ONLINE SAFETY BILL: SECOND READING BRIEFING NOTE

[Note: This is an initial take on the Online Safety Bill as we get to grips with its complexities. For those new to the topic a simple one-page guide is attached at the end of this brief.][1]

Summary

- There are welcome improvements from the draft Bill that make the regime work better, giving OFCOM more powers to investigate and tackle harmful systems in companies (through better risk assessment).
- Victims now get more protection – such as measures on protecting children from pornography and (some) users from online fraud and scams.
- But **the Bill remains too complex – bad regulation for both victims and companies.**
- **The regime relies upon vital yet unknown details in secondary legislation and OFCOM codes of practice/guidance – the Government should urgently publish its thinking to help debate and aid democratic transparency during the Bill's passage.**
- The Bill's structure and drafting still pushes services to addressing harmful content (often palliative), rather than harmful systems, business models and algorithms (more lasting and systemic). **Consolidating the focus on systems would make the regime more effective**.
- The route to the start-up of the regime is Byzantine and lengthy. The regime is unlikely to be fully operational until 2024. This leads to delayed protection for users and uncertainty for companies. **The Government should bring some aspects forwards**.

Specific recommendations (with CUK amendments to follow)

- **Secretary of State powers:** there is still too much unjustified intrusion by the executive and parliament into the work of the independent regulator, which goes against international norms for communications regulation. We suggest that the **Secretary of State's powers to direct OFCOM on the detail of its work (such as codes) are removed. For National Security, government should have carefully constrained powers.** OFCOM's Board needs to be bolstered to oversee National Security issues.
- **Harms to adults:** priority content that is harmful to adults will not be known until the Secretary of State brings forward secondary legislation (despite already having three years to decide on this). It will be difficult for Parliament to assess the impact of the Bill without an indication from the Government as to what it intends. **We suggest that the Government should list harms both to children and adults in a new Schedule 7(a) and 7(b).**
- **Mis/disinformation:** the Bill largely won't tackle mis/disinformation. **Government should create a formal mechanism for state actor disinformation, such as Russia, and for public health issues such as COVID**. The Government should bring the unaccountable DCMS 'Counter Disinformation Unit' under OFCOM's supervision and make it transparent.
- **Fraud:** the scope and effect of the new fraudulent advertising powers is too limited. Fraudulent advertising has the same impact on victims wherever they encounter it: **the new powers should make all companies run an effective system to mitigate fraud.**
- **Categorisation**: despite criticism from the Joint Committee and others, the Government is sticking with arbitrary categories of companies to which the rules apply largely based on size. This is a major hole in a regime that claims to be based on risk. It is wrong to suppose that smaller size means lower risk: users of these platforms still require protection. **We recommend that categories of providers are removed and risk assessment duties apply across the board**
- **Trafficking offences:** human trafficking is a serious omission from Schedule 7 and should be rectified. Also advertising is significant for indentured servitude and should clearly be in scope for that offence. Similarly organ trafficking and animal trafficking.
- **Coordination with other regulators:** The Government is on the cusp of creating a powerful network of regulators, but the Bill does not create powers for domestic inter-regulator cooperation. The system must work effectively if it is to protect users. The Government should give clear powers to OFCOM to ensure that case files can flow between regulatory systems in accordance with the law.

For more information, contact: maeve.walsh@carnegieuk.org

[1] All our work on Online Harms can be found here: https://www.carnegieuktrust.org.uk/programmes/tackling-online-harm/

Issue: systems and risk assessments vs focus on content

The 'category' system needs to be replaced with a proportionate, risk-based one, rooted in OFCOM's risk assessment of how dangerous platforms are. Small but harmful platforms must not be let off the hook.

The Bill is an improvement on the draft Bill, making subtle but important changes to reinforce risk-based regulation of systems rather than simply palliative 'take down'. The system that delivers the content (to millions of people, to those who didn't ask for it, to those who might be vulnerable to it) is more impactful than the content itself. The Government will apply the regime mainly based on size categories – smaller companies will have lower risk management obligations even if they have a high risk of harm.

Our work to describe and advocate for a duty of care regime for online harm reduction has always been rooted in our belief that systemic, risk-based regulation - such as that which is established in countless other sectors - is the most appropriate approach for the online environment, requiring companies to account for, and mitigate, the harm that arises from the design and operation of their systems rather than focusing on individual items of content.

Compared to the draft Bill, the approach is now more clearly systems-based. But the structure of the Bill, the addition of content-specific new sections, and its drafting still pushes services to addressing harmful content, rather than systems - including the business model and algorithms. **Further amendments to consolidate its focus on systems would make the regime more effective** and provide reassurance to those worried about its impact on free speech.

Analysis:

- The requirement that risk assessments must now be "suitable and sufficient" is an improvement. But the language chosen throughout the Bill pushes platforms mainly to addressing the problem - that is the content - rather than the underlying causes and exacerbating factors of platform design. (For example, the specific duties in clause 9(3) (takedown of content and minimisation) can be seen this way.) As a result, the guidance and codes of practice that will come from OFCOM take on a higher significance.

- There is a welcome emphasis that the safety duties "apply across all areas of a service, including the way it is operated and used as well as content present on the service" - though this language is not replicated in relation to content that is harmful to adults. In the expanded definition of "harm" (clause 187) it refers to the "the manner of [content's] dissemination (for example, content repeatedly sent to an individual by one person or by different people)". But whether this is sufficient, given the omission, in the safety duty for content harmful to adults itself remains to be seen

- Another issue in this context is that the fact of dissemination - in the context of the children's safety duty - is specifically excluded in relation to some of the duties: 11(3) (prevention from encountering content) and 11(5) (terms of service in relation to clause 11(3)) There is some degree of tension between this and clause 11(4).

- The definition of harm itself is modified to be equivalent to "risk of harm and potential harm" which is important given the centrality of risk assessments (which take place before any harm has occurred) to the regime (clause 187).

- OFCOM can carry out a broadly based risk assessment of all harms. This assessment – largely unchanged from the draft Bill - underpins the entire regime. Here, there remains a welcome focus upon the "characteristics" of the service (that is functionalities, user base, business model, governance and other systems and processes) rather than just the content.

- A significant and positive change to risk assessment in the regime is the inclusion of specific provisions allowing OFCOM to take action against deficient risk assessments.

- With the removal of the exemption for paid-for advertising in the Bill, ad delivery systems in general may be in scope and relevant to the risk assessment and risk mitigation duties. This we feel to be potentially an important positive step given the role of the advertising funding and the overall business model in supporting certain types of problematic harms.

Categorisation of services

- By retaining the categorisation of services - which we have argued against previously, as did the Joint Committee - the risk-based regime does not apply across the board and will lead to gaps in enforcement and the likelihood of harms arising and proliferating unchecked on smaller, but potentially fast-growing platforms, before the process for recategorising them can kick in.

- Very large size itself can be an absolute indicator of risk and using very large size as a proxy brings administrative simplicity, but it is wrong to suppose that smaller size means lower risk. **We continue to argue for the categories of services to be removed and replaced with a system rooted in OFCOM's risk assessment of how potentially harmful a platform is.**

Issue: too much is left for secondary legislation and OFCOM's codes/guidance; this makes scrutiny hard and delays the regime start up to 2024

The Bill still leaves much to do in secondary legislation - with resultant delays to clarity about the regulatory scope and concerns (as set out below) relating to the role of the Secretary of State. **The Government must do more to set out their thinking during the passage of the Bill, which would reduce uncertainty and make the Parliamentary debate more practical than theoretical.** They have, after all, had three years to come up with this thinking. For example:

- 'Priority harms' are central to understanding the Bill's impact – Government **should add the categories of priority content for both content harmful to children and to adults as a new Schedule 7(a) and 7(b) and make its position clear by, or at, Second Reading.**

- **A provisional list should be published of the large and small platforms the Government and OFCOM considers pose the highest risk of harm and to which the most rigorous risk assessment will apply. This gives some certainty to companies and victims.**

- **The regime must start quicker than 2024: the Government must reduce the wait for the downstream work – perhaps, for example, making companies' terms and conditions on terrorism, illegal content and protecting children enforceable from Royal Assent.**

<u>Analysis</u>

- Companies will not know which category of service they fall into until after the Secretary of State has published definitions on thresholds and laid these as secondary legislation; and as a result they will not know all the duties that could apply to them.

- The Children's Access Assessment (CAA) is likewise dependent on the publication of Ofcom's risk assessment.

- The scope of protection offered by the Bill also will not be clear until after secondary legislation. While there is a preliminary list of priority criminal content in schedule 7, the same clarity is not available relating to the other two pillars of the Bill: priority content harmful to adults, and both primary priority content and priority content for children, will be introduced by statutory instrument (for which there is no timing given). These areas are critical for victims seeking to understand if the Bill will protect them in future, as well as for companies that might have to manage these risks.

- More detail on what companies will be expected to do to comply with the regime will follow in OFCOM guidance and codes of practice. which cannot be produced or consulted upon until after Royal Assent.

- The process used to make regulations also requires the affirmative process. This is an improvement on the draft Bill but still does not allow Parliament the same freedom to consider the substance of the text as when matters are dealt with by primary legislation.

- It seems that the regime will not start working properly until 2024. **The Government should seek to bring some aspects forwards** - one area worth more study could be making companies' terms and conditions on terrorism, illegal content and protecting children enforceable under the regime from Royal Assent, which is expected at the end of 2022.

Issue: The Secretary of State's powers are still too broad

The Secretary of State's powers to instruct OFCOM should be trimmed back to national security alone.

The Secretary of State should be able to give high level guidance on national security issues to the regulator, but not interfere in its detailed work such as codes, guidance and enforcement strategy. It's an important free speech principle.

OFCOM's board should be beefed up to have oversight of the Secretary of State's power to intervene on national security – with suitably cleared members in a subcommittee.

Compared to the broadcasting regime, there is considerably more intrusion by the executive and parliament into the work of the independent regulator. We have written extensively on why this was problematic in the draft Bill - and it remains so here. It's an international norm in democracies for the executive not to interfere in day-to-day communications regulation. The UK used to champion this.

Analysis

- Clause 40 permits the Secretary of State to direct OFCOM to change a code of practice. Whilst the draft Bill permitted this 'to ensure that the code of practice reflects Government policy', clause 40 specifies that any code may be required to be modified 'for reasons of public policy'. While this is more normal language, it is not clear in practice what the difference between the two sets of wording is. Implicitly it seems that this excludes 'national security or public safety', which are specifically dealt with in relation to the CSEA and terrorism codes in clause 40(1)(b). This provision would be unnecessary, given clause 40(1)(a) applies to any draft code include CSEA/terrorism, if public policy were to cover national security or public safety. Different rules apply in relation to CSEA and terrorism codes in that they are reviewed[1]. There appears to be no Parliamentary control over this process nor oversight by a competent body such as the National Police Chiefs Council or Directors of Public Health for public safety.

- **We suggest that Secretary of State intervention in the substance of the codes is, as a matter of principle, problematic**. We do, however, recognise the importance of the Government to identify when there are national security issues that need to be addressed; this flagging of a problem is different from saying how it should be resolved, which should be a matter for OFCOM. **We also think that any special intervention by the State in public speech must be limited to national security.** When public safety issues become sufficiently serious to allow the Government to issue directions to a regulator (such as COVID) we suggest that they are national security issues.

- The Secretary of State also has powers to amend the Online Safety Objectives (Schedule 4, paragraph 7) - and indeed the Bill (clause 173) - by regulations too.

- The new relationship between intelligence services and OFCOM (see clause 99) is now codified but with no oversight. And also - while protecting security advice is necessary - the caveat that allows this as a reason for redacting information from reviews of codes (clause 43 (6)) does not have any oversight. Who will ensure that it is only the national security/public safety relevant content that has been legitimately removed or obscured before publication?

- **We suggest that the Secretary of State should not have powers to direct OFCOM on the detail of its work (such as codes); in the case of national security the Secretary of State should be able to raise the issue but not specify the implementation**. The public policy and public safety sections of Clause 40 should be deleted. OFCOM should have sufficient capability to assess and discuss national security issues with the Government - such as board members with appropriate backgrounds and sufficient security clearance for key staff as well as the Chair and CEO.

Issue: The Bill is weak on harms to adults

If the Bill does not deal with the large-scale racism (that was short of illegality) on social media suffered by young footballers after the Euros, then it will have failed. Harmful misogyny is not illegal but not yet tackled in the Bill. Until we see the proposed 'priority harms', we will not know whether they could be caught.

These sorts of harms to adults are dealt with badly in the Bill: only the very largest platforms will have to address them if the Secretary of State lists them and even then, the action required is weak. **Tackling serious harms to adults should be required for all regulated platforms.**

Analysis

- The types of harms to adults to be prioritised are as yet unknown and will not be set out until the Bill has received Royal Assent. Non-designated content that is harmful does not require action on the part of service providers, even though by definition it is still harmful.

- Many campaigners have made the case that protections for women and girls are not included in the draft Bill, a concern supported by the Petitions Committee in its report on Online Abuse. While Schedule 7 does include a list of sexual offences and aggravated offences, the Bill makes no concessions here and the wider context of Violence Against Women and Girls (VAWG) is not addressed. We will be looking further at the types of harms that might need to be included to ensure the protections required are delivered.

- We also have some concern that the overarching risk assessment for adults in clause 12 (which only covers category 1 companies), which expects services to consider the fact that some groups are more likely to encounter harmful content and behaviour and are more likely to be harmed by it (cl 12(5)(d), is constrained by the scope of harmful content. As noted above, there is a quantitative threshold for determining which content is harmful (and therefore to be taken into account in the risk assessment) which might not well serve smaller groups.

Online hate and abuse

- There are many high-risk, high-harm platforms that are likely to fall into category 2b, due to their size and functionality (a definition that does not include risk). Many small platforms host huge volumes of racist and extremist content which, while it might fall below the threshold of "illegal", could certainly provoke real-world harm to its targets. These services will not be covered by the category 1 "harms to adults" duties. Similarly, search engines are also exempt from this obligation.

Issue: the scope of harms covered by the Bill needs to be wider

The Government needs to list 'priority harms' in the Bill, not in secondary legislation. This list should go alongside 'illegal harms' in Schedule 7 to reassure victims and provide certainty for Parliament.

Human trafficking, organ trafficking, animal trafficking and cruelty to animals should all be listed in Schedule 7

Explicit provision needs to be made for COVID/health disinformation, and state actor/Russia disinformation which are both highly incongruous omissions.

The Government's concessions on a number of criminal offences now listed in Schedule 7 (such as fraud; sale of a realistic imitation of firearms) mean that the priority illegal harms route has opened up areas of harm which are not specifically directed at individuals. **The new definition of harm also possibly opens the door for societal harm to be included as it recognises that members of a group can be affected by comments directed at another member of a group.** For clarity, we will have to wait and see on statutory instruments as regards content harmful to adults and children and, as we have suggested, we feel it would be preferable for the initial list of priority harms to be included in the bill. Presumably, societal harms that could be harmful to adults could equally (if not more so) be harmful to children.

Analysis

- We know that many civil society organisations remain concerned about the lack of provisions for mis/disinformation. It is notable that the Government's response to the Joint Committee's report, which rejected its recommendations in this area, went no further than all its previous statements on this issue during the course of the development of this legislation. Given the level of evidence-based concerns about the scale and impact of this - which are comparable to those expressed by campaigners in relation to e.g. fraud and scams, or anonymity - it is difficult to understand objectively why the Government was not prepared to consider similar concessions here.

- There are two significant disinformation issues that the Bill does not address: disinformation supported by state actors and COVID disinformation. Several unaccountable civil service groups (such as the Counter-Disinformation Cell/Unit and the Rapid Response Cell/Unit) exist to nudge service providers on these issues but we have no record of their effectiveness. This very direct state interference in the media gives rise to concerns. **The Government should reform this system and bring disinformation firmly into the scope of the regime and put the disinformation cells under OFCOM's independent supervision.**

- Human trafficking offences (noted by Frances Haugen's whistleblowing revelations) are a serious omission from Schedule 7 that should be rectified. Advertising is an important route for modern indentured servitude and should clearly be in scope for that offence. We understand there are also issues with illegal organ trafficking on social media. We are aware of serious issues raised by campaigners on animal trafficking and animal cruelty which also appear to be omissions from the Schedule 7 list.

Issue: advertising - potential gaps

The new rules on fraudulent advertising are good as far as they go – but they should apply evenly to all regulated companies and be at least as strong and systemic as those for illegal content. A victim will suffer in the same way on whichever platform they get ripped off.

Fraudulent advertising and scams

- The Bill's measures will not apply to all online advertising providers. These rules do not apply to services defined by the government as 'Category 2b' — which are smaller, 'user-to-user' websites that host adverts. There is a risk that scammers will target consumers through paid-for content on these sites.

- The legal requirement for search engines to tackle scam adverts seems less onerous than for social media platforms. All the way through the Bill search engines are subject to different, less onerous rules than user-to user services, especially those in 'Category 1' — which are large user-to-user sites such as Twitter and Facebook. This difference can be seen here too but on top of that, the obligations on Category 2a services with regard to fraudulent ads are thinner than their obligations in relation to illegal content and specifically for fraudulent advertising there is no equivalent of cl 24(4) which requires category 2a services to look at their design and the role that plays in harm, staff policies and practices and risk management arrangements. This raises concerns about whether the legal duty for search engines is stringent enough.

- Moreover, the consequences of the boundary between advertising and other content being removed is not clear. If adverts fall within the definition of user-generated content, then adverts are regulated content and the machinery behind advert delivery comes within scope where the content is either criminal or harmful to children or to adults. This inclusion is likely to be a step forward though there will be awkward boundaries to navigate, especially given the special regime for fraudulent ads is applicable only to some service providers. Fraudulent advertising has the same impact on the victim regardless of where they are harmed by it: the new powers should apply with similar strength to all companies.

Issue: futureproofing

The regime probably applies to 'the metaverse' which is 'user to user' – the government should clarify that, as it would be genuinely world leading.

OFCOM needs more discretion to add things easily to the regime's scope as technology and society change and new harms arise. It is trusted to do so for TV and radio so it should be here, without a cumbersome process.

A duty of care focused on risk-assessment and outcomes would enable both flexibility in a new regulatory regime, as well as futureproofing. The complexity and specificity that has been worked into the new draft of the Bill – partly to account for demands for greater clarity on scope, for example – has an impact on its ability to take account of future, as-yet-unknown harms. With regard to the metaverse, this is a cause for concern.

Analysis

- The regime seeks to be dynamic and there are specific measures in place at key points that seek to ensure it remains up to date.

- As we have written at Carnegie UK, it seems likely that a user-to-user regime would encompass the metaverse. There are two sets of questions arising: do the lists of measures in the safety duties seem appropriate for the dynamic, real-time environment of the metaverse? If harms that require action are described by reference to current criminal offences, is there a danger that those offences will themselves become outdated (consider a sexual assault on an avatar)? Of course, the Bill provides for updating but, in the case of the need for new criminal offences, how long will this take. This is not a problem with a systems-focussed regime itself but more generally illustrates the difficulties of relying on lists of types of content in terms of keeping the regime relevant.

- There is a process for reviewing new categories of content that are harmful to children and harmful to adults; but, in the end, it requires secondary legislation. The Secretary of State process for adding in new harm areas is cumbersome. In TV, radio advertising and cinema regulation, the regulator - based on research - can move to combat novel harms because it was given the job of dealing with harmful content as a general category (without further specification).

Issue: working with other regulators

The Bill should give OFCOM authoritative powers and incentives to work with other regulators so that enforcement across regulators is coherent and coordinated – and specifically so that case files can pass between them easily without legal challenge.

The requirement to work with other regulators was dropped between the response to the White Paper and the draft Bill. Despite a significant suite of recommendations on this matter from the Joint Committee, there is no mention at all of any requirement to cooperate or coordinate with other regulatory bodies - though the ICO has been added in a few places as a statutory consultee.

Analysis

- While the Government was clear in its response to the Joint Committee that OFCOM does not need a new "co-designation" power, it will need to work with other regulators - for example, the FCA in relation to OFCOM's powers in enforcing the new duty on fraudulent advertising. This is a different relationship from co-designation. The lack of any requirement on them to do so has consequences not just for- e.g. sharing of information between the regulator or ensuring clear lines of responsibility and cooperation in relation to evidence-gathering, horizon-scanning or enforcement - but also for upstream policy oversight.

- For example, which department holds the ring on the policy oversight and related Ministerial advice on the implementation of the duty on fraudulent ads? DCMS, as the sponsor of OFCOM, or HMT, as the sponsor of the FCA, or Home Office, as the department with the policy responsibility for combatting fraud?

- From the other end of the process, it is instructive to contemplate what would happen to a case file on an issue as it winds its way between regulators. Are all the powers in place to allow information to cross boundaries and for bureaucracies to resource their teams for cross boundary working?

- It would do no harm to set out in the Bill a requirement on OFCOM to define the terms of its relationships with other regulators and the power, if needed, to get them to work effectively together.

The Bill is too complex

It is in the Government's interest to make the regime easier to understand - it will help the passage of the legislation as well as reducing the regulatory burden. If they insist on keeping the complex structure, then better supporting materials are required – flow charts, timelines etc - that chase complex issues out into a simple form

Calling for these at Second Reading might make them appear at Committee stage.

When we published our proposals for extensive amendments to the Online Safety Bill in November 2021, we argued that the Bill was too complex and needed to be simplified and strengthened:

> *A simpler Bill will lead to better outcomes for victims. Others benefit too: legislators, who will need to scrutinise and amend it further; companies (and their lawyers) who will need to comply; the regulator, Ofcom, who will take enforcement decisions based on it; and civil society organisations advocating for victims.*

The Bill's structure remains complex and opaque.

Analysis

- There are some simplifications to the structure from the draft version, including the incorporation of the child sexual exploitation and abuse (CSEA) and terrorism offences into priority illegal content; and the reordering of the risk assessment duties to sit next to the relevant safety duty.

- But the re-ordering proposed by the Joint Committee to make the objectives of the regime clearer, which were similar to proposals we made in our amended Bill, have not in the main been actioned and the Bill still lacks any general explanation at all.

- The structure of the Bill is cumbersome, with much nesting of qualifiers on terms scattered through the Bill – for instance, risk assessments link back to illegal or harmful content; and harmful content depends on an amended definition of harm (at clause 187) and of content (clause 189).

- Definitions are listed at the end, with other definitions scattered throughout the Bill, and an index brings them all together at clause 190. While this is not unusual, the implications are hard to assess because of this nesting.

- The Online Safety Objectives (which frame OFCOM's work in the regime) are in schedule 4, rather than say Clause 2 which is unhelpful. These objectives, in addition, then have an overlap with some of the requirements in each of the duties in the main body of the Bill re illegal content etc.

Where new concessions have recently been made, they are introduced as new sections (for example on pornography, user verification and fraudulent advertising); and the impact on the overall schema of these additions is unclear.

ANNEX

THE ONLINE SAFETY BILL: AN OVERVIEW

The Online Safety Bill is about reducing harm caused by the operation of some "user-to-user services" (social media) and search engines. Since the draft Bill, there are now two add-on chunks: fraudulent advertising and age verification for pornography. In addition, requirements for user verification are added as a separate section within the adult safety duties. The Bill appoints OFCOM as regulator of the regime.

The regime's duties of care require regulated companies to do risk assessments of harms arising from certain types of content and the operation of the service. Companies then must put in place effective and proportionate mitigation plans. This is not just about take down but also about how algorithms work and how the service is designed. OFCOM regulates whether the risk assessment and mitigation is "suitable and sufficient". OFCOM also has some role in identifying risks and developing codes of practice to help with compliance.

The principal duties focus on illegal content, content harmful to children and content harmful to adults (there are other duties such as record keeping etc). Within these duties, some types of harmful content are seen as 'priority'. There is a list of priority illegal content in the Bill (Schedule 7) but priority content in relation to the other two categories will be specified in secondary legislation. Content harmful to adults is regulated comparatively weakly to that considered harmful to children or that which is illegal.

The new rules for pornography providers apply wider than social media and search (to "internet services" that display "regulated provider pornographic content") requiring that in the UK children must not normally be able to encounter such content online, using measures such as age verification.

The Bill has size and 'functionality' -based categories of services. These have been said elsewhere by Government to account for the largest sources of risk: Category 1 – user-to-user platforms that are of significant size and functionality, Category 2(a) large search engines, Category 2(b) other user-to-user platforms passing a size threshold. The thresholds will be contained in secondary legislation acting on OFCOM's advice. Services need to carry out a Children's Access Assessment (CAA) to determine whether or not they have to comply with the children's duties.

Category 1 services have to consider: harm to adults, anonymity rules to allow users to avoid content from unverified accounts and protection of both journalistic content and 'content of democratic importance' when applying the regime. All regulated services are required to take account of rights to freedom of expression and privacy.

Broadcast and print media, already regulated or self-regulated, has a carve-out so that it is not caught by the regime when distributed on regulated social media and search services.

New rules on fraudulent online advertising apply only to category 1 and category 2(a) services.

If OFCOM decides a platform has failed in its safety duty, then it may make orders to correct behaviour and fine the service. *In extremis*, OFCOM can apply to the courts to injunct companies providing, say banking and advertising, to a platform and require them to stop or as a last resort order internet service providers to not carry and offending service.

The Bill is a framework regime - OFCOM and the Secretary of State have to provide guidance on how most aspects of the regime works and a plethora of secondary legislation before the regime gets going (likely 2024).