

Age verification and online pornography under the Digital Economy Act 2017: whose fine is it anyway?

Neil Brown takes a detailed look at the scope of the Digital Economy Act 2017's age verification obligations, and the various actors upon which they fall.

The Digital Economy Act 2017 was passed by Parliament at the end of April 2017, introducing a range of measures likely to be of interest to IT lawyers, including rules around communications service provision, IP, direct marketing, and digital government.

Part 3 of the Act contains the framework relating to access to online pornography by under 18s in the UK, which is the focus of this article.

Online pornography and age verification

The primary obligation relating to online pornography is contained in s14(1):

"A person contravenes this subsection if the person makes pornographic material available on the internet to persons in the United Kingdom on a commercial basis other than in a way that secures that, at any given time, the material is not normally accessible by persons under the age of 18."

The enforcer of this Part, the newly-formed "age-verification regulator" can impose a financial penalty on such a person — administrative / civil, rather than criminal, in nature — of up to the greater of £250,000 or 5% of that person's qualifying turnover.

Unfortunately, the Act does not clarify what is meant by "makes ... available on the internet", leaving the reach of the primary obligation unclear, both in terms of what it covers, and who it covers.

What is "making available"? Does it apply to those who upload pornographic videos? Or those who live-stream them? What about "porn sites" — sites which are dedicated to the dissemination of pornography? Social networks and online forums, with video upload capabilities? What about internet service providers?

The scope of "makes ... available"

A copyright perspective

"Making available" is one of the rights reserved to authors under the WIPO copyright treaty, under Article 8. In 2011, in the *TV Catch Up* case ([2010] EWHC 3063 (Ch)), the High Court of England and Wales considered the right to control the "making available" of a work to be a subset of the broader right of "communication to the public". This position was adopted by the CJEU in the *C More* case (C-279/13) in 2015. The CJEU went on to state that:

"in order to be classified as an act of 'making available to the public' within the meaning of [Article 3(2) of the InfoSoc directive], an act must meet, cumulatively,

both conditions set out in that provision, namely that members of the public may access the protected work from a place and at a time individually chosen by them."

This right is, according to the CJEU, "intended to refer to 'interactive on-demand transmissions'. ... That is not the case of transmissions broadcast live on internet...".

If the scope of "making available" under the Digital Economy Act was interpreted in this way, s14 would cover only videos, audio or photographs which were streamed on-demand to each individual user, and would not appear to cover live transmissions of pornography, such as live-streaming or webcam transmissions.

The more likely approach

It seems unlikely that Parliament intended the Digital Economy Act to be limited in this manner, nor that a court would consider itself constrained to follow the jurisprudence arising from the copyright use of the term. Given that the overall intent of Part 3, according to the initial explanatory notes, is to "restrict access to harmful sexualised content online", the type of transmission would seem immaterial.

Moreover, even if a court did adopt a copyright-based approach, while it may give some clarity to *what* is meant by "making available", it does not assist in determining *who* it is that makes the content available.

Who is a "person"?

In terms of *who* is in scope, let's start with the obvious. As well as a living individual — what most normal people would consider to be a "person" — by virtue of the Interpretation Act 1978, "person" includes a "body of persons corporate or unincorporate".

Individuals, companies, unincorporated associations, all of these could fall within the prohibition.

Intermediary liability shields

s14(3) provides that "Regulations 17 to 20 and 22 of the Electronic Commerce (EC Directive) Regulations 2002 (S.I. 2002/2013)" — the intermediary liability shields — "apply in relation to this Part, despite regulation 3(2) of those Regulations".

Broadly speaking, these regulations shield service providers for liability arising from content transmitted or uploaded by a third party, where the service provider's role is limited to "activity ... of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored" (Recital 42, 2000/31/EC).

Internet access providers

An access provider is shielded from liability for what it transmits, provided that it does not initiate the transmission, select the receiver of the transmission, or select or modify the information contained in the transmission.

As such, since the shield has been expressly afforded to access providers under the Digital Economy Act, it seems safe to assume that, even if their transmission of someone's content means that they "make available" online pornography within the meaning of s14(1), ISPs are excepted from liability.

This does not mean that access providers are home and dry, though, as s23 permits the regulator to compel ISPs to block access to "offending material": a statutory framework for an administrative blocking order. An ISP served with such an order has a statutory duty to comply with it.

Although Parliamentary debate focussed on blocking access at retail ISP level — providers of connectivity to subscribers in the UK attempting to prevent their customers from accessing the sites notified to them — it is conceivable that the age-verification regulator might attempt to impose a notice on the provider of connectivity to a pornography provider's server, stopping the server from connecting to the Internet, rather than requiring each retail ISP to implement a block.

However, in such a case, considerable care would need to be taken to avoid "overblocking". While s23(3) explicitly permits an administrative blocking notice to "have the effect of preventing persons in the United Kingdom from being able to access material other than the offending material using the service provided by the internet service provider", the age-verification regulator's actions must be consistent with the general requirement of proportionality.

Website operators and social media providers

In terms of website operators, and hosting service providers, such as social network sites and operators of online forums, the position is less clear.

As the Act expressly states that the intermediary liability shields apply, Regulation 19 — the hosting shield — offers initial protection to some service providers.

For sites disseminating pornography (as defined by s15) which the sites' operators have selected and uploaded, the protection of the regulations will not be available: these operators are not merely technical intermediaries. Where the service in question is operated "on a commercial basis", the s14 requirement will be made out, and age verification will be required.

For services which consist of the storage of information provided by a recipient of the service — for example, Twitter — the hosting shield will be available.

However, the hosting shield is more porous than that offered to access providers, and Regulation 19 excludes a service provider's liability only until the point at which the service provider has knowledge of the problematic information and acts expeditiously to "remove or disable access to the information".

Ancillary service providers and the notice regime

Considerable Parliamentary time was spent on which service providers should be required to do what. Twitter, Tumblr, Facebook and Instagram were all individually named.

On the sixth sitting of the House of Commons on the Bill, on 20th October 2016, Matt Hancock MP (Minister of State for Digital and Culture at the Department for Culture, Media and Sport) said that "social media sites can be classified by the regulator as ancillary service providers for facilitating or enabling the making of available pornographic material".

In his view, there was a "difference between somebody who is actively putting up adult material and choosing not to have age verification, and a platform where others put up adult material, where it is not necessarily impossible but much harder to have a control over the material. There is an important distinction here. If we try to pretend that everybody putting material onto a platform ... should be treated the same way as a porn-providing website, we will be led into very dangerous territory and it makes it harder to police this rather than easier".

Lord Ashton of Hyde summarised the government's position in respect of such services in the second reading of the Bill in the Lords, namely that "services, including Twitter, can be classified by regulators as ancillary service providers where they are enabling or facilitating the making available of pornographic or prohibited material".

Who is an "ancillary service provider"

Defined in s21(5), an "ancillary service provider" includes a person who appears to the age-verification regulator to "provide, in the course of a business, services which enable or facilitate the making available of pornographic material or extreme pornographic material on the internet by [the person who breaches s14]".

As described above, the definition is intended to include social media service providers. It is likely also to cover other intermediaries, such as web hosting providers or "web performance" companies such as CloudFlare. Amendment 91, which did not make it into the Act, proposed that the term "includes, but is not limited to, domain name registrars, social media platforms, internet service providers, and search engines". DCMS's —the Department for Culture, Media and Sport's — "Draft Guidance to the Regulator" adds to the list "Online advertisers ... Discussion fora and communities in which users post links ... Cyberlockers' [sic] and cloud storage services ... App marketplaces that enable users to download Apps".

In October 2016, Matt Hancock commented that "it would be surprising if ISPs were not designated as ancillary service providers". The DCMS guidance of March 2017 takes a different stance, commenting that "[as] a specific provision is included in respect of internet service providers ... it is not expected that the Regulator will notify internet service providers" under the ancillary service provider framework. This guidance is not binding, but is at least somewhat persuasive: the age-verification regulator must, according to s27, "have regard" to it.

The age-verification regulator is compelled by s25 of the Act to publish guidance "about the circumstances in which it will treat services provided in the course of a business as enabling or facilitating the making available of pornographic material" so, in time, clarity will (I hope) be brought to this issue.

The impact of being an ancillary service provider

The age-verification regulator is empowered to issue notices to ancillary service providers, where it considers that a person is contravening s14(1).

Unlike the imposition of a statutory duty to block on an ISP given an administrative blocking notice, the Act does not impose any positive obligation on an ancillary service provider. There is no new statutory framework compelling such a provider to remove "offending material".

However, a notice of this nature is likely to give a hosting services provider "actual knowledge" for the purposes of the eCommerce Regulations. Faced with such knowledge, the provider must act "expeditiously" to remove or disable access to that information, to retain its protective shield.

But against what liability is that shield protecting the ancillary service provider? The impact of losing the shield, in respect of this particular content, is unclear. Are they liable for the primary obligation of ensuring age-verification is in place, failing which they could be fined?

This seems a stretch. If we go back to the language in s14, the contravention of not having age verification in place applies to a person who "makes pornographic material available" on the internet. However, to be an "ancillary service provider", a person must merely "enable or facilitate" making porn available. The definitions do not appear to overlap, and there is no reason why, simply by being served with a notice, a service provider moves from "enabling or facilitating" to "making available".

As such, it seems highly questionable that, in failing to take action once in receipt of a notice under s21, an ancillary service provider breaches the s14 prohibition.

There was no debate in Parliament as to whether an ancillary services provider would, in failing to take some form of action in response to a notification, commit an inchoate offence, such as "assisting" or "encouraging" under ss44-46 Serious Crime Act 2007. As with direct liability under s14 of the Digital Economy Act 2017, liability under these provisions seems unlikely too.

Voluntary action... or else?

In the draft Impact Assessment for the bill, the government states that it "will work closely with social media companies to make sure they are committed to protecting children who use their platforms". DCMS's factsheet suggests that, in the context of payment service providers, the age-verification regulator will "work with [those providers] to enable them to withdraw their services from infringing sites".

The approach, it seems, is one of encouraging them to take action under their own terms of service, to withdraw the service in question. In the context of payment service providers, the government has assumed in its impact assessment that each major provider will need to employ a dedicated, full-time member of staff, to engage with the age-verification regulator, but there is no similar assumption in respect of non-payment ancillary service providers.

It is, of course, entirely conceivable that, if sufficient support is not forthcoming on a "voluntary" basis, more direct obligations or liabilities might be imposed by future regulation.

Compelling an ISP to block an ancillary service provider

Could an ISP be compelled to block Twitter or other social media provider if they did not remove content following a notice? The regulator's power to order blocking applies only in respect of a person who contravenes s14(1) (or who makes extreme porn available, but that's another topic) and, as above, it seems unlikely that a social media provider does that. As such, without overstepping their mark legally, the age-verification regulator would not appear to have that power.

(Even if it did, exercising it in a manner which blocked a service like Twitter would seem disproportionate. As the Earl of Erroll put it during a debate in the House of Lords, "It is probably unrealistic to block the whole of Twitter—it would make us look like idiots".)

"Porn sites" and apps

Where a site falls outside the hosting shield — for example, because it is distributing its own content — and the material in question is pornographic within the meaning of s15 and is available to persons in the United Kingdom, that person would be within the scope of the s14 requirement if the provision is on a "commercial basis".

"Commercial basis"

Unsurprisingly, "commercial basis" is to be interpreted more broadly than merely in situations where payments exchange hands. The draft Online Pornography (Commercial Basis) Regulations 2017 provides, at clause 3, that a commercial basis is found where payment, reward, or benefit is made or received "in connection with" the making available of the pornography, including where received by "other companies owned or controlled" by the person making the pornography available.

The government's impact assessment notes that:

"if [providers of pornography] charge a fee, by whatever means and for whatever duration for access to the material, sell advertising directed at users of the material or otherwise receive a commercial benefit (for example, through the usage of user data), even if that commercial benefit is not significant or is offset by losses whether from that business or associated businesses, we want them in principle to be caught by the provision."

Whether this goes as far as the CJEU's interpretation of "within the course of its economic activity" in *McFadden* (C-484/14) is unclear, but the scope is clearly intended to be broad.

Encyclopaedias and similar resources

Clause 6 provides a limited exception for sites where "it is reasonable to assume that the overwhelming majority of persons who visit [that site] do not view content of a pornographic nature on [that site] or if it is reasonable to assume that the overwhelming majority of the overall content [on that site] is not content of a pornographic nature".

It is not the clearest piece of drafting, but it would appear to mean that, for example, a general encyclopaedia, or a site offering sexual education or sexual health information, would not be treated as making pornography available on a commercial basis, even if they did include pornography within their service offering. According to Lord Ashton of Hyde,

speaking in the Lords in March 2017, such sites could still be “enabling and facilitating the availability of commercial pornography” and subject to an ancillary service provider notification although, as above, it is unclear what, if anything, this means in practice.

A popularity-based approach

For those running sites which fall squarely within the s14 requirement, it appears that the age-verification regulator is likely to take a systematic, popularity-based approach. David Austin of the British Board of Film Classification — the body to act as the age-verification regulator — was invited as a witness to the Public Bill Committee, in October 2016. As part of his evidence, he commented that:

“[The BBFC] would devise a proportionality test and work out what the targets are in order to achieve the greatest possible level of child protection. We would focus on the most popular websites and apps accessed by children—those data do exist. We would have the greatest possible impact by going after those big ones to start with and then moving down the list.”

In the Lords in early 2017, Baroness Howe stated that “the Government have made clear that they are expecting a “proportionate enforcement” targeting the biggest pornography sites ... likely to be the top 50 to start with”.

This type of “top down” approach is borne out in s26, which permits the age-verification regulator to exercise its powers as against persons who make pornography available to a “large number of persons” or who “generate a large amount of turnover” by doing so.

Not just websites

Although websites received the most discussion in Parliament, and the most attention outside Parliament, the Act is not limited to websites. Someone making pornography available online other than through a web interface would also be in scope.

For example, DCMS’s factsheet on the bill described it as covering “all websites and “apps” containing pornographic material”. It would seem likely that any online interactive system, including peer to peer distribution, would count as “on the Internet”.

What about an individual who uploads pornography?

There has been some discussion as to whether an individual who uploads pornography — for example, a pornographic photograph which they have taken — would breach the requirement of s14 if they failed to ensure that the material was not accessible to persons under 18.

Relatively little Parliamentary time was spent on this issue, although this is not surprising given the early acknowledgement that the strategy is one of focussing on the “top 50” providers initially. In his witness evidence to the Joint Bill Committee, Alan Wardle, of the NSPCC, commented that “[w]e know that there are porn stars with Twitter accounts who have lots of people following them and lots of content, so it is important that that is covered”, but there was no further Parliamentary debate on this point.

“commercial basis”

In terms of individual user liability, as a starting point, we can exclude users who are not acting “on a commercial basis”. The consultation document underpinning the legislation provided that there was no intent that the proposal “should impact on individuals who engage in consensual sharing of private sexual photographs and films”, and the draft Online Pornography (Commercial Basis) Regulations 2017 do not appear to intrude onto this territory.

Where a user has a connection to a commercial pornography site, there is likely to be a reasonable argument that any posting by them of pornography, perhaps otherwise than in a truly anonymous manner, confers a benefit on them, such as traffic to their commercial site.

“makes ... available”

There is, perhaps, some scope for argument around the interpretation of “makes ... available”, and whether the act of uploading, rather than just the act of hosting, is sufficient. On the one hand, as it is the act of hosting the content which, in a literal sense, is what makes the content available to others over the Internet, a restrictive approach might hold that this, and only this, falls within the scope of the framework.

On the other hand, uploading is an unavoidable pre-requisite of the overall “making available” of that content, and it seems unlikely that the age-verification regulator (or a subsequent appellate body) would draw a meaningful distinction between the two acts where the intention of the uploader is to make the content available.

Likely approach

Given that the intended approach of the age-verification regulator is one of tackling the biggest sites first, it seems unlikely that individuals uploading pornography to ancillary service providers’ services will receive particular attention, at least initially.

If there is to be any movement against individual uploaders, one would have thought that it would be in the context of asking ancillary service providers to enforce whatever rules they might have in place regarding the acceptability of content on their platforms.

Twitter’s rules, for example, state that “You may not use our service for any unlawful purposes or in furtherance of illegal activities.” The age-verification regulator might expect Twitter to disable a user’s account in response to a notice to Twitter that it considers that a user is breaching s14(1).

The responses of each social media site, and other ancillary service providers, will be interesting to see.

What next?

Part 3 of the Act is not currently in force. This requires an appropriate statutory instrument (s118(6)) which, presumably, will be laid before Parliament after the general election. Similarly, although the government indicated in October 2016 its intent to appoint the British Board of Film Classification as the age-verification regulator, the formality of this appointment will also need to be conducted.

We will also need to await guidance on who the BBFC considers to be an “ancillary service provider”, and the types of arrangements for making pornographic material available that it will treat as complying with section 14(1). This guidance must be prepared in draft form and submitted to the Secretary of State, who must lay it before Parliament. There is then a 40 day period in which Parliament is afforded an opportunity to object to the guidance. If no resolution to reject the guidance is passed, the BBFC must publish that guidance as the finalised version.

Conclusion

The precise scope of s14 of the Act remains unclear.

Through a process of elimination, predominantly reliant on the eCommerce Regulations' intermediary shields, other provisions of the Part, and governmental guidance, it appears that ISPs are unlikely to fall within the s14(1) requirement. It is less clear in the context of ancillary service providers, but it seems that a “notice and strong expectation that they will do something” is the approach at this time.

For individuals connected with the commercial provision of pornography, their personal uploading of pornographic material is likely to fall within s14. However, it seems more likely, in the short term at least, that the regulatory focus will be on major pornography sites, and that such uploading will not receive regulatory attention. Failing this, the most likely course of action is for the regulator to notify the ancillary service provider in question, to take some form of action under their terms of service, such as removing the content in question or even suspending or deleting the user's account.

Neil Brown is an experienced Internet, telecoms and technology lawyer and managing director of law firm decoded:Legal (<https://decodedlegal.com>). For many years, he was responsible for legal aspects of Vodafone's “content control” filtering system, and for liaison with the BBFC on content classification matters.