We need to talk about Malory: A critical view on proof of age solutions

EHSAN TOREINI

This article takes a critical view on the current infrastructures for proof of age. We recognise the accuracy and efficiencies of such systems for adults; however, we argue there are fundamental issues with the adsversarial model. Unlike conventional identity management solutions, the adversary in these systems is children, who are themselves considered a vulnerable group with strict privacy requirements. This particularly makes the efficient protection against fraudalant actors a challenging problem. In this paper, we first elaborate on the nature of the adversary, a child who intends to manipulate the proof-of-age infrastructure to access services. Then, we discuss the privacy aspects of such an adversarial model. Finally, we explain our views on the blindspots in this domain.

ACM Reference Format:
Ehsan Toreini. 2025. We need to talk about Malory: A critical view on proof of age solutions. 1, 1 (August 2025), 7 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The current identity infrastructures are facing three parallel trends: first is the rapid transition of legal identity from physical credentials into verifiable digital credentials. Second, protection against new forms of identity fraud combined with recent developments in machine learning, and third, the government legislation to restrict online contents and the requirements for age–approrpiate content behind identity walls. These trends make *proof of age* a challenging problem that requires critical thinking and innovation.

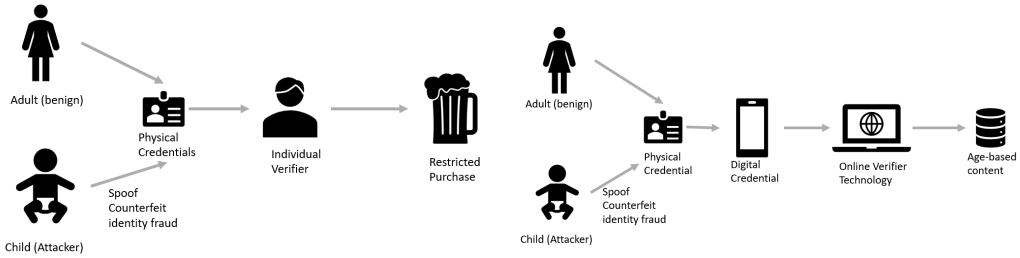
Meanwhile, fraud for children is on also on rise. Especially, identity fraud is rapidly growing worldwide. According to Javelin Research, approximately 1.25 million children in the U.S. were victims of a form of identity theft and fraud between July 2021 and July 2022, leading to nearly a total of 1 billion dollars losses [1]. Moreover, child identify theft is on the rise. According to recent data from the Federal Trade Commission, child identity theft surged by 40% between 2021 and 2024. According to Federal Reserve, the fastest growing form of identity theft is Synthetic Identity Fraud (SIF) [2]. Children are the most common victims, and SIF accounts for billions of dollars in losses annually. This highlights the notion of *differential vulnerlabilities*[7], that a consequence of a vulnelabilty in a system has various consequences across demographics, emphasing any privacy issue in the proof of age solution will have substantial (possibly lifetime) consequence for a child.

Proof of age presents a particularly complex challenge. Naturally, an adult has no problem presenting your credential (regardless of its being digital or physical) to a verifier. This is seamless as first, an adult has various forms of identity to prove their age and also, they are legally responsible to undertake the consequences of not presneting a valid one. However, in this process, the adult is not an adversary, a child is. A child has enough motivation to manipulate

[1] https://javelinstrategy.com/press-release/child-identity-fraud-costs-nearly-1-billion-annually-according-new-study-javelin
[2] https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/synthetic-identity-payments-fraud/

Author's address: Ehsan Toreini.

Manuscript submitted to ACM



(a) Process of age verification in physical world (b) Age verification to access digital content

Fig. 1. Comparison of the age verification in to access a physical and online object

the issuance, presentation and verification protocols and consequently, bypass the protections to access the restricted content. However, in this model a child is a vulneralable group; therefore, even if they act maliciously, their privacy is vitally important.

In summary, there are various complications in designing a reliable proof-of-age solution. First, the adversary is not an adult, but an under-aged individual. In some countries one cannot legally charge a child under age for a fraud. Moreover, any protection against such adversary should be designed with the rights and needs of children in mind. This positions privacy–by–design at the heart of any proof of age solution. Second, the balance between privacy and efficieny is a delima in designing any privacy-preserving systems[1]; however, privacy is a necessity in proof of age solutions, not an optional requirement. Therefore, the designers do not have the liberty to sacrifice some levels of privacy for accuracy. Third, the issues of trusting a reliable presentation of a proof of age, in digital format is challenge [8]. This is mainly because the transition between digital and physical credential is not clealry defined for all physical credentials.

Accessing age-based online content extends age estimation to digital services. Now, there needs to be presentation protocol to access many services in the UK, based on a recent legislation recognised as *UK Online Safety Act*. This process makes reliance on privacy-preserving solution more serious. The shifting nature of the current age verification systems are demosntarted in figure 1.

1.1 Contributions

In this short position paper, we review current standards and call for the necessity of privacy-preserving solutions *in presence of a vulnerable adversary*. In this paper, we will focus on the issues with the proof of age systems, in presence of a minor as adversary. While we acknowledge it needs deeper discussions on threat modelling and the capabilities of our threat actors, we decided to focus on three areas that we recognise to be more vulnerable:

(1) Current trends in legislation and standardisation on age-based content
(2) Critical analysis on limitations in transition from physical to digital credentials
(3) Requirement on trustworthy, privacy-preserving and transparent age estimation

In the rest of this paper, we will extends our discussions on each of these topics.

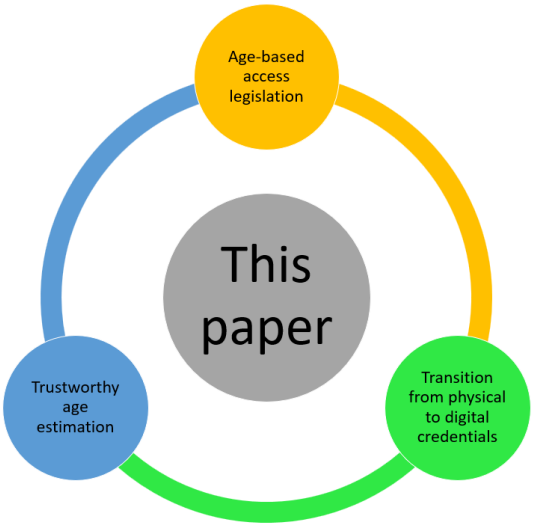


Fig. 2. Comparison of the age verification in to access a physical and online object

2 LACK OF COORDINATION IN AGE-BASED ACCESS REGULATIONS AND STANDARDS

Proof of age regulations vary significantly across the world, reflecting cultural, legal, and societal norms. In many countries, proof of age is required for activities such as purchasing alcohol, tobacco, or entering age-restricted venues. For example, in the United States, individuals must be at least 21 years old to purchase alcohol, and valid identification such as a driver's license or passport is typically required to verify age. In other regions, proof of age regulations may extend to activities beyond substance use. For instance, in Australia, individuals must be at least 18 years old to enter licensed venues that serve alcohol, and proof of age cards are commonly used in addition to traditional identification documents. In Japan, the legal drinking age is 20, and strict enforcement of proof of age requirements is observed in bars and restaurants.

Recently, there has been a more serious approach towards the regulation of age-based content online, particularly in frameworks like the UK Online Safety Act 2023. The framework mandates strict age assurance measures to protect minors from harmful online content. This extends the definition of age-based items from physical consumables or services to online services too. In the Online Safety Act 2023, "age-based content" refers to digital content, services, or platforms that are restricted based on the user's age. This content is classified into categories that pose varying levels of risk to children and young people. Primary priority content, for example, includes material that is deemed highly harmful, such as pornography or other explicit content that is strictly prohibited for minors. Secondary priority content may include material that is less harmful but still inappropriate for certain age groups, such as violent or mature-themed content. The legislation *mandates that providers of such content implement highly effective age assurance systems to ensure that only users who meet the minimum age requirements can access these materials.* This approach aims to protect children from exposure to harmful content while allowing adults to access age-appropriate services; however, questions delicate matters such as public access to information in the web.

The UK Online Safety Act 2023 encourages businesses to align with international standards like IEEE 2089.1 and ISO/IEC 27566. These standards provide a structured approach to implementing age checks, ensuring they are

proportionate to the risks posed by specific content or services. Additionally, the legislation highlights the importance of interoperability and data security, ensuring that age assurance systems are both effective and compliant with privacy regulations.

Meanwhile, the age verification industry encourages the development and adoption of international standards. The sector is currently transitioning to adopt IEEE 2089.1, which is set to replace BSI PAS 1296:2018 as the industry's global benchmark. Once approved, the industry will also incorporate the requirements of ISO/IEC 27566. Each method or combination defines varying levels of confidence in the outcome, technically termed the "level of assurance." This allows websites and regulators to determine the appropriate level of scrutiny based on the risk of harm specific goods, services, or content pose to children.

The IEEE 2089.1 Standard for Online Age Verification, published in May 2024 after over two years of deliberation by a global working group of industry experts, sets out a best practice process for implementing age verification (including age estimation). It begins by identifying relevant legislation in jurisdictions where compliance is necessary, selecting appropriate age assurance methods, conducting the checks, measuring their level of assurance while ensuring privacy protections, applying data security measures, and promoting interoperability. For the first time, this standard defines a common, multi-dimensional approach to measuring the effectiveness of an age assurance process applicable across diverse methods, including both estimation and verification.

Children are protected in proof of age systems through a combination of strict verification processes, age-appropriate access controls, and robust fraud prevention measures. These systems are designed to prevent minors from accessing age-restricted content or services by employing high-assurance verification methods that accurately confirm a user's age. For instance, identity verification processes ensure that only individuals who meet the minimum age requirements can proceed, while age estimation techniques provide an additional layer of scrutiny when identity documents are unavailable.

A fundamental issue in this trend is the lack of coordination between industries, governmental legislation and standardisation. While there are benefits for the legislation, the lack of matured standards will sacrifice interoperability, privacy and ultimately, decreases trust in the legislative sector. However, the adoption of the UK safety act shows there can be unprecedented consequences, and clear dissatisfactions in accessing many services.

3 TRANSITION FROM PHSYCIAL TO DIGITAL CREDENTIALS.

The physical identification documents come in different forms and depending on the criticality of the purpose. The cutting–edge physical physical credentials contains various forms of security features with the purpose of making the verification process intuitive and easy. There are various mechanisms to protect them against attack arrays such as tampering, forging, counterfeiting and more. The new–generation identity documents include application of "System–on–Chip processing units" and sophisticated manufacturing processes, which is mainly focused on a form of plastic known as "polycarbonate".

A reliable "verification" of the physical credentials a.k.a. *Identity Document Validation Technologies (IDVT)*, usually consists of visual examination of the physical credential, e.g. verification if the hologram or whether the photo on the ID is matching the face of an individual who presents the credential. The issuance of the physical credential is strictly held in the hands of government, while the verification protocols has many levels of security, depending on the case, ranging from strict passport checks in border checks to loose proof of age checks while purchasing alcohol in local corner shop.

With digital verifiable credential in the horizon, form of issuace and presentation protocols are more formalised, leading to emergence of new methods in identity validation and verification. Mobile–based identity platforms spiked as form of *identity wallets*. Smartphones are desirable choice for governments and private sector for implementation of a identity wallet as they are highly accessible (more than 7 billion devices in circulation bin 2025, according to IHS market research) and also packed with various sensors, computational power and hardware–based cryptographic modules for extra security. The latest report from Juniper Research predicted there will be over 3 billion citizens around the world with government–initiated identity wallet. Moreover, the private–sector identity wallets (such as Yoti) are popular worldwide (with more than 7 million downloads and active in 200+ countries). The latest UK government document on IDVT technologies embraced smartphone as a reliable IDVT platform.

The transition of phsyical to digital credentials changes the verification and validation process, too. The recent development in verification of such identity documents is application of Artificial Intelligence solutions for recognition of counterfeit documents. These AI–based solutions are commonly implemented in mobile apps for verification of uploaded snapshots of identity documents. While the adoption of such automated counterfeit detection systems facilitated the efficiency and accuracy of the digital identity verification process, there are inherent problems with AI–driven solutions (such as vulnerability to various forms are black–box and white–box attack vectors [5]) that require careful consideration.

However, the reliable validation of physical credentials is now limited to specific credential formats, where there are more standards and regulations for. The current digital credential emphasies a lot on mDoc credentials (e.g. US driving license), in which the credential itself is equipped with cutting-edge secure architecture, with strong standardisation compliance. This model, coupled with liveness test such as 3D modelling from the smartphoen camera and facial recognition is reslient against adult fraulant in the digital identity presentation/registration scenario. This way, instead of physical presentation, a standrad digital format, that is securely stored on individual's device, is presented with associated cryptographic assurances. This is refered to as remote IDVT. This way, the verifier is not in physical proximity of the person to ensure the physical touch. This leaves door to many frauds, including presentation of a synthetically AI-generated phytsical credential, to manipulation of AI-based counterfeit detetcion systems.

Narrowing down the scope of trends to the proof of age, the validation and verification process usually requires presentation of a digitally verifiable credential in your smart phone (using various identity wallet, ranging from official government wallet to privately owned ones). There are various security properties described in the literature for this verification, ranging from usability of the presentation of digital credential on the individual's smartphone [4] to cryptographic schemes for privacy-preserving data minimisation (e.g. properties such as *selective disclosure*, in which one can reliably disclore a proportion of the digital credential) to privacy-preserving data presentation (e.g. properties such as *Zero-Knowledge Proofs*, in which an individual proves the age without disclosing the age itself). Many cryptographic schemes introduced to achieve these properties, such as BBS, BBS+ and idenetity ZKP [3].

Children under 18 will not have access to such credentials due to legal barriers. Instead, they can present a form of credentials known as "proof of age". In the UK, for instance, people over 18 can acquire a proof of age card (a.k.a. PASScard [3]) from specific locations, such as the Royal post office. This card is not equipped with secure chip or antenna; however, it can be scanned and imported into non-government digital wallets. This is problamatic as the architecture for such systems are considered as the intellectual property of the private sector; thus, it is not clear how they protect children from doing fraud in a privacy-preserving manner. For instance, Yoti, as one of the companies that can use

[3] https://www.pass-scheme.org.uk/pass-digital-page/

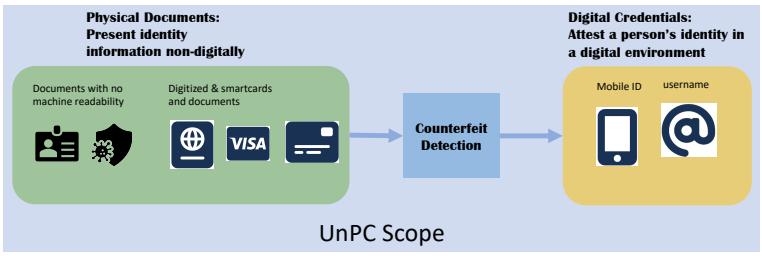


Fig. 3. Comparison of the age verification in to access a physical and online object

PASScards, mentions they acquire a privacy-preserving facial age estimation system using machine learning to perform the age verification. There is no technical detail of such system accessible though.

The easy access to forged and counterfeit documents for some formats of identity (i.e. proof of age credentials) is an ongoing problem. The merchandised items in black–market in dark web reveals such protections are not sufficient to prevent counterfeiting and tampering since the multiple forms of cloned documents are easily accessible with reasonable prices (while the forgers managed to replicate the modern security mechanisms successfully).

There are a few examples of privacy-preserving age estimation (usually focused on face recogntion) in the academic literature [2, 6]. However, the widespread issues with responsible and trustworhty machine learning makes the adoption of a *reliable age estimation solution* an important topic to discuss.

4 CONCLUSION

Proof-of-age is a key issue in digital identity verification and verification. In this short position paper, we take a critical view on the current infrastructures for proof of age. We first elaborate on the nature of the adversary, a child who intends to manipulate the proof-of age infrastructure to access services. Then, we call for the necessity of privacy-preserving solutions in presence of a vulnerable adversary. Finally, we review current standards and call for privacy protections, emphasising the importance of interoperability and privacy, ensuring that age assurance systems are both effective and compliant with privacy regulations.

REFERENCES

[1] Alshamari, M., et al. A review of gaps between usability and security/privacy. *International Journal of Communications, Network and System Sciences 9*, 10 (2016), 413.

[2] Ashiqur Rahman, S., Giacobbi, P., Pyles, L., Mullett, C., Doretto, G., and Adjeroh, D. A. Deep learning for biological age estimation. *Briefings in bioinformatics 22*, 2 (2021), 1767–1781.

[3] Dieye, M., Valiorgue, P., Gelas, J.-P., Diallo, E.-H., Ghodous, P., Biennier, F., and Peyrol, E. A self-sovereign identity based on zero-knowledge proof and blockchain. *IEEe Access 11* (2023), 49445–49455.

[4] Ide, A., and Sharma, T. Personhood credentials: Human-centered design recommendation balancing security, usability, and trust. *arXiv preprint arXiv:2502.16375* (2025).

[5] Mohseni, S., Wang, H., Xiao, C., Yu, Z., Wang, Z., and Yadawa, J. Taxonomy of machine learning safety: A survey and primer. *ACM Computing Surveys 55*, 8 (2022), 1–38.

[6] Ye, L., Li, B., Mohammed, N., Wang, Y., and Liang, J. Privacy-preserving age estimation for content rating. In *2018 IEEE 20th international workshop on multimedia signal processing (MMSP)* (2018), IEEE, pp. 1–6.

[7] Zhang, B., Yu, R., Sun, H., Li, Y., Xu, J., and Wang, H. Privacy for all: Demystify vulnerability disparity of differential privacy against membership inference attack. *arXiv preprint arXiv:2001.08855* (2020).

[8] Zhang, M., Wei, E., Berry, R., and Huang, J. Age-dependent differential privacy. *IEEE Transactions on Information Theory 70*, 2 (2023), 1300–1319.