HERZOG

HERZOG FOX & NEEMAN

Age Verification Laws

Herzog's Guide to the Evolving Legal Landscape

May 2026

INTRODUCTION

In recent years, there has been a significant rise worldwide in the **regulation of online platforms** that provide or disseminate content, such as **adult or social media platforms**. There has been a focus on implementing **age verification laws** in many jurisdictions including the US at the state level, Australia, the United Kingdom and the European Union.

The purpose of age verification laws is generally to **protect minors online** (commonly defined as individuals under the age of 18 years old, or in some jurisdictions under 16, with the applicable threshold varying by jurisdiction) by creating a safer environment for minors online, including by specifically limiting minors' access to harmful content.

Age verification laws vary among jurisdictions, and generally require platforms to use different **age verification methods** to ensure the age of their users prior to being able to open a social media account or access adult content, typically by submitting an approved type of **identification** (e.g., government ID, Digital ID wallet, credit card, social security number) or using **age estimation software** (i.e., a user takes a selfie and an AI software assesses the age of the individual).

Age verification laws tend to fall into the following principal categories:

- **Adult Content Age Verification Laws -** These laws require online platforms that host a substantial portion of sexually explicit content to verify that users are at least 18 before granting access;
- **Social Media Laws -** These laws specifically target social media platforms and impose requirements such as mandatory age verification for account creation, parental consent for minors' access, restrictions on targeted advertising and data sales involving minors;
- **Privacy, Consumer Protection and Age-Appropriate Design Frameworks -** These laws or codes, whether implemented through standalone statutes, amendments to existing privacy/consumer protection laws, or dedicated **design codes**, impose a dual set of obligations on online platforms: (i) to restrict the processing of minors' personal data to specific, explicit purposes and prohibit its unnecessary retention; and (ii) to proactively design and operate services in a manner that is safe and appropriate for minors, including by limiting or eliminating harmful or manipulative features (e.g., addictive algorithms, infinite scroll, dark patterns, or appearance-altering tools), rather than relying solely on notice-and-consent mechanism;
- **App Store and Developer Accountability Acts -** These laws impose age verification obligations at the point of download by requiring app store providers (e.g., Apple App Store and Google Play Store) and application developers to verify users' ages before granting access;

INTRODUCTION

As of today, **two key regulatory approaches can be identified**. In the US, there is no federal framework for age verification, so a **fragmented approach** across different states is emerging; some US states are implementing age verification regulations for accessing social media platforms, while others are doing so specifically for adult platforms when such platforms disseminate "material harmful to minors."

In contrast, other key jurisdictions, including the European Union, the United Kingdom and Australia, have enacted **comprehensive and unified regulations** to protect individuals online, particularly minors, and may require online platforms to integrate age verification requirements.

The lack of effective industry self-regulation in recent decades and the harmful impacts of social media and access to adult platforms on minors have driven the rise of these regulations, amongst other reasons (e.g. political pressure, escalating lawsuits, available technology, lobbying). These emerging frameworks shift responsibility for access control and the protection of minors away from user self-declaration onto platforms themselves. In practice, **platforms are now required to implement and enforce mechanisms to determine who can access specific categories of content, reflecting a formalization of a duty-of-care toward users.**

This guide provides a snapshot in time for online platforms, showcasing a high-level overview of age verification laws currently in force in key jurisdictions for both adult content platforms and social media platforms. These laws are evolving in real time in governments and courthouses around the world, and thus the information in this guide is subject to change, may not reflect the status of ongoing litigation or injunctions, and does not constitute legal advice.

REGULATIONS IN THE UNITED STATES

Age Verification Laws for Adult Content

Several US states have introduced age verification laws with the objective of preventing minors' access to adult content online.

These laws generally provide for a **civil remedy for damages** (i.e., private right of action) against online platforms that publish or distribute a "substantial portion" of "material harmful to minors", on their respective services. Some laws also impose **statutory damages** (e.g., Louisiana provides for damages of up to $5,000 per violation), and some also include provisions for **state attorney general enforcement**.

Entities subject to these laws would be required to put in place reasonable **methods of age verification** (e.g. providing digitized ID card or age verification system) to each user entering its platform.

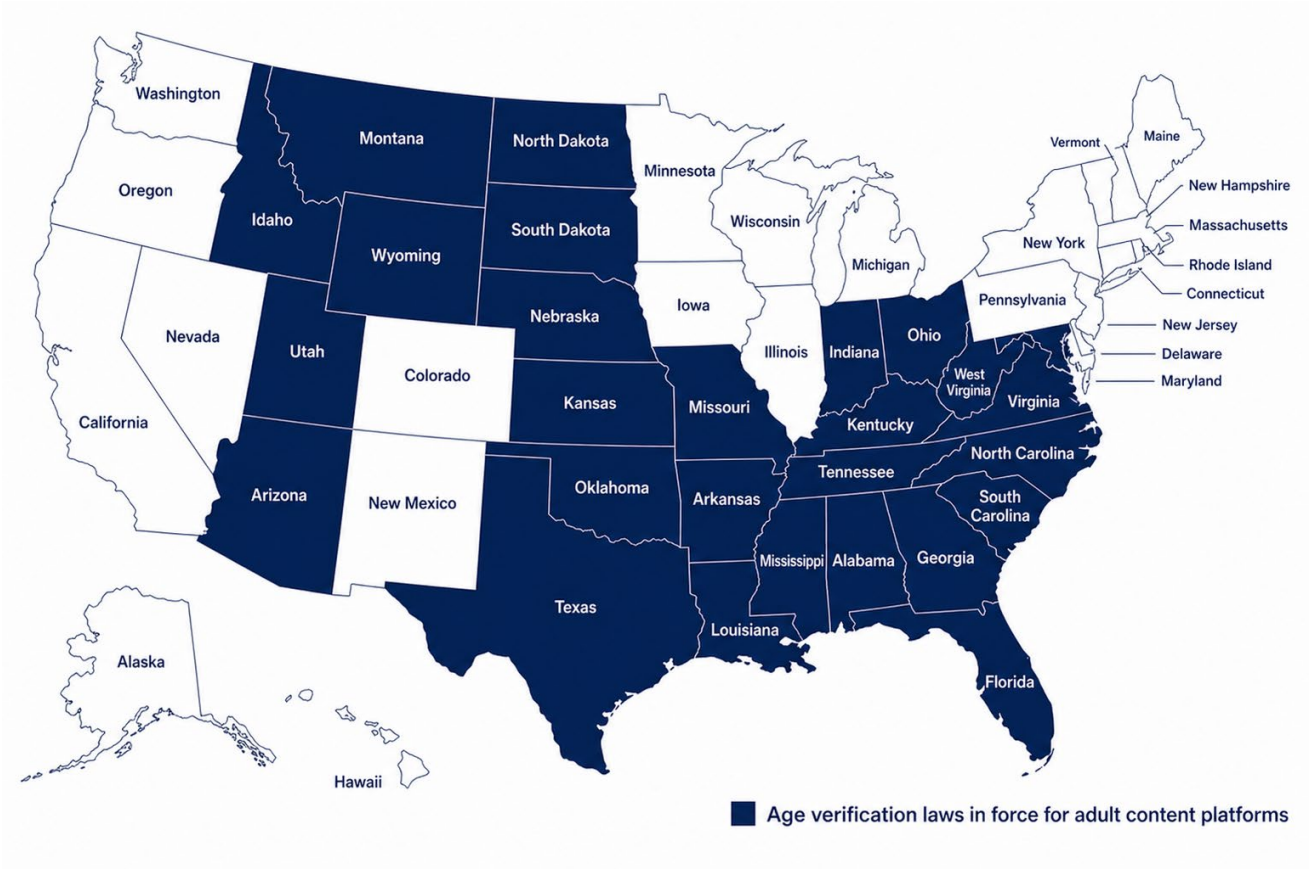
Louisiana was the first state to enact this kind of legislation in 2023, and many other states have enacted substantially similar laws. Across states, these laws appear to have identical criteria for application, that being to entities distributing or publishing "material harmful to minors" [1] beyond a certain threshold. The term "material harmful to minors" is generally defined broadly, particularly including:

- Any content designed to be sexually appealing or offensive to minors;
- Any content that exploits or depicts simulation of sexual acts, nudity in a patently offensive way (e.g., genitals, sexual intercourse, bestiality, exhibitions or any other sexual act); or,
- Materials lacking "literary, artistic, political or scientific value" for minors.

In most cases, age verification is required by law where a "**substantial portion**" of the materials presented or distributed by the entity is considered as "**material harmful to minors**". The term "substantial portion" is usually defined as thirty-three percent (33.3%) of the entity's total materials presented on the company's online services.

[1] These age verification laws would generally not apply to: (a) Bona fide news or public interest broadcasts, website video, report, or events or news-gathering organizations; and, (b) Internet service providers, search engines and cloud service providers would generally not be considered liable for providing access to materials, since they are not responsible for the creation of the content. However, there is some uncertainty regarding the scope of the exclusions, such as whether a social media platform that hosts user-generated news content qualifies for the news organization exemption.

Mapped below are the key US states that have enacted age verification laws applicable to adult content platforms.



Age Verification Laws for Social Media

The second type of law requiring age verification are those that apply to **social media platforms.**

If a user is a minor, age verification laws typically require a parent or a guardian to, first, verify their own age, and may then consent to, or later revoke, the creation of the minor's account on the social media platform or download of an app ("**parental consent**"). Depending on the regulation, a parent/guardian may also have oversight or control over the minor's account ("**parental controls**"), or platforms may be required to provide additional safety settings to protect minors ("**platform safety settings**").

Examples of parental controls include parents/guardians being able to change a minor's privacy or other account settings, view and set daily usage limits, and enforce time restrictions (e.g., minors cannot access the account during school hours or overnight).

Examples of platform safety settings include ensuring default settings are at the highest level of protection by default (e.g., for privacy), no profiling or targeted advertising (unless a user opts-in), and a prohibition for ads for products that may harm minors (e.g., gambling, drugs, alcohol or tobacco).

As of the publication date of this guide, **the following US states** have enacted regulations specifically for social media platforms with age verification obligations (or at least contain platform safety settings):

HERZOG
HERZOG FOX & NEEMAN

Age Verification Laws
Evolving Legal Landscape

State & regulation	Effective date	Age verification requirement	Parental consent	Parental control	Platform safety settings
Arkansas Act to Amend the Social Media Safety Act	21 April 2026	✓	✓	✓	✓
Florida An Act Relating to Online Protections for Minors	1 January 2025	✓	✓	✗	✗
Georgia Protecting Georgia's Children on Social Media Act of 2024	1 July 2025	✓	✓	✗	✗
Mississippi Walker Montgomery Protecting Children Online Act	1 July 2024	✓	✓	✗	✗
Nebraska The Parental Rights in Social Media Act and the Age-Appropriate Online Design Code Act	21 May 2025	✓	✓	✓	✓
New York Stop Addictive Feeds Exploitation (SAFE) Act	20 June 2024	✓	✓	✗	✓
South Carolina South Carolina Social Media Regulation Act	5 February 2026	✓	✓	✓	✓
Tennessee Protecting Children from Social Media Act	1 January 2025	✓	✓	✓	✓
Utah Utah Minor Protection in Social Media Act	1 October 2024	✓	✓	✓	✓
Virginia Chapter 53. Consumer Data Protection Act § 59.1-575	1 January 2026	✓	✓	✓	✓

In addition to the above social media platform obligations, several US states including **Alabama, California, Louisiana and Utah** are increasingly enacting App Store Accountability frameworks shifting age verification responsibility upstream to app store operators (e.g., Apple, Google) and developers of online platform.

REGULATIONS IN KEY INTERNATIONAL JURISDICTIONS

Australia

Australia's Online Safety Act 2021, was designed to protect Australians from severe online abuse, including by enabling the eSafety Commissioner to remove abusive and harmful material online. Depending on the service provided or type of material, requirements on online platforms may include risk assessments, reporting obligations or communication with the commissioner.

On 10 December 2025, an amendment to this act, the Online Safety Amendment (Social Media Minimum Age) Act 2024, made Australia the first jurisdiction in the world to implement a comprehensive and nationwide "social media ban" - uniquely **without exceptions** for parental consent.

The act requires "age-restricted social media platforms" - currently including Facebook, Instagram, SnapChat, TikTok, X and YouTube - to take reasonable steps to prevent Australians **under 16 years of age** from having accounts, and is applicable to any existing account holders under the minimum age, and new accounts being established. In effect, it locked Australian minors out of their social media accounts on the day the ban came into effect by restricting access through the use of age-assurance technology.

On 27 December 2025, the Age-Restricted Material Codes under the act came into effect and are intended to reduce children's accidental and unsolicited exposure to online age-restricted material, including material such as pornography, and apply across multiple sections of the online industry, like social media services. These regulations are legally enforceable with ongoing failure to comply risking civil penalties of up to AUD $49.5 million per breach.

United Kingdom

In the United Kingdom, the Online Safety Act 2023, is aimed at protecting children online by putting a range of new duties on online and search services, including to reduce the risk that services are used for illegal activity and to take down illegal content. The act is enforced by the Office of Communications ("**Ofcom**"). **The act applies to online services even if they are based outside of the UK, providing they have a "significant number" of UK users.**

If the act applies to a particular service, an Illegal Content Risk Assessment will be required; and, as of July 2025, if the social media or other user-to-user service has pornography or other potential content harmful to children, it is required to complete, *inter alia*, a Children's Access Risk Assessment. If children are assessed to be at risk, the platform is required to prevent children from accessing the service by implementing "highly effective age assurance" that is not self-declaration. Ofcom has strong enforcement powers under the act, including the ability to impose fines of up to £18 million or 10% of qualifying worldwide revenue, whichever is higher.

European Union

Lastly, in the European Union, the Digital Services Act ("**DSA**"), is a very comprehensive regulation that introduces rules for online services used by individuals in the EU and improves their online safety by creating a digital space that respects their fundamental, consumer and democratic rights, while also establishing clear accountability for online platforms.

Like the regulations above, the DSA also focuses on the protection of minors to ensure their privacy, safety and security. Risk assessments are also required by the largest platforms (i.e., those with more than 45 million monthly users in the EU), who must also implement mitigation measures for systemic risks that may affect the wellbeing of minors.

While at the EU level the DSA does not explicitly mandate age verification, implementing protections for minors is increasingly being actioned through **age verification requirements in a growing number of EU Member States**; this includes **France**, **Germany**, **Italy** and **Spain**, which have each enacted their own regulations to require age verification for adult and social media content platforms.

The European Commission has recently announced that a new age verification app designed to protect children online is ready for deployment. The app will allow users to prove their age when accessing online platforms, helping protect children from harmful or inappropriate content.

KEY CHALLENGES FOR ONLINE PLATFORMS

Age verification laws face several challenges. A primary concern of facilitating age verification is its tension with **data privacy**: to protect minors, users' personal data must be collected and processed by platforms (e.g., biometric data, government ID numbers). However, regulators expect platforms to implement proportionate, risk-based and privacy-preserving age assurance mechanisms that minimise data collection and avoid identifying users where possible.

There is another tension between age verification regulations and **freedom of speech**. In the United States, there continues to be litigation under the First Amendment regarding age verification for adult content websites, and increasingly for social media platforms. While proponents argue that these regulations protect minors, opponents argue that they reduce online anonymity, freedom of speech, create surveillance and are generally overbroad. Ongoing litigation across multiple US states have led to **divergent outcomes at different procedural stages**, including injunctions and stays, creating **operational uncertainty for platforms as obligations may be enforceable in some jurisdictions but not others**. This has, in some cases, prompted platforms to restrict access or withdraw services in certain states rather than implement age verification measures. While similar concerns around privacy and proportionality arise in other jurisdictions, such as the EU, the degree of legal uncertainty is currently more pronounced in the U.S. context.

Another key issue is that age verification regulations do not apply internationally nor are standardized amongst jurisdictions. As a result, there is an evolving patchwork of laws around the world, requiring online platforms to: (1) assess the regulatory environment for each jurisdiction; (2) consider whether risk assessments or other obligations may be required; (3) implement age verification software and any other obligations prescribed by each regulation in each of the jurisdictions in which they operate; and, (4) monitor regulatory developments for new laws, as well as amendments to existing laws, in their operational jurisdictions which may impact the platform's obligations.

From a practical perspective, these laws are not foolproof - age verification software can be circumvented by virtual private networks (VPNs); and age assurance software specifically can result in bias and discrimination (e.g., disabilities, race, minor, demographic groups). Although most regulations have enforcement provisions, these generally apply to platforms and not to users circumventing these technologies.

At the same time, age verification technology continues to evolve to account for these issues; and similarly, jurisdictions may recognize certain age verification software as meeting the requirements in their regulation.

We anticipate age verification laws to continue to increase in jurisdictions around the world (recent developments include Indonesia's "social media ban," which took effect on 28 March 2026, and similar measures under consideration in Denmark, France, Germany, Spain, Greece and Slovenia) **and evolve over time, requiring online platforms to be more accountable, proactive, and conscientious to create a safer environment for minors online.**

HERZOG'S TECHNOLOGY REGULATION DEPARTMENT

Herzog's Technology Regulation Department is a recognized market leader in its field.

The team is led by domain experts who possess a unique combination of **legal**, **technological** and **operational** expertise, and is uniquely positioned to advise a wide range of clients, including leading multinational technology companies as well as start-ups and vendors of disruptive technologies, on regulatory and compliance considerations across the digital ecosystem.

We understand that companies operating in digital environments face regulatory scrutiny that extends far **beyond one jurisdiction or discipline**. As our clients are often at the forefront of rapidly evolving markets, we recognize the impact that **global enforcement trends, platform rules and design-related compliance requirements** have on their products and operations. Our team maintains in-depth knowledge of the growing body of regulation, enforcement actions and industry standards that govern online interfaces, user journeys and commercial communications. This enables us to offer practical and holistic solutions for complex situations arising from innovative technologies and fast-moving regulatory expectations.

Digital products, online platforms, eCommerce, advertising and user-facing interfaces now form a core component of almost every business. Advising on these issues requires deep understanding of the intersection between legal requirements, UX and UI design practices, behavioral economics, product architecture and commercial strategy. We help clients navigate interdisciplinary and sometimes conflicting obligations that arise under privacy, consumer protection, online safety and advertising laws together with platform guidelines and industry codes.

Our advisory support for online platforms, including social platforms and platforms involving heightened regulatory sensitivity, spans the full lifecycle of product development and ongoing operations. This includes:

- Analyzing product flows, content journeys and monetization mechanics to identify potential dark patterns, safety risks, age-related compliance gaps and areas of regulatory exposure;
- Advising on global regulatory frameworks applicable to online platforms, including content moderation obligations, online safety regimes, age assurance and verification requirements, and restrictions on manipulative or exploitative design practices;
- Supporting the structuring of platform policies, community guidelines, notices and disclosures, including those tailored to sensitive content environments;
- Developing governance frameworks and internal processes for content moderation, escalation, trust and safety, and cross-functional compliance integration across product, legal and operations teams;
- Assisting with regulatory engagement and enforcement matters, including investigations relating to user protection, harmful content, deceptive practices and platform accountability.

HERZOG
HERZOG FOX & NEEMAN

Age Verification Laws
Evolving Legal Landscape

Ariel Yosefi | Partner
Head of Technology Regulation
yosefia@herzoglaw.co.il

Dan Shalev | Partner
Technology Regulation
shalevd@herzoglaw.co.il

Eden Lang | Partner
Technology Regulation
lange@herzoglaw.co.il

Or Noy | Partner
Technology Regulation
noyo@herzoglaw.co.il

On Dvori | Associate
Technology Regulation
dvorio@herzoglaw.co.il

Zohar Malul | Associate
Technology Regulation
malulz@herzoglaw.co.il

Omri Bar On | Associate
Technology Regulation
barono@herzoglaw.co.il

Adaya Ziv-Kisos | Associate
Technology Regulation
Zivkisosa@herzoglaw.co.il

Eden Lapid | Associate
Technology Regulation
lapide@herzoglaw.co.il

Yoel Toledano | Associate
Technology Regulation
toledanoyo@herzoglaw.co.il

Clara Qubti | Associate
Technology Regulation
qubtyc@herzoglaw.co.il

Roni Sharir | Intern
Technology Regulation
sharirR@herzoglaw.co.il

Korin Arbel | Pre-Intern
Technology Regulation
arbelk@herzoglaw.co.il

Max Shternberg | Law Student
Technology Regulation
shterenbergm@herzoglaw.co.il

Ido Manor | Partner
Technology Regulation
manori@herzoglaw.co.il

Ruly Ber | Partner
Technology Regulation
berr@herzoglaw.co.il

Dima Zalyalyeyev | Partner
Technology Regulation
zalyalyeyevd@herzoglaw.co.il

Kevin David Gampel | Associate
Technology Regulation
gampelk@herzoglaw.co.il

Tal Habas | Associate
Technology Regulation
habast@herzoglaw.co.il

Yonatan Glatt | Associate
Technology Regulation
glatty@herzoglaw.co.il

Liron Adar | Associate
Technology Regulation
adarl@herzoglaw.co.il

Kobi Plotkin | Associate
Technology Regulation
plotkiny@herzoglaw.co.il

Yuval Glazer | Associate
Technology Regulation
glazery@herzoglaw.co.il

Gal Mechtinger | Associate
Technology Regulation
mechtingerg@herzoglaw.co.il

Elias Shehadeh | Intern
Technology Regulation
shehadehe@herzoglaw.co.il

Tamara Mascisch Cohen | Visiting Intern
Technology Regulation
cohentam@herzoglaw.co.il

Noya Schwartz | Law Student
Technology Regulation
schwartzn@herzoglaw.co.il