

Cost of implementation

Using a merchant acquiring services to check an individuals age is at a cost, not only in terms of cost of checking the age, but also in terms of being able to make that connection via the necessary acquirers, card schemes and then card issuers. The engineer and integration costs also make this an unattractive option to adult site providers – unless they have other use cases for card acquiring servicers.

Acquirer risk appetite

Many adult content-based businesses struggle to form relationships with card acquirers, primarily because their business is seen as high risk (in terms of fraud but also in terms of displaying illegal content). As a result, many sites will struggle to be able to form these relationships, and as such, will turn to potentially non-legitimate processors, which in turn raises the risk of cyber criminals.

[Acquirer and underlying acquiring bank risk appetite should be reviewed as evidence. Many banks and acquirers refuse to handle adult based businesses]

Accuracy

Providing a credit card or debit card does not confirm the identity of the person holding that card – rather it confirms the card itself and the identity of its owner. In many households, cards are shared along with card numbers. As there is no loop back method to confirm the account holder is the one holding the card, the card data could easily be used by a child to gain access to inappropriate content.

Open Banking

Connecting a user to their bank account, for them to enter their login details to login, and then share an access credential is a safe and secure process. If that is, the user is indeed on the bank website.

Many cases of fraud take place because an end user is sent to, what they believe is threir banks website. The website looks and acts exactly the same as the banks website, and the user inputs their login credentials. In reality, the site is not real, and is scraping the login data from the end user.

In sophisticated cases, as the user inputs their data, software utilises screen scraping techniques **[initially used pre open banking to provide similar features and functionality]** to input the users details into the banks real website. The fraudulent activity is completed with the real bank site sending the end user their one time passcode etc to the end users mobile device, for them to enter correctly. At this time, the fraudsters are now in control of the users bank account.

[Building a screen scraping application is relatively easy. There are numerous tools and, how to guides online. This screen scraping approach was initially used by companies pre–Open Banking and PSD2 compliance. Even as part of early compliance, screen scraping was a legitimate way of accessing a customer's bank account]

Facial age estimation

Facial age estimation is just that, an estimation. While some companies believe that their AI is accurate here, the reality is that when tested by wider groups, age ranges can be highly variable.

As a company, ID Crypt Global was using AI (in partnership with Microsoft) to look at age estimation and other features associated with the identity. Results were very promising regarding expression, especially those related to a form of stress or distress. However, age estimation was concerning, especially when more accurate results are required (is a 16 year old over 18?).

While AI may prove to be promising, we must understand that the way in which facial age estimation works. Each face scanned is used to help improve the AI, which in itself raises great issues with regards to privacy, and equally as important, ethics regarding how that AI is used.

As a company, we took the decision in March 2023 to decommission our AI solutions. We did this partly due to privacy concerns but primarily due to concerns on how that AI could be used. When AI is used, it can be used to then proactively discriminate or breach individuals' privacy.

In terms of age verification for adult content on a website, from a privacy perspective alone this is highly concerning. It can also lead to rogue sites exploiting this technology, to capture individuals watching adult content, and then use this in later scams, ransomware or for the purpose of blackmail.

Photo identification matching

Uploading a copy of a photo-id document is a breach of privacy and could for legitimate sites cause a raft of compliance challenges (GDPR). For age verification, there is no business case for the vast majority of data associated with a photo document – such as an individual's address found on a driver's license.

Again, this technology and implementation is costly for legitimate adult content site providers. It also is quite a painful experience for the end user.

More worryingly, again such an option provides cyber criminals with an additional avenue to exploit. Cyber criminals could capture adult content traffic in order to capture personal details, shared from a photo id. This could include their address. Such a capability when paired with various other identity-based scams and phishing exercise will lead to an increase in identity theft, and cases of blackmail of the end user.

Mobile phone operators

Many underage users have access to a parents mobile device. In a similar way that debit/credit cards cannot be linked directly to an end user using them, the same is true of a mobile device. As there is no continuous need to prove age on each visit to an adult site, it is a highly ineffective method of protection.

Digital Identity Wallets

This is the safest and preferred method for sharing age. However, there are a number of issues that must be addressed across the multitude of providers. These include:

- Method for verifying the age of an individual
- What data is captured, collected and stored
- Sharing of stored data
- Method for sharing the age verification and what data is used

Method for verifying an individuals age: This must comply with the "highest confidence levels" as set out by the UK government. Many providers however openly admit to confirming to lower confidence levels, or even use self-attestation as a proof of age.

What data is captured, collected and stored: When issuing a digital identity the data captured should be transparent to the end user. They must understand what and why that data is being captured. Almost all digital wallets do this well, however, the method for data storage is vastly different.

As an issuer, data collected for the issuance of an identity should be stored (so the identity can be re-issued if required). However, the data should never be stored in a way that it is required to access certain services or prove any attribute of the identity. For example, some digital wallet providers send verifiers back to their own site to read the data directly from their storage servers. This creates a honeypot of centralised data for a cybercriminal, which if breached compromises everyone's identity data.

Sharing of data: Data should never be shared by an identity issuer, the data should be managed 100% by the identity owner. This means that digital wallet providers should never provide communication capabilities back to the identity owners data captured and stored by the issuer.

Identity information should be self-sovereign and therefore owned and live on the identity owners personal devices. When being shared or accessed, that data MUST be shared form the identity owners personal device, as to ensure the highest levels of privacy and security of that data.

Method for sharing the age verification and what data is used: The method for sharing data MUST be that of peer-to-peer, as in identity owner with verifier directly. This ensures

- Greater levels of control over the data (privacy management)
- Greater levels of security (no API/access path for cyber criminals to attack)
- Service resilience (resilience of such services must be of utmost importance, identity age verification services will be a critical and systemically important function – poor service availability will hamper confidence, trust and revenues of sites)

SSI Principles

Ideally supported digital wallets should follow the 12 principles of SSI (Self-Sovereign Identity) to ensure privacy, security and interoperability at all times.