OLIVIA WHITCROFT

"Was I being a bad mother by allowing my three-year-old daughter to watch *Frozen*?"

What do the Children's Code and UK Online Safety Bill mean in practice? Lawyer Olivia Whitcroft brings us up to date on developments

A few years ago, I was watching the TV reality show *The Circle*. Contestants could only communicate with each other via *The Circle*'s social media platform. Each contestant could be themselves or play as a "catfish", posing as someone else. One young male player pretended to be a mother of a one-year-old, but the other contestants thought they had caught "her" out as a catfish when "she" was shown an image from the film *Frozen* and didn't know who one of the characters was. Every mum with a one-year-old would know this, right? There I was, with my three-year-old daughter, having never seen *Frozen*. I immediately bought it on DVD before someone reported me to the authorities for motherly neglect.

Fortuitously, the Disney+ streaming service then started, and we were able to feast on Disney movies. But *Frozen* (as well as many other classic Disney movies) has a 6+ age rating. So was I actually being a bad mother by allowing my three-year-old daughter to watch it? If the pre-school birthday parties we subsequently went to are anything to go by, where the majority of girls (and some boys) were dressed as Elsa, I'm guessing I'm not the only parent with this quandary.

Mine is a light-hearted example, but this is a hot topic: the risks of children accessing or sharing inappropriate content online, in particular over social media, which can lead to significant emotional or physical harm, including cyberbullying and online abuse. Parents have a role in protecting their children's interests, but the risks are not all within a parent's knowledge or control.

Legal and regulatory protections have been in development over the past few years. These include the Children's Code published by the Information Commissioner's Office (ICO) ("Age appropriate design: a code of practice for online services") and the UK Online Safety Bill. September 2021 was the deadline for online service providers to follow the Code. The Bill is currently making its way through Parliament, and will require services allowing content-sharing between users to take steps to protect against illegal and harmful content.

Olivia is principal of the law firm OBEP, which specialises in technology contracts, IP and data protection
@ObepOlivia

"The risks are not all within a parent's knowledge or control"

What is the concern with social media?

Away from social media, there are of course other offline and online risks of children getting hold of harmful material. The concern is that existing controls to protect against these activities may not be working as well in a social media environment.

As *The Circle* demonstrates, the anonymity of social media makes it easier for anyone to set up accounts, and form relationships with other users (who may be catfishing). If an underage child tries to buy alcohol in the offline world, they may be turned away or asked for physical ID. But they might easily hide their age to get an account on social media.

One of social media's key features is the ability to access and share user-generated content easily. Sophisticated algorithms can also increase exposure to particular types of content. Children may encounter vast amounts of unscrutinised content compared to, for example, an educational platform where the provider selects the content that can be accessed. There's also the risk a child may over-share information and create long-lasting records.

BELOW It's a huge challenge to protect children from online bullying and abuse

Terms of service

Social media platforms generally have terms of service with pre-conditions for access (such as age limits), and which prohibit users from sharing illegal or harmful content. But if these are to provide practical protection, the provider must enforce them. It may choose not to, or find it difficult to do so without plenty of monitoring in place. In its recent findings against TikTok, the ICO determined that the platform had been collecting data on children under 13 in breach of its own age requirements. In March 2023, it was reported that a father had complained to the ICO that YouTube was doing the same.

Traditional publishers can be held liable for unlawful content, but social media platforms have a potential defence under the Electronic Commerce (EC Directive) Regulations 2002. This applies where a provider is hosting content provided by another party (one of its users, say) and has no knowledge of anything unlawful. It must take steps to remove unlawful content once it becomes aware of it, but this is reactive rather than preventative. And it's difficult to take action against multiple individuals, and to limit distribution of illegal content that may have been shared thousands of times across different forums within minutes.

How do the new rules help?

The Children's Code requires that online services are developed in a way that protect children in relation to use of their personal data, for example by limiting what data is collected and retained. It sets out 15 core standards, including transparency, high privacy default settings, data minimisation and parental controls.

The Online Safety Bill (if enacted in its current form) will require social media platforms to take more

responsibility for preventing illegal content and access to harmful content by children. Larger providers must also give adults more control over exposure to harmful content. The Bill also requires that terms of service include provisions on protection from illegal content and prevention of access by underage children. These terms must be applied consistently.

As a lawyer, this is initially a joy to hear – lovingly crafted terms will no longer be neglected! But on second thoughts, it also affects the provider's commercial choice. When I assist my clients with their standard terms, we often discuss provisions allowing them to remove content or suspend services if specified requirements are not met. These can act as a deterrent, with a choice of whether to enforce them in practice, depending on the wider context (such as the severity of the breach and the relationship with the user). If platforms are required to enforce their terms, more care may be needed in drafting content and access obligations, and enforcement mechanisms, to ensure they can and will be applied consistently.

Age assurance

In defining services within the scope of child-protection provisions, both the Code and the Bill refer to services "likely to be accessed by" children. As well as services aimed at children, this captures services with a significant number of child users, or which are likely to attract a significant number.

To demonstrate that children are unlikely to access a service, or to ensure only appropriately aged children access a service, the Code and the Bill envisage use of age assurance measures. Tools for age assurance can take the form of age verification (verifying someone's precise age) and age estimation (estimating someone's age category, often using algorithms).

However, there are concerns that these age assurance measures, though designed to protect children, may have a negative impact on privacy, and create personal data records that would not have been created in offline methods of checking age. There are some incredibly sophisticated tools to estimate a person's age, including through automated analysis of facial features. I recently attended a conference at which we discussed whether the process of estimating age from an image would necessarily identify an individual, or whether anonymity could be preserved; there was disagreement around the table!

So, to add another layer, how do we provide data protection assurance over age assurance? One option may be certification under the Age Check Certification Scheme, which can be used to demonstrate compliance with data protection rules (as an ICO-approved certification scheme).

Can older kids make their own decisions?

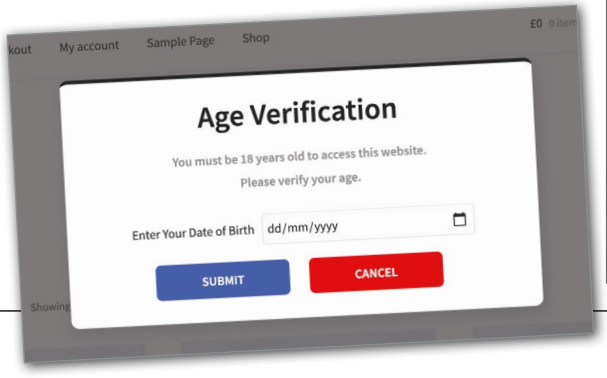
I am frequently asked at what age a child is legally old enough to make their own decisions in relation to use of their information. The age of 13 is often quoted, as specified in Article 8 of the UK GDPR. This is the age at which online services using children's data can rely on consent given by the child, rather than needing parental consent. Looking at the Explanatory Notes to the Data Protection Act 2018 (in which this age limit was set), the age of 13 is in line with the minimum age for access set by popular social media platforms (which includes YouTube and TikTok, as raised above).

However, 13 is not a magical age at which children are suddenly mature and invulnerable. Article 8 doesn't mean that children over 13 require no further protections once they've got themselves online. But it also doesn't mean that younger children should be locked out of the internet and unable to access its educational and social benefits. And some children will be more mature than others of the same age, meaning that they are more able to navigate the risks.

To address this, a key feature of both the Code and the Bill is the need for providers to carry out risk assessments of what protections are needed in the context of their specific services and the children who may access them. So, while some level of protection is always needed, it can be tailored to the age and maturity of users. The child protection obligations continue to apply until a user reaches the age of 18 (when they are no longer deemed a child).

ABOVE It's vital that regulations don't lock younger children out of the internet

"Thirteen is not a magical age at which children are suddenly mature and invulnerable"



BELOW If you see a message like this, it isn't true verification –ages must be checked

Two sides of the coin

September 2022 marked the first anniversary of the Children's Code, and the ICO reported on positive changes made by online providers. However, it also highlighted areas where more work may be needed, such as children's access to adult-only content. The requirements for younger children was also emphasised by the ICO's £12.7m fine to TikTok in April 2023. The ICO determined that TikTok was using data about under 13s without obtaining parental consent.

At the time of writing, the Online Safety Bill continues to be hotly debated. There has been much controversy in how it should strike a balance between its protections, and rights to freedom of speech and privacy. Many think it doesn't go far enough to protect children and vulnerable adults. Particular debate has arisen over the removal of requirements relating to "legal but harmful" content for adults, and whether senior managers of social media providers should be criminally liable for failures in the protections.

On the other hand, there are those who thinks the Bill goes too far. Platforms may take an over-cautious approach to removal of content, and some of the measures designed to protect children may have a negative impact on privacy, such as age verification and monitoring of content. In February 2023, it was reported that messaging app Signal said it would not offer services to the UK if the Bill requires it to undermine privacy given by encryption.

As a lawyer and a parent, I shall continue to follow the developments. And last night around the dinner table we were discussing whether or not to watch a movie rated 9+…

olivia.whitcroft@obep.uk