THE GOVERNMENT RESPONSE TO THE FOURTEENTH REPORT FROM THE HOME AFFAIRS SELECT COMMITTEE SESSION 2016-17 HC 609:

Hate crime: abuse, hate and extremism online

Presented to Parliament
by the Secretary of State for the Home Department
by Command of Her Majesty

December 2017

Cm 9556

This publication is available at https://www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at:

Prevent Directorate
Home Office
2 Marhsam Street
London
SW1P 4DF

PreventCommunications@homeoffice.x.gsi.gov.uk

ISBN 978-1-5286-0162-7

CCS1217596236 12/17

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty's Stationery Office

Conclusions and Recommendations - *Removal of illegal content*

Recommendation 3

Social media companies must be held accountable for removing extremist and terrorist propaganda hosted on their networks. The weakness and delays in Google's response to our reports of illegal neo-Nazi propaganda on YouTube were dreadful. Despite us consistently reporting the presence of videos promoting National Action, a proscribed far-right group, examples of this material can still be found simply by searching for the name of that organisation. So too can similar videos with different names. As well as probably being illegal, we regard it as completely irresponsible and indefensible. If social media companies are capable of using technology immediately to remove material that breaches copyright, they should be capable of using similar content to stop extremists re-posting or sharing illegal material under a different name. We believe that the Government should now assess whether the continued publication of illegal material and the failure to take reasonable steps to identify or remove it is in breach of the law, and how the law and enforcement mechanisms should be strengthened in this area. (Paragraph 30)

Government Response

The UK Government is a global leader at securing the removal of online terrorist content. The Metropolitan Police Counter Terrorism Internet Referral Unit (CTIRU) assesses material against UK terrorism legislation for referral to the hosting platform for removal.

There is provision in UK law for the police to issue a notice of request to take down terrorist content (section 3 Terrorism Act 2006) where they consider that the content is hosted in the UK. However, as the vast majority of content is hosted overseas, CTIRU pursue voluntary arrangements with industry based on their own terms and conditions. CTIRU have developed relationships with over 300 internet companies, and industry cooperation has significantly improved as a result. Through this work CTIRU have secured the removal of over 300,000 pieces of online terrorist content since February 2010.

These arrangements also mean that where companies take action content is removed from the whole platform, not just for users accessing it from the UK. However, we expect companies to do more to proactively detect and remove terrorist content from their platforms. The Home Secretary chaired a roundtable on 30 March 2017 with communication service providers (CSPs) to explore what more they could do. Subsequent to this, Twitter, Facebook, YouTube and Microsoft launched the Global Internet Forum to Counter Terrorism (GIFCT). The first meeting of the forum took place on 1 August 2017. The Home Secretary presented at the event. This forum has committed to focus on a number of key strands, including technological innovation; sharing best practice and building capacity with smaller companies; commissioning research, and increasing counter speech. We continue to engage with industry leaders and international partners to ensure the GIFCT makes meaningful progress in addressing this challenge.

We remain committed to this approach, and alongside this the Government will also consider various options for strengthening UK law if the companies do not make sufficient progress in tackling the issue.

Recommendation 5

We recommend that all social media companies introduce clear and well-funded arrangements for proactively identifying and removing illegal content – particularly dangerous terrorist content or material related to online child abuse. We note the significant work that has been done on online child abuse and we welcome that, but we believe similar cooperation and investment is needed for other kinds of illegal and dangerous content. (Paragraph 32)

Government Response

The Government agrees with the Home Affairs Select Committee that social media companies should introduce clear and well-funded arrangements for proactively identifying and removing all illegal and dangerous content.

The WePROTECT Global Alliance is a multi-stakeholder approach to tackling the issue of online child sexual exploitation, by bringing together governments, civil society, law enforcement and industry members to galvanise global action and eradicate this horrendous crime. Under WePROTECT, industry members committed to statements of action to improve their own response to the issue of child sexual exploitation, including the increase and uptake of 'hashes' or digital fingerprints of known indecent imagery of children, and the adoption of new tools and technologies. But there is much more industry could do to tackle child sexual abuse on their platforms proactively. We will continue to work with companies to improve their response to child sexual exploitation.

In October 2017 the Home Office announced the establishment of a new national police-led hub to tackle the emerging threat of online hate crime, ensure better support for victims and help drive up the number of prosecutions. The hub, which is expected to be operational by the end of the year, will work with social media companies to ensure that appropriate cases are referred for action.

We will also be introducing a code of practice as laid out in the Digital Economy Act 2017. The code will not cover unlawful content which the legal framework already addresses. However it will include guidance to address conduct that involves bullying or insulting an individual online, or other behaviour likely to intimidate or humiliate the individual.

We have also been working with industry to ensure they adopt a more proactive approach to removing terrorist content. As a result the four leading platforms – Twitter, Facebook, Microsoft and YouTube – have launched the GIFCT, which had its first meeting on 1 August 2017 in San Francisco. The Home Secretary presented at the event. Following the first meeting of the forum, the Prime Minister co-chaired an event jointly with the leaders of France, Italy, and a representative of

the GIFCT, at UNGA on 20 September in New York, to highlight our commitment to the forum's success, and upcoming milestones.

Recommendation 6

We note that football teams are obliged to pay for policing in their stadiums and immediate surrounding areas under Section 25 of the Police Act 1996. We believe that the Government should now consult on adopting similar principles online - for example requiring social media companies to contribute to the Metropolitan Police's CTIRU for the costs of enforcement activities which should rightfully be carried out by the companies themselves. (Paragraph 33)

Government Response

The Government set out the idea of a social media levy in the Internet Safety Strategy and will explore the recommendations suggested by the committee regarding funding, whilst continuing to encourage industry to take a leading and more proactive approach to terrorist and extremist content online.

Recommendation 7

Here in the UK we have easily found repeated examples of social media companies failing to remove illegal content when asked to do so—including dangerous terrorist recruitment material, promotion of sexual abuse of children and incitement to racial hatred. The biggest companies have been repeatedly urged by Governments, police forces, community leaders and the public, to clean up their act, and to respond quickly and proactively to identify and remove illegal content. They have repeatedly failed to do so. That should not be accepted any longer. Social media is too important to everyone—to communities, individuals, the economy and public life—to continue with such a lax approach to dangerous content that can wreck lives. And the major social media companies are big enough, rich enough and clever enough to sort this problem out—as they have proved they can do in relation to advertising or copyright. It is shameful that they have failed to use the same ingenuity to protect public safety and abide by the law as they have to protect their own income. (Paragraph 36)

Government Response

The Government agrees with the Home Affairs Select Committee that social media companies should respond quickly and proactively to identify and remove illegal content.

Companies should invest in ensuring the safety of their users and to prevent misuse of their platforms to perpetrate serious crimes. We expect social media companies to respond quickly to incidents of abusive behaviour on their networks. This includes having easy to use reporting tools, robust processes in place to respond promptly when abuse is reported, and suspending or terminating the accounts of those who do not comply with acceptable use policies. Both social media sites and users need to take responsibility. The law does not differentiate between criminal offences committed on social media or anywhere else – it is the

action that is illegal. What is illegal offline, is illegal online. In order to aid the effective prosecutions of those acting illegally online, in 2016 the CPS revised Guidelines on Prosecuting Cases Involving Communications Sent via Social Media."

We will also work with industry through the GIFCT, the Internet Watch Foundation, the WePROTECT Global Alliance and others to promote innovation and encourage the prompt removal of terrorist and known child sexual abuse material.

Recommendation 8

Social media companies currently face almost no penalties for failing to remove illegal content. There are too many examples of social media companies being made aware of illegal material yet failing to remove it, or to do so in a timely way. We recommend that the Government consult on a system of escalating sanctions to include meaningful fines for social media companies which fail to remove illegal content within a strict timeframe. (Paragraph 37)

Government Response

Currently, the government works with social media companies to remove illegal content on a voluntary basis through the CTIRU and WePROTECT, and will escalate any non-compliance with the relevant company where possible.

The GIFCT will continue the collaboration of government and industry, and will seek to ensure industry is significantly more proactive in its efforts. The WePROTECT Global Alliance is also working with industry to develop new solutions, build best practice, and put in place appropriate measures to respond to illegal content and secure its removal.

At the same time, the Government will look to consider alternative, regulatory options if faced with continued non-compliance by companies, that would give regulators the ability to fine or prosecute companies that fail in their legal duties and to order the removal of content where it clearly breaches UK law.

Conclusions and Recommendations - *Community Standards*

Recommendation 10

We recommend that social media companies review with the utmost urgency their community standards and the way in which they are being interpreted and implemented, including the training and seniority of those who are making decisions on content moderation, and the way in which the context of the material is examined. (Paragraph 40)

Government Response

The Government agrees with the Home Affairs Select Committee that social media companies should review their community standards and the way in which they are interpreted and implemented.

Next year, we will publish a code of practice which will provide platforms with guidance on a number of issues including maintaining arrangements so individuals can notify platform providers about conduct that involves bullying or insulting an individual online, or other behaviour likely to intimidate or humiliate the individual. The code will also include guidance about maintaining processes for dealing with notifications, ensuring relevant matters are clearly included in terms and conditions for using platforms and providing the public with information about action providers take against their platforms being used for harmful conduct.

As part of our Internet Safety Strategy, we are also consulting on introducing an annual internet safety transparency report so that we can better understand the prevalence and types of harmful content and conduct online and how complaints are dealt with.

Conclusions and Recommendations 11, 12 and 13 - *Social media companies' response to complaints*

Recommendation 11

We have heard time and time again that, for people without the platforms available to Members of Parliament or journalists, responses from social media companies to reports of unacceptable content are opaque, inconsistent or are ignored altogether. It should not rely on high level interventions for social media companies to take action; and there must be no hierarchy of service provision. We call on social media companies urgently to improve the quality and speed of their responses to reports of dangerous and illegal content, wherever those reports come from. (Paragraph 43)

Recommendation 12

It is unacceptable that Twitter, Facebook and YouTube refused to reveal the number of people that they employ to safeguard users or the amount that they spend on public safety initiatives because of "commercial sensitivity". These companies are making substantial profits at the same time as hosting illegal and often dangerous material; and then relying on taxpayers to pay for the consequences. These companies wield enormous power and influence and that means that such matters are in the public interest. (Paragraph 45)

Recommendation 13

We call on social media companies to publish quarterly reports on their safeguarding efforts, including analysis of the number of reports received on prohibited content, how the companies responded to reports, and what action is being taken to eliminate such content in the future. It is in everyone's interest, including the social media companies themselves, to find ways to reduce pernicious and illegal material. Transparent performance reports, published regularly, would be an effective method to drive up standards radically and we hope it would also encourage competition between platforms to find innovative solutions to these persistent problems. If they refuse to do so, we recommend that the Government consult on requiring them to do so. (Paragraph 46)

Government Response

The Government agrees with the Home Affairs Select Committee that social media companies should improve the quality and speed of their responses to reports of dangerous and illegal content, wherever those reports come from; that social media companies should be more transparent in their efforts to tackle illegal and dangerous material; and that social media companies should be more transparent in their approach to pernicious and illegal material.

We are consulting on introducing an annual internet safety transparency report so that we can better understand the prevalence and types of harmful content and conduct online and how complaints are dealt with. The Government agrees that regular reporting could drive improvements by helping to benchmark companies' progress and encourage the sharing of best practice.

Conclusion and recommendations - *Technological responses*

Recommendation 14

We welcome the development of technological solutions to tackle the problem of inappropriate content on social media—including Twitter's new mechanisms to prevent dogpiling, and new matching technology. We recognise that technology cannot solve all the issues and that human judgement will often continue to be needed in complex cases to decide whether material breaches the law or community standards. But we are disappointed at the pace of development of technological solutions—and in particular that Google is currently only using its technology to identify illegal or extreme content in order to help advertisers, rather than to help it remove illegal content proactively. We recommend that they use their existing technology to help them abide by the law and meet their community standards. (Paragraph 49)

Government Response

The Government also welcomes social media companies' efforts to tackle the problem of inappropriate content on their platforms, and looks forward to the development of new and innovative technical solutions to continue to proactively tackle the spread of content. We are continuing to work with companies through the WePROTECT Global Alliance and the GIFCT to encourage industry to develop new solutions and best practice to take effective and proactive action.

The Government set out in the recently published Internet Safety Strategy green paper, that it wishes to embed the principle of 'think safety first' into the development of new technology. This will encourage developers to consistently consider safety as new products and platforms are developed. We plan to build on the work of the UK Council for Child Internet Safety (UKCCIS) Technical Working Group by creating a Technical Network which will bring together a specialised group of engineers and innovative technology businesses who will work together to develop and share new ideas and communicate and challenge each other.

Conclusions and Recommendations - *Legislative framework*

Recommendation 15

Most legal provisions in this field predate the era of mass social media use and some predate the internet itself. The Government should review the entire legislative framework governing online hate speech, harassment and extremism and ensure that the law is up to date. It is essential that the principles of free speech and open public debate in democracy are maintained—but protecting democracy also means ensuring that some voices are not drowned out by harassment and persecution, by the promotion of violence against particular groups, or by terrorism and extremism. (Paragraph 56)

Government response

The Government notes the Committee's acknowledgement that the current legal framework is comprehensive and its recommendation that this should be reviewed to ensure it is up to date, effective and properly balanced. The Government will consider the current legal framework in the context of its wider work on hate crime, terrorism and extremism. It hopes also to be informed by a further report from the Committee's own wider consideration of these matters. In due course, the Government will also be considering the report from the Committee in Standards in Public Life into the intimidation experienced by Parliamentary candidates.
The recently enacted Digital Economy Act will help to ensure that online abuse is more effectively tackled by requiring a code of practice to be established. The code will set out guidance about what social media providers should do in relation to conduct on their platforms that is directed at an individual and involves bullying or insulting the individual or other behaviour likely to intimidate or humiliate the individual. The code of practice will include guidance on arrangements for notification by users; the process for dealing with notifications; terms and conditions in relation to these arrangements and processes; and the giving of information to the public about the action providers take against harmful behaviour. We are consulting with social media and other interested parties on what the code will look like. We will publish the code in 2018.

CCS1217596236
978-1-5286-0162-7