How the Online Safety Bill could change liability rules, and what this means for digital firms across the UK

February 2022

COADEC

About Coadec

The Coalition for a Digital Economy (Coadec) is an independent advocacy group that serves as the policy voice for Britain's technology-led startups and scale ups.

Coadec was founded in 2010 by Mike Butcher, Editor-at-Large of technology news publisher TechCrunch, and Jeff Lynn, Executive Chairman and Co-Founder of online investment platform Seedrs.

We fight for a policy environment that enables early-stage British tech companies to grow, scale and compete globally. We have over 3000 startups in our network and have been instrumental in building proactive coalitions of businesses and investors on issues that are integral to the health of the UK's startup ecosystem. Our work has seen many successes, from the establishment of the Future Fund and the expansion of the Tier 1 Exceptional Talent Visa, to the delivery of the UK's Patient Capital Fund.

We represent the startup community on the Government's Digital Economy Council, and the UK on the board of the international group, Allied for Startups.

Executive Summary

The UK has a world-leading tech ecosystem made up of tens of thousands of startups and small firms. Widely regarded as the tech capital of Europe, the UK is now the third country in the world to pass 100 tech unicorns, after only the United States and China. This saw the UK attract £30 billion in tech investment in 2021, and before the pandemic, **the digital sector contributed £148 billion (8%) of total UK GVA**. The sector is one of the best sources of economic growth and job creation across the country.

But new Government plans to reform online safety laws put this success at risk. The Online Safety Bill threatens to rewrite the rules around when digital firms are liable for the actions of individual users. These rules are the basis for the UK's tech success. Taken to its fullest extent, proposals could see almost 300,000 firms, overwhelmingly small or micro-businesses, regulated under this new regime with direct compliance costs of a crippling **£2.5 billion a year**.

This is a significant departure from where the UK is at present and would make the UK a global outlier in how liability is policed and enforced online. The framework provided for by the EU eCommerce directive has underpinned the success of new and growing UK digital firms for the last two decades and has offered firms both certainty and flexibility to operate across global markets.

With its departure from the EU, the UK is no longer required to legislate in line with the principles of the eCommerce Directive. The proposals put forward in the draft Online Safety Bill upend the legal and regulatory basis for the UK's tech success, creating instead an environment that is legally risky, costly and hugely burdensome for businesses. This will create substantially more barriers and red-tape than current rules. This threatens the UK's future economic growth and makes it a significantly less attractive place to start, grow and maintain a tech business. This is not building back better, but undermining the UK's potential.

In order to protect the UK's economic position and support post-pandemic recovery and growth, the draft Online Safety Bill needs significant reworking to bring it in line with historic global norms around online liability, as well as ensure that small firms and growing startups are not adversely burdened.

What is platform liability and how does it work?

Online service providers in the UK are not typically held liable for content uploaded to their platforms. This is a long-standing principle that has been underpinned for over two decades by the EU's eCommerce Directive which came into force in June 2000.

The eCommerce Directive sets out a wide range of rules for online services. This includes requirements around transparency and consumer information, and rules on what is permitted across commercial communications like advertising. But the Directive also sets out the framework for the liability of online platforms for the content which they transmit or host.[1]

The eCommerce Directive created a framework commonly known as the 'safe harbour' principle. Under safe harbour, online platforms are not held liable for the content which they transmit or host, provided they are unaware of any illegality. Once platforms become aware of illegal content, the Directive requires that services then act quickly to remove it - something which is strengthened by notice and take-down obligations. This matters for a wide variety of businesses: from social media platforms to online food delivery services. Any business that allows a user to upload content, from a photo of their holiday to a menu, is protected and enabled by the current liability framework.

This framework limits the liability faced by a service for the content that it facilitates, provided that it is not aware of the content's presence . Further to this, the Directive prohibits Member States from imposing general monitoring obligations on services to monitor users' content - a measure intended to protect privacy and freedom of expression. Individuals who upload and share illegal content are still individually liable for the content they share.

This framework has been successful in balancing the responsibilities of online platforms, protecting users from illegal content and in protecting users' rights.

This regime has offered certainty and flexibility to businesses, allowing them to adapt and to grow - accessing a global market with regulatory standards that are largely the same in key markets around the world. This has seen innovation thrive. Products and services can be created quickly and can operate under legal clarity. This has brought enormous economic benefits to the UK and has seen it become a genuine world leader in digital services. Figures from the Department for Digital, Culture, Media and Sport showed that, before the pandemic, the digital sector contributed £149 billion to the UK economy, growing by over 30% in under a decade. This represented almost 8% of total UK GVA.[2]

The UK has a large digital ecosystem comprising many tens of thousands of startups and small firms. The UK is the tech capital of Europe and is now only the third country in the world to pass 100 tech unicorns, after the United States and China.[3] Figures released last year by the Government show that **the UK tech sector received £30 billion in investment last year alone**. This sector is a continued source of economic growth and job creation across the country.[4]

The Online Safety Bill's changes to the UK's liability regime would put this investment, and the associated growth and job creation, at serious risk.

What has changed?

With its departure from the EU, the UK is no longer required to legislate in line with the principles of the eCommerce Directive, allowing it to erode the liability and general monitoring framework that has supported the growth of the UK's tech sector for 20 years.

The UK Government has stated that it intends to uphold the existing liability regime but has made no such commitment regarding the ongoing prohibition of general morning requirements.[5]

Despite this statement, the UK Government's forthcoming Online Safety Bill looks set to upend platform liability in the UK and inflict serious and long term damage on the UK's tech sector and the wider economy.

The draft Online Safety Bill and platform liability

The UK's forthcoming Online Safety Bill aims to make the UK 'the safest place in the world to be online'. The Bill will establish a regulatory regime that aims to address both illegal and "legal but harmful" content online - and it rewrites the rules for determining whether a platform is liable for the content which it hosts.[6]

To achieve the Government's ambitions, the Bill sets out new requirements for user-to-user services online to comply with new 'duties of care'. These duties of care set out the responsibilities of firms in relation to content that appears on their platform.

The Online Safety Bill will create new rules for user-to-user services. These rules will have a direct implication for how platforms are to be held liable for content in the UK:

- **Priority illegal content** - Where content is 'priority illegal content' services are required to use "proportionate systems and processes" to: minimise the presence of that content, minimise the length of time that it is present, minimise its dissemination, and to take it down once notified if it hasn't been removed already.
- **Other illegal content** - Where content is illegal, but not 'priority illegal', services are required to take "proportionate steps to mitigate and effectively manage the risk of harm to individuals" from illegal content.
- **Legal but harmful (children)** - Where content is 'primary priority content' services are required to prevent children from encountering it. Where content may be harmful but is not defined in secondary legislation, services are required to 'protect' children from encountering it.
- **Legal but harmful (adults)** - The largest (Category 1) services are required to specify in their terms of service how they intend to deal with legal content which may be harmful to adults.

These proposals are significant and represent a complete rewriting of how firms have historically been required to deal with illegal and potentially harmful content. The Online Safety Bill creates a framework where firms are required to act to minimise the presence of content proactively, rather than once they become aware or have been notified.

The Bill sets out a framework that effectively rolls back the eCommerce Directive's prohibition of general monitoring requirement by setting out a series of duties that requires services to proactively monitor, consider and moderate content. This is because firms will need to be aware of the content which is present across their platforms to prevent access.

To achieve this, the Bill proposes the creation of a new online safety regulator - a role which is to be fulfilled by Ofcom. Ofcom, as the regulator and enforcer of the new regime, is to be backed by significant powers to take enforcement action, such as issuing fines of up to 10% of the global revenue of services and by placing liability onto senior managers directly backed by prison sentences of up to two years.

The Online Safety Bill rewrites the platform liability rules for services operating in the UK. Firms will be:

- Held liable for a failure to prevent access to content on their platforms, rather than simply for a failure to remove such content once they become aware of it.
- Required to monitor and moderate content that is uploaded, ending the prohibition of a general monitoring obligation stemming from the eCommerce Directive.
- Held liable for a failure to prevent access to legitimate but potentially harmful legal material on their services.
- This is a significant departure from where the UK is at present and would make the UK a global outlier in how liability is policed and enforced online. This will make the UK a significantly less attractive place to start, grow and maintain a tech business.

What does this mean for businesses in the UK?

The UK has a world-leading digital ecosystem, and new, innovative companies are increasingly making use of flexible online platforms to offer new services, reach new customers and drive the UK's economic prosperity. Changing platform liability places all of this at risk.

These changes would fundamentally and negatively affect how online services can operate in the UK, with platforms facing both new legal risks as well as the large costs to implement additional processes to comply. This will likely impact on the profitability of all digital firms in the UK, ranging from the very largest, to the smallest with all having to comply with a new regime. In turn, this will affect employment, wage growth and more.

Who will it impact?

Until the scope of the Bill is finalised, it is not clear just how wide the net will be cast. The Government's risk assessment states that roughly 24,000 firms can be expected to be caught up in the new online safety regime, with the overwhelming majority of these (86%) being small or micro-businesses.[7] But the draft Bill does not have any criteria defining the size, scale or operational requirements of firms to be in scope, raising

serious questions about the accuracy of this assessment. Further, with the legislation still subject to change there remains the distinct possibility that the number of in-scope services will increase dramatically.

Proposals surrounding B2B services are particularly unclear. Without adequate and explicit definitions of and exemption for B2B services, then, according to the Government's own figures, approximately 180,000 businesses would be caught up in the new regime. That could be as many as 155,000 small and micro businesses saddled with enormous additional administrative burden and legal risk.

Added to this, it has been suggested by the Joint Committee on the draft Online Safety Bill that the scope of the Bill should be expanded to include "internet society services" likely to be accessed by children. If such a test were applied then, according to the ICO's impact assessment ahead of the introduction of the Age Appropriate Design Code, as many as 290,000 businesses would end up covered by the new online safety regime.[8] **If taken forward this would see around a quarter of a million small and micro businesses impacted by liability rule changes.**

	Current proposal (based on Government estimates without definition of scope)	If B2B remains in scope (based on Government estimates without definition of exemptions)	Joint Committee recommendations
Total number of businesses in scope	**24,000**	**180,000**	**290,000**
Direct compliance costs per year (£m)	**£205.8**	**£1543.5**	**£2486.75**

Table 1: Estimated number of businesses in scope, and direct compliance costs incurred per year under possible implementation scenarios.

In all of the above scenarios, the overwhelming number of businesses brought under a new online safety regime would be small or micro-businesses. This will mean that legislation, intended to regulate the very largest tech firms, would instead fall onto smaller firms. This is likely to see:

Disproportionate costs of compliance:

All in-scope firms in the UK will have to front expensive compliance costs to adopt new processes to comply. The Government's impact assessment for the Online Safety Bill put these costs at **£8,575 per business per year.** This will be especially pronounced for smaller firms, who will not be of sufficient size to roll out solutions at scale. Previous research, commissioned by the Government, found that for video-sharing platforms the cost of rolling-out of new online safety measures for small platforms paying up to £45 per user while larger firms had costs of between £0.25 and £0.50. Meaning that smaller firms in that market, many of which would be fast-growing and more likely to be loss-making, face compliance costs of **between 90 and 180 times more than their larger counterparts.**[9] This makes the Bill a gift for incumbents and a death knell for startups and innovation.

Indirect chilling effect:

The divergence of the UK from the existing liability regime created by the eCommerce Directive could have a significant and chilling knock-on effect. The rules and requirements for platforms operating in the UK will be stricter, and more costly, than elsewhere in Europe. It could be the case that larger firms choose instead to invest in other jurisdictions, or that smaller firms determine that it is too costly to start up in the UK at all. The Government's economic assessment of the impact of the new regime makes no attempt to qualify these indirect effects across innovation, competition, privacy or trade. All of this will cost the UK a great deal more.

As demonstrated in Table 1, the scope of the new online safety framework will have significant impacts on the economy. If the Government were to adopt the recommendations of the Online Safety Bill Joint Committee and extend the framework to cover all 290,000 internet society services operating in the UK, **the cost of direct compliance with the regime alone would total £2.5 billion a year.** Indeed, even the Government's own conservative estimate of compliance costs reaches £206 million a year - but this assumes that only 24,000 businesses are in scope of the new regime - something which is not guaranteed as inclusion thresholds are not set out in the draft legislation.

It should be noted again that compliance with new legislative requirements could make the running of smaller services economically unviable - and yet it is not these firms who the legislation was not designed to target. This includes new and innovative firms from across the UK's startup ecosystem - including food delivery, B2B, SaaS, digital collaboration tools, video games and dating apps. These new and burgeoning digital sectors have raised tens of billions in investment across the last decade, something which could be placed at risk.

Data adequacy and the wider economy:

Proactive monitoring of user-to-user interaction and activity will require data collection, storage and use in explicit breach of both the UK and EU GDPR's standards. The UK is currently considered to be data adequate by the EU. This allows for the free flow of personal data between jurisdictions, and is an enormous economic enabler, not just for digital businesses but for the whole economy.

Requiring general monitoring of all user-to-user interaction will be the end of the UK's adequate status, and will be a body blow for the majority of UK businesses, creating enormous compliance costs and hampering growth for UK PLC. **The Government's own estimates suggest that a loss of data adequacy would cost £1.4 billion in compliance costs.**

The UK's digital sector and data ecosystem is increasingly responsible for the UK's economic growth. Upending platform liability rules and creating general monitoring obligations in direct contravention of data protection norms won't just damage incumbent businesses, it directly threatens the UK's future growth. In order to protect the UK's economic position, and not to damage its future competitiveness, the draft Online Safety Bill needs significant reworking and the Government must not tamper with the UK's liability framework.

Businesses in scope and impacts: case studies of composite businesses

Case study 1 - A niche social platform

Niche Social Platform (NSP) is a relatively small business. They have less than 20 employees, and just over a million users. They are UK founded and based in London.

NSP's service provides a place for people to come together around social causes that matter to them. They can sign petitions, start campaigns and recruit colleagues and friends.

The nature of the platform means that users often start campaigns and petitions that are contentious to others. That might be calling for a business to give its employees a pay rise, or for a pension scheme to divest certain holdings. Sometimes, the subjects of these campaigns are unhappy about being named, and sometimes they will seek to take action against the user or NSP.

Currently, NSP is protected by the UK's liability regime, which has its roots in the e-Commerce Directive. NSP are, broadly speaking, not liable for content posted by their users, unless they obtain actual knowledge that it is illegal. A business that is being asked to pay its workers more via a campaign on NSP cannot, with any prospect of success, sue NSP.

It is this protection that allows the positive leverage that technology and the internet provides. It allows a team of under 20 to facilitate campaigns and petitions for good on behalf of more than one million people.

Any change to the UK's liability regime would not only be enormously damaging for the economy, but also for society.

Case study 2 - A messenger app

Messenger App is a startup app-based internet messaging service. It considers itself a competitor to services like WhatsApp. Messenger App's differentiating feature is that it collects no personal data on its users and does not serve advertising.

The service is used by privacy and data-conscious individuals, as well as by others who simply prefer the user experience. People use Messenger App to chat to friends and to keep in touch with family who are in different countries. Because Messenger App's messages are sent via the internet, it is much cheaper than SMS and MMS services. Indeed, it is free as long as the user's device is connected to mobile internet or WiFi.

The team at Messenger App is small. There are six full time employees, and they are mostly focused on engineering and keeping the service running. Messenger App is used by around 5 million people globally.

Messenger App does not, either through machine-based or human review, read and limit user messages. This is mostly because the team thinks it would be an invasion of privacy. Customers of Mobile Network Operators don't expect their calls to be listened to and their texts read by their providers. Similarly, users of Messenger App do not expect their private communications to be read by a company.

It is also because it would be impossible for Messenger App to operate if it had to monitor all messages sent using the service. Each user sends tens of messages a day, and so a startup with a team of six would need to monitor, and perhaps assess, upwards of 100 million messages a day.

The Draft Online Safety Bill recognises to some degree that this would be a ridiculous thing to require any private messaging service, never mind a startup, to do. SMS, MMS and one-to-one live aural communications are all excluded from the scope of the Draft Bill. But, currently, Messenger App would be in scope.

This must change. Not only would it be an invasion of privacy, it would also create a regime that was not applied equally to comparable services and that crushed startups.

Case study 3 - A two-sided marketplace

Haircut App is a UK-based two-sided marketplace app. The ambition of the service is to let customers get haircuts, colourings and blow dries at times and places convenient to them, while providing hairdressers and barbers with either an additional or alternative source of income to working in a traditional salon or barbershop.

Haircut App has raised two rounds of funding and has a team of around 50 people. They have about 3 million users, predominantly in London and other major cities.

The service allows hairdressers and barbers ("providers") to list themselves, their services, and portfolio images, alongside their prices and their areas and hours of operation. They are also allowed to set their prices, although Haircut App sets a floor price to prevent a race to the bottom. Customer users of the service can then browse by need, area and price before booking an appointment.

Once the booking is confirmed the provider and the customer are connected via Haircut App's basic messaging system. This allows them to confirm location, time and any special requirements or pieces of essential information. For instance, some hair treatments require heavy equipment, so it's important to know whether and how many flights of stairs there are.

This is an important part of the service, but the ability to communicate is a functional requirement rather than the purpose of Haircut App.

The Draft Online Safety Bill, however, barely distinguishes between Haircut App's functional communication and a Silicon Valley tech giant's instant messaging service. Because Haircut App facilitates user-to-user interaction, they will be required to monitor and assess for a range of content that there is little to no risk of on their service. They will have to undertake burdensome risk assessments and be able to demonstrate that they have taken account of the right to free speech.

The Government surely never intended for services like Haircut App to be in scope of the Online Safety Bill, but the current drafting firmly makes this the case.

Case study 4 - A social network for new parents

ParentPals is an online forum for new and experienced parents to connect, share stories and seek advice. Users can start threads and discussions, as well as comment on those started by other users.

The service has been going for just under ten years. The team is just under 25 people, and ParentPals has 10 million users, most of whom are based in the UK.

Alongside threads about the latest episodes of Succession, users have frank, firm discussions about parenting and what works and what doesn't. Language can be disagreed on and sometimes people can feel hurt that they have been disagreed with. ParentPals works to make sure that all conversations are civil, but it encourages diversity of thought and opinion. Parenting is an art, not a science.

It is also the case that ParentPals has content that other services, not targeted at parents, might consider graphic or explicit. This might be to do with breastfeeding, or the biology of pregnancy and childbirth, or with the challenges of conceiving. This content isn't obscene or inappropriate, but advertisers and algorithms often consider it and flag it as if it is.

ParentPals have long since accepted this, but they consider both robust conversation and reference and access to basic biological facts as crucial parts of the service that their users benefit from.

But now they are worried they may have to remove this content or risk falling foul of the Online Safety Bill. The Draft Bill describes content that is "legal but harmful" for both adults and children, but doesn't give a definition of what this content might be. ParentPals think that content they consider to be entirely appropriate might be considered "legal but harmful" by others, potentially including the regulator. As a small business, ParentPals will have to err on the side of caution. They cannot afford major regulatory uncertainty that might lead to fines they cannot afford to pay.

The Online Safety Bill was not designed to limit access to services like ParentPals, but without a real tightening of the scope and definitions in the Bill, it will.

Case study 5 - A food delivery app

FoodApp is a UK scale up that connects restaurants, delivery drivers and consumers. It allows for restaurants to sell their food as takeaway, allows delivery drivers to make extra money, and allows consumers to access their favourite food. FoodApp still has a relatively small team of around 100, and is used by just under two million consumers in the UK.

Restaurants upload their menus to FoodApp to allow consumers to make their orders. Further, FoodApp has developed a limited chat functionality to allow two parties to talk to one another if they need an update on the order status, or specific instructions for collection or drop-off.

FoodApp's users - whether restaurant, rider or consumer - don't have any ongoing contact with one another and cannot message each other outside of the specific delivery. FoodApp certainly don't think of themselves as a service that offers a true user-to-user service or allows for user-generated content.

Despite this, FoodApp's business is at major risk from the forthcoming Online Safety Bill and a revised liability framework. They will be responsible for making sure that nothing legal but harmful is said by any user of the service in the service, and further will be liable for anything that is legal but potentially harmful in the menus that are uploaded.

The Online Safety Bill was not designed to capture businesses like FoodApp, but in its current form it will seriously threaten the viability of businesses like this.

What the Government needs to do to protect startups, micro and small businesses

The forthcoming Online Safety Bill aims to create a safer online environment in the UK, but instead it will encumber some of the most innovative and growing businesses in the UK with new liability rules, out of step with other countries. In order to make the Bill fit-for-purpose, the Government must make the following specific changes to protect the wider digital services ecosystem in the UK from significant damage:

Maintenance of the intermediary liability regime and protections:

There is a real risk that the Government, through the Online Safety Bill, will upend the intermediary liability regime that has seen the UK's tech sector go from strength to strength, providing jobs, investment and growth. Significantly altering or even removing the regime and its protections would be a hammer blow not only to the UK's tech sector, but the wider economy with the risk of losing data adequacy. The Government should commit, immediately, to maintaining the UK's intermediary liability regime and its protections.

Explicit carveouts for B2B and SaaS:

The draft Online Safety Bill does not properly consider the range of business models across the tech sector. While there are some explicit exemptions, such as for emails or SMS, the Bill makes only limited mentions of 'internal business services'. But this wording could still see many business-to-business (B2B) or software as a service (SaaS) models, which make up a large proportion of the UK's digital landscape, and which pose incredibly low risks for harmful content, brought into scope of the new regime. The Government should include carveouts for such firms on the face of the Bill.

Taking legal content out of scope:

The types of content covered by the Bill are far too broad. It creates a mechanism where duties towards perfectly legal content in the UK are more burdensome than towards illegal content in the EU. All in-scope firms are required to meet this requirement in some form, and in doing so will face increased compliance costs as a result. This approach is not sustainable in the long run. The Government should reduce the scope of the legislation to apply only to illegal content to reduce knock-on impacts across extending liability and to reduce the direct costs of complying with a new online safety regime.

Reflecting the 'safe harbour' principle:

The Bill marks a significant departure from the existing principle of safe harbour. It creates new legal duties for firms to proactively monitor and remove content, backed by significant fines. Instead, the Government should reflect other approaches around the world to modernise online safety rules, such as the EU's Digital Services Act which introduces tough new rules for illegal content with fines for non-compliance but that protect the principle of safe harbour and the liability framework that has underpinned the tech sector's enormous success and positive impact.

References

[1] *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce), European Commission, June 2000*

[2] *DCMS Sectors Economic Estimates 2018: GVA, DCMS, February 2020*

[3] *The UK hits milestone of 100 UK tech companies valued at $1bn or more, Tech Nation, June 2021*

[4] *UK tech sector achieves best year ever as success feeds cities outside London, DCMS, December 2021*

[5] *The eCommerce Directive and the UK. DCMS, January 2021*

[6] *Draft Online Safety Bill, DCMS, May 2021*

[7] *The Online Safety Bill, Impact Assessment, April 2021*

[8] *Age Appropriate Design Code, Impact Assessment, July 2020*

[9] *Understanding how platforms with video-sharing capabilities protect users from harmful content online, EY, August 2021*