Online Harms White Paper Consultation Response

JUSTICE consultation response

July 2019

For further information contact

Tariq Desai, Criminal Justice Lawyer

email: tdesai@justice.org.uk direct line: 020 7762 6416

JUSTICE, 59 Carter Lane, London EC4V 5AQ tel: 020 7329 5100

fax: 020 7329 5055 email: admin@justice.org.uk

website: www.justice.org.uk

Introduction

1. JUSTICE is an all-party law reform and human rights organisation working to strengthen the justice system – administrative, civil and criminal – in the United Kingdom. It is the UK section of the International Commission of Jurists.
2. We are pleased to be able to provide this response to the call for evidence on online harms.
3. In June 2019, JUSTICE published its working party report, *Prosecuting Sexual Offences,* chaired by HH Peter Rook QC.[1] It addresses many of the issues related to child sexual abuse contained within the Online Harms White Paper, and concludes that that preventing online offending from taking place must be a key part of the strategy in reducing the burden sexual offences are placing on the criminal justice system.
4. We would like to highlight the following recommendations from our report which are aimed at stopping child abuse imagery and materials being uploaded online. These recommendations have been selected as they directly relate to a number of questions within the White Paper:
    a. Pre-screening technology;[2]
    b. Quality mark for safe online spaces;[3]
    c. The Internet Regulator and liability for failing to prevent the existence of Indecent Images of Children on a platform;[4] and
    d. Sex and relationship education for children.[5]
5. We will also comment on the question of whether some organisations should be able to bring 'super complaints',

<u>Pre-screening technology</u>

[1] JUSTICE, *Prosecuting Sexual Offences* (2019), available online at https://justice.org.uk/our-work/criminal-justice-system/prosecuting-sexual-offences/.

[2] *Prosecuting Sexual Offences*, pp. 21-23.

[3] *Prosecuting Sexual Offences*, pp. 23-25.

[4] *Prosecuting Sexual Offences,* p. 23.

[5] *Prosecuting Sexual Offences*, pp. 12-20.

6. We consider that stopping child sexual abuse images from being available on the internet must be a priority in tackling the problem.[6] To this end, pre-filtering or pre-screening content before it is either uploaded or downloaded from the internet is possible through technology that screens and filters all uploads and downloads on platforms. Requiring internet service providers to utilise such technology would significantly reduce the availability of child sexual abuse images online.

7. The pre-filtering and pre-screening technology works by comparing the digital signature of the image being uploaded (its 'hash') to the hashes of known illegal content. If the hashes match, the content cannot be uploaded.[7] This technology would require a database of known images as well as algorithms to detect images that are not known but which appear to be IIOC. By automatically blocking content that matches or is similar to illegal content, and not requiring the company to determine what is or is not illegal content, the impact on the privacy and free speech rights of internet users should be minimal.

8. UK law enforcement has its own database of IIOC, called the Child Abuse Image Database (CAID). It holds records of IIOC known to UK law enforcement, gathered from worldwide sources.[8] The Internet Watch Foundation also has its own, smaller database and there are plans to share it with CAID to make both databases more effective.[9] A method of connecting internet service providers to this database should be explored to ensure effective prevention.

---

[6] There are currently 1,000 referrals for Child Sexual Abuse imagery to the police every month, creating a large burden on the criminal justice system.

[7] Will Kerr, Director of Vulnerabilities, National Crime Agency, Home Affairs Select Committee, Oral Evidence: Policing for the Future, Tuesday 13 March 2018, available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/home-affairscommittee/policing-for-the-future/oral/80543.pdf

[8] The Child Abuse Images Database consists of over 1,000,000 images. 'Child abuse database containing millions of images to launch', BBC News, 2014, available at https://www.bbc.co.uk/news/technology-30175102) ; HM Home Office, 'The Child Abuse Image Database (CAID)', May 2018, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759328/CAID_Brochure_May_2018_for_gov_uk.pdf ; It was created to assist the police both with the cataloguing and grading of IIOC and victim identification. It uses software to review files on any seized device, comparing those files with the known data in the database. CAID uses 'hash' values in the image metadata to process images. After being graded by three police forces, an image will be stored by CAID and approved as a 'trusted' grade. This reduces the need for investigators and prosecutors to view large numbers of images, saving time and avoiding distress: Crown Prosecution Service, 'Indecent Images of Children (IIOC)', available at http://www.cps.gov.uk/legal/h_to_k/indecent_images_of_children/

[9] The IWF's database consists of around 300,000 images ('New technology', Internet Watch Foundation, available at https://annualreport.iwf.org.uk/#new_technology : 295,389 images on it at end of 2017).

Quality mark for safe online spaces

9. Many platforms, such as Periscope, now offer a livestreaming service, which can result in 'contact offending by proxy', with the recipient of the live streaming directing the nature of the abuse. Another concern is the proliferation of online gaming. Many online games enable players to talk to each other, which can increase the risk of an adult grooming a child, as there are few safeguards in place to prevent adults playing online games with children.[10]

10. A solution to this would be to develop a quality mark, similar to a 'Kitemark'[11] for safe online spaces. This would demonstrate to users and their parents that the website or platform in question has signed up to some safeguarding functions. It would allow companies that are doing the right thing to receive recognition for this. The basic functions that would result in a Kitemark could be that a company:

    a. Ensures that their websites are 'secure-by-design' by implementing features such as pre-filtering and the proactive searching of their sites for IIOC material;

    b. Uses algorithms to identify adults trying to engage in grooming offences with children;

    c. Takes a proactive duty to engage with law enforcement;

    d. Takes a proactive duty to make sure that some anonymisation tools do not work on their online platform; and

    e. Has safeguards in place on livestreaming services to ensure that children are not at risk of grooming when using those services.

11. One concern with an approach that engages with known websites and platforms is that web pages on the 'Dark Web'[12] will not be impacted greatly. However, we understand that although some of the worst offending takes place on the Dark Web, it has a smaller

[10] Instagram has been found to be the site most used for Grooming purposes: 'Instagram biggest for child grooming – NSPCC finds' BBC News, March 2019, available at https://www.bbc.co.uk/news/uk-47410520

[11] A BSI Kitemark gives a product or service immediate status – hard earned through rigorous tests at a BSI centre of excellence, or through rigorous assessments. It is a voluntary mark that manufacturers and service industries use to demonstrate safety, reliability and quality, see https://www.bsigroup.com/enGB/kitemark/

[12] The internet is divided into three main segments: (1) the 'clear' or 'surface' web; (2) the 'deep' web; and (3) the 'dark' web. The clear web makes up about 4% of total internet content and consists of sites such as Google and Wikipedia. They are publicly accessible web pages usually indexed on search engines. The deep web makes up the remaining 96% of the internet. These are regions that are hidden from the public, either because they require credentials to access the material within, or because they are intentionally hidden from view using the dark web. As well as being hidden from the public, the dark web allows uses to access sites anonymously.

number of images on it.[13] In addition, we have been told that many of these images are pulled from easier to access websites. As such, stopping the uploading of images on easier to access websites should reduce the number of images on the Dark Web. What is more, it will allow law enforcement agencies to focus more resources on the Dark Web, to ensure that this is no longer seen as a safe space for offenders.

12. We have been informed that the National Crime Agency (NCA) has already identified a number of dark web sites, coordinating engagement by specialists both domestically and internationally. Enabling increased capacity for this important work is vital, and designing out offending on known websites will assist this.

The Internet Regulator and liability

13. We welcome the proposal for an Online Harms Regulator, which we consider must be a new public body. The internet is a fast-paced environment which evolves quickly, as do the methods criminals use to exploit it to their ends. This requires a body that has institutional expertise of the internet and the ways criminal activity can take place within it.

14. JUSTICE welcomes the acknowledgement by Government of the need for stronger regulation of companies. The approach is similar to obligations in the Companies Act 2006 on corporate social responsibility. However, the Companies Act sets out more concrete requirements that we consider should be in place for stopping IIOC, given the clear cut nature of whether or not material is IIOC. We consider that adapting the approach within the Companies Act for online harms would combine well with the proposed codes of practice and the powers of the new regulator to tackle online harms. Such an approach would mean:

    a. Internet companies whose products are available in the UK should be subject to a UK regulator who can fine the company (and possibly any director responsible for content);

    b. Internet companies which have a footprint in the UK should be required to make a return to Companies House to declare:

        i. That it is satisfied its platform contains no material the possession of which would amount to an offence under IIOC legislation; or

[13] The Dark Web accounts for 0.01% of the total number of webpages on the internet. The most common way to access the Dark Web is through 'The Onion Router' (Tor) which has between 100,000 and 200,000 users. We stress that it is estimated that only 1.5% of Tor users visit hidden/Dark Web pages.

ii. That it cannot confirm that its platform contains no material the possession of which would amount to an offence under IIOC legislation but that it has taken specified steps to check for content offending under that legislation; or

iii. That is has found offending material on its platform and it has taken specified steps to remove it.

c. A failure to provide such a statement as part of the annual report or the making of a false statement would be penalised with a fine for the company and in the case of a responsible director a sentence of up to five years' imprisonment.

15. This approach would require the internet company based outside the UK and EEA to appoint a nominated representative in the UK or EEA.

16. Should the regulator be empowered to disrupt business activities or undertake ISP blocking, we consider that a fair, transparent and accessible procedure is required before such actions are taken. The right to appeal should be embedded within this process and be merits based. This will ensure that any disruption to an internet company's services are fully reasoned and justified, as opposed to judicial review, which has narrow grounds for review based on procedural propriety.

Education

17. Our *Prosecuting Sexual Offences* report highlights the educational requirements that we consider will make children safer online. We consider that education about online child sexual education must be done holistically, together with education on consent, coercion, exploitation and healthy relationships. Child sexual abuse online does not exist in a vacuum, and giving children a broad understanding of appropriate sexual behaviour, healthy relationships and consent will provide them with the foundation they need to stay safe online.

18. We consider that the minimum requirements to ensure that education is effective are that the national curriculum and any programmes that educate about sexual behaviour should begin as early as possible in all schools and at least from year 6 (ten years old) and teach children:

a. What appropriate sexual behaviour is and what a healthy relationship consists of. This will include education on consent, coercive behaviour, exploitation and gender and sexual orientation stereotypes.

b. The law relating to:

i. Sexting;

ii. Underage sex; and

iii. Image-based sexual abuse (which should be taught from year 7).

c. Being safe online. This will include raising awareness of grooming tactics and practical advice on how to avoid being exploited online.

19. Organisations such as SPITE for Schools[14] and LimeCulture[15] have already developed programmes that address some of these areas and should be consulted on the development of such education, and supported to deliver their programmes to schools while the national curriculum is being developed.

20. The NCA's Child Exploitation and Online Protection Command has also developed its own education programme. 'Thinkuknow'[16] aims to provide children with appropriate advice and guidance for navigating the online world. As well as educating children, the NCA provides training to front-line professionals, stressing that it is essential to establish safeguards to protect vulnerable children – especially those who may have experienced abuse or exploitation – whether or not this has been disclosed. For instance, front-line professionals are taught to avoid victim-blaming language when they hear it. This is vital as even the most detailed education programme cannot be relied on alone to protect children online. Providing the NCA with appropriate funding to continue, expand and raise awareness of its work must be a priority.

Complaints

21. JUSTICE considers that designated bodies should be able to bring 'super complaints' to the regulator. Such bodies will often be alert to where breaches are taking place,

[14] Sharing and Publishing Images to Embarrass. 'SPITE for Schools Project', Queen Mary School of Law, available at https://www.qmul.ac.uk/law/undergraduate/pathways-to-law/schools-andteachers/spite-for-schools-project/

[15] See: https://limeculture.co.uk/

[16] 'Thinkuknow', CEOP, National Crime Agency Command, available at https://www.thinkuknow.co.uk/5_7/ ; The NCA has developed this information resource because it believes that a key way to protect children online is to support children to develop skills, understanding and confidence. This will help them to stay safe from abuse and exploitation and to seek help appropriately when they need it. In this vein, the NCA has developed the 'Play Like Share' animation for eight to ten year olds. Over three episodes, it helps children to recognise features of manipulative behaviour and consider strategies for resisting it. The NCA launched new resources for four to seven year olds in March 2019. These have been developed in line with best practice, agreed with the PSHE (Personal, social, Health and Economic) Association and following consultation with over 2,000 parents, carers and professionals. The young ages that these resources are aimed at indicates that the earlier children are educated about these issues, the better.

and by whom, as well as the number of people affected by these breaches. Moreover, they will have the capacity and expertise to lodge effective complaints to the regulator.

22. Where there is a gross violation of the Codes of Practice, the designated bodies should be able to bring a complaint regardless of the number of people that are affected. Where the violation is less serious, there should be evidence of at least 100 people who are affected by the breach before a complaint can be brought.

23. An Internet Ombudsman should be created for individuals, to take concerns about specific pieces of harmful content or activity and/or breaches of the duty of care,. This should be a free service that would mediate between user and company in an attempt to resolve the complaint.

24. We consider that implementing these proposals will have a great impact in reducing online child sexual abuse and child sexual abuse imagery. We would be happy to discuss our response further.

JUSTICE

June 2019