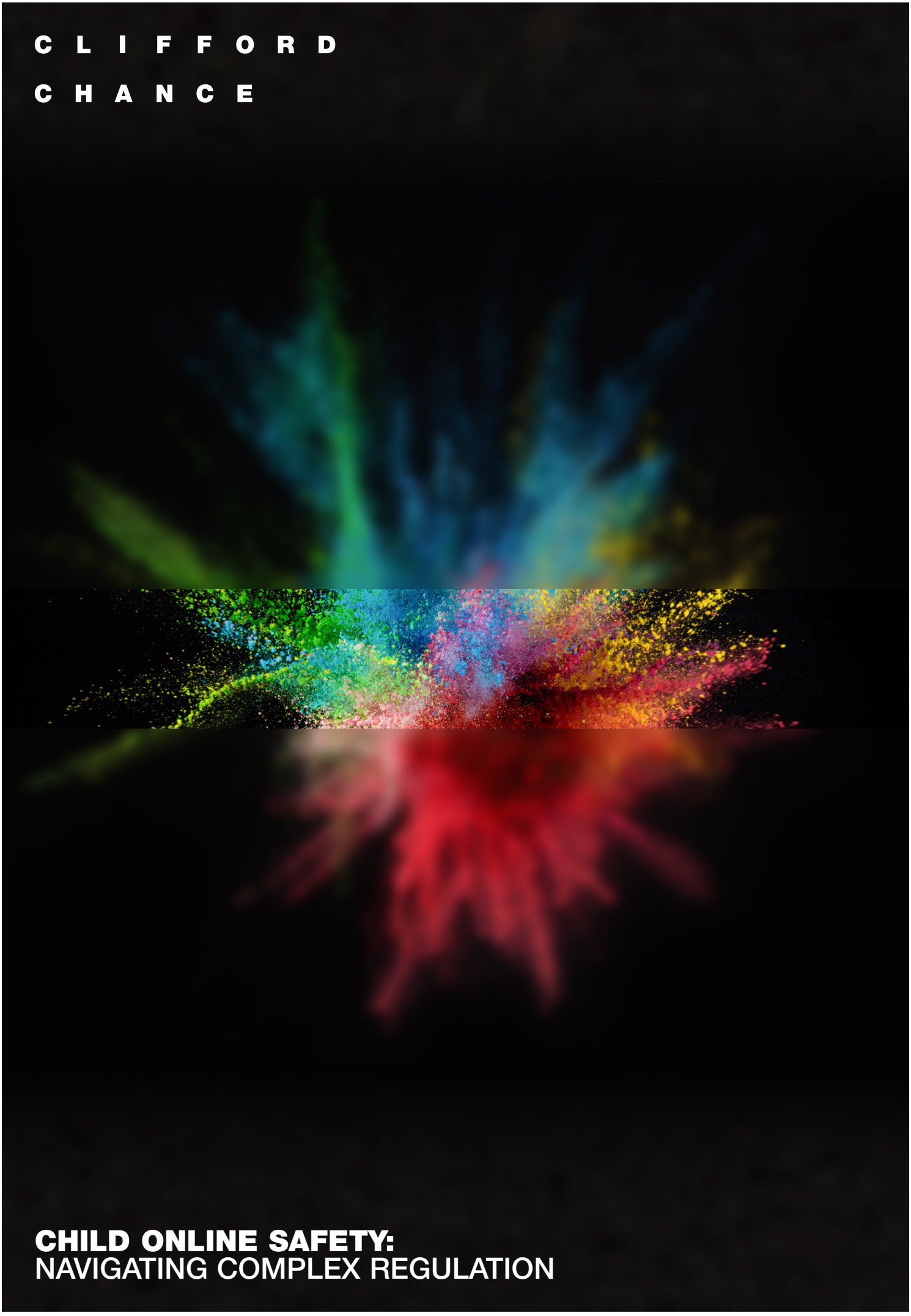
CLIFFORD

CHANCE



CHILD ONLINE SAFETY:
NAVIGATING COMPLEX REGULATION

CHILD ONLINE SAFETY:
NAVIGATING COMPLEX REGULATION

Protecting children online has become a major focus for policymakers, legislators and regulators, and online service providers are under increasing pressure to take action. A range of laws, statutory codes and guidelines has already been introduced around the world and more is expected. Regulatory enquiries and enforcement action in relation to child online safety are also on the rise.

From access controls and age-appropriate services to transparency, service design and content moderation, we examine key considerations for businesses in ensuring the online safety of children, and highlight some areas where additional legislation or guidance is likely.

What does ensuring the safety of children in the digital world mean for businesses?

The combined effect of various existing, new and upcoming laws relating to the protection of children online is that the following key steps will assist digital service providers in addressing child online safety on their services:

- Adopting a holistic approach to child protection across their digital services, taking account of the applicable multi-layered regulatory framework.
- Monitoring the regulatory landscape and contemplated future changes, to anticipate potential impacts and define priorities accordingly.
- Putting in place age assurance access controls and ensuring digital services are age-appropriate, in each case where required.
- Ensuring that transparency, service and online interface design and content moderation practices meet relevant requirements.

We set out below key considerations for businesses when implementing these measures in practice.

1. Identifying the applicable concept of a 'child'

The UN Convention on the rights of the child, as well as the European Commission's 'Better Internet for Kids +' strategy[1], refer to children as individuals under 18 years of age. However, across the global legislative landscape, there is no single, unified concept of the 'child' to be protected in the digital world.

1 See https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids.

Different terms – such as 'children', 'minors' or 'youth' – as well as different age thresholds are used to refer to distinct vulnerable groups of young individuals that policymakers aim to protect, depending on the capacity of the relevant group and the specific protection that the relevant law is seeking to create. Also, different jurisdictions may take different approaches.

The protection of young individuals' personal data and the prevention of sexual abuse are notable examples of the distinction. In the EU, the General Data Protection Regulation (GDPR) generally sets 16 as the age below which a 'child' cannot in principle alone consent to the processing of their personal data in the context of using online services. The GDPR gives Member States flexibility in that respect, however, allowing them to set that age anywhere between 16 and 13[2].

On the other hand, to afford protection to a larger group of young individuals with respect to the sensitive issue of sexual abuse, the EU's proposal for a Regulation to Prevent and Combat Child Sexual Abuse (CSAM Regulation) defines a 'child' as a person under 18 years of age[3].

In China, likewise, the Minors Protection Law defines a minor as a citizen under the age of 18. However, other regulations, such as the Personal Information Protection Law and the Provisions on the Cyber Protection of Children's Personal Information, provide for the protection of minors under the age of 14. Singapore's Code of Practice for Online Safety applies to a 'child' who is also defined as an individual under 18 years of age.

In the US, the definition of a 'child' varies across federal and individual state frameworks. The Children's Online Privacy Protection Act (COPPA) aims to protect the privacy of children under 13 by requiring parental consent for the collection or use of their personal information[4]. State privacy laws differ in approach and either specifically focus on children's privacy or are comprehensive privacy laws that incorporate special protections for children: e.g., Virginia applies restrictions to data processing of individuals under 13, while California provides different restrictions for individuals under 13 as well as individuals between 13 and 15, with another layer of requirements for services aimed at individuals under age 18. Meanwhile, reflecting the mosaic of regulatory measures aimed at safeguarding young individuals in the digital sphere, proposed federal laws such as the Kids Online Safety Act (KOSA)[5] and the Children and Teens' Online Privacy Protection Act (informally referred to as COPPA 2.0)[6] extend protections to individuals under 16 years of age.

2 Different EU Member States have indeed set different ages, e.g., 16 in Germany, 15 in France and 14 in Spain. In the UK, which has implemented the GDPR into its post-Brexit domestic law, that age is 13.
3 The European Commission's proposal had included an additional notion of 'child users', defined as users under the age of 17 years. Both the Council of the EU and the European Parliament have proposed to remove this notion, however.
4 Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501-6505.
5 S.3663 – Kids Online Safety Act.
6 S.1418; H.R. 7890 – Children and Teens' Online Privacy Protection Act.

2. Putting in place access controls for 'age-appropriate' services where required

Regulations may impose access controls

Digital services may contain content considered harmful to children or that may impair children's development (e.g., pornography, online gambling and betting). Accordingly, in Europe for instance, providers of such services are, in certain circumstances, required to put in place access controls. Other regulations mandate that access controls be implemented specifically through age-verification measures, preventing children from accessing online services or content that are not appropriate for their age.

Little guidance from authorities is available at this stage

Often, regulations do not specify what constitutes the specific technical access controls or age-verification measures that must be put in place, and there is limited guidance from authorities at this stage.

Certain data protection authorities have issued guidance on online age verification specifically. In France for instance, the *Commission Nationale de l'Informatique et des Libertés* (CNIL) suggests that service providers might use a trusted third-party provider which would confirm the age of an individual to the online service provider, avoiding the disclosure of other personal data to the latter. In Spain, the *Agencia Española de Protección de Datos* (AEPD) has advocated for a system where an age verification app selected by the user certifies that the user meets the condition of 'person authorised to access' certain content.

In France also, in the context of the proposed law 'to secure and regulate the digital space', the French Audiovisual and Electronic Communications regulator (ARCOM) has opened a public consultation on a standard regarding minimum technical requirements for age assurance techniques in the context of online platforms hosting pornographic content, which aims at striking a balance between reliability of age assurance techniques and privacy[9]. That standard could impose the use of at least one 'double anonymity' technique, relying on third-party age assurance providers.

In the UK, as part of the consultation process on the Online Safety Act (OSA), the Office of Communications (Ofcom) also issued draft guidance on age verification for pornographic content, requiring that methods for determining whether a user is a child must be technically accurate, robust, reliable and fair.

Examples of age-verification obligations in Europe

At the EU level, the Audiovisual Media Services Directive[7] requires that age-verification measures be put in place to protect children from harmful content. The proposal for a CSAM Regulation may also impose age-verification measures on providers of communication services and application stores, where they identify a significant risk that these services will be used to solicit children.

At the EU Member State level, there are laws that require online service providers to put in place age-verification measures where their services display pornography or allow access to online gambling or betting. Recent proposals also contemplate specific measures to ensure more effective controls. For instance, in France, a proposed law 'to secure and regulate the digital space' notably aims at reinforcing age-verification obligations for online service providers[8].

In the UK, the OSA now mandates providers of user-to-user services and search services to implement 'highly effective' age verification and estimation mechanisms to prevent harmful content from being displayed to children. Likewise, providers of pornographic content must publish a statement regarding their use of 'highly effective' age assurance methods.

7 Directive (EU) 2018/1808 of 14 November 2018.
8 Known as the '*Projet de loi visant à sécuriser et réguler l'espace numérique*'. This law was challenged by the European Commission as potentially infringing the EU legal framework. Changes have been made, but as at the end of April 2024 the process is still ongoing.
9 ARCOM, proposal for a standard regarding minimum technical requirements for age assurance techniques in the context of online platforms hosting pornographic content (French only), 11 April 2024.

The effectiveness of access control measures has been questioned

In Europe, a number of authorities have queried or challenged the effectiveness of certain types of access control measures including, at times, advocating for measures that require additional steps, checks or intermediaries. At the same time, access control and age-verification efficiency have to be balanced with users' interests, which is not straight-forward. In particular, users' right to privacy must be taken into account. Where the GDPR applies, the principle of data minimisation will mean that only personal data that is relevant and limited to what is necessary may be collected. As a reflection of this established GDPR principle, the DSA states that compliance with the obligations related to the protection of minors '*shall not oblige providers of online platforms to process additional personal data in order to assess whether the recipient of the service is a minor*'. Similarly, the OSA requires that companies keep records of the implementation of age verification and document how data protection regimes (such as the ICO's Children's Code) have been specifically considered.

Implementing satisfactory access control measures is a complex task

Against this background, it may be difficult for businesses to determine which measures to control access and verify users' age are satisfactory. As a first step, these measures should be adapted, based on the type of online service concerned and the sensitivity of content that can be found on the service, as well as the countries in which the service is operated.

In practice, available guidance from data protection authorities and the like can be a starting point. Those providing services online will want to monitor the publication of further guidance, and consider their approach to non-binding initiatives such as proposals for codes of conduct. In this regard, the European Data Protection Board, at the initiative of the AEPD, has recently approved a joint action on the issuance of guidelines for age-verification systems on the Internet[10].

Solutions are envisaged for more effective online access control

Policymakers are considering how to make access control requirements more effective whilst balancing them with individuals' right to privacy.

In the EU, one of the contemplated solutions is the European Digital Identity Framework under the eIDAS Regulation[11]. This could enable minors to use the EU Digital Identity Wallet to prove their age without disclosing other personal data. EU authorities are also working on non-binding initiatives, such as the EU Code of conduct on age-appropriate design ('BIK+ Code')[12]. EU Member State national authorities are also contemplating standardisation in the field of age-verification mechanisms.

10 Blog of the AEPD published on 15 March 2024. See https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-agencia-impulsa-la-elaboracion-de-las-directrices-del

11 See Regulation (EU) 2024/1183 of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

12 https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design.

In the US, the federal law, COPPA, provides for a 'safe harbor' programme that allows industry groups to submit self-regulatory guidelines for approval that would meet the protections required by COPPA. These programmes allow industry groups with approved guidelines to regulate members, including through certification, annual reviews and disciplinary procedures.

3. Adapting transparency and service design for children

Even where digital services are age-appropriate, they may need to be adapted to children, especially where they are directed at children. The EU legal framework, for example, generally strengthens obligations related to compulsory information and design transparency when it comes to children.

Information may need to be tailored in a way children understand

A number of EU regulations relating to the online world require that mandatory information be made available to individuals in respect of activities that affect them. These regulations may also provide that this information must be adapted to children, so that they can understand it. For instance, the GDPR and the DSA require information provided to individuals to be in plain and clear language. These regulations also provide that, where relevant information is directed at children, it must be in a language that they can understand[13].

Specific information may need to be provided to, or concerning, children

In certain areas, the law imposes providing additional information to minors as an additional safety measure. This is the case in the EU for instance, where specific transparency requirements can apply in relation to children, in addition to the transparency requirements that may apply from a privacy standpoint under the GPDR. By way of example, media service providers are required to provide information to viewers about content which may impair the physical, mental or moral development of minors, using a system describing the potentially harmful nature of the content.

Also, a recent French law[14] will require providers of online social networking services to implement functionality controlling the time spent by all minors on their services and providing related information to them[15].

In the US, COPPA requires that website operators of online services directed at children, or those that knowingly collect personal information from children, must be transparent about their data collection practices. This is primarily achieved under the Act through clear and accessible privacy policies that detail: (i) the types of information collected from children; (ii) how this information is used and whether it is disclosed to third parties; and (iii) parental consent mechanisms and the rights of parents to review and control their child's personal information. In December 2023, the US Federal Trade

13 The Article 29 Working Party's guidelines on transparency under the GDPR (WP260 rev 01), adopted on 29 November 2017 and revised on 11 April 2018, contain useful information in this respect. Under the DSA, the obligation concerns information on the conditions for, and restrictions on, the use of the service contained in the terms and conditions, and it applies where the intermediary services are *'primarily directed at minors or […] predominantly used by them'*.

14 Law no. 2023-566 of 7 July 2023 setting a digital majority and combating online hate.

15 In parallel, there are a number of studies, developments and initiatives around children's exposure to screens, and regulating that exposure and children's time spent on screens.

Commission (FTC) proposed amendments to its rules implementing COPPA to introduce new protections such as strengthened prohibitions on conditioning a child's participation on collection of more personal information than is reasonably necessary for the child to participate in an app or service, and strengthened disclosure requirements for COPPA safe harbor programmes.

In the UK, the OSA requires companies to include details of reporting mechanisms in their terms and conditions for parents and children to flag inappropriate content or behaviour[16]. These must be presented in a way that is easily accessible for children.

Service and online interface design and operation may need to be adapted

As they are deceiving and materially distort or impair individuals' ability to make free and informed decisions, 'dark patterns' on online platforms are prohibited in the EU, including by the DSA[17] and the GDPR[18]. This also complements the EU Unfair Commercial Practices Directive, which prohibits manipulative online practices against consumers, in both the physical and the online worlds.

In practice, directing individuals towards certain choices through either visual design or choice of language, or hiding information from them with the aim of making them enter into a contract or make a more expensive choice (e.g., subscription to more expensive products or delivery options), or making it harder for them to terminate a service that to subscribe to it, may constitute dark patterns. The prohibition therefore impacts how online platforms design, organise and operate their online interfaces. Guidelines on dark patterns under the DSA have yet to be adopted by the European Commission. The European Data Protection Board has already adopted guidelines on 'deceptive design patterns' in the context of social media platforms. There are also publications and studies regarding dark patterns and manipulative practices in the context of unfair commercial practices.

More generally, in the EU and beyond, online platforms and providers of online services must be mindful of their services' design. In particular, they should implement designs that are transparent and do not manipulate users – especially children – towards making certain decisions, be it by choice of words or through visual cues. In the EU also, providers of online platforms that are accessible to minors must put in place relevant measures '*to ensure a high-level of privacy, safety, and security of minors, on their service*'. In the US, the California Age-Appropriate Design Code (AADC), the first US State legislation specifically focused on children's privacy, would require companies

16 Art. 31 OSA.

17 Under the DSA, dark patterns on online interfaces of online platforms are described as practices that '*materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions. Those practices can be used to persuade the recipients of the service to engage in unwanted behaviours or into undesired decisions which have negative consequences for them (…)*'.

18 Dark patterns are construed by the European Data Protection Board as 'deceptive design patterns', in particular in the context of social media. 'Deceptive design patterns' are defined as '*interfaces and user journeys implemented on social media platforms that attempt to influence users into making unintended, unwilling and potentially harmful decisions, often toward a decision that is against the users' best interests and in favour of the social media platforms interests, regarding the processing of their personal data. Deceptive design patterns aim to influence users' behaviour and can hinder their ability to effectively protect their personal data and make conscious choices.*' (European Data Protection Board, guidelines 03/2022 on deceptive design patterns in social media platform interfaces, adopted on 14 February 2023).

to implement privacy by design and default principles and configure default privacy settings for children to a 'high level of privacy' that goes beyond those established for non-minor users. However, on September 18, 2023, NetChoice, LLC, a national trade association of online businesses, obtained a preliminary injunction from the District Court for the Northern District of California, which prevents the State of California from enforcing the AADC on the grounds that the law likely violates the First Amendment. On October 18, 2023, the State appealed the preliminary injunction decision to the Ninth Circuit. While the AADC is enjoined, businesses are not required to meet the AADC obligations. More judicial decisions with guidance on the intersection between the First Amendment and online services regulation are likely.

In addition, the addictive nature of certain online services for young individuals has also recently been in the spotlight. In a report on addictive design, for instance, the European Parliament considers the current EU legal framework does not efficiently protect children from the risks induced by the addictive nature of certain digital services[19]. This report could be the first step to additional bans on certain features, alongside control measures under the DSA. When it comes to online video games, a ban on paid loot boxes could also be envisaged at the EU level to protect minors[20].

The upcoming EU Artificial Intelligence Act (AI Act) is another example of EU legislation providing certain guardrails around the rights and interests of children. Amongst other things, the AI Act will prohibit AI practices linked to the deployment of subliminal, manipulative or deceptive techniques, as well as those that exploit vulnerabilities based on age, and causing or likely to cause significant harm. Despite the prohibitions themselves not explicitly referring to children, the protection of the rights of the child, a fundamental right notably protected by the Charter of Fundamental Rights of the European Union, is one of the justifications provided by the AI Act.

In China, the Regulations on the Protection of Minors in Cyberspace outline key measures to ensure children's safety online. These regulations, which took effect on 1 January 2024, place a heavy emphasis on the prevention and control of Internet addiction. For instance, relevant online service providers are required to establish anti-addiction systems, avoid offering addictive products or services to minors, promptly modify potentially addictive content, functions and rules, and annually disclose their anti-addiction efforts to the public. The Regulations also specify that providers of online games, live broadcasts, audio and video, and social services must create a minor mode, offer guardians clear and convenient oversight methods, and limit minors' spending based on age.

In the US, and similar in some respects to the position in other jurisdictions including the EU, COPPA encourages the development of services that are inherently secure and privacy-preserving. Key design principles under COPPA include:

19 European Parliament resolution of 12 December 2023 on addictive design of online services and consumer protection in the EU single market (2023/2043(INI)).

20 European Parliament resolution of 18 January 2023 on consumer protection in online video games: a European single market approach (2022/2014(INI)).

- **Data Minimisation**: Services should collect only the amount of personal information from children that is necessary to participate in the online activity. This limits the potential for misuse of children's data.

- **Parental Involvement**: Certain services must provide mechanisms for parental oversight, such as tools to review their child's personal information and the ability to revoke consent and request the deletion of data.

- **Prohibition of Conditioning Participation**: Websites and online services cannot condition a child's participation in a game or other activity on the disclosure of more personal information than is reasonably necessary to participate in that activity.

The December 2023 FTC amendments to the FTC's rules implementing COPPA also propose, among other things, a restriction on and required disclosure of 'nudges' that prompt or encourage children to return to and stay on an app. In addition, several proposed bills aim to further strengthen federal children's privacy protections, including KOSA and COPPA 2.0. If passed, these bills would extend certain protections to children aged 13 through 16, and require developers to consider potential risks and harms to children and teens when they design their apps and services.

There may be restrictions / prohibitions on profiling children for advertising purposes

Using children's personal data for advertising purposes is now subject to specific rules in the EU. The use of this data in marketing, or for profiling purposes or in connection with the supply of online services to children, are areas of specific concern under the GDPR. In addition, the DSA now expressly bans targeted advertising on online platforms based on profiling using minors' personal data – at least, where the provider is aware '*with reasonable certainty*' that the service recipient is a minor. Businesses should ensure that they have implemented appropriate measures to ascertain if and how they process children's personal data for advertising purposes, including profiling and to ensure compliance with applicable rules.

In terms of advertisement content, both the Unfair Commercial Practices Directive and the Audiovisual Media Services Directive prohibit direct exhortations to purchase where they exploit minors' vulnerabilities. As EU directives need to be implemented into each Member State's national law, a local analysis is required on this specific topic.

In China, the Regulations on the Protection of Minors in Cyberspace further prohibit providers of online products and services from using automated decision-making for commercial marketing to minors. Similarly, the Singapore Code of Practice for Online Safety, implemented on 18 July 2023 with the aim of mitigating the risks from harmful social media content to Singapore users and especially children, stipulates that social media services should not target children with any content, including advertisements, that would reasonably be considered detrimental to their physical or mental well-being.

4. Monitoring and moderating illegal and harmful content

Online service providers may need to moderate illegal content

Generally, there are measures that prohibit certain content in the online world. Some of these measures specifically focus on children, and may require action on the part of online service providers.

For instance, providers of online intermediary services in the EU may have to remove illegal content present on their service upon receipt of an order to that effect from an EU authority, or when they are notified of the presence of certain illegal content (e.g., child pornography, terrorism). This is true even if they do not have a statutory obligation to actively monitor content on their services.

The new framework set out by the DSA builds on this, and provides additional obligations. For instance, providers of hosting services, including online platforms, must put in place a mechanism allowing third parties to notify them of the presence of 'illegal content' on their service. This requirement protects the public at large including minors, who are expressly singled out: according to the regulation, they are 'at particular risk of being subject to hate speech, sexual harassment or other discriminatory actions'. Assuming the notice allows the provider to identify the illegality of the relevant activity or information, without carrying out a detailed legal examination, the provider needs to expeditiously remove or disable access to the illegal content.

In addition, very large online platforms (VLOPs) and very large online search engines (VLOSEs) are required to carry out systemic risk assessments to identify and assess the risks of negative impact of their services on minors, and to mitigate them. When it comes to the protection of children, these mitigation measures may include age verification, parental control tools as well as tools aimed at helping minors signal abuse or obtain support.

In the UK, the OSA now requires all providers of user-to-user services or search services to conduct risk assessments to understand the likelihood and impact of illegal content (including child sexual exploitation and abuse) appearing on their services and implement proportionate safeguards to remove it. Where services are likely to be accessed by children, it imposes an even broader obligation for providers to implement controls to reduce the risks of children being exposed to '*harmful content*' (e.g., pornography, content encouraging self-harm or eating disorders).

Specific requirements may apply to protect children against particularly harmful materials

Within the broad category of illegal content that can be found online, there are specific types that are or will be subject to more specific or stricter rules due to their high level of danger for children.

One example is child sexual abuse material. In the EU for example, the proposal for a CSAM Regulation aims at supplementing the DSA by reinforcing the obligations of providers of hosting and interpersonal communication services (messaging services,

Balanced moderation

How companies balance content moderation with fundamental rights and values including free speech protection is a complex issue.

This balance has come into sharp focus in the US where a wave of narrow laws aimed at social media platforms have been challenged – and blocked – in court for violating constitutional protections for free speech. Further complicating moderation requirements in the US is the fact that online service providers enjoy some legal immunity under Section 230 of the Communications Decency Act (CDA), which courts have interpreted to bar suits against providers because they are not considered to be publishers or speakers of user-generated content. The balance between content moderation and the protection of free speech continues to evolve across the US legal landscape.

social media, app stores) in this respect. The proposal includes targeted obligations for service providers to detect abuse, to report it and, upon an order from a competent authority, to remove or to block access to the content concerned. In addition, following a similar approach to the DSA, the proposal includes obligations in respect of specific risk assessments regarding the risk of use of hosting and interpersonal communication services for the purpose of online child sexual abuse[21]. The proposal is quite specific as to the types of functionalities which need to be taken into account, such as the possibility '*for adult users to search for child users*'. Based on the risks identified, providers would have to adopt mitigation measures.

In China, the Regulations on the Protection of Minors in Cyberspace target two types of content: one that is outright harmful to minors, including obscenity, pornography, gambling, violence, and other illegal activities; and another that could negatively affect minors' physical or mental well-being (such as information that may cause or induce minors to imitate unsafe acts, commit acts in violation of social morality, have extreme emotions, and/or develop bad hobbies) which must be clearly marked. Whilst the Regulations provide certain examples for reference, this type of content is inherently challenging to pinpoint as it is characterised by its effect on minors rather than its explicit content. Relevant online platforms are tasked with the responsibility of ensuring that such content is appropriately marked. In instances where users fail to label this content correctly, service providers are required to intervene by instructing users to amend the issue or by removing the content themselves. Moreover, platforms must prevent this content from appearing in prominent positions, including 'trending topics', pop-up advertisements or on home pages. It is also prohibited to distribute this content to minors or to prompt them to engage with it. Non-compliance with these rules can lead to severe penalties, including fines, profit confiscation and business licence revocation.

In Singapore, the Code of Practice for Online Safety also includes detailed requirements on how social media services should protect children from harmful and inappropriate content. For instance, it requires social media services to provide children with differentiated accounts and incorporate robust settings for the tools to minimise exposure and mitigate impact of harmful and/or inappropriate content and unwanted interactions, and set restrictive levels that are age appropriate by default. Social media services must also have reporting mechanisms for individuals to report concerning or unwanted interactions.

21 Article 3 of the proposed CSAM Regulation (European Commission's proposal). The EU Parliament slightly specified this obligation in its negotiating position, notably referring to 'systemic risks'.

Developments to watch in this area in 2024

Europe

2024 is already packed with developments regarding the safety of children online. Depending on the timing – and taking account of political elections in the EU – key developments that online services providers should monitor include:

- Secondary legislation and further guidance from authorities under the DSA, notably on 'dark patterns' and 'transparency reporting'.
- Continued political negotiations or legislative developments on key EU regulations such as the proposal for a CSAM Regulation.
- Developments and the work of the special group on the European code of conduct on age-appropriate design.
- Developments following the European Parliament's call to legislate in the area of addictive design of online services in the EU.
- National legislation on the topic of children protection. For instance, and in addition to other developments mentioned in this paper, France adopted in February 2024 a new law to better protect the image rights of children online. The Spanish Government is also taking steps towards the adoption of a law regulating access of children to harmful content.
- Guidance from data protection authorities. In France, for example, the CNIL announced that the protection of children's personal data online is a priority of its 2024 investigations programme, with a focus on age-verification mechanisms and data minimisation. Also, the European Data Protection Board, at the initiative of the AEPD, has recently approved a joint action on the issuance of guidelines for age-verification systems on the Internet.
- Guidance and codes of practice to be published in connection with the UK's OSA. In particular, Ofcom is to issue Children's Access Assessment Guidance (to help companies determine what it means for services to be 'likely to be accessed by children') and protection of children codes.

US

In his State of the Union speech, President Joe Biden referred to the protection of children online for a third year in a row – will 2024 be the year for new legislative developments? To be ahead of the curve, businesses should be reviewing:

- Developments in state and federal laws that impact the design and deployment of an online service, paying particular attention to the age of the user and the different requirements applicable to different users.
- The potential implementation of the California AADC, which would require in-scope businesses to conduct DPIAs on the purpose of the online service and how children's data is used. Attention should also be given to the UK ICO's guidance on age-appropriate design, which is intended to be applicable to the California AADC.
- FTC guidance and resources relating to the compliance and enforcement of COPPA, including new proposed rules issued in December 2023.
- New proposed bills such as KOSA and COPPA 2.0.

APAC

In general, the developments regarding the safety of children online across APAC are more fragmented and less advanced than in other parts of the world.

AUTHORS AND CONTRIBUTORS

EU

Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

Alexandre Balducci
Senior Associate
Paris
T: +33 1 4405 5137
E: alexandre.balducci@cliffordchance.com

Blanche Barbier
Associate
Paris
T: +33 1 4405 8290
E: blanche.barbier@cliffordchance.com

Lisa Fournier
Associate
Paris
T: +33 1 4405 5937
E: lisa.fournier@cliffordchance.com

Alexander Kennedy
Knowledge Director – CE Tech Group
Paris
T: +33 1 4405 5184
E: alexander.kennedy@cliffordchance.com

US

Manel Santilari
Senior Associate
Barcelona
T: +34 93 344 2284
E: manel.santilari@cliffordchance.com

Devika Kornbacher
Partner
Houston
T: 17138212818
E: devika.kornbacher@cliffordchance.com

Inna Jackson
Tech Knowledge & Innovation Attorney – Americas
New York
T: +1 212 878 3292
E: inna.jackson@cliffordchance.com

Brian Yin
Associate
Washington DC
T: +1 202 912 5902
E: brian.yin@cliffordchance.com

Lucy Cole
Trainee
Washington DC
T: +1 202 912 5919
E: lucy.cole@cliffordchance.com

APAC

Stella Cramer
Partner
Singapore
T: +65 6410 2208
E: stella.cramer@cliffordchance.com

Jane Chen
Senior Associate
Beijing
T: +86 10 6535 2216
E: jane.chen@cliffordchance.com

Sian Smith
Senior Associate
Tokyo
T: +81 3 6632 6320
E: sian.smith@cliffordchance.com

Clarice Yue
Counsel
Hong Kong
T: +852 2825 8956
E: clarice.yue@cliffordchance.com

UK

Rita Flakoll
Global Head of Tech Group Knowledge
London
T: +44 20 7006 1826
E: rita.flakoll@cliffordchance.com

Richard Jones
Tech Group Knowledge – UK
London
T: +44 20 7006 8238
E: richard.jones@cliffordchance.com

Nicole Kidney
Associate
London
T: +44 20 7006 1302
E: nicole.kidney@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

2404-010503