Fountain Court

Quarterly Commercial Crime Newsletter:

COMMENTARY

The Online Safety Bill – Making the UK the Riskiest Place in the World to be a Compliance Officer?

APRIL 2023

AUTHOR

Clare Sibson KC
Call Date: 1997
Silk Date: 2016
Read more

This article considers the Online Safety Bill in the context of the government's manifesto commitment to make the UK the "safest place in the world to be online". The article gives an overview of Ofcom's enforcement powers, highlighting in particular the Bill's unconventional approach to holding individual senior managers criminally liable for corporate failures to comply with information notices.

The Online Safety Bill was introduced in the House of Commons in March 2021. At the time of writing (and one Parliamentary Session later), the Bill is before the House of Lords: it has had its second reading and awaits consideration in Committee.

Although the Bill's objectives are relatively narrow (particularly when compared with the more comprehensive aims of the EU's Digital Services Act[1]) its passage has been neither swift nor smooth. One third of the government's original flagship measure (designed to deliver its manifesto commitment to "*make the UK the safest place in the world to be online*") has been withdrawn. In terms reminiscent of several police forces' recent attempts to monitor and prevent 'non-crime hate incidents',[2] the Bill originally sought to impose a duty on the largest platforms to moderate 'legal but harmful' (that is, offensive but not criminal) content accessible to adults.

[1] Entered into force on 16 November 2022.
[2] See *R (Miller) v College of Policing* [2022] 4987.

Faced with compelling opposition, this has been abandoned. The main focus of the Bill is now the control of 'illegal content' (a concept itself defined,[3] with priorities that include terrorism offences and child sexual exploitation and abuse) and the imposition of age restrictions to access online pornography.

Nevertheless, even as amended, if passed the Bill will represent to online service providers a steeper increase in burden of regulation than has ever been experienced by the finance and banking sectors, including in the wake of the 2008 banking crisis. It will represent a greater degree of supervision of social media platforms than was ever proposed for print media – even at the height of public concern over the 2011 phone hacking scandal. In short, the Bill attempts to impose upon digital service providers a series of brand new, self-styled 'duties of care' (largely, obligations of process) which will – if enforced – revolutionise the relationship between Big Tech and the State. Will Cathcart, head of WhatsApp for Meta (the company formerly known as Facebook), has already indicated[4] that the company will not comply with what it perceives to be the Bill's requirements[5] in respect of moderation of end-to-end encrypted messages between private users – leaving open the question whether Meta would withdraw WhatsApp from UK users in the event the Bill passes in its current form.

This article – concerned as it is with commercial crime – will focus upon the Bill's most significant offence creating provisions from the perspective of the online services industry. If enacted, the Bill will create other offences – not discussed here – for which online service *users* will be liable. These include the offence of false communication (where a person, without reasonable excuse, sends a message knowing it to be false and intending to cause non-trivial psychological or physical harm to a likely audience)[6] and the offence of threatening communication (where a person conveys a threat of death or serious harm, intending, or reckless as to whether, an individual encountering the message will fear that the threat will be carried out).[7] Significant as these might be in protecting members of the public from harassment and abuse, they are unlikely to be an immediate focus of concern for the industry itself: by clause 163(4) of the Bill, "*a provider of an internet service by means of which a communication is sent, transmitted or published is not to be regarded as a person who sends a message.*"

Although (as discussed in the conclusion of this article) this is likely to change, in the form the Bill was brought from the House of Commons to the House of Lords, the offences for which online service providers will be liable are limited to 'information offences'. Despite their name, these *do not* concern the dissemination of false, illegal, or otherwise harmful information or messages. Rather, they are provisions designed to enforce compliance with 'information notices' (in substance, production orders) issued by Ofcom.

It is these information notice offences which will be the focus of this article. In particular, the article will examine the highly unusual form of individual criminal liability the Bill proposes for these offences.

Before turning to that topic, it is worth considering the narrowness of the policy objectives behind the Bill; these contrast with the more ambitious aims of the EU's Digital Services Act.

---

[3] See Clause 53.
[4] See here.
[5] It remains to be seen whether the 'disapplication' provision of Part 2 of the Bill in fact addresses Mr Cathcart's concern.
[6] Clause 160.
[7] Clause 162.

The UK and the EU: Different Policy Objectives

The Explanatory Notes to the Online Safety Bill as brought to the House of Lords on 18 January 2023 make clear the government's policy objective:

> "*As use of the internet has expanded, there is growing public concern about the prevalence and spread of illegal online content, as well as the risk to children's safety arising from exposure to inappropriate content, such as pornography.*"

Consistent with this statement, the Bill has two, primary areas of focus: service providers' own systems and processes for the prevention and removal of 'illegal content'; measures designed to protect minors from harm and from accessing online pornography.

In contrast, the EU's Digital Services Act ("**DSA**") seeks to regulate almost all functions of the online platforms that act as intermediaries (or '*gatekeepers*') between different individuals, between individuals and the markets, and between individuals, the media and the State. Countering illegal online content is *one* of the EU's aims, but it is one of many and amongst the least ambitious. The dominant impetus behind the DSA was Community concern about the long term social and political impact of opaque algorithms designed to connect online users with products (which they are likely to buy) and with other users (who are likely to share and reinforce their views). EU policy makers were at least as concerned about consumer protection in online marketplaces, and about the growing prominence of online 'echo chambers' as *the* source of public understanding of national and international affairs, as they were about teenagers' ability to work around parental controls for X-rated videos.

To this end, the EU's DSA contains new rules which (among other things):

- ban the use of 'dark patterns' (tricks that manipulate users into choices they otherwise wouldn't make);
- ban advertising that is based upon profiling of children, or upon certain categories of personal data (e.g. ethnicity, political views and sexual orientation);
- increase transparency over the algorithms used by online platforms to recommend products, or select news stories for users;
- enable the tracing of online sellers and their products;
- allow users to challenge a platform's content moderation (such as when a user's account is removed or restricted);
- impose new obligations on very large online platforms and search engines to mitigate against certain risks, including election manipulation and the spread of disinformation.

The Online Services Bill is nothing like as comprehensive as the DSA. Algorithms explicitly feature in the Bill, but mainly to the extent that they might be used to reduce the spread of 'illegal content', or access to pornography by minors. As for all the other concerns which drove the introduction of the DSA in Europe, some have echoes in the Bill – but the echoes are weak and buried in clunky, circuitous drafting. For example, where the EU has banned dark patterns, prohibited the use of targeted campaigns based on political or ethnic profiling, and imposed obligations to mitigate the risk of election manipulation, clause 13 of the Bill will simply oblige Category 1[8] service providers to adopt:

"*… proportionate systems and processes designed to ensure the importance of the free expressions of content of democratic importance is taken into account when making decisions about how to treat such content.*"

[8] The highest reach user-to-user services with the highest risk functionalities. See here.

This is the context in which the duties of care proposed in the Bill should be understood. In reality, the Bill will impose little by way of substantive or objective standard upon online service providers. Instead, when passed into law, it will require service providers to design and adopt their *own* procedures to minimise illegal content, protect children and restrict underage access to pornography, as well as to consider other 'important' matters (like 'democracy') in their 'decision making'. This is not to deny that the Bill will impose a considerable burden of red tape on online platforms, nor to detract from Ofcom's powers (under the Bill if enacted) to issue codes of practice and develop guidance further to define what is meant by concepts like 'harmful to children'. It is only to say that the primary legislation itself will impose burdens which are, first and foremost, process orientated. Ironically for the first major program of legislation written from scratch by the UK since its exit from the EU, the Online Safety Bill looks very much like a framework for bureaucracy – with all substantive decisions about standards being passed to an as-yet-to-be-established relationship between Ofcom and the industry.

Online Safety Bill: Principal Duties

The principal duties which the Bill will impose on all online user-to-user and search engine services are:

- illegal content risk assessment duties, together with a duty to use proportionate measures in the design and operation of the service to prevent users from encountering priority illegal content and to prevent the service being used to commit or facilitate priority offences;
- children's risk assessment duties, together with a duty to use proportionate measures in the design and operation of the service to mitigate and manage the risk of harm to children and to prevent children of any age encountering primary priority content that is harmful to children (for example, by using age verification measures);

On Category 1 service providers, the Bill will impose additional duties, including:

- a duty to provide features which enable adult users, if they wish, to increase their control over their exposure to certain types of content (including information about suicide and self-harm behaviours);
- a duty to consider the importance of 'democratic importance content' when making decisions about content;
- a duty to consider the importance of 'journalistic content' when making decisions about content;
- a duty to notify the relevant 'news publisher' before taking action in relation to 'news publisher content'.

Category 1 and Category 2A service providers will also be subject to a duty to use proportionate measures to prevent the use of their services for fraudulent advertising.

Ofcom's Powers

To ensure the digital services industry complies with these new obligations of process, the Bill[9] enlarges Ofcom's duties. To Ofcom's existing functions under section 3 of the Communications Act 2003, the Bill will add responsibility:

> "*to secure…the adequate protection of citizens from harm presented by content on regulated services, through the appropriate use by providers of such services of systems and processes designed to reduce the risk of such harm*."

Arguably, this does no more than hand Ofcom responsibility to audit the internal procedures by which online service providers monitor content (by their own

[9] See clause 82.

internal standards). It remains to be seen to what extent Ofcom will succeed in using this obligation as a normative power, declaring what content is and is not acceptable. In this respect, there is a potential contradiction between the removal of the Bill's original objective to moderate 'legal but harmful' content, and the definition of harm which it will be Ofcom's role to protect all 'citizens' from: the Bill[10] continues to define 'harm' as 'physical or psychological' – and does not tie the concept either to unlawful content, or to children.

Alongside this new function, in Part 7, the Bill hands Ofcom new enforcement powers, backed by financial penalties up to a maximum[11] of the greater of £18 million and 10% of the service provider's qualifying worldwide revenue. To facilitate these powers of enforcement, Chapter 4 of Part 7 provides Ofcom with investigative powers to issue information notices ("**INs**"). These oblige a relevant service provider to produce any information required for the purpose of Ofcom's exercising, or deciding whether to exercise, any of its online safety functions. Failure to comply may result in the service provider committing a criminal offence: see clause 98.

In themselves, INs are unremarkable: many statutory regulators have powers to compel production of information. What is highly unusual – unique, even – to this Bill, is the way individual criminal liability for non-compliance with an IN is determined.

Information Notices: Individual Criminal Liability

By clause 93(2) of the Bill:

> *"OFCOM may include in the information notice a requirement that the provider must name, in their response to the notice, an individual who the provider considers to be a senior manager of the entity and who may reasonably be expected to be in a position to ensure compliance with the requirements of the notice."*

The consequences for the senior manager whom the entity elects to name can be grave. In the event that the entity fails to comply with the IN (becoming liable to criminal conviction under clause 98), the named senior manager may become liable to conviction for a range of new offences under clause 99, the least serious of which carries an unlimited fine, the most serious of which carries a maximum sentence (on indictment) of two years' imprisonment.

Clause 93(4) and (5) define 'senior manager' to mean a person who has a significant role in making decisions as to how the entity manages its 'relevant activities' – that is, those regulated functions to which the information notice in question relates. (One imagines, for example, an employee who supervises decisions about 'content of democratic importance' – where that is the subject of Ofcom's enquiry.) Combining the requirements of clause 93(2), (4) and (5), it follows that to qualify as a 'senior manager' capable of being named in response to an IN, an individual must have managerial responsibility *both* for the entity's compliance with the IN, *and* for those activities which form the subject matter of the IN.

What is most remarkable, however, about clause 93(2), is the manner in which it would empower the online service provider itself to nominate in advance, and without the consent of the individual most affected, a single employee who will run the risk of criminalisation in the event that the entity fails to comply with the notice. In every other instance of statutory crime in English law, Parliament has defined who is liable for the offence. Most commonly, the definition is conduct-based. For example, any person (above the age of

[10] See clause 205.
[11] See Schedule 13.

criminal capacity) who dishonestly appropriates property belonging to another, with the intention of permanently depriving the other of it, is guilty of theft.[12] Often, especially in the context of commercial crime, liability is defined by reference to a particular class of persons: for example, if statutory requirements to file company accounts and reports are not met, every person who immediately before the end of the relevant period was a director of the company commits an offence;[13] other examples are the secondary forms of criminal liability which attach to company officers who 'consent or connive' in a wide range of corporate offending, from corruption[14] to sanctions violations[15]. More unusually, Parliament identifies one person to carry overall responsibility for a particular function – for example the Principal Accountable Person[16] under the Building Safety Act 2022. But in each instance, the parameters of liability are determined by Parliament within the language of the statute, which is then applied by enforcement agencies when making charging decisions, and ultimately interpreted by the courts. In any one equation of personal criminal liability, an individual suspect's fate is decided by a balance of power between legislative wording, governmental agency, and judicial authority.

That balance would be destroyed in any case brought consequent to clause 93 of the Bill. The clause breaks the mould of existing precedent by allowing a private entity - the internet service provider itself - to decide in advance of responding to an IN, which single employee will carry the can of criminal accountability if something goes wrong.

There are multiple problems with this approach. Here are four of them.

Clause 93: Problems

The first problem (foreshadowed above) is one of constitutional principle. Assuming (as the Bill appears to envisage) that more than one person fits the statutory definition of 'senior manager' within a company, why should the job of selecting *one* such person to carry the risk of criminal penalty lie with a private, corporate entity? The task of deciding who to hold accountable for crime is both a privilege and an onerous duty; this is no less the case with corporate crime than with any other type of offending. In principle, charging decisions should be made by a public prosecutor in accordance with standards that have, since 1985[17], been codified. The Code for Crown Prosecutors ensures the basis on which charging decisions are made is clear to everybody; it sets a standard against which – in cases of error – initial decisions may be challenged. It is hard to understand what has motivated the government to propose outsourcing a very significant precursor to the decision to charge, not merely to private commerce, but specifically to the very entity which is under scrutiny from Ofcom.

It is also hard not to wonder at the naivety of the draft provision. If the government believes that clause 93(2) will render the highest ranks of executive function inside tech companies accountable for corporate responses to Ofcom's information notices, it is probably going to be disappointed. One can imagine promotions, or the enlargement of job descriptions, being motivated by a corporate desire to have someone (possibly, an expendable someone) to nominate in the event that an IN is issued. Upon receipt of any actual IN containing a clause 93(2) requirement, one can well imagine the conversations that

[12] Theft Act 1986, section 1.
[13] Companies Act 2006, section 451.
[14] See section 14, Bribery Act 2010.
[15] See para 81, Russia (Sanctions) (EU Exit) Regulations 2019.
[16] Who may be an individual or an entity.
[17] Prosecution of Offences Act 1985, section 10.

might take place inside a company; one can imagine the frictions, and the bias that might seep in – or appear to seep in – in terms of the type of person the company is willing to name. One can imagine an individual feeling like a scape goat. The Bill gives no convincing justification for handing online platforms such enormous power over their own employees.

This lack of justification is starker when placed in the context of clause 176(4):

> "*Where a penalty* [i.e. a regulatory penalty] *is imposed on an entity in respect of an act or omission constituting an offence under section 98* [service provider failing to respond adequately to an IN], *no proceedings for an offence under section 99* [failure by named senior manager to prevent a section 98 offence] *may be brought against an individual in respect of a failure to prevent that offence.*"

This provision might have been motivated by the desire to prevent a named senior manager from being prosecuted where the service provider (whose offence the senior manager failed to prevent) has already been made subject to a regulatory (as opposed to criminal) penalty for its own offending. However, in the context of the immense difference in power that exists between online service providers and the individual managers they employ, clause 176(4) will likely exacerbate the conflict of interests between the two. It can only increase the apparent motivation of the former to scape goat the latter – which clause 93 risks creating.

The second problem concerns the inequality with which the provision will impact entities of different sizes. For small and medium-sized platforms (e.g. local community forums, Mumsnet) the job of selecting a senior manager to name in response to an IN might not be so hard; at an extreme, in a micro-operation, the entity might have only one 'senior manager'. But inside a global tech giant, the opposite may be the case: there might genuinely be no single individual who can reasonably be expected to 'ensure compliance' with the IN across the company; it may be even harder to identify such an individual who could also be described as having a 'significant role' in decision making in the area of regulated activity to which the IN relates. Many tech companies do not operate in accordance with old-fashioned, corporate models of centralised control; significant decisions may be taken, and multiple functions performed, across a wide network of hubs. A global company may well be in a position to respond to a clause 93(2) requirement by saying, "*No such individual exists.*" It is difficult to understand why Parliament – apparently intent on introducing individual criminal liability for non-compliance with INs – would wish to create this lacuna.

The third problem concerns how, in the real world, a named individual might be expected to react. The Bill requires the service provider to inform the named senior manager that he or she has been nominated by the company to carry the risk of individual criminal liability for non-compliance. But there is no provision in the Bill for the individual to object to being named. (It is not even incumbent on the prosecution to prove that the individual was appropriately identified in the first place.[18]) The Bill seems to envisage that the named person – like a literal scape goat – will meekly accept their fate and refrain from taking action to avoid danger to themselves. In practice, an individual might immediately resign, or at

[18] In addition, while there are formal notification requirements (clause 176(1)) which Ofcom must fulfil before proceedings are brought for an offence under clause 99(2) (failure by named senior manager to prevent offence under section 98(1)), these requirements relate to the clause 98(1) breach (committed by the service provider). There is no requirement in clause 176(2) that Ofcom independently notify the named senior manager that it is considering bringing proceedings against him or her.

least consult a lawyer about their rights in light of their employer's decision to nominate them (and not someone else, arguably better placed) for possible criminal prosecution. It is inevitable that in some circumstances, an individual will suffer serious anxiety at being so singled out – which may necessitate a period of leave, potentially complicating any subsequent liability. Again, it is hard to fathom why Parliament would consent to create this situation, instead of replicating conventional penalties which attach to non-compliance in respect of existing statutory production powers.

Fourthly, in passing clause 93 in its current form, Parliament would kick a very difficult set of questions down the road to the courts. If Ofcom were to use its clause 93(2) power with any degree of frequency, it is inevitable that employment tribunals, Crown Courts and the High Court would be obliged to do their best to ameliorate all the problems the clause creates. Since the power to require a provider to name an individual manager is discretionary, the High Court will likely receive applications judicially to review Ofcom's decisions, brought by providers and possibly by named individuals too. If prosecutions are commenced, Crown Courts (ultimately, juries) will have to do their best to interpret the 'reasonable steps' element of the associated offences against the terms of an individual's contract of employment. Employment tribunals may well have to grapple with the question of unfair discrimination in the manner in which corporations select which senior manager to name.

Clause 93: Unnecessary

These four problems are considerable. What Parliament should not lose sight of, is the modest purpose for which these significant problems would be incurred. Clause 93 is not directly concerned with controlling online safety for children or minimising online terrorist content. The provision concerns a service provider's administrative response to an information notice. Information notices will certainly play an important part in regulation of the industry in future, but they are far from ground-breaking and do not require the type of innovation clause 93 would involve.

There is no shortage in English law of working examples of statutory powers that are daily used by regulators to compel the production of information – complete with sensible mechanisms to punish non-compliance. Indeed, so effective are the conventional forms of penalty in motivating co-operation with production orders, that only rarely do regulators find it necessary to commence proceedings for non-compliance with their terms. (When production orders do land up in court, this is often at the deliberate instigation of a recipient seeking to challenge the regulator's position on a question of law, such as privilege or jurisdiction.) That Parliament should resort to the highly irregular approach of allowing private tech companies to single out one employee for sanction, in the (probably mistaken) belief that this will improve rates of compliance with Ofcom's production powers, is strange to say the least.

The proposal is all the stranger when one considers the timing. In the recent past, criminal enforcement agencies in the UK (most particularly the SFO) have faced growing criticism for cutting deals with corporates that either wrongly blame individual managers, or otherwise make it impossible successfully to prosecute them. As such, this is an odd moment to choose to throw away decades of jurisprudence about the fair way to select individuals for charge and pass into the hands of private commerce a function that ought rightly to be shared between statutory language and prosecutorial decision-making instead.

Conclusions

Immediately before the Online Safety Bill was brought to the House of Lords, the government announced that it intends to introduce a further clause creating criminal liability where an online service provider fails to comply with duties designed to protect the safety of children online.[19] In a far more conventional approach than the approach of clause 93, under this new proposal, the service provider would carry principal criminal liability for the failure; where the provider is an entity, any officer *or senior manager* whose 'consent, connivance or neglect' had contributed to the offence would be personally liable too – with a maximum penalty of two years' imprisonment. While the proposal is to define 'senior manager' in this context by reference to clause 93 of Part 7 (i.e. a person who has a significant role in making decisions as to how the entity manages its relevant activities), there is no suggestion that the service provider itself should be entitled to nominate a single such senior manager, in whom personal liability will be isolated or contained.

The addition of this clause to the Bill would present a good opportunity to re-examine the merits – in principle and in practice – of what is currently clause 93. Indeed, an alternative to clause 93 exists in the Bill as currently drafted. Existing clause 178 already provides that where an offence (including an information notice offence) is committed by an entity, any officer who consents or connives in the commission of that offence, or to whose neglect the offence may be attributed, is criminally liable too. Importantly, the definition of 'officer' in clause 178(3) already includes any manager (whether senior or not). It follows that clause 178 already makes a larger pool of people potentially liable for a service provider's failure adequately to comply with an information notice than does clause 93 – making the latter's function all the more difficult to fathom.

In the meantime, while the claim that the Online Safety Bill will render the UK the "*safest place in the world to be online*" is open to question (particularly when compared to the EU's Digital Services Act), it is easy to see why individual compliance officers inside Big Tech might consider the UK to be the riskiest place on earth to be employed.

---

[19] Per Michelle Donelan, Secretary of State for Digital, Culture, Media and Sport, 17 January 2023, Hansard volume 726. See here.

ABOUT THE AUTHOR

Clare Sibson KC

Call Date: 1997 I Silk Date: 2016

Clare is a leading silk who brings extensive experience to the intersection between criminal and regulatory risk, commercial obligations and directors' fiduciary duties. Commended as one of "the brightest legal minds at the Bar", Clare has advocated for individuals and companies in the most serious and complex cases within her fields, both at first instance and on appeal. Recent instructions involve disqualification proceedings, corruption investigations, allegations of fraud, proceeds of crime investigations, asset recovery, sanctions and advising Big Tech on forthcoming safety legislation.