

# Speech: Home Secretary launches Online Harms White Paper

## **Intro: the benefits of tech**

Thank you, Jeremy, for those rousing words.

It's always a great pleasure to be back here at the British Library.

I remember that one of my very first jobs as a Cabinet Minister, almost exactly five years ago, was to open the hi-tech newspaper reading room here. It's on the second floor of the main building if you perhaps want to take a look later. I'm not sure if there's a plaque there with my name on it, but if there is please do give it a little polish...

Back then I actually had Jeremy's job and my children still very much miss that job as Culture Secretary all the sporting advice and those gigs and tickets that were offered. I must say ever since then as far as my children are concerned every job I have had has been a demotion.

This library is a great resource – one that not only provides access to something like 400 years of newspapers, but also gives a very real example of how communication has been revolutionised by technology. Because while the British Library's National Newspaper Archive stretches back to 1620 and boasts some 750 million pages, the UK Web Archive that sits alongside it – an archive that, by definition, cannot go back any further than 1989 – is home to more than a billion individual pages, with each one available around the world.

The internet has given the world access to an explosion of information unparalleled in human history. And, over the past decade or so, the rise of social media has allowed people to connect in ways we have never seen before.

Facebook and Instagram have built communities that span the globe. Twitter and YouTube have given voices to the voiceless, they've bridged oceans, they've flattened mountains and they've made national borders all but irrelevant. WhatsApp has connected families and friends wherever they may.

## **The threat we face**

The growth of the online sphere, and the apps and platforms through which we access it, has been and continues to be an unparalleled force for good worldwide. And I will always applaud the individuals who spin the thread of an idea into some multibillion dollar, multinational company, but we cannot turn a blind eye to the darker side of social media.

It's less than a month since a terrorist murderer used Facebook to live broadcast a killing spree so the whole world could see.

This year we've also seen a boss of a nursery convicted for prowling child

sexual abuse chatrooms, we've seen teenage girl admitting she travelled to Syria after watching Daesh beheading videos online.

Every single one of the 2017 terror attacks had an online element, and every month in the UK, some 400 people are arrested for online sexual abuse and exploitation offences. Last year, Facebook removed over 14 million pieces of content relating to terrorism or violent extremism. And in just three months they removed 8.7 million items that breached policies on child nudity and sexual exploitation. But how much more illegal material remains? And how much damage is being done by this cruel content is even less clear. The cyber-bullying, trolling and posts glorifying self-harm. Truly harmful content that's linked to depression, anxiety, mental health problems and even suicide.

Social networks bring great joy and great comfort to a great many people, but we, as a government and a society, we cannot ignore the fact that individuals and groups around the world are using them to facilitate, encourage and commit some of the most vile and abhorrent crimes.

We cannot abdicate our responsibility to protect our children and vulnerable people from such dangers. And we cannot allow the leaders of some of the tech companies to simply look the other way and deny their share of responsibility even as content on their platforms incites criminality, abuse and even murder.

To be a bystander is to be complicit. And I am not prepared to let them stand by any longer.

### **Moral duty – on/offline**

Because it's very simple: if you run a business, any business of any kind, you have a duty to protect your customers. That's why a retailer cannot sell alcohol and tobacco to children. It's why a car manufacturer cannot put a new vehicle on the road without making sure it's safe. It's why a landlord cannot rent you a room in a house if they know that's about to fall down. It's a moral duty, yes, but it's one underpinned by legal responsibilities – that offenders can be punished if they break the rules.

Yet, for some reason, some tech companies have long got away with the claim that they cannot possibly be expected to take any more responsibility for the safety of their customers. They'll take your money, they'll harvest your data, they'll sell your details to advertisers, but protect you from harm? They say no can do.

Too many social media firms still seem to think that they can get away with providing a service without providing the protection for users. That anyone who challenges them must be some kind of luddite who just doesn't understand the modern world. That a little progress here and there is acceptable while countless lives are being destroyed. Enough.

## **Time to act**

I said in September, I warned the web giants. I told them that keeping our children safe is my number one priority as Home Secretary. That they needed to do more to protect our young people online. And that if they didn't then I wouldn't hesitate to take action.

There has been some progress. For example, in the US I saw experts brought together by Microsoft to build an online anti-child grooming tool. Some companies are they are waking up to their responsibilities and they are trying to drive change.

But it's clear that the industry as a whole has not done anywhere near enough. So, as promised, I am now forcing them to so.

## **Duty of care**

Today we're announcing a new regulatory regime – one that will make sure that all tech firms play their part. At the heart of this our new statutory duty of care will legally oblige tech firms to protect their users. Compelling them to take reasonable and proportionate steps to stop and prevent harmful material.

## **CSEA and CT**

It is only right that the rules will be even tougher for the most serious of harms. So, there will be specific and stringent obligations to tackle online child sexual exploitation and terrorist content. Tech companies will be expected to take active steps to stop users accessing this vile material.

They must develop new ways to find illegal content– including illegal activity featured in live streams, and online grooming. And they will be compelled to take steps to identify offenders and to work with law enforcement to bring them to justice.

## **Transparency**

Tech firms will be required to submit annual transparency forms outlining the scale of the threat and their response. These reports will be published online to make them fully accountable to their users.

## **Regulator**

And, as Jeremy said, we're creating an independent regulator to enforce this new regime. It will make sure tech firms fully deliver on their duty of care – prioritising the greatest threats and the most vulnerable users. And it will draw up codes of practice that make it crystal clear what tech firms must do to stay on the right side of the law – whether that's adopting certain tools, or its setting appropriate terms and conditions, or acting within a specified timeframe. The first interim codes will be published later this year.

## **Enforcement**

And don't be under any illusions, this regulator will not be some kind of paper tiger. Rather, it will be backed up with a suite of tough enforcement powers that will give it real teeth.

So if companies fail to fulfil their safeguarding obligations they will face serious consequences. We're consulting to make sure we get it right but we are proposing in a white paper a series of hard-hitting penalties.

First, that tech companies who don't comply will be hit with heavy fines, linked not only to the scale of the offence but also to the size of your company – so the bigger your turnover, the bigger your fine.

Second, that offending companies will be named and shamed with public notices about failure to meet expected standards.

Third, websites and apps who refuse to protect users could be blocked in the UK.

And finally, individual senior managers could face criminal charges – becoming personally liable for any major breaches.

Tough penalties, yes. But entirely in keeping with the seriousness of the issue.

They had their chance to put their own house in order. They failed to do so, they failed to protect our children, and I won't let them fail us again.

## **A shared responsibility**

Because, as a society, one of our greatest responsibilities lies in keeping our children safe. It doesn't matter if you're a parent or not – we all know that young people need protecting, nurturing, steering in the right direction.

Yes, we need to give them the freedom to explore their world and to realise their ambitions. But we also need to provide a safety net, to defend them against those who would do them harm. And, as a society, I actually think we're pretty good at it. If we saw a child being abused or threatened, I'm sure all of us in this room would step in and do something. If we saw them wandering the streets alone at night, we wouldn't just walk on by and leave them to it – We'd step up. We'd do something. And we'd do something because we know, in our hearts, we know that protecting the vulnerable is our shared responsibility.

It's not controversial, it's not authoritarian. It's just what you do in a civilized society,

Yet for all these good intentions, right now all of us are failing. And I know we are failing because, every day and every night, millions of young and vulnerable people here in the UK still head out alone, there is nobody to help them.

They leave behind our protection and supervision and go online to a place that is a hunting ground for monsters. Where child there are child abusers trawling they are looking to victimise them. There are gangs that lure young people into violence. There are terrorists who groom new recruits, then encourage them and teach them to carry out the most appalling atrocities. And where the same algorithms that allow people to build communities around shared interests can also lead young people into a devastating spiral of darker and more depraved material.

As parents, and as a society, we can – and we do – warn of the dangers that can lurk online: in games, apps, chat rooms and more. As parents we try to limit screen time, we try to monitor their use of social media, and teach our children how to be safe online. But once they enter the online realm they are beyond our reach we can't help anymore. If we want to enjoy the benefits of the online world we have no choice but to put our faith in the tech companies that run that world. We trust them with our children and we rely on them to keep their platforms safe.

## **Conclusion**

Right now, the tech giants are not repaying that trust.

For too long they have failed to go far enough and fast enough to help keep our children safe. They have failed to do the right thing – for their users, for our families, and for the whole of society. And they have failed to show the moral leadership we expect of those trusted with the right of self-regulation.

They have dodged and evaded. They have hidden behind the distinction between platforms and publishers. They have failed to take responsibility for the content posted by others online but they are quite happy to profit from that very same content. And if they had used just a fraction of that money from their deep pockets to start dealing with the problem, then we wouldn't be where we are today. But they've made their choice, and I've made mine.

I'm giving tech companies a message they cannot ignore.

I warned you. And you did not do enough. So it's no longer a matter of choice. It's time for you to protect the users and give them the protection they deserve, and I will accept nothing else.

Thank you.