Written supplementary evidence submitted by The Football Association and Kick It Out (OSB0234)

Damian Collins MP
House of Commons
Westminster
London
SW1A 0AA

29th November 2021

Dear Damian,

We were very grateful to be amongst the first witnesses to give evidence to the Joint Committee on 9th September on behalf of English football, alongside Rio Ferdinand. As we outlined during the session, online discriminatory abuse is a significant problem in football, and one that urgently needs to be addressed.

The football authorities very much welcome the Online Safety Bill, and we are keen to continue working with the Committee members, Government, and parliamentarians as it progresses through its various stages.

We have closely followed your various evidence sessions with great interest but given that our evidence was quite early in the process, we wanted to take this opportunity ahead of your report and recommendations to the Government next month to reiterate three points of significant importance if the aim of the Bill is to truly help us address the prevalent discriminatory abuse experienced online. This is not only experienced by individuals but is often visible for others to see. Of course, it is not a football-only issue, but a broader societal issue across all walks of life where abuse is directed at real people who are real victims.

We have been working closely with football stakeholders on the three key points that we would like you to consider as you go into the final stages of this process, which are as follows:

1. **There needs to be a mandatory and specific Code of Practice on racism, discrimination and hate speech, which puts Parliament's intent with the Equality Act 2010 into practice in the online sphere**. This will signify the severity of this abuse and allow no scope for social media platforms' community standards to allow a loophole for triggering and vile words, emojis or imagery to be used as an abusive weapon. We know this is currently the norm with existing social media terms and conditions, and this needs to be addressed through this legislation. It is critical that this Code adequately clarifies a minimum standard and best practice that social media companies will be expected to adopt to keep all users safe. This mandatory Code must ensure the intent of pre-existing legislation is implemented in the online space. The evidence to date shows why this is absolutely necessary and the baseline of the pre-existing legislation needs to be the absolute minimum standard enveloped within the Code.

   We recognise the challenges on the issue of anonymity. However, if the Committee is sympathetic to the position of traceability, this must be mandatory for all users at an absolute minimum - with the reach of anonymous accounts being limited. We of course

accept that there are a minority of users who have a legitimate reason to maintain their anonymity online. However, we are concerned that a move towards traceability does not provide a sufficient ability for personal identification and enforcement action to take place. The ability to trace back to an IP address or a location does not provide proof on the person operating behind an account and for years we have seen how VPNs and other tools are used to cloud traceability. There are also certain problems that will need to be overcome – for instance, how a perpetrator will be traced if they live in a household with five other people and share the same computer and IP address. We believe that some mechanism of back-end ID verification by social media organisatio ns would help to address these issues, whilst still enabling users to appear anonymous on the f ront-end of the platform. In addition, traceability without individual level verification does not tackle the issue of people simply shutting down and re-registering new accounts to continue abusing people. We also believe that it cannot be right that anonymous accounts currently have the same reach as other accounts, given the significantly increased risk quotient of anonymous accounts. We strongly recommend that the increased risk quotient should be tied to a limitation of reach on platforms, so that anonymous users cannot post abusive messages that are then amplified by algorithms causing severe impact not only to direct victims of abuse but also to viewers of content. It cannot be right that users are able to hide behind the cloak of anonymity in order to direct hateful abuse at others, with no real-world consequences.

2. **We acknowledge the call to simplify the draft Online Safety Bill and understand the challenges around legal but harmful content. However, it cannot be left to the social media companies to address these challenges. It is critical that sufficient enforcement powers are given to the regulator to tackle content that whilst legal, is incredibly harmful.** We strongly believe that simplification of the Bill should not come at the expense of the protection of all users. We must explicitly provide protection for all from verbal or pictorial abuse, particularly given that a lot of current pictorial abuse is legal by definition. If we are still allowing social media boardrooms to be the place where this threshold is decided, then we risk permitting and indeed facilitating a situation where the outpour of abuse that was experienced after EURO2020 happens again, impacting victims and the rest of society. The legislation must ensure that we are providing explicit protection for groups that we have already identified as vulnerable or in need of additional protections through other existing legislation, and the regulator must be given the enforcement powers to act where such harm is being caused.

We firmly believe that the Online Safety Bill presents an invaluable opportunity to lead the way and set a precedent across the globe by addressing the scourge of online hate and discrimination. We are very keen to work with you and the Government to ensure that the legislation is effective and fit -for- purpose - but that most importantly, it actually addresses the issues at hand. We are very concerned that without the implementation of the suggestions made above, we risk the abuse that happened at EURO2020 occurring repeatedly.

We do hope that you will be able to take on board our three points as you finalise your recommendations, and please do let us know if it would be helpful to have a further conversation, or if we can provide any additional information.

We have also attached a summary of additional information on the question of legal and harmfulwhich the Committee asked us to follow up on.

We have written in similar terms to the other members of the Joint Committee.

Kind regards,

Edleen John
International Relations,
OutCorporate Affairs and Co-partner for Equality,
Diversity and Inclusion Director, The Football Association

Sanjay Bhandari
Chairman, Kick It

ONLINE SAFETY BILL: ENGLISH FOOTBALL'S ADDITIONAL SUBMISSION TO THE JOINT COMMITTEE

The following submission builds upon evidence given by English Football, both written and oral, to the Joint Committee on the draft Online Safety Bill.

1. How could existing jurisprudence be leveraged as a justification for the regulation of lawful, but harmful online conduct?

Most online abuse falls within a grey area which is legal but harmful. This includes content that may not currently be illegal, but is still sufficiently triggering to be incredibly distressing and dangerous to the recipient or purveyors. There is existing legal precedent that the Bill should incorporate in order to capture the scope of legal but harmful content within it, and thus meaningfully tackle discriminatory abuse online.

The law of conspiracy renders an action unlawful even where it might otherwise be lawful, if a coordinated action is taken in agreement between partners, with the sole or predominant purpose of injuring the victim. Previous case law has already clarified that this agreement does not need to be express, nor does participation need to be active - but that perpetrators must have the same intentionsand objectives to cause deliberate and intentional harm to the victim.

The courts have ruled that whilst undertaking a lawful act with intent to injure is not ordinarily unlawful, when individuals conspire with a common intention to cause harm, this combination is sufficient to cross a moral line which warrants a cause of action. It is the intent to harm which converts an otherwise lawful act into an unlawful act. With social media abuse, the intent of users to cause harm to specified or unspecified victims in their posts can be reasonably inferred – it is tolerably clear to a reasonable person reading them.

As such, the combination of the intent to cause harm, taken alongside the unprecedented access to other users, the presently high level of anonymity online and the considerable amplification of harmful content on social media platforms, is equally sufficient to cross the same moral line as within conspiracy law. There is a clear rationale to justify transforming a lawful (but horrible) act into one which should create legal consequences and therefore come within the scope of Ofcom's powers.

We believe therefore that intentionally harmful conduct spread online in this way, even if such content is not directly illegal, could be regulated within the scope of the Online Safety Bill. There is sufficient historical jurisprudence to be confident that regulators or courts would not be inventing a completely new legal concept with concerns round unintended consequences and lack of safeguards; there is plenty of case law to aid interpretation in the analogous area of the tort of conspiracy.

2. Are the required parliamentary checks and balances in place sufficient for OFCOM?

English football believes that for the Bill to impact meaningful change, it needs to grant Ofcom the regulatory flexibility to govern in a dynamically evolving and complex online landscape. The Bill shouldgrant Ofcom the power to issue Codes of Practice for regulated services (s.29.(3)), as well as a duty to keep such Codes of Practice under review (s.34(5)), in order to provide the necessary flexibility for the regulator to respond to the ever-changing nature of online abuse.

Ofcom should prepare a specific Code of Practice in relation to online racism and abuse, as is the case for child sexual exploitation and terrorism, to clarify the standards and best practice social media platforms will be expected to adopt. In order for this Code to be effective, Ofcom should be able to request information from relevant platforms to ascertain the root causes of online hate, so that it can build a full picture of how abuse online operates and is spread.

We recognise that Ofcom's publishing of Codes of Practice must be balanced and governed by the required level of Parliamentary oversight. In the Bill, checks and balances on Ofcom are set out, including:

- A duty to consult the Secretary of State (s.29(5)(a));
- A duty to submit the prepared code to the Secretary of State (s.32(1));
- That the Secretary of Statemay direct Ofcom to modify the code to ensure that the code reflectsGovernment policy (s.33(1));
- That, should the Secretary of State not modify the code, that it must be laid before Parliament
  (s.32(2)). Parliament can resolve not to approve the code and direct Ofcom to prepare another version (s.32(3)), or to approve the code through not making any further resolutions (s.32(4)).

As has been made clear, Codes of Practice will require scrutiny from the Secretary of State and potentially Parliament before it is approved. To avoid any further delays to the development of thisCode, Ofcom should be empowered to request the relevant information from social media platforms assoon as possible.

3. **How should the Online Safety Bill uphold the Equalities Act 2010 within Ofcom's duties?**

Under the Equality Act 2010, Parliament has afforded certain groups statutory protection from discrimination. Various public bodies, including regulators like the Heath and Safety Executive, are subject to the duties of the Equality Act, which require them to "eliminate discrimination, harassment, victimisation and any other conduct prohibited by or under the EA". We believe Ofcom, too, should be subject to the Public Sector Equality Duty, in order for the Online Safety Bill to ensure the same protection is afforded to protected characteristics online as it is offline under the Act.

The Online Safety Bill could apply this duty to Ofcom within the language of the Bill, as it does in amending Ofcom's duties under the Communications Act 2003, or this could be achieved throughsecondary legislation[1]

Guidance given to Ofcom should also reference for it to give due regard to duties imposed upon it by the Communications Act 2003: "those whose circumstances appear to OFCOM to put them in need of special protection" (s.3(4)(h)) as well as "different ethnic communities within the United Kingdom"(s.3(4)(l)). Ofcom could further be required to set out how it intends to comply with its duty under s.3(4)when carrying out its functions under the Online Safety Bill.

4. **Should the current data-accessing provisions in the Online Safety Bill be amended to better allow Ofcom to request the data that it will need?**

Access to Data

The Online Safety Bill does not currently reference data, a gap which is of concern given the power androle of data by the companies being scrutinised in this legislation. While s.70 provides Ofcom

with the power to require information for the purpose of exercising, or deciding whether to exercise, any of its online safety function, this is vague and allows for concerning levels of ambiguity as to what information can be requested and whether those providing it are allowed to screen, analyse or process information before passing it to Ofcom. We believe adding an explicit mention of data to s.70 would aid clarity in legislation, whilst allowing Ofcom to retain the breadth of powers provided by the Bill.

In comparison, the EU draft Digital Services Act focuses far more on the types of data which may be required (e.g. data on the accuracy, functioning and testing of algorithmic systems for content moderation, recommender systems or advertising systems / data on processes and outputs of contentmoderation or of internal complaint-handling systems). Whilst the purpose-led approach is helpful to give Ofcom the flexibility it needs, it would be useful to the Online Safety Bill to set out a non-exhaustive list of the types of data that Ofcom could require, which could be further supplemented by secondary legislation.

Powers of Skilled Persons

The Online Safety Bill provides for Ofcom to appoint a "skilled person" to assess information submitted and to identify and mitigate the risk of a regulated service failing to comply with requirements. However, as currently drafted, there is no ability for Ofcom to pass information to the skilled persons for the purpose of identifying instances and trends of online abuse. By comparison, the Digital Services Act allows "vetted researchers", who perform a similar role, to understand "significant systemic risks" identified within the information, rather than simply its failure to comply with regulation.

We believe the remit of the skilled persons employed by Ofcom should be widened to allow for scrutiny of the underlying issues and trends involved in online abuse, as well as the methods that providers useto mitigate them, so it is better able to understand the nature of this abuse and how it can be prevented as well as managed long-term.

---

[1] Draft language could include: "*Part 1 of Schedule 19 to the Equality Act 2010 (public authorities) under "Regulators", after "The Nursing and Midwifery Council, in respect of its public functions." insert — The Office of Communications, in respect of its public functions under the OnlineSafety Act*".

2 December 2021