Don’t Judge Me – Systems for Age Verification From a Feminist Perspective

Elisa Lindinger and Elina Eickstädt

Age verification systems (AVS) are used to prevent children and adolescents from accessing websites with allegedly harmful content. Adults have to verify their age to access such services. There are increasing demands for children to be age-verified online as well to protect them against being contacted by adults, to restrict the functional scope of an application, or to prevent adults from accessing digital platforms intended solely for children and trained personnel.

There are numerous technical solutions for AVS: Some systems require official identity documents that are checked by external entities, either technical (e.g., “Online-Ausweisfunktion” in Germany) or manually (e.g., the PostIdent method provided by Deutsche Post AG). Others use methods such as biometrics and artificial intelligence to estimate the age of the user. Both approaches are viewed critically by digital rights organisations.

Social assumptions and problems regarding technical age verification

The concept of age verification in the virtual world is based on a fixed definition used to determine which digital areas and services should be available to whom and to what extent. In contrast, very few areas in the physical world are categorically closed off for children and adolescents from a legal point of view. It is usually up to the parents or legal guardians to individually decide the scope of what a child can and cannot do according to the development status of the child in question.

This form of parental permission is also partially used in the digital world (e.g., when installing apps on an end device), but may be linked to excessive data requirements that can reach right up to the evaluation of family registers. Hard age limits that can be technically implemented are more frequently deployed than the nuanced approach based on individual development. This is problematic and risky.

For instance, age verification using identity documents presupposes that children, adolescents and adults always have access to their identity documents and that these meet the German legal requirements for optical security features. Structurally, this also excludes adults without identity documents or with different national identity cards that do not meet these requirements. Algorithmic age estimation instead requires the presence of specific technical aids such as a functional camera. As with all AI methods, this works with low error rates within the data range defined as “normal”, but is significantly more prone to errors for data that lie outside this range – and thus for the people behind the data. Common AVS tend to underestimate not only women's ages, they also misjudge the age of people with Down Syndrome. It is therefore more likely that discriminatory exclusion can occur, for instance, for individuals with illnesses or disabilities that can affect facial features.

Not only does this pervasive, AI-based biometric age evaluation normalise the obligation to identify oneself constantly and everywhere. It also normalises the ubiquitous use of risk technologies in the sector of private Internet usage. It creates a technical system that controls access – something that children, adolescents and adults can hardly legally counteract in the event they are incorrectly rejected.

The social impacts of digital age verification are obvious: Structural disadvantage or discrimination also hinder access, which can in turn increase potential social inequalities. The blanket use of AI systems in the context of a diverse population is diametrically opposed to the principle of "from the margins to the centre". It also collides with individual, trusted family negotiation processes regarding which areas young people can grow into – and does not leave any scope for the growth or experimentation that is essential in the critical phase of personal development.

Establishing technologies online cannot be a national consideration

The internet is a global network. Legal regulations which vary from country to country are implemented in different ways by the operators of digital services: The IP address of the user is frequently used during website access to assign the corresponding national legal framework. However, an IP address can be easily changed to circumvent national restrictions by using simple technical tools such as a VPN or the Tor network – which are legal and essential tools for human rights activists, among others. In the USA, one study shows that 41 percent of the surveyed children aged between 11 and 14 use a VPN.

If technical AVS are only considered on a national level, they can be easily circumvented, at least with a browser. At the same time, this implementation of digital access control is spreading globally: A clear trend is seen where the use of these technologies is spreading to other contexts, leading to the massive curtailing of free access to information, for example about sexuality or reproductive rights. This is highly problematic – particularly for adolescents with marginalisation experiences and who are particularly dependent on such relevant information. The legal rejection of this kind of expansion is not much more than lip service because, from a technical aspect, such access restrictions cannot be limited to a specific application case. We are therefore creating censorship tools for the whole world.

Further technical measures for access control, such as blocking or filtering of content at network level, are primarily used in illiberal and authoritarian states. Such interventions lead to a "splinternet", a localised Internet whose basic functionalities are no longer working globally. Even the German Chancellor Olaf Scholz spoke out against this development, not least because of the extreme potential for misuse.

In the case of apps for smartphones, age verification is possible via the settings for parental control without the need for AVS on individual platforms and applications. They enable customised rules – based on the individual development of the child concerned.

Systemic dimensions: What world are we creating with engineered age verifications systems?

Some areas, whether off or online, should solely be for children or for adults. However, safe areas for children and adolescents should not be created through the massive use of monitoring and control technologies because care cannot be engineered. On the contrary: Technical solutions, even if motivated by care, are not tailored to exactly those people who need the most care.

Technical solutions make it factually impossible for legal guardians to individually assess what rights children and adolescents are entitled to or to enter into a negotiation process with them regarding these rights. Instead, they are superimposing the power of the State on an area that should be characterised by learning, growing, trust and experimentation. These fundamental principles of responsible upbringing are not compatible with solutions based on a fully engineered, non-negotiable, one size fits all system. Not least because these solutions do not permit or offer simple options to correct incorrect decisions made by such technology.

The desire for solid technical solutions is based on the tangible pressures faced by many parents and educators. Semi-technical and individually modifiable solutions for parental control, for instance parental control settings on smartphones, are an important starting point for protecting children and adolescents online. They are however currently difficult to implement for most parents. More information and communication about the possibilities of these functions and an improved, easier to use design are urgently required.

This is a central starting point: What can we offer parents, teachers, educators, children and adolescents for them to be able to discuss what young people want and can experience online and how they can make use of their rights? Without the fear that the only possible answer is to restrict their digital opportunities.

Published on feministtechpolicy.org/

A project of

SUPERRR Lab
Oranienstr. 58A
10969 Berlin

Contact: Elisa Lindinger

elisa@superrr.net