The Online Safety Bill - a Ticking Time-Bomb for UK Startups

September 2022

COADEC

Authors

Dom Hallas
Executive Director
The Coalition for a Digital Economy

Camilla de Coverley Veale
Policy Director
The Coalition for a Digital Economy

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 2000 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 is home to a thriving and world-leading tech ecosystem. At the heart of this lies tens of thousands of startups and small businesses. Widely regarded as Europe's leading startup hub and topping nearly every metric of Europe's startup universe, the UK is now the third country in the world to pass 100 tech unicorns, after only the United States of America and China. The UK attracted £30 billion in tech investment in 2021. The sector is one of the best sources of economic growth and job creation across the country.[1]

Yet, plans to create the democratic world's strictest internet laws threatens this success and risks the UK being branded a global outlier in digital regulation.

The Government's Online Safety Bill will regulate a wide range of both illegal and so-called "harmful content". It plans to do this by making any business that enables, or could enable, user-to-user interaction - for example chat forums, cloud storage and certain productivity tools - have systems and processes in place to deal with content deemed unacceptable by the legislation. This includes content which is legal. The systems and processes platforms are expected to take are complex and exacting, and effectively make platforms liable for the legal actions of their users.

By the Government's own estimates, more than 25,000 businesses and other organisations will fall under scope of the new rules. And the Government's impact assessment acknowledges that 180,000 businesses will have to consider whether they are in scope, the overwhelming majority of which would be small and micro platforms.[2]

For these businesses, the Bill is a difficult to navigate minefield of duties, considerations, and obligations, littered with issues. As it stands, the Government's approach to online safety is wide-ranging, convoluted, and risky. If the Bill moves forward in its current state, startups operating in the UK will inevitably face a heavy compliance burden and will be forced to front expensive administrative costs to comply. This will very likely have the knock-on effect of pushing startups to other nations and depressing innovation in the UK.

Worryingly, there is also scope for the Bill to get a lot worse. With the Bill still open to further significant changes, there is a real risk that amendments could be rushed through with little Parliamentary scrutiny. Any further expansion of an already problematic Bill has the potential to decimate the thriving startup ecosystem the Government has worked hard over more than a decade to create.

The Online Safety Bill a ticking time bomb for the UK's startup ecosystem, but it can be defused. There are a number of significant improvements that will need to be made to the Bill for it to make a positive impact for individuals and society, and for it to be workable for startups and business more broadly. These improvements would protect the UK's world-leading tech ecosystem while achieving the Bill's aims.

The Online Safety Bill - a Minefield of Bad Regulation

The Government, in a bid to make the UK “the safest place in the world to be online”, has created a sweeping piece of legislation that goes beyond anything else in the democratic world, and far beyond the initial ambitions for online safety in the UK. These wide-ranging and draconian measures will be seriously detrimental to the digital economy, to digital innovation, and to the digital experience of citizens in the UK.

As it stands, the Online Safety Bill is full of issues that will be disproportionately felt by the startup community, the drivers of innovation in business across the UK. Over 97% of the firms in scope of the Bill are micro, small, and medium-sized businesses: the backbone of the British economy.

To date, the potential implications of the Bill on free speech have garnered the most public attention. We believe the Bill is a risk to free speech because of the way it will incentivise over-removal of content. Provisions in the Bill also effectively outsource policing to platforms - startups do not want to be put in this position. But there are many serious issues with the Bill that go beyond free speech concerns.

A real risk of over-moderation and an impact on free speech

One of the most problematic aspects of the Bill is the types of content it covers, ranging from “priority illegal” content through to “harmful” content that is legal, with various shades in between.[3]

This approach to moderating content is complex, convoluted and a complete departure from how firms have historically been required to deal with illegal and potentially harmful content. Inevitably, this will create confusion for services attempting to comply and result in the over-moderation of content.

Instead of explicitly setting out which content is and is not legal online, the Bill leaves this determination to services themselves. Government amendments that attempt to clarify how services should approach different kinds of content, while language such as "reasonable grounds to infer that content is content of a particular kind", create a very low bar.[4] Indeed these amendments suggest that service providers will be required to apply a significantly lower standard of proof to online content than a criminal court would apply to offline content. Consequently, we anticipate that companies will take a precautionary approach to content, erring on the side of over-removal to avoid penalties for non-compliance. This will have an impact on the freedom of expression of citizens.

Broad scope capturing the UK’s entire digital economy

While the Government set out to design a framework that reined in the largest social media companies, a steady and constant expansion of scope has left us with a Bill that captures and regulates almost every online service provider operating in the UK. By the Government’s own estimates, more than 25,000 services will fall in scope of the Online Safety Bill. Of these, over 20,000 will be micro businesses.

This means that even the smallest businesses will have to comply with burdensome safety duties created for the biggest digital players. According to the Government’s own figures, 81% of businesses in scope of the new requirements will be micro businesses, and SMEs will make up over 97% of all services in scope. Less than 3% of the services in scope will be the larger firms, such as popular social media platforms, that the regime was intended to capture.

Table 1: Number and size of businesses in scope of the new regime in the Bill's Impact Assessment

Business Size	Micro	Small	Medium	Large	Total
Number	20,250	1,220	2,910	680	25,060
% of Total	80.81%	4.87%	11.61%	2.71%	
Cumulative %	80.81%	85.67%	97.29%	100%	

The Bill tries to create a graduated approach to tackling content depending on the size of and risk presented by services but fails. The biggest and riskiest user-to-user services (Category 1 services) will face the most burdensome requirements. Services that allow user-to-user interaction or the sharing of user-generated content where the risk of harm is considered to be lower than Category 1 will be considered Category 2B services. The biggest and riskiest search services will be considered Category 2A. The Government has estimated that based on current policy intention, between 30-40 platforms are expected to be designated as either Category 1, 2A, or 2B. This estimation leaves approximately 25,060 services captured as "other regulated services". The Government's impact assessment says that 20,200 of these will be micro businesses. These will include new social media platforms, startup chat forums and niche social dating sites to name a few. These "other regulated services" will have a duty to comply in essentially the same way as those considered both larger and riskier. This includes startups developing productivity and collaboration tools that were never intended to be the target of forthcoming regulation.

Costs of compliance

All in-scope firms will have to front expensive compliance costs to adopt new processes to comply. The Government's own Impact Aassessment for the Online Safety Bill put these costs at £9,988 per business per year.[5] For micro businesses, the same impact assessment assesses the incurred cost of the Bill at £3,259 over ten years. We believe these costs are a considerable underestimate.

Table 2 : Compliance costs for businesses by size in the Bill's Impact Assessment

	Total Costs (10 year)	Businesses	Costs for Business
Micro[6]	£66,000,000	20,250	£3,259
Small[7]	£10,200,000	1,220	£8,361
Medium[8]	£608,700,000	2,910	£209,175
Large	£1,522,900,000	680	£2,283,676

The Government's estimates say that they expect the costs to Category 2A, Category 2B and 'other regulated services' to be about 1.9% of turnover, but that this could be as high as 3.8% in the assessment's high cost scenario. This can be compared to a figure of 7.5% of annual turnover for Category 1 services - with the potential to be as high as 15%. However, the Impact Assessment only considered the costs incurred for services removing illegal content. It does not factor in that the platforms, through child safety duties, will have to take action against legal content designated 'primary priority'. Such action will drastically increase the cost of compliance.

And while only in-scope platforms will be required to front compliance costs, some platforms that could potentially fall in scope under a broad interpretation of the regime will have to read and familiarise themselves with the regulations. For many firms this will mean hiring specialised lawyers to interpret the Bill's application. Given that 180,000 services could potentially be in scope, the overall familiarisation costs faced by services operating in the UK are monumental and have been seriously underestimated by the Government.

The Government's Impact Assessment estimates that one regulatory professional at an hourly fee of £20.62 is expected to read the regulations for each potentially in-scope business, spending just four hours to read the 52,000 words of explanatory notes accompanying the Bill.

Not only does it seem farcical that any capable regulatory professional would charge less than £90 for four hours of work, according to the costs estimated by the Government, but it is also hard to believe that in four hours this professional would read, digest, and analyse a Bill that has been five years in the making and required significant reworking. The Impact Assessment goes on to assume that firms would only seek one hour of legal advice, with a central estimate of £0.8 million, meaning that advice was secured at less than £33 an hour for small and medium-size businesses, a fraction of the likely actual cost. A trainee at a mid-tier law firm bills out at closer to £200 an hour.

These large underestimates are repeated throughout the Impact Assessment. For example, it assumes that some micro businesses could amend reporting functions to comply with the Bill with only one hour of programmer time. It even assumes that this could be achieved in the largest, riskiest platforms with only 20 hours of programmer time.

Table 3: Assumed amount of programmer time to develop or amend reporting functions by business size and risk in the Bill's Impact Assessment

Platforms	Micro	Small	Medium	Large
Low risk	1 hour	2 hours	4 hours	6 hours
Medium risk	2 hours	4 hours	6 hours	8 hours
High risk	8 hours	12 hours	16 hours	20 hours

Given that the Bill provides that all services in scope will have to conduct children's risk assessments, illegal content risk assessments, and high-risk firms will have to submit annual transparency reports to Ofcom, these figures are divorced from the reality of compliance.

It is also worth noting that the Regulatory Policy Committee's assessment of the cost-benefit analysis associated with the Bill was only 'satisfactory', stating that it would have been improved by focussing on the costs associated with legal but harmful content for adults, and risks to freedom of speech and privacy.[9]

The Government stated that it has only estimated the costs of the published primary legislation. And that it has not yet included estimates of the costs to services as they familiarise themselves with the secondary legislation underpinning the Bill, or with Ofcom's future codes of practice.

The scanning of private communications

While at present, the Bill does not explicitly mandate the scanning of private communications, it does require services in scope to prevent individuals from encountering certain content - such as priority illegal content. For providers of private communications services, prevention is only possible if messages and other communications are monitored, thereby undermining any end-to-end encryption. Exemptions in the Bill for certain private communications providers, such as email, SMS, and MMS services, do not go far enough. Even the largest encrypted messaging services, including Whatsapp, have already warned that their services may have to be pulled from the UK market if the Bill reaches the statute books in its current form.[10] This will also inevitably mean that any startup offering private communications with end-to-end encryption will be forced to tear down their business model or be pushed out of the UK.

Age verification

The Online Safety Bill will force services in scope to verify the age of their users to undertake a child user assessment and then to comply with safety duties. This requirement will stifle competition, damage consumers, and destroy startups.

While the Bill does not explicitly state that services must implement age verification measures, it will be essentially impossible for regulated services to comply with all the duties the Bill places on them without knowing the age of their users. This is because the Bill places additional duties on services likely to be accessed by children. But this will inevitably impact any service that could possibly be accessed by a child. As a result, any online service that might have even the smallest number of children using it will have to consider one of two options - developing multiple different products for child and adult users, or implementing an age-gate to bar younger users from accessing the service altogether. Both options would require the service to collect age verification or assurance data for all adult users and would create a two-tier internet that will remove the agency of children. This would be an immense cost and effort for startups that may not have the technologies available to them in the same way larger services do.

How Bad Can it Get?

Worryingly, there is also the scope for the Bill to get a lot worse. The legislative progress of the Bill was paused in mid-July, leaving it open to amendments in both Houses of Parliament. There is real potential for the Bill to be steered in a direction that would be catastrophic for startups and for the UK's innovative tech ecosystem. To avert danger, the Government needs to avoid the following:

A Bill that would direct R&D spend

Any duties or requirements that would constitute a significant and invasive interference in service providers' freedom to conduct their business would be disastrous for startups. This includes any changes to the Bill that would direct the R&D spend of providers in a way that is not already set out.

For example, the Bill currently provides that for user-to-user services, the future online safety regulator, Ofcom, may issue a notice requiring the use of Ofcom-accredited technology to prevent individuals from encountering certain types of content. This already creates expectations which only largest companies will be able to fulfill: expecting startups and scale-ups to avail themselves of those tools could already have a detrimental impact on the UK tech sector's healthy competitive environment.

Any move that would extend this provision to mandating that service providers develop their own technologies to address certain types of content would be unnecessary, disproportionate, and would defy existing domestic regulatory precedent as well as international precedent. It would also have the inevitable consequence of stifling innovation amongst compliant service providers who will be reluctant to commit significant expenditure in research and development in safety tech in circumstances where Ofcom has the powers to undermine such investment decisions.

A Bill that is extended in scope to cover all internet society services

By the Government's own estimates, more than 25,000 services will fall in scope of the Online Safety Bill. And the Government's impact assessment acknowledges that 180,000 businesses will have to consider whether they are in scope, the overwhelming majority of which would be small and micro platforms. This goes far beyond the original intention of the Bill which was aimed primarily at the largest social media platforms. But the 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.

Added to this, it was suggested by the Joint Committee on the draft Online Safety Bill that the scope of the Bill be expanded to include all "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. If taken forward this would see over a quarter of a million small and micro businesses impacted by liability rule changes.

Any extension of the scope of the Bill, further than the Government's own estimates would crush the UK's thriving tech ecosystem and push innovative businesses to other regions.

A Bill that upends the existing liability regime

The UK's existing liability framework 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. This framework limits the liability faced by a service for the content that it facilitates, underpinned by a prohibition of general morning requirements.

The proposals put forward in the Online Safety Bill set out that firms will be required 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 where it is considered "priority illegal content" and "harmful to children".

While the Government has stated that it intends to uphold the existing liability framework it must honour this commitment by ensuring that the Bill does not create a regime by which services are held liable for failure to prevent access to content, including failure to prevent access to legitimate but potentially harmful legal material on their services.

A Bill that upends the existing liability regime would create an environment that is legally risky, costly, and hugely burdensome for businesses and would inflict serious and long-term damage on the UK's tech sector and the wider economy.

Is the Bill Fixable?

If the Online Safety Bill continues down its current path, or if it is steered in an even more extreme direction, it will encumber some of the most innovative and growing businesses in the UK. But it is not too late. The Bill can be fixed so that it supports the UK's thriving startup ecosystem, rather than destroying it. To achieve this, the Bill will need significant reworking. As the Bill enters a new stage of negotiations, the following principles need to be brought to the fore:

A Bill that is easy to comply with

The hallmark of good regulation is that it should be easy for companies to understand and fulfill their duties. But, as it stands, the Bill is both abstract and overly complex. For it to be workable for startups and positive for individuals and society, we need to adopt a back-to-basics approach.

The proportionate systems and processes approach at the core of the new framework is right, but this is undermined by other parts of the Bill. Of particular concern are the types of content covered by the Bill, which 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. What's more, the Bill places the determination of what content is unacceptable, and how this content should be approached, on the services themselves whilst providing a significantly lower standard of proof than a criminal court would.

To aid compliance amongst services in the scope, the Government needs to reduce the scope of the Bill to apply only to illegal content to reduce the direct costs and complexity of complying with a new online safety regime.

A Bill that is clear on scope

As it is, the Bill does not properly consider the range of business models across the tech sector. In doing so, tens of thousands of businesses for which the Bill was not initially intended fall in scope of regulation intended for the biggest online platforms. This will have a chilling effect on competition in digital markets and on the willingness of entrepreneurs to found businesses that may be within scope of the online safety regime.

To avoid this the Bill must be clear in scope, explicitly setting out which types of services fall in scope and under which category. The Bill is right to take a graduated approach to tackling content depending on the size of and risk presented by services, but it is unhelpful that more than 20,000 micro businesses will be considered an “other regulated service” and forced to comply with many of the same duties as those in Category 2B.

And while there are some explicit exemptions, such as for emails or SMS, the Bill makes only limited mentions of “internal business services”. This exemption for “internal business services” is overly vague and could 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 carve-outs for such firms on the face of the Bill.

A Bill that mandates outcomes rather than routes to get there

Despite its commitment to make the UK “the safest place in the world to be online”, the framework as set out in the Bill does not mandate specific outcomes to reflect this commitment. Instead, the Bill mandates very specific routes for services to take, many of which are not appropriate nor proportionate for the large majority of businesses who will be affected by the legislation - micro, small and medium-sized businesses.

For example, the ability for the regulator to require services to tackle certain types of content through the use of specific accredited technology, including the use of proactive technology, could be a counter-productive for many services. For private communications providers, they could be left with no option but to undermine the end-to-end encryption model underpinning their service.

It is also only reasonable to assume that tech giants would benefit from their ability to license compliance support and systems if certain technology is mandated. This could include content detection and reporting systems, for startups to purchase, creating the irony where the companies targeted by the legislation will ultimately profit financially from it. We can absolutely foresee a situation where those companies become the de facto outsourced regulator for startups and scaleups, screening UK startups’ data flows through content filters run by companies already guilty of global and fundamental privacy violations.

The lack of flexibility created by the Bill, in mandating routes to improve online safety, rather than outcomes risks pushing away innovative tech businesses from setting up shop in the UK and taking the tech sector further away from a healthy competitive environment.

Businesses in Scope and Impacts: Startup Case Studies

Case study 1 - An online dating platform

AuthenticMe is a London-based niche social and dating mobile app geared towards mature professionals working in the creative industries. Founded in London in 2016, AuthenticMe has just over 300,000 users and employs 6 full-time employees. The company's mission is to make dating simple and stress-free, allowing like-minded individuals to connect in safe and meaningful ways.

The platform is proximity-based and uses proprietary technology to suggest compatible matches to users. It generates revenue through subscription of premium services only, which allow users to connect, and chat with, an unlimited number of profiles each day. As well as providing an in-app chat experience, AuthenticMe also has media-sharing features that allows users to upload photos and videos of themselves onto a public profile.

AuthenticMe designs and markets its platform towards mature professionals, and employs various measures to prevent anyone under the age of 18 from registering or using any of the service. AuthenticMe is therefore concerned about proposals in the Online Safety Bill that amount to a requirement for services to verify the age of their users. Any requirement to incorporate age-verification features would not only be largely redundant given the platform's user base, it would be a huge compliance cost that would undermine the age assurance measures already in place.

In fact, the overall burden of compliance is concerning for AuthenticMe who fear they will have to bear a number of additional costs to adhere to the new regulations. The platform already faces huge competition in the social and dating app space and larger competitors, who have had better resources in place for years, will be much better placed to implement the costly systems and processes needed to comply with the new regime. Duties, including those related to risk assessments, and high familiarisation costs could result in AuthenticMe relocating and opting out of serving UK users in order to avoid compliance issues.

The Bill would not only serve to give a leg-up to the platform's larger competitors in an-already heated market, they would also undermine AuthenticMe's users' safety on the platform.

Case study 2 - An encrypted messaging service

SecureApp is a free and secure communications start-up based in the UK. The company says that it is more secure than other encrypted messaging services, and has recently seen a fourfold increase in its new users following controversial data policies implemented by larger competitors in the space. The service is used by privacy and data-conscious individuals, as well as by others who simply prefer the user experience.

SecureApp's selling point is that it is not only end-to-end encrypted, but also that 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 SecureApp is small. There are five full time employees, and they are mostly focused on engineering and keeping the service running. SecureApp is used by around 7 million people globally, including by government officials.

SecureApp was founded on the basis of true end-to-end encryption. That means that only those participating in a conversation through the service can see the conversation. Those in the conversation host the conversation, and keep the data which means that the app itself does not keep eavesdrop or keep tabs on what is said between users. SecureApp believes that this would be an invasion of privacy.

It would also be impossible for SecureApp 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 five would need to monitor, and perhaps assess, upwards of 100 million messages a day.

The Online Safety Bill rightly provides exemptions for certain types of private communications such as email, SMS and MMS services. But, currently SecureApp would be in scope.

The current provisions in the Bill, exempting certain types of private communications need to be extended to all forms of private communication including startups like SecureApp. If not, the Bill will destroy the ability of SecureApp's users to trust or even use its service, effectively bringing the businesses to an end.

Case study 3 - A Web 3.0 social media platform

Grow is a blockchain-based social media network dedicated to growing a community of like-minded people to learn and do business with. Grow was founded in the UK in 2020 with the goal of shaking up and providing an alternative to the largest social networking platforms. Like many Web 3.0 startups it is working towards being a fully decentralised platform. It operates on top of the Ethereum network.

Grow is a website as well as a desktop and mobile app. The network works by awarding tokens built on the Ethereum network to its users based on their engagement with the site. In turn, users spend tokens to post and promote their content. The tokens can also be bought and redeemed for cryptocurrencies or conventional funds. As such, users on the network interact through the medium of a 'digital wallet' rather than as an individual, and this wallet address is the only identifying factor for each individual interacting with Grow. At the same time, individual users interacting with the crypto world, including Grow, often control more than one wallet, and there is no limit to the number of wallets an individual can control.

Unlike a Web 2.0 social media platform, Grow's users are essentially part-owners of the network. They share in any value creation while also being able to participate in the platform's governance and operation. This means that instead of being owned by a centralised institution, like traditional social media platforms, the community owns the network in a way that is increasingly decentralised.

Grow will find it very difficult, if not impossible, to comply with the Online Safety Bill. This is because Grow interacts with wallets not individuals - therefore attempts at verification are not feasible (or are at least very hard to implement). Ownership and governance is also decentralised - meaning there is no strong central body that could easily implement regulation.

With its strong record in financial services and Fintech, the UK has the potential to be a world leader in the crypto asset sector. Grow benefits from operating in this environment and has seen its user base grow considerable over the last few years. In 2021, Grow experienced 20 million visits to its network.

Where the United States of America won the Web 2.0 race, the current regulatory environment here means that there is a good chance the UK could win Web 3.0 - but the future regulatory regime proposed by the Online Safety Bill could completely scupper this.

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 both "harmful to adults" and "harmful to 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 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.

Case study 6 - 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 7 - 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.

References

1. UK tech sector achieves best year ever as success feeds cities outside London, DCMS, December 2021
2. The Online Safety Bill, Impact Assessment, 31 January 2022
3. The Online Safety Bill, DCMS, as amended in the Public Bill Committee, 28 June 2022
4. The Online Safety Bill, as amended 11 July 2022
5. The Online Safety Bill, Impact Assessment, 31 January 2022
6. Microbusinesses are defined as those employing between one and nine full-time equivalent (FTE) employees, Better regulation framework: guidance, March 2020
7. Small businesses are defined as those employing between 10 and 49 full-time equivalent (FTE) employees, Better regulation framework: guidance, March 2020.
8. Medium-sized businesses are defined as those employing between 50 and 249 full-time equivalent (FTE) employees, Better regulation framework: guidance, March 2020.
9. Regulatory Policy Committee, The Online Safety Bill, February 2022
10. Whatsapp CEO Will Cathcart speaking on BBC's Tech Tent podcast, 29 July 2022