House of Commons

Petitions Committee

Oral evidence: Tackling Online Abuse, HC 766

Tuesday 2 November 2021

Ordered by the House of Commons to be published on 2 November 2021.

Watch the meeting

Members present: Catherine McKinnell (Chair); Tonia Antoniazzi; Martyn Day; Christina Rees; Matt Vickers.

Questions 1 - 40

Witnesses

I: Nancy Kelley, Chief Executive, Stonewall; Danny Stone MBE, Chief Executive, Antisemitism Policy Trust; Matthew Harrison, Public Affairs and Parliamentary Manager, The Royal Mencap Society.

II: Ruth Smeeth, Chief Executive, Index on Censorship; Chara Bakalis, Principal Lecturer in Law, Oxford Brookes University; Dr Joe Mulhall, Head of Research, HOPE not hate.

Written evidence from witnesses:

- Danny Stone MBE, Chief Executive, Antisemitism Policy Trust;
- Matthew Harrison, Public Affairs and Parliamentary Manager, The Royal Mencap Society

HOUSE OF COMMONS

Examination of witnesses

Witnesses: Nancy Kelley, Danny Stone MBE and Matthew Harrison.

Q1 **Chair:** Thank you for coming in today to talk to us about tackling online abuse. I am sorry that there are not more Members here today, but several members of the Committee are sitting on Public Bill Committees that are meeting at the same time.

This session marks the resumption of the Committee's inquiry into this topic. It is under heavy scrutiny at the moment in Parliament across a number of Committees, and it comes at a good time, following the Government's publication of the draft Online Safety Bill earlier this year.

We heard evidence from petitioners last year about the impact of online abuse on them and their families, but it is clear that action is needed on this issue and has only become more urgent since we took that evidence and heard from those petitioners.

Before we launch into our questions for you today, can I please ask you to briefly introduce yourselves?

Danny Stone: I am Danny Stone. I am the chief executive of the Antisemitism Policy Trust. It is a charity that works to educate decision-makers about antisemitism.

Nancy Kelley: My name is Nancy Kelley. I am the chief exec of Stonewall. We are an LGBTQ+ rights organisation that works for the rights of LGBT people here in the UK and around the world.

Matthew Harrison: I am Matthew Harrison. I am the public affairs and parliamentary manager at Mencap. We are there to support the 1.5 million people with a learning disability in the UK to access better healthcare services, care services, employment and education. We also provide direct support to more than 5,000 people with a learning disability.

Q2 **Chair:** Before we start, I should also declare that I co-chair the All-Party Parliamentary Group against Antisemitism, for which the Antisemitism Policy Trust acts as the group secretariat.

I will take the Chair's privilege by asking the first question today. Sadly, we know that the communities that your organisations campaign on behalf of are frequent targets of online abuse. We heard very powerful testimony from petitioners who really want to see change in this area. Can you briefly set out the impact that this abuse has had on the recipients that you are here to represent?

Danny Stone: First, thank you very much for the opportunity to appear before you. It is always good to be able to highlight the issues. Antisemitism online is widespread and pervasive. The numbers of incidents have risen. The Community Security Trust, which is another charity and an excellent organisation, collects data. We know that, in 2017, 247 of the 1,300 incidents were online. These are incidents that are proactively reported to the CSC. They do not go searching for antisemitism online; they would be there forever. It was 18% of the incidents in 2017. By 2020, we are up to 38% of the incidents. It is regularly now about 40% of the incidents.

When I say "incidents", the range of this includes criminal behaviour. Some of it is abusive and discriminatory. There are death threats. Intimidation of people in public positions and in public life has been well documented. We have seen conspiracy theories, which lead to real-world harms. We have seen, particularly, abuse of Jewish women. We see intersectional abuse. If there is an opportunity, I will happily talk more about that. It ranges.

We know that there is poor enforcement across the platforms. Specifically, we also know that some so-called alternative platforms, smaller platforms, are designed for harm, and some of them have significant levels of abuse. Gab is an antisemitic Twitter. It might be best to characterise it like that. The Britfam group has 4,000 members, with 1,000 posts per day, including antisemitism and holocaust denial.

It is not just the Twitters and Facebooks of this world; there are a range of harms occurring across a range of different platforms. It is sinister, we have a problem and, at the moment, it is completely unregulated. Something needs to be done.

***Nancy Kelley*:** I would start by saying that the digital world also brings enormous benefits to LGBTQ+ people, particularly those of us who live in unsupportive homes, unsupportive communities or hostile environments. There is a real balance here in terms of the benefits of online participation for LGBTQ+ people in particular, but it is also very clear that online harm has a devastating impact on LGBTQ+ people.

In terms of what that looks like on a day-to-day basis for ordinary LGBTQ+ people, if you look at the online hate report by our sister organisation, Galop, you see that a very high proportion of people have experienced online harm. Nearly 100% of us have been insulted; 63% of people have been threatened with physical violence; 41% of people who have experienced online hate have experienced threats of sexual assault; and 39% have experienced death threats. It is quite a severe form of online abuse that we see, and the prevalence is very high.

You can look at international studies. The Pew Research Center in the US does a state of online harassment report. It will show you that about 70% of lesbian, gay and bisexual adults have encountered online harassment. It is only about four in 10 straight adults, so it is much higher than for the straight population. As the Committee will know, the trans community has really faced devastating, escalating abuse. We can look at 2019 research from Ditch the Label and Brandwatch that looked at 10 million posts, and 1.5 million of them were severe transphobic content.

All of our community, including here in the UK, experience this very high prevalence of abuse. In terms of the impact that has, you will see impacts that will be probably very similar across all of our groups, about mental health, about people’s confidence participating, not just digitally but in the real world, but also for LGBTQ+ people you will see some very direct impacts beyond that. Being outed and being doxed are both very common forms of online abuse for our community. That can mean LGBTQ+ people becoming homeless, losing their job, feeling like they need to leave their job or feeling like they need to leave their community or their church. Forms of abuse that we might think of as purely digital for our community very quickly can have very major real-life impacts.

***Matthew Harrison*:** I would start by putting it in context. People with learning disabilities face social isolation and stigma in the real world. That very much carries across into the digital environment and digital world. In terms of the bullying and harm that is carried out, there is already high prevalence in the real world. One in three people with learning disabilities told us that bullying is one of the things they fear most before they leave the house.

Unfortunately, as I said, this is carried across into the online sphere. Leonard Cheshire and United Response found in 2019-20 that disability hate crimes online went up 52%. We suspect it has probably increased in the last year, just because of the pandemic and people being forced to socialise more and more in the digital world or on social media platforms. It has a knock-on effect whether that is happening in the real world or online as well.

As I said, this group already faces high levels of social isolation, and experiencing online harms can lead to increased levels of isolation and seclusion in their own home. We know that that impacts life opportunities, whether that is employment or socialising. We also know that actually has an impact on a person’s physical health as well. These are very much real-world impacts. Even though it seems like they are just a tweet or a post, they do actually impact people’s lives and well-beings and health.

Q3 **Chair:** You have all painted quite a challenging picture. What would you say are the most important issues to address if we are to tackle the abuse and the impact that you are describing?

***Danny Stone*:** The Online Safety Bill is the main game in town now. My view is that, at the moment, some of the duties as drafted are too specific. It creates different duties on platforms to deal with illegal content in respect of adults and children, and then legal but harmful content, but only for certain types of platforms and with specific exemptions. For example, search is exempt from addressing legal but harmful content, and where legal but harmful content is addressed, the companies or platforms that are involved have only to have terms and conditions that deal with the harm. That is it; that is the wording.

There should be a more general foundational duty of care that comes either above or instead of those various duties. We need stronger penalties. Again, I would be happy to talk more about this, but at the moment there is not really a proper senior manager liability structure in the Bill. There is sort of one but not a full one, in my view.

We should also ensure that anonymity is dealt with. At the moment, there is no reference to anonymity in the Bill. There has been lots of discussion about this. I have particular ideas about how I think that could be dealt with in a way that balances respective freedoms and interests.

Those are the top ones that would be helpful in respect of the Bill.

Q4 **Chair:** Can I just probe that slightly? You talked about having an underlying, foundational or what you might call overarching duty of care, but you all described various harms and abuse that are experienced. Do you think that we have a clear enough picture of how to establish the harm in order to establish the duty of care? Do you think we are recording the harm sufficiently to be able to implement a duty of care?

***Danny Stone*:** At the moment, it is slightly difficult to say. if one listens to Frances Haugen, the Facebook whistleblower, she was pretty clear that the data that we are being given is not accurate. It is based on an interpretation of what is being asked. That is why some of the transparency duties that are in the Bill are going to be important to try to work out what is going on.

There are various bits of data out there. The European Commission, for example, has some. We have a bit of an understanding. Obviously, organisations like ours and CST in the antisemitism space understand that. Harms develop. Whatever we do will need to be flexible. At the moment, the proposal is that the harms will be listed in secondary legislation.

I am relatively comfortable with the way the Bill is drafted at the moment, but the foundational duty of care in any event will be useful, because it refocuses on systems rather than content, and that is where we need to be—not on the specific content but on the systems that are enabling that harmful content to be spread. I hope that answers the question.

***Nancy Kelley*:** I will build on some of what Danny has said and then range a bit more broadly than the Online Harms Bill. We completely agree about the value of having a foundational duty of care and really shifting responsibility to platforms to be thoughtful and to demonstrate the way in which they are providing a safer online experience. We are concerned to make sure that not only the largest platforms are covered, as is currently the case, the category 1 platforms, because what we know from our community is that much of this hate is fomented on smaller platforms that would be completely unregulated under the current scheme. Regulation would need to be appropriate to the size and nature of the platform, but to leave that space untouched in terms of legal but harmful content is a major loophole.

We have some concerns about tightening up the definition of some of the exemptions that are currently on the face of the Bill, particularly for conversations of democratic importance and journalistic importance. I am happy to come back to those things, but I very much endorse everything that Danny said.

If I could just point to a couple of other issues more broadly outwith the context of the Bill, first, existing platforms can already do a much better job of enforcing their community standards that they have, and they can already do a much better job of the safety by design challenge. Picking up the theme from Danny around Facebook, one of the things that was very clear in the Facebook papers is to do with the algorithmic amplification of hate. For a very long time, angry faces were getting upweighted in the algorithm. They were getting promoted more and were associated with hateful content.

We know that there are system-wide processes that platforms could improve right now, and there are also individual processes, responses to complaints, that platforms could improve right now. We should not need to legislate to make them do it. We should hold them to account for that. For those of you who have ever tried getting posts removed from a platform, it is quite instructive what is not considered to be against community standards.

I will point to one last issue and then hand over to my colleague Matthew. A lot of people concerned about online safety are rightly concerned about creating positive online citizens, so education for young people, and we would agree that that is really important. However, it is equally if not more important to understand that a lot of the online hate we see is being produced by a very small number of people who have become very radicalised and often are expressing that hate across multiple groups. There are huge overlaps between antisemitism, homophobia, transphobia, ableist abuse and racism of all sorts. It is really important to think about what de-radicalisation looks like in the space of online hate and how we set up both systems and supportive programmes that prevent people becoming prolific producers and amplifiers of hate online.

Matthew Harrison: I find it really hard to disagree with quite a lot of what my colleagues have said here. On the Online Safety Bill, I would definitely agree about the duty of care. That is something that we would like to see put back in. We have the same concerns about some of the ambiguities in the Bill, around those terms of legal but harmful content. One particular phrase that concerns us is "ordinary sensibilities". Who is the provider of said ordinary sensibilities? As we have highlighted, quite a lot of the Bill is being left to codes of practice, to secondary legislation and to the Secretary of State's strategic priorities; that is the official term. We would like to see some of those ambiguities ironed out. We do welcome the Bill itself in terms of actually bringing enforcement in industry standards.

That is one that has been covered quite a bit. The second is some of the Law Commission's current work looking at hate crime and offensive communications laws. They seem to be moving in the right direction, which the Law Commission is suggesting. That is something that needs to be looked at at the same time as the Online Safety Bill, because they do interplay between each other, and sometimes the reforming of those laws is actually overlooked.

Q5 **Tonia Antoniazzi:** Do you all accept that conversations about public policy and law making should not be unduly censored on online forums? You are all nodding.

***Danny Stone*:** Yes. I have always been of the view that freedom of speech is fundamental to who we are in Britain. Particularly, of course, in policy circles there needs to be the freedom to have difficult conversations responsibly and to lead public debate. Some of the major concerns about antisemitism were that there were people in public positions who were not talking responsibly. It is about having a proper, thorough debate, and having a responsible one.

I do not believe in censorship, in that sense, but at the moment in the Bill it talks about content of democratic importance, and there is an exemption for that. Again, as colleagues were saying, I worry that that is not carefully defined. What will that look like and who will get the protections there? Is there the potential for those seeking to cause harm deliberately to get those protections?

***Nancy Kelley*:** I completely agree with everything Danny has said. If it is helpful, I can give an example of a public policy conversation that can cross the line, which we are involved with in Stonewall. We were set up to advocate for LGBTQ+ inclusion in schools—the repeal of Section 28 30 years ago—and we still work on LGBTQ inclusion in schools today. There is a very wide range of views about what relationships and sex education should look like in schools, including a very wide range of important views that are very different from mine and my organisation's and that absolutely should be able to be expressed.

One of the things that happens when you have a public policy debate about LGBTQ inclusion in schools, and sex and relationships education, is you have all of that debate, and you also have people calling lesbian, gay, bi and trans people paedophiles as part of their argument. The abusive part should not be covered by an exemption, but somebody who absolutely disagrees with the idea that children should be talked to about sexuality at all on religious or secular grounds, for instance, should absolutely be able to express all of those things. It is about how you make it possible for people to exercise their rights to free speech without straying into exercising those rights in a way that is directly abusive of, in this case, minority groups.

***Matthew Harrison*:** That is a good point. We very much do not want to censor reasonable views, but direct targeted prejudiced harms or hatred is something that does need to be tackled. There was a good point about the Online Safety Bill and those terms, "journalistic content" and "democratic importance". I was racking my brain for a situation where an online harmful or hateful comment would actually fall under either of those terms. It is about having that reasonable approach. It is a very small minority of people who cross that line. The majority of people realise who has crossed the line and what crossing the line is. We can have that balance, but it is a perpetual tension when you talk about these issues. I hope the Online Safety Bill is not just a one-off. It is something that requires renewed discussions to keep up with the times and with changes in language and attitudes, as well as societal changes.

It is something we should always keep an eye on, but there is a balance that the majority can find.

***Nancy Kelley*:** We often talk about this as if the two ideas, protection and safety online and free speech online, are in tension. Indeed, they can be, but they are not always. All three of us have given examples, and having a safer online space is a precondition for all of the groups we represent to be able to participate and express their own free speech rights. Indeed, some of the issues around anonymity for LGBTQ+ people are about being able to express their views as well. It is important to think also about the way in which a more secure online environment makes it possible for people to express themselves.

Q6 **Christina Rees:** We have received several petitions that have suggested that being able to post anonymously online encourages abusive behaviour. Is this something you have found?

***Danny Stone*:** Yes, it does; that is the direct answer. There are various studies that can be referenced that would show that people have less inhibition when they are anonymous and that they will post in a more harmful or hateful way. I have data from the Community Security Trust for the month of October 2020, and 40% of the online incidents in that month were from anonymous accounts; that may have been voice recordings and anonymous usernames. More broadly, we know about the QAnon movement and the fact that anonymity emboldens people to act in a harmful way.

My view is that our organisation has the most balanced and sensible approach to all of this, which is that we are not calling for a ban on anonymity. We recognise the value. Nancy has spoken about the importance of anonymity, and we certainly recognise that it must be there for certain people. There are important protections that anonymity provides. However, there are things that we might be able to do through the Bill that would ensure safety for people so that there is not the abuse that we see using the shield of anonymity.

For example, a simple thing to do would be to amend Section 61 of the Bill in respect of the risk assessments that companies do. Anonymity is a risk. We know it is a risk and we can prove it is a risk. Should a company not have to risk-assess how it addresses that risk and what it is that it puts in place to ensure that anonymous abuse does not happen?

The other thing that we may be able to do—I am talking to various solicitors and barristers at the moment—is about police powers. In certain cases, the police can demand a revelation of identity in respect to, say, terrorism. There are production orders. Are those working effectively? We know from our initial discussions with police that the platforms are patchy in their responses to police. It is fair to say that the way in which they respond is not consistent. Might there be a way to look at police powers? What are the police powers that need underlining through the Bill that could be restated or taken across from that terrorism or child sexual exploitation and abuse space, and effectively mirrored in respect to threats?

Ultimately, my view is that the platforms should be liable. If they cannot provide the information, there needs to be some liability. It cannot be down to me or our organisation. There is a platform liability. If you cannot show us who is behaving in a criminal way on your platform, then you should be liable for it.

***Nancy Kelley*:** I would certainly agree with Danny that there is ample evidence that anonymity contributes to severity of harm and proliferation of harm. I do not think anybody disagrees with that at all.

The note of caution we would sound about some of the approaches to dealing with online anonymity is about the potential impact on LGBTQ people’s ability to participate online. In the case of forms of identity verification that display at least some personal information—parts of real names, and so on—which is one of the proposals that people talk about, that would create a very direct risk of harm. If you think back to the kinds of impacts I talked about, being outed or being doxed is harmful for LGBTQ+ people, including here in the UK, if you come from a socially or religiously conservative family community background or just do not want to be out. That visible verification would really prohibit parts of our community from being able to fully participate online.

People talk about banking, know your own customer and middleware approaches; that obviously mitigates that risk quite a lot, but it is very important to think about the amount of personal data that goes into those approaches. I checked this morning and, if you want a gov.uk Verify account, you are getting credit-checked on a credit check agency. You are providing photographic ID. You are providing quite a lot of personal ID to verify your identity. That feels proportionate if you are talking about a bank account, your benefit payment or paying taxes. It is a lot of personal identification to hand over to do an Instagram post.

We think that is fairly likely to have a chilling effect on LGBTQ people's participation or being out online. We know that, particularly for people from our community that come from those more conservative, less inclusive communities or backgrounds, sometimes online is the main place they can be their full selves. We think there is a lot to think through in terms of how you would identity-verify in a way that did not raise all of those risks for LGBTQ+ people.

***Matthew Harrison*:** I agree a lot with what Nancy says. We look at it through the lens of people with learning disabilities. Our main concern, or what we are thinking through whenever we hear of various proposals and suggestions, is about whether it is accessible to people with learning disabilities. As you say, opening a bank account involves quite a lot of ID, and we know that people with learning disabilities have lower levels of ownership of most forms of ID. Should we move through to quite a stringent ID process, we have concerns that perhaps the system might end up excluding people with learning disabilities from having a profile. You end up in this odd position where, by trying to make the space safer, you end up excluding someone from actually using the platform.

We can see the arguments on both sides, and they are very strong arguments, but we would like that discussion about how it actually works for users who are not going on there with the intention of causing harms but could fall foul of the regulations, keeping them from using it.

Q7 **Christina Rees:** Nancy, I was going to ask you a follow-up question, but I think you have answered it. I was going to ask you whether we can tackle the misuse of anonymity online while still acknowledging that it is important for users who genuinely need it. If so, how do we do that? It is the fear, isn't it, that you have stressed? How do we get around that?

***Nancy Kelley*:** Sadly for this Committee, I am not a technical ID verification specialist, but the $54,000 question is whether there is a way of having enough verification of identity that does not fall foul of the kinds of barriers that Matthew and I are pointing to in terms of participation. We know that the forms of verification that get pointed to a lot in this space, which tend to be things like Verify or bank account opening, do not meet that test. We know that they involve handing over quite a lot of personal information in quite a complicated process. Unhelpfully, we are presenting a challenge rather than a solution, which is never ideal, but a challenge it is, nonetheless.

One of the concerns that we have additionally is that, given the nature of these platforms globally, if approaches to verifying identity were then uniformly adopted on, say, a platform such as Facebook or Twitter, it would have an enormously harmful impact in other countries. We work a lot at the minute to support LGBTQ Afghanis to safety. Afghan people would absolutely not be able to meet each other. LGBTQ Afghan people would not be able to meet each other or communicate online at all if there were any fear, even of back-end verification of identity. Something that is risky in the UK becomes overwhelmingly risky if transported to less supportive environments.

Q8 **Christina Rees:** As a follow-up to Danny, what are your views on ID verification?

Danny Stone**:** On the principle of ID verification, I agree with what Nancy was saying. We have to be careful about how much is required to verify people, but, as I say, it should be proportionately to a platform to determine how much verification it needs, and that liability and that that risk then falls on the platform.

By the way, there is an interim solution that is being touted. I know Siobhan Baillie MP is running a campaign around ensuring that platforms allow users to only engage with verified accounts, for example, which would not force you to be verified but would, for example, enable individuals who only want to engage with people who they know can be traced to do so. That may be a way of bridging the gap. I think she is working with Clean up the Internet. There are other proposals out there that take that into account specifically.

My view is that we need to be careful, but, again, I am not the expert. Middleware will play a solution in this, so some kind of technology that sits in between the platform and the individual. Again, I would see that as the platform's responsibility to investigate.

Chair: I am just going to say that time is ticking. It is a really rich session, and it is always frustrating that we do not have all the time in the world, but we just need to bear that in mind. If somebody has made a point, obviously add to it, but let us get as much out of this session as we can.

Q9 **Martyn Day:** That is an ironic opening because I was going to comment that this issue has been debated quite extensively by a whole range of other committees, and a number of them have commented on the gap between the community standards that the various social media companies have and the actual reality of what they allow on their sites. What do you think explains that gap?

Danny Stone**:** I am sure it is a range of things. Sometimes it is a lack of numbers. I remember YouTube, in front of the Home Affairs Select Committee, not being able to say how many moderators it had. It just did not know. It could not work that out, because some are employed by YouTube and some are external companies. Sometimes it is a pure numbers thing.

Sometimes the technology is not there. We know that Google SafeSearch was designed, as Google says, to keep out child pornography—the explicit images. The categories that they use at the backend to filter their pictures include RACI and Spoof, for example, in terms of the way they categorise them. That is pretty rudimentary in terms of its understanding of the kind of images that may go through the system. There is just a lack of developed technology to deal with this stuff.

I have talked about voice technology and Clubhouse—this app that seems to have died a death somewhat, but it was a voice platform, a social media platform. How do we regulate that? Spotify is unable to pick up quite a lot of the hateful podcasts that appear on its site. The technology is not there. There is a range of different things, but certainly the understanding from moderators of their own policies is not there, and we are not quality-assuring the training for those moderators. Take your pick. It could be any of that.

***Nancy Kelley*:** I am mindful of not talking too much, but I will build on that. One of the things that was really striking in the Facebook papers dump, which is also consistent in many whistleblowing accounts of various social media platforms over the years, is that there is a fundamental imbalance in power and investment within the companies. If the technology does not exist, it probably does not exist because the ethical side of the business has been long-term underinvested in. That is such an important facet of this: that you have businesses whose entire model is based on engagement, and we know that this content drives high engagement.

There are huge financial and structural incentives that pull in the opposite direction, and if you do not invest sufficiently and equally in ethics and ethical technological development to counterbalance that, there is always going to be a pull that weights all of these platforms in a way that has these outcomes. That would be the only additional point I would make.

***Matthew Harrison*:** The one point I would make on top of that is probably about the lack of consequences for not taking action. That has led us to the path where we are having this draft Bill in front of us today, because self-regulation has been tried, and at the moment it is just not working, which has bent everyone's hands towards doing that. The underlying factor is that self-regulation and the lack of consequences.

Q10 **Martyn Day:** That leads me on to what was I about to come on to. Looking at the draft Online Safety Bill, the Government's approach is to make the social media companies liable for enforcing their own rules on acceptable content. Is it really just a question of enforcement or do those rules need strengthening as well?

***Danny Stone*:** I talked about senior manager liability. This was raised at PMQs the other day. We were told there would be tough sanctions. At the moment, it is two years. There is going to be a two-year gap. The Government are reserving the powers. There is going to be a two-year gap, and the senior managers could be imprisoned for up to two years, but probably more likely fined, for failing to produce information, essentially, like transparency reports. That is important and useful, but I would like to see that linked to the duty of care more generally.

In banking and the financial sector, it is seven years in prison. In my view, seven years is pretty tough; two years is less so. If you have been warned of a problem and you have failed repeatedly and deliberately to address it, there should be a tougher sanction. Fines, certainly for the larger companies, are just the cost of doing business. Everything must be applied proportionally, but we could do more there.

***Nancy Kelley*:** I would really emphasise the enforcement side of the picture. If we pick up the point that you were making about the existing community standards, if those standards that exist in the platform were effectively enforced, to a reasonable person's understanding of no hate speech, everybody's experience of the online space would be transformed immediately. Just enforcing the standards as they are would be an enormous transformative step forward for the experience of participating for all of us online.

***Matthew Harrison*:** I agree about enforcement. I made a point to the joint committee around ensuring Ofcom has the knowledge, staff and the ability to enforce these rules themselves. I can imagine there are a few people scratching their heads over how you go about regulating what are huge companies that operate across the globe. There is a lot of discussion to be had around how Ofcom can actually have the tools and resources to do the job that they are given.

Q11 **Martyn Day:** That is great. What mechanism should the Government use to force social media companies to either enforce their current rules or strengthen them?

***Nancy Kelley*:** I will briefly pick up some of the threads in what Danny and all of us have been speaking to. Imposing a positive duty and regulating against that positive duty is the key here. For me, one of the benefits of a positive duty is it enables learning over time, and it involves evolution over time. Our understanding of what is legal but harmful might change, which is a point that Matthew was making earlier, but also our understanding of what is possible will evolve, in terms of the points that Danny was making about technology. That allows the regulator to hold platforms to account for doing an effective job this year, next year and the year after.

Thinking about that positive duty as a way of creating a requirement to adapt, and to adapt to a good standard, feels really powerful.

***Danny Stone*:** The media literacy strategy that accompanies it needs to be well funded, so that we are not just talking about the platforms. We are talking about wider public and civil society, educating people about how to engage online and how to do so with consideration to—whether it be fake news or doing something in the heat of the moment—understanding the way the online world works and embedding that in our education system.

***Matthew Harrison*:** The other crucial part is actually bringing social media companies on board with the regulations. I was quite heartened to hear Facebook, which said that it was looking forward to the Bill and the regulations and the clarity it brings. There is a big job for the Government and parliamentarians to try to create that positive working relationship so that the regulations and enforcement do not feel like a negative but rather a positive relationship.

The media literacy strategy is a huge one, to tackle that core issue about stigma and negative attitudes. Hopefully, through a well-resourced and well-run media literacy campaign, in the long term we can start to remove the attitudes that develop over time and lead to that content and that radicalisation, as Nancy was talking about.

Q12 **Tonia Antoniazzi:** I just wanted to pick up on something you said, Danny. You spoke about fines and penalties, but what penalties should these companies face for breaches of a duty of care? Would it just be fines? Do you want to expand on that?

***Danny Stone*:** In the financial sector and in health and safety, senior managers are held responsible where there are significant breaches of a duty of care or responsibilities. We know that seven years in prison in the financial sector has worked. It has been an equaliser, and you have seen the market respond to it. Facebook will write off fines as the cost of doing business. Fines are important, but so is having a named manager who faces the prospect of going to prison if they are failing to address things that are brought to their attention repeatedly. We are not talking about a one-off, where there is a problem or there is a piece of content. We are talking about repeated failures in respect of that duty of care once they had been notified about it. People should face the prospect of going to prison.

This is why, for example, the financial regulation in this space is good and that Ofcom should be co-designating at least other regulators. The financial regulation and the expertise that that will bring across would be helpful. We ought to look to what we are doing in the country that works, and we know that those penalties work. There are consequences that we have brought in for failure in financial institutions. These companies, in some cases, have wider reach than individual financial institutions and wider impact. Why are we not thinking of it in those terms? That is what we should do.

***Nancy Kelley*:** We do not have a specific perspective on sentencing, but it strikes me that there would be a lot of work to do to understand what the nature of the persistent repeat failure would be that would attract that kind of sentencing. We are talking about a very wide range of behaviours when we think about the behaviours you are seeking to regulate, some of which probably should not attract that kind of a penalty, and some of which perhaps should. You would want to probably be quite a lot more specific for a seven-year jail sentence.

Q13 **Tonia Antoniazzi:** That leads me quite nicely on to something, Nancy. Is there abusive content you are concerned may not be covered under the draft Bill's definitions of illegal or harmful content?

Nancy Kelley**:** We are broadly happy with the way that the draft Bill defines legal but harmful content. We would like to see really close inter-relationships made between the legislation here and hate crime and hate speech legislation in the UK, but also things like the interaction with the proposed ban on conversion therapy, where promotion of conversion practices is going to be reserved for the Online Harms Bill. We need to link all of those pieces of legislation across, one to the other, so they form a seamless package together that protects our communities. In broad terms, we think that linking across those pieces of legislation effectively and then into Equality Act protected characteristics, in terms of priority content, is a good approach.

Q14 **Tonia Antoniazzi:** Does the link between online abuse and protected characteristics need to be specifically reflected in the Government's proposed regulatory model?

Nancy Kelley**:** We would say yes for a range of reasons, including that we know that there is quite a direct relationship between online and offline harm, for some of the reasons that I pointed to earlier, such as outing. Outing lesbians itself leads in many cases to serious consequences, homelessness, et cetera. We also know that there is a link between online threats and offline physical harm, et cetera. That is both in terms of one-to-one harassment, such as a cyber-stalker who then becomes a stalker in real life, but also the kind of volume behaviours we are pointing to. A climate in which many people are homophobic, biphobic or transphobic online enables and emboldens people who may take discriminatory actions in real life. We would like to see those kinds of protected characteristics reflected in terms of priority content.

Matthew Harrison**:** I fully agree with both those points. We would very much like to see the protected characteristics in the Equality Act referred to or almost explicitly in the Bill.

The point I would add on top of that is to help with a sense of direction around some of these ambiguous terms that I referred to, and to give a sense of direction for all of these consultations that are listed within the Bill. At the moment, it is all over the place, and you get these legalistic terms of, "Relevant persons must be consulted". Once you start adding in the protected characteristics you give a sense of direction to groups that tend to be targeted more online.

Tying in with the hate crime laws and the offensive communications reforms is really important, and it will help to bridge that gap between where the legal but harmful content ends and where it starts to move into an offence, because at the moment it is quite a network and quite a jumble to try to get through. That is part of the reason why you see quite low prosecution rates or referral rates to CPS in terms of hate crime.

Danny Stone: On that specific, I agree that the Law Commission's hate crime review is really important here, and it would equalise some of the protections in relation to aggravated offences, which at the moment are only related to race and religion. Similarly, the communications offences pick up some really important things, and the Government have indicated these will be in the Bill. For example, think of someone committing an offence who is outside of the UK but habitually in the UK, such as in the Wiley case, with the grime artist who was overseas when he posted his rant, but, as I understand it, is habitually in the UK. That would change the way in which the offence was recognised and addressed.

Similarly, the Law Commission looks at newspaper comments boards, which the Online Safety Bill provides a specific exemption for. It might be that we could see some joining up if these proposed offences are now brought in through the Bill.

Q15 **Tonia Antoniazzi:** I will move on, but I am probably taking in a lot of what you said there, Danny, in the following question. As you have said, the Law Commission has recently suggested changes to the law on online communications to help ensure that harmful online content does not escape criminal sanction. What are the key changes that you would like to see to the law in this area? Are they covered by the Law Commission's recommendations?

Danny Stone: As I say, aggravated versions of communications offences with stricter penalties, stirring up offences extended for legal clarity in relation to online behaviours, a liability for actual knowledge of dissemination of unlawful materials—there is a lot of good stuff. I would want to see some of the detail about intended audiences. If you post something on Gab and you know that you are posting to a mainly male audience, and it is misogynist, antisemitic content, will that be caught or not? The audience that it may reach is going to be different from the audience that you have posted it to. How will the law apply in terms of the audience that you are seeking to reach, and will that be a consideration? Some of the language will need probing, but, generally speaking, these are good recommendations.

Nancy Kelley: I completely agree with everything Danny has just said. The thing that I would caution against, which is why I was wrinkling my forehead a bit, is that we know already that fewer than half of hate crimes against LGBTQ people that are committed online—I mean very serious forms for abuse—are reported. It is really important for us to have as much, if not more, focus on online safety that falls below the threshold of criminality. We know that most people will not report even very serious harmful content online. Thinking about safety by design, algorithmic approaches to safety and these positive duties is certainly as important, if not more important, than making sure we have the appropriate criminal sanctions.

For our community, we know the majority of people will not feel comfortable coming forward and reporting even very severe forms of hate speech against them. For me, there is always this point about balancing creating overall a safer environment, and proactive things that we can do through regulation and legislation that create that, against sanctions for the minority of cases that will get brought for criminal content.

Q16 **Tonia Antoniazzi:** How do you know how many people are not coming forward to the police? This is a real issue that we have, about how we collect that data but also how that data is then communicated to the relevant authorities and how it is addressed.

***Nancy Kelley*:** The best source we have in the UK is Galop, the specialist LGBT abuse charity. Galop did a great survey on online hate in our community. Around 40-something percent of LGBTQ+ people report online hate speech, and the rest of us do not. I say "us" mindfully; I have been the target of hate speech online that I also have not reported. I suspect the figures will be even higher for the communities that Matthew represents in terms of people's propensity to report and come forward.

There are things that we can do about making LGBTQ+ people, or indeed disabled people and other marginalised groups, feel more confident reporting to the police or reporting to regulatory bodies, but we also have to focus on proactively making the space safe for the majority or for the half that we know do not come forward.

Q17 **Tonia Antoniazzi:** That really concerns me because, obviously, when you are working with your LGBTQ+ community, you need to be looking at not just self-selected surveys but how would you reach more people. For example, I think your survey might have been done over a short period of time and only reached so many people. How can we ensure that the data that you are getting is more robust?

***Nancy Kelley*:** It is not ours. I wish it was ours. It is a great report by Galop. It has more than 1,000 people in the sample. It is a pretty good sample for an LGBTQ+ survey. The point you are making about a lack of data is really important. As someone who used to work in social statistics, thinking about what national statistics we could use to gather good data is important. Is it the British Crime Survey? Is it surveys like Health Survey for England, which have a lot of mental health measures in them? The Government investing in some good, basic data in this space, about experiences of online abuse, would be really valuable.

Q18 **Tonia Antoniazzi:** I saw that you had worked in research and data—that it was your expertise—and I think that getting more robust data for the community that you represent is really key to moving forward.

***Matthew Harrison*:** Just on the data point, we think levels are very high, but the data is just very poor. Even data around hate crime is very difficult to get, and it is not disaggregated under disability. It is really difficult to understand what the picture is. Part of that is that the official statistics are not quite there yet, but on the other side the perennial issue we have is trying to reach out to the community. As I said at the start, a lot of them are quite socially isolated or secluded, so it is quite difficult to understand or reach that person who might have experienced online harms but has not reached out or has not reported it. All they might have done is given up on social media or deleted their account.

That is something we are looking at now. Hopefully, we will have some data going forward, or at least do our best to try to get a picture of what is going on.

Q19 **Christina Rees:** Two things really concern me. First, Dan, you said a named manager should be prosecuted.

***Danny Stone*:** Yes, they could be liable.

Christina Rees: What worries me about that is it is always going to be someone lower down the line who is sacrificed. I am really worried about that. Maybe it should be the CEO who should get it. That is just my own personal opinion.

The second thing that really worries me is this. If someone reports a crime—a hate crime or whatever online crime—and nothing happens and then it escalates, are they going to be willing to report again? I am not sure. I have two major concerns there that I just wanted to vocalise and share with you. I wonder if you have any thoughts on that.

***Danny Stone*:** Senior manager liability is established in the UK anyway, so we have that. You are right: there are always concerns about people being scapegoated. I understand that concern, but it is an established principle.

***Nancy Kelley*:** On reporting, first, you are right that people's experiences of reporting, whether it is hate crime or whether it is abuse, into a platform really affects whether or not they then report again. You are pointing to something that is really important. For me and LGBTQ+ people, it really illustrates the need for making sure that people are well trained—whether it is police in the case of criminal activity, or online safety teams and standards teams within platforms—which is the point that Danny was making, to support people who may feel less safe coming forward.

There is a very specific piece around the interaction with reporting and platforms—reporting to Facebook, reporting to Twitter, et cetera. For LGBTQ+ people, a lot of these platforms have quite a bad track record of removing LGBTQ+ content that is not harmful. There can be quite poor trust between LGBTQ+ people and some of these platforms that have a track record of treating our community differently and of removing content that is not problematic just because it features LGBTQ+ people or talks about LGBTQ+ lives.

***Matthew Harrison*:** There is a lot to be said around information and the accessibility of information. A lot of trust has been broken, around people not understanding what the terms of service are, what the rules are or even what the complaints and reporting processes are, which leaves a lot of people with learning disabilities with a sense of broken trust with the platform, in terms of why things are being done in what seems to be a very inconsistent manner. The Online Safety Bill has that provision around accessible information, and that will actually help to tackle some of that broken trust that have happened over time and give people the reassurance that these are the rules, there is an enforcement mechanism and this is the complaints process you can follow.

Q20 **Matt Vickers:** This Committee's 2019 report on the online experiences of disabled people found that hate speech and criminal abuse were under-prosecuted. Has the situation improved since then?

***Matthew Harrison*:** As I said, some of the stats I gave at the start show that the picture has not changed for disabled people and people with learning disabilities. That is going to continue until we see some of these more systematic and structural changes around the law and the bringing in of these industry standard regulations for social media.

There is also some good work that is going on at the moment. Dimensions is doing a wonderful campaign that is helping to train police around supporting people with learning disabilities, who sadly are often seen as potentially unreliable witnesses by the police or the CPS, and that does not help with prosecuting criminal cases. As I say, we need to do some more training and get better understanding about how people with learning disabilities can access criminal justice. There are also more systematic changes that could help bring those cases to trial.

Q21 **Matt Vickers:** Across the piece, in your experience, do the police and prosecutors have the right information and resources to be able to effectively investigate and prosecute online abuse where needed?

***Danny Stone*:** The police are under-resourced. It is always difficult, and that is why some of the Law Commission's hate crime law review is important, because it will give a bit more clarity on where and when they can take action. Similarly, on the communications offences, generally, there is not as good a prosecution of antisemitic hate crime as we would like to see. The numbers are relatively low. We put this in our submission to the Law Commission.

I would also like to see the use of other facilities: for example, community impact statements during prosecutions and the use of restorative justice, which we think might play a part. There is more that can be done to take some of the pressure off the police, but at the moment they are under-resourced and do not necessarily always have the right skillset in terms of the training in relation to online harms. That goes for the judiciary as well, in terms of applying particular banning orders or whatever else. There is more to be done there too.

***Nancy Kelley*:** I would echo everything Danny has just said, but to pick up the previous question that you posed to Matthew, over recent years we have seen quite a significant rise in reported hate crime in our community. This is primarily not online, but including online hate crimes. We do think that is a combination of two things. One is good news: more people are coming forward and reporting, and feeling confident reporting to the police, which is a really important first step.

The other thing, which is really concerning me, is that we think there is a real rise in hate crime. We know from the research that exists internationally that online hate speech against our community is rising. It is proliferating, particularly anti-trans speech. There is a race to catch up online with a very rapidly evolving picture and a picture that then targets across groups. Danny talked earlier about intersectionality, and one thing just to make the Committee aware of is that very prolific online abuse is often not against one community; people that become prolific abusers of one community very often are prolific abusers of multiple communities. I would really encourage the Committee to reflect on that fact as well when thinking about how we create a safer online space.

***Matthew Harrison*:** I have touched on the police in my previous answer, but they definitely are resource-constrained, as we can expect in every area. That is the main issue. As I said, better training, better awareness and those structural issues will also help because of all the guidance that will come with those if they are implemented. Hopefully that will help the police, the CPS and the judiciary actually bring more cases to justice.

Q22 **Matt Vickers:** Beyond the legal and technical responses we have talked about, what are the steps you would like to see the Government taking to promote behaviour change online and help prevent abuse? Is there a role for the media literacy strategy?

***Danny Stone*:** 100%. Yes, absolutely. There is a phrase, "cyber-phronesis", the building of moral knowledge over time. It is that kind of approach, one that we start at a basic level, at primary school, and we build this all the way through, as we do with safety awareness in IT. It is just that moral knowledge and understanding that what you see online does not necessarily represent the truth.

One of my children told me, "There is a problem with Facebook. It is going to be closed down because it is illegal, because a lady said so in Parliament". That is because of what they had heard from a friend who had read something online and had not understood it. It is about how we have those conversations about that online material, including fake news, as I was saying, and misinformation. That is really important.

***Nancy Kelley*:** I agree. I would really amplify the need to teach everybody, not just children. We think about it as if it is schoolchildren who are the problem. It is mostly not schoolchildren who are committing online hate. I have to say that.

With the general public engaging around critical appraisal of evidence, there is a cohort of people who are being taken in and radicalised by misinformation, and that is something that we can do something about. It is less about debunking; debunking and fact-checking does not work. It is more about building empathy with people and their perspective and helping them bring their own critical faculties to bear on the information they are being presented with. There is a cohort of people where it really is about de-radicalisation, because it is not really about facts and people having believed something they read on the internet. It is about a whole complicated set of factors.

I would really emphasise that the young ones are pretty good in this space. It is the rest of us who probably need the educative work.

***Matthew Harrison*:** It is very important for both children and adults. There is a role for the national disability strategy to play. There is an awareness campaign as part of this strategy, and that should be really taken up by the Government and hopefully other parliamentarians as well, and the whole civil space, to try to change that narrative and tackle that stigma, because it is not just aimed at children; it is aimed at wider society.

The other part as well is around media literacy work for people with learning disabilities and parents, around empowering them and educating them about staying safe online, and also for parents about how to engage with their child with a learning disability, to stay safe online but in a way that still promotes independence and learning. Unfortunately, sometimes parents are a bit cautious. It actually leads to the person not perhaps using social media or using it in an incredibly sanitised way, so it does not have its intended purpose.

Chair: Thank you very much indeed, panel. We really appreciate you coming in today and contributing with your evidence.

Examination of witnesses

Witnesses: Ruth Smeeth, Chara Bakalis and Dr Joe Mulhall.

Q23 **Chair:** Welcome. Can I ask you to start by briefly introducing yourselves?

Ruth Smeeth: Thank you, Chair. I am Ruth Smeeth. I am the chief executive of Index on Censorship. For those parliamentarians sitting around the table, I used to be on that side of the table. It is very strange to be sitting on this side for the purposes of giving evidence.

Chair: Yes, I wondered whether I should declare an interest, being a great admirer of Ruth.

Dr Mulhall: My name is Joe Mulhall. I am head of research at HOPE not hate. We are an organisation that monitors and disrupts far-right extremism, both online and offline.

Chara Bakalis: My name is Chara Bakalis. I am a principal lecturer at Oxford Brookes University, and I have research expertise in hate speech and hate crime.

Q24 **Chair:** I will kick us off. I am wondering who to direct this to. Just indicate if you want to come in first, because we are not starting off with gentle questions; we will get straight into it. What differences, in your expertise, already exist between the legal restrictions or other limits placed on abusive speech online rather than offline?

Ruth Smeeth: I should also declare an interest, because I am on the board of HOPE not hate and the Antisemitism Policy Trust. I have a slightly different approach this time.

Index on Censorship is celebrating its 50th birthday this year. We were established to be a platform for dissidents behind the Iron Curtain to publish their work when they would have been killed for it if they had published it in their own countries. We start from a position of free expression as a liberal democratic value. That is why this is so important, which is why I am here today.

One of the things that is really clear, having listened to your conversation with the previous panel, is that this is about how we do cultural change. One of the things that this building has a bad history of is trying to regulate cultural change. We have to start from the position of, "What do we really want to achieve?" That is only going to be made harder if the rules that we have online are different to the rules that we have offline. What we are really talking about are both the users and the targets of abuse. There is a difference here that we cannot lose.

There are a couple of issues that highlight this for me. Something is already twice as likely to be deleted if it is in Urdu or Arabic than if it is in English. With the current algorithms and how they work, we are already removing some people's speech. There is an issue about transparency and how we are going to do it.

We also need a really clear understanding of what we are trying to achieve and what the impact is. When I was sitting on that side of the table, I had no idea how much we exported policy. When the draft legislation was published earlier this year, it used the phrase "legal but harmful". I am very nervous about the application of this. The definition is very poor and will end up in court. That definition was uniquely British, and now it is not. It has been added at amendment stage to the Digital Safety Act that is going through the European Union. There are consequences to that. It has also been cited by the Pakistani Government as justification for how they are going to do their online regulation, as well as by Bolsonaro and Modi.

There are unintended consequences to what we are trying to do in terms of how we will manage speech online. Our language and our legislation will be adopted by others. We will have a version of "legal but harmful";

we will have a version of saying that potentially staff who work for tech platforms should be arrested. When you consider that through a British liberal prism, that is one thing. When you think about it from the perspective of a repressive regime, it is very different. We need to be very careful about what we are exporting at the same time, which means there is an onus on you to make sure the language is so incredibly precise, so that we are actually achieving what we need to achieve.

Q25 **Chair:** I will come to you for your views on that, but the other aspect that I would put—I will give Ruth a right of reply on this as well—is that clearly one of the different aspects to online and offline is the speed and rapidity of the amplification of something. I would challenge slightly the notion that everything should be the same online and offline. Should we be applying a slightly different standard? I would be interested in your views on that.

Chara Bakalis: I agree with you. We need to think about the online world in a completely different way to the way we think about the offline world. That mantra about how what is a crime offline should be a crime online, and that the two should mirror each other, was a really useful phrase to use when we first started thinking about how to regulate the online world, because people were not taking the online world seriously and they were not thinking about how speech online could harm people just as much as offline speech. That was a really useful mantra.

We have now decided that we do need to do something about it, and the question is, "What do we do?" We have to look at this a bit more carefully. We should not consider the two the same. For a start, it does not really make sense to say that what is a crime online should be a crime offline. Even in the offline world, we draw distinctions. There are things that you can say in some places but you cannot say in others; we take context into account. Which bit of the offline world are you talking about when you are saying that the two need to mirror each other? Even if we think about something like public order offences, they draw a distinction between the public and what is happening in somebody's home. We draw that distinction in the offline world. It does not make sense to me to say that the two should mirror each other.

You brought up the point about the speed at which communications can now travel across the world. These things are permanent. If somebody says something about you, it is there forever. Unless somebody is able to remove it, it is there. These things are searchable. Anybody who searches under your name will find these things about you. Those things do not exist in the offline world in anywhere near the same way. Again, we cannot treat the two the same. We have to take very seriously that this is a new world, and we have to have quite targeted offences for the online world that take into account the context and the nature of online hate speech.

Dr Mulhall: I completely agree. It is difficult disagreeing with Ruth, who is on my board.

Ruth Smeeth: I will forgive you.

Dr Mulhall: At HOPE not hate, we monitor online and offline hate groups, organised hate groups and individuals. There are enormous differences. At its core the hatred is the same, but the internet has revolutionised the way in which it is distributed and the way that it works. We have to take that into account.

There are a number of ways in which the online space is different. One has been mentioned. Harmful content can be amplified in an online space in a way that is often not possible in an offline space. That can be amplified by the platform itself or it can be done by thousands of other people simultaneously online. The number of people who you can reach instantaneously and simultaneously is remarkably different, and there are hugely lower levels of cost for mobilisation. Think of all the things that you would need to speak to 10,000 people on the streets versus the ease of having the ability to speak to 10,000 people online.

The ease with which one can reach victims online is also often far greater. You can sit in a bedroom in Australia and send antisemitic abuse to somebody in London or transphobic abuse to someone sat in Canada. The ease with which you can come across individuals who you want to target is much greater than it is offline.

The speed at which that harm spreads is also fundamentally important. If we look at the events at the Capitol back in January, the spread of misinformation, anti-vaccine information and Covid conspiracy theories or QAnon, as Danny mentioned earlier, you can see the speed with which they have moved across the Atlantic in the last two and a half years, moving from tiny or niche corners of the internet to large global movements. Again, these can happen offline, but the ease with which they happen online is remarkable.

The social cost is also much lower. Joining an organisation or a hate group, et cetera, and getting involved in street politics or standing on a street corner selling a far-right newspaper comes with a social cost that does not come from doing a lot of this activism online.

The final thing that I would say is that there is the ability for this speech to have an amplified sense of harm online, in that you can create such toxic spaces that you suppress the freedom of speech and rights of whole communities online in a way that is much harder to do offline.

Chair: Tonia, you wanted to come back on this. I also wanted to give Ruth a right of reply to the point I made.

Q26 **Tonia Antoniazzi:** I am not picking on you at all, Ruth. It was very interesting to hear what you said about the unintended consequences of what we say being adopted by others. I am thinking not necessarily about what we are going to export but about what we are importing, particularly around artificial intelligence. When I think about Silicon

Valley, it is predominantly male and white. We have been at risk, and we have seen this on the internet. Do you consider what we have imported and what has influenced us rather than what we are likely to export?

Ruth Smeeth: In the proposed legislation, one of the biggest concerns is the lack of scrutiny. One of my concerns is that we are outsourcing regulation and what is appropriate language from this building to people sitting in Silicon Valley without any scrutiny. I say this with the hugest of respect, but there are very few people who sit in that Chamber who have any understanding of how an algorithm works and how to read code. I definitely do not.

There is a genuine issue in terms of our expertise to do this. It is why I referenced the fact that something is twice as likely to be deleted if it is in Urdu or Arabic than if it is in English. An algorithm is still done by a human being; it is still designed by a human being. They will have inbuilt bias. To take one example, I do some work with the Syrian war archive. For the first time in history, social media data has been used as evidence for war crimes tribunals in Europe. It is a really important thing. They download it as they find it. When they have gone back, over a third of what they have downloaded has been deleted. It has been deleted because of the nature of the content. Some of it is illegal because it is evidence of crime, which means it is permanently deleted. That brings us to another issue that I want to talk about at a later stage, which is a digital evidence locker.

There is also an issue with people's inbuilt bias. There is one really interesting example, in my opinion, of an anti-Government demonstration in Lebanon. They were chanting anti-Government messaging on the demonstration, as you would expect, anti-Hezbollah messaging, but the algorithm picked up the word "Hezbollah" so the videos were deleted. From a British perspective, we would welcome anti-Hezbollah messaging being retained online. The fact it is being deleted is not helpful for us either. It is the unintended consequences; it is the lack of transparency; it is the lack of our knowledge and understanding of the algorithms. It is about access to these things.

Honestly, it should be the people in this building who decide what language is or is not relevant, what is and is not deleted and what we want people to see. I would very much welcome a national conversation about our online world and about how our online world operates. I completely agree, by the way, about context and nuance. What we expect to see on Facebook is different to what we expect to see on Mumsnet or in Amazon reviews, for example. That level of nuance is not covered by this legislation. How we do nuance and context is really difficult, but it needs to be explored further.

Chair: There we go. I am sure we are going to try to ask you what the answer is to that.

Q27 **Matt Vickers:** How can we best balance the need to make our online spaces safe with the need to not over-regulate on freedom of speech?

Ruth Smeeth: Freedom of speech is a fundamental freedom. You all know of my own personal experiences as a target for online abuse. I of all people will have a level of cynicism about and interest in how we apply. We need to protect free speech and protect language, especially because words evolve and language evolves. We need to make sure that we are regulating in such a way that we are protecting the opportunity for you and me to debate from a different political perspective and to make sure that constituents can engage in the democratic process without undermining other communities and being targets.

There are a couple of elements to this. You touched on one of them with your final question about cultural change and what we needed to do. We absolutely need to give resilience to young people. One of the nicest things is the Scouts badge. Have you seen this? Nominet and Scouts have developed an online citizenship badge that you can earn.

Honestly, we have just come through Covid. Everyone is upskilling and reskilling. There should be a digital citizenship element to every upskilling course that we are asking people to do. FE is key to this. We need to get the civil service involved, as we did when the original training was done. We have to get the WI involved. We need to give people the tools to know how to use social media in a constructive way. My concern about the legislation is that we talk a great deal about the platforms and not about the perpetrators. You have to balance the two out. We also have to be really clear about language and what is and is not acceptable language.

The other part of this, which for me is the protection, is the digital evidence locker. I apologise, Chair, but I am just going to engage on this slightly. I say this as someone who has been the target of abuse. If we are going to use AI to automatically delete content, I would not know when I am at my most vulnerable. The most recent person to be arrested for harassing me was in April this year. My abuse has not stopped since I left this building. They live three miles from my house. I would have been very vulnerable and they would not have been arrested. What we need is a digital evidence locker—we need a legal framework for it, because one does not exist—so that the platforms can store illegal material. Currently, they cannot legally store illegal material. They need this digital evidence locker so that the security services can look at it, so that journalists can see how much is being deleted and so civic society can see whether this legislation is being applied appropriately.

Most importantly, from your perspective, in terms of the question, we will be able to see how language is evolving, what language is being deleted and why it is being deleted. You can do an academic analysis of that. There has been a lot of discussion about Prevent recently. Dog-whistle politics is really unfortunate. Language evolves and different words will become trigger words. We will miss them if words are being deleted or if certain content is being deleted. We need to know what is happening, and in order to do that we need the evidence base. That will be a digital evidence locker, which also means the security services could still make prosecutions and we could still prosecute the perpetrators of these crimes.

Q28 **Chair:** I can sense agreement breaking out across the panel. Did you want to come in there, Joe?

Dr Mulhall: Yes. I agree with some of it.

Chair: I did not mean complete agreement. I just meant that Chara was nodding at the idea of the evidence locker.

Dr Mulhall: Yes, the free speech point is absolutely central. Understandably, everyone is incredibly nervous about getting this wrong and unduly suppressing freedom of speech. To speak to what Danny was saying earlier, placing the emphasis on design problems and platforms rather than individual content and users is going to be a better and safer way.

When it comes to the free speech debate and the "legal but harmful" element of this, it is worth realising that the content we are talking about is often very extreme. Holocaust denial would fit within this framework, as would misogynistic abuse and Covid misinformation, et cetera. When we have this debate about free speech, the big problem is that we take such a narrow discussion around it, which is, "What content will be removed?" That takes such a narrow view of what these online spaces already look like and the amount of suppression of free speech that is currently happening on them. It is not just about what will be removed; it is also about what is already missing.

If we address "legal but harmful" properly, we can vastly expand the amount of free speech on online platforms. We have a wide range of people whose freedom of speech is already suppressed: women, LGBT people, people of colour, you name it. I could go on. We have such toxic online spaces that there are whole areas of the internet where people do not feel comfortable raising their voice and cannot be heard or would be shouted down if they did. As a result, by protecting that sort of speech in some way, we are allowing the amplification of it and we are also, in the long term, stopping the ability for whole communities to have a voice.

Removing this sort of hateful content is not going to suppress free speech; it is going to massively and dramatically increase the amount of people whose voices are heard. If we continue with this very narrow debate, which places free speech against regulation, the danger is that we will end up continuing to have these toxic online spaces. Especially if we see social media as a central space for public debate—nowadays it is so ubiquitous that it is—we have to look at the content that is missing as well as the content that is going to be removed if this legislation goes forward.

Chara Bakalis: Joe and Ruth have both come up with really good ideas. We are going to have to accept that there is no easy solution here. We are not going to come up with a law that is going to make everything okay, that is going to protect victims and protect free speech. That is not going to happen. We need a raft of measures in place.

There is room for a criminal law, but there is also room for regulation. Broadly speaking, I am in favour of the Online Safety Bill. However, I do share Ruth's concerns about the detail of how that is going to operate. I am not going to talk about education and so on, because you have already talked about it. This is going to require several things to be in place. There is no magic key here that will make everything okay.

Q29 **Matt Vickers:** There is the big question about ID, verification and how that balances with holding people to account. What is your perspective on that?

Ruth Smeeth: Surprisingly, given my previous employment, I am opposed to online anonymity for several reasons. First of all, people use anonymous accounts for different reasons. As Danny outlined, there is probably a compromise to be found here. My dissidents use social media platforms to contact me, and they do it anonymously. It is the only safe way that they can contact me, given the countries that they live in. We have helped people in Myanmar, Belarus and Afghanistan. In Hong Kong at the moment there are limited ways of communicating, and anonymous accounts are key. This morning I was talking to someone in Hong Kong on Twitter via an anonymous account. Again, we have to be careful about the unintended consequences.

As was touched on by the previous panel, if you are experiencing domestic violence, using an anonymous account to reach out for services might be the only safe way for you to do so. If you are finding your sexuality, using an anonymous account might be the only way of finding yourself, especially if you live in an area that does not have a significant LGBTQ community. We have to be really careful about what we are doing and why.

For the majority of my abuse—and I got a lot—people were pretty proud to be using their own names, so I do not think my abuse would have stopped. The reason why we were able to prosecute some is because we knew who they were. I do not think that that helps, but what does help is prosecution. You apply cultural change by making sure that people are prosecuted.

If I can just beg your indulgence briefly, I had two significant death threats arrive during the 2019 general election. One was hand-delivered to my office. We got CCTV and fingerprints. They were not very bright, so we got a picture of them. They were arrested and through the criminal justice system within weeks. I got loads of abuse, but the second significant one is due to go to court this month. That is two years after. That was all on social media. We knew exactly who it was. They were a constituent, and yet it has taken two years because of the resourcing associated with this.

Anonymity sounds like it is a really easy way to deal with the abuse, but unless we are using the criminal justice system to prosecute and unless we are making examples of what is or is not acceptable, all of this just becomes irrelevant anyway.

Dr Mulhall: This one is easy, in that I agree with Ruth. Anonymity is fundamental. I get extremely nervous about any attempt to tamper with it or reduce it in any way, for a number of reasons.

I will say from the outset that the most sensible ideas so far have come from Danny Stone and the CST in terms of a way that might be able to get through this. There are lots of reasons why it is so important. We mentioned LGBT people and victims of domestic abuse, but this is also something that we use a huge amount at HOPE not hate in terms of our research into far-right terror organisations, et cetera, to try to keep ourselves safe and the information that we find safe.

There are two things here. First, would removing anonymity actually work? In one sense, it would possibly reduce the issue here, but there is a whole host of other ways. A huge amount of the most toxic abuse that we come across is by named accounts. It is worth differentiating in terms of what is an anonymous account. In some senses, if someone creates an account and instantaneously sends a footballer or an MP abuse and then disappears straightaway, it is almost impossible to find that person online, if they are clever.

There are ways that you can reduce the impact of that. For example, you can encourage what you call stable accounts. This means you have to have an account for a certain period of time before you can write to someone with a blue tick or before you can write to an MP, et cetera. As a result, an individual has to be online for a prolonged period of time before they accrue benefits in the social media space. In that way, you can significantly reduce the instantaneous creation of accounts and then disappearing.

This is important because stable accounts are much easier to find or track down even when they are anonymous. At HOPE not hate, our job is finding people engaging in hate speech who are anonymous and exposing them. There are cases like the terrorist Luke Hunter. It took us many weeks, but we did manage to find out, through various anonymous accounts, who the person was.

I agree with Ruth that one of the things here is not necessarily just that it is anonymity. There are not the resources to find people. It takes us a long period of time to find these people, and one of the issues is of course law enforcement and the resources required to do this. The Online Hate Crime Hub does remarkable work, but it is about three people. A huge amount of the problem is that, when you report anonymous abuse online, in some cases there are ways to find people, but it may take time and resources. It takes time and resources that the current online policing hub does not have. We notice a difference when we report terror content or we find terrorist content. Invariably, those people are found and prosecuted, because they are prioritised, resources are put towards them and they are tracked down and prosecuted.

If there were resources to look into these anonymous accounts properly, there would be much less of a bar in terms of reaching that level of prosecution. There are other things, especially around encouraging stable accounts and increasing friction in the system that make it harder for individuals to create completely anonymous accounts and disappear. Of course, we also need to stop the social media companies from allowing the promotion of harmful and divisive content through algorithmic amplification and those sorts of things. There are other steps that we can take without getting near to touching anonymity, which is too important to go near.

Chara Bakalis: I agree. The only thing I would add is that focusing so much on anonymity and trying to make people say who they are online may mean that we might be misconstruing or misunderstanding what the real problem is here. It is not necessarily the individual perpetrator who we want to hold to account. Of course, there will be some instances when we do. A lot of the problem with the hate occurring online is not that there is an individual person who has said one thing that has been really hurtful; it is the drip, drip, drip effect of all these different comments added together that creates a negative atmosphere.

That is why anonymity or not anonymity is not really the important thing here. We need to focus on how we force platforms to remove those comments that we think are adding to this negative atmosphere. That is the only thing I would add.

Q30 **Matt Vickers:** You articulate very well the need for legitimate anonymity. There are two things here: first, holding people to account, and secondly preventing someone banging another account up when they have been banned from a platform. How do we control that?

Ruth Smeeth: There are some really interesting proposals out there. The amount of information that the social media companies have on all of us is quite significant. They could put holds on or suspend people full stop. They could change what data you have to give them. I potentially like the idea of one-stage verification and what that could look like; for example, a mobile phone number. If it is one of my dissidents, they could then delete their mobile phone number if they needed to. There are ways and means of doing it.

I am also very nervous about the people who I work with, and the people who we all work with, in terms of safeguarding. For them, a data breach would kill them. I am not over-egging that. They would be very, very, very vulnerable. We have to be careful about how much data we are demanding that the companies have, because that could make others vulnerable. There are ways and means. It could be IP addresses. There are ways and means in the technology that you could apply to do it. As Joe just outlined, an account could also have to be live for a matter of weeks before a person could engage. Engaging in that way is quite an interesting way to set up a platform. You are protecting both ends. One of the other proposals is around whether you choose to see non-verified accounts or not.

When I arrived in 2015, I did my own social media and there were hardly any protections in place at that point. It was very noticeable that, by the time I left this place, the protections were huge. I now only know when I am in the middle of an online Twitter storm when I see that someone has defended me, because that has broken through into my comments. I go, "I wonder why they are being nice about me", and I really wish I had not gone to look. There is balance here about making sure people know what protections they can use now. It is slightly different for the 2019 intake, but, if you were in Parliament before then, everyone handed it over to their staff. They had no idea about the protections that now exist. We ran away from it, because it got really horrible. The world has changed, but politicians did not keep up with the changes that happened; our staff did.

Dr Mulhall: The only thing that I would add briefly on that is that of course we should give individuals more control over the social media that they see. We have to try to do it in a way to make sure we do not further marginalise voices that are already extraordinarily marginalised. When we talk about undocumented migrants, sex workers or young LGBT people, these are people who are often extremely marginalised in public discourse. If we create a system where, for example, MPs can only ever see completely verified accounts, they will never hear those voices. I do not have the exact solution for that. One thing to keep in mind is that if we go too far down that road, we could further marginalise those voices.

In terms of accounts that come back, there are a few things. We send lists to the tech companies endlessly, saying, "These people have been banned; we have found them still on the platform". We are a small NGO. They could be doing that themselves if they wanted to put the time and resources to look into accounts that were causing harm, but they do not. I would throw a lot of the onus back on platforms. They also have such vast amounts of data on people that they can target advertising to within an inch of our lives. They can work out a whole host of things. A huge amount of this is about the will of the tech platforms just not being there.

The real issue is not the accounts coming back. The real issue is whether or not the accounts are causing harm. If you reduce the way that those accounts can cause harm, it is less important whether or not the person has been banned and has come back, if they come back and all they are posting are videos about cats. If we reduce the harm, we reduce the impact of returning accounts.

Q31 **Tonia Antoniazzi:** Chara, what are your views on the Law Commission's proposed changes to the criminal law on online communications and the kind of harmful content that could face criminal sanctions? You have argued that changes to the law on online abuse are needed to help ensure groups that are frequently targeted online feel safe. Do you feel the commission's recommendations go far enough to help achieve this? I know you have done a lot of work on online safe spaces for women.

Chara Bakalis: They probably do not go far enough, overall. On the positive side, the new offence they want to create around threatening communications is a good offence. That will go some way towards mitigating some of the problems people are having at the moment in getting prosecutions and convictions.

To be honest, I do not like their new offence based on serious psychological harm. I have a problem with it on two levels. These may seem contradictory to begin with, but they are not really. The scope of it means that it will rarely be used. You are talking about having to show that somebody intended to cause serious psychological harm and persuading a jury that was likely to happen. This is a one-off communication. If it is a pattern of behaviour, we are talking about a harassment offence. This is a one-off offence. I am not sure how many offences would come within that. That is much narrower than the current Malicious Communications Act and Communications Act offences. It will probably give less protection to victims.

That may be a good thing from a freedom of expression point of view. I do not like the Malicious Communications Act and the Communications Act. There are serious concerns from a freedom of expression point of view. That is why I would advocate for a much more targeted approach here. I have argued that we should have tailored online hate speech offences where you are specifically dealing with hate speech. At the moment, it is anything indecent or grossly offensive. Under the new offence, it will be psychological harm. That is not the right approach. I am not even sure that psychological harm is the thing we are trying to guard against here.

Q32 **Tonia Antoniazzi:** Is it something that can be measured?

Chara Bakalis: I am actually writing a paper at the moment with somebody who is a cyberpsychologist. We are still in the beginning stages of it, but part of the problem is that you may or may not be able to measure it. Quite often it is a person's initial psychological state that can determine whether or not they reach and go over that threshold. Then it depends on a particular individual. The way the offence is defined means you do not need an actual victim; it is just that this is likely to happen.

I am not really sure that this is the harm that we are trying to guard against here. When we listen to victims groups, this is the harm that they tell us is happening. When you look at the evidence that the Law Commission used, the evidence they were using was really based on harassment offences where there is a pattern of behaviour and not a one-off comment. Part of the problem is that we have never done a proper comprehensive study of what the speech that people are being impacted by is. Is it hate crime? Is it hate speech? Is it nothing to do with hate? Is it personal abuse? We do not really understand what the problem is that we are trying to tackle.

Because we do not know that, we are not in a position to create properly targeted offences that would protect victims and, if they are targeted enough, satisfy freedom of expression concerns. The problem with the current offences and the new offences is that they are too vague and too broad. That immediately causes problems from a freedom of expression point of view. If you could be much more targeted, the balance between the two is much more easily satisfied.

Q33 **Tonia Antoniazzi:** When will you finish your piece of work?

Chara Bakalis: It will not be for a few months. I have also just started a piece of work with another group. We have managed to get some money from the Agency for Fundamental Rights—it is EU funding—to undertake some analysis. We are going to do a scraping of various comments from social media websites, not from the UK but from Europe, to do this kind of categorisation and try to work out what is going on. I will have to share that as well. That is still quite a long way off in the future.

Q34 **Tonia Antoniazzi:** If these proposed new offences were adopted, how would they affect social media platforms and their response to online abuse?

Chara Bakalis: If the Online Safety Bill says, "You have to make sure you get rid of illegal content", it will of course form part of their duty of care and their code of conduct that relates to illegal content. They will have to follow whatever the law says, whatever the new proposals are. Does that answer your question? I am not sure.

Q35 **Tonia Antoniazzi:** Yes, it does. I do not know whether anybody else has anything to add to what I was focusing on.

Ruth Smeeth: In terms of the Malicious Communications Act, all of this is irrelevant if we are not policing it. We have not put the resources into policing. When I got my first death threat in 2014, at that point the police did not have access to Facebook. It was banned. It was an HR issue because it was timewasting for them. They might waste their time looking at Facebook. We had to download and print off everything for my first set of abuse. Although they can now see it, they do not have the resources available to help them prosecute. Whether the legislation is amended or not, it is so incredibly important that the criminal justice system can do its work. To do that, they need resources. That is part of this conversation. This is the first time that this element of it has been discussed in all of this stuff.

Chair: The polluter pays.

Ruth Smeeth: Yes.

Dr Mulhall: Just very briefly, Tonia, I very much defer to Ruth's expertise. There are a few things to say in terms of the Law Commission's recommendations. There is a general point, which is that they certainly start to push the Bill towards focusing on content and users and away from systems. That is where we might see overreach.

There is also a general point here around the fact that so much of this is a global phenomenon. This is not just about what is happening on our streets, in our communities or even in the UK. The hate can come from anywhere in the world, which makes it very difficult when it comes to prosecution or taking a legal route around this. Again, that is why the emphasis needs to be on the platforms rather than just the content and the users necessarily.

Broadly speaking, there clearly has to be some sort of update. At HOPE not hate, when we look at far-right individuals who are prosecuted for things they are doing online, that is generally under terrorism legislation, public order offences or the Communications Act. They are often prosecuted under legislation that happened before I was born, let alone the creation of the internet. There are clearly some holes. At the very beginning, we talked about online versus offline. There have to be some updates.

The positive element of the recommendations is the shift from this broad notion of "grossly offensive" towards looking specifically at harm. How we define those things is going to be important. Moving towards more context-specific analysis of these things is going to be a really useful way forward.

Q36 **Tonia Antoniazzi:** Joe, I want to pick up on something you just said then. I asked a question to Danny Stone earlier about the penalties that a company should face for breaches of their duty of care. He went on to talk about how somebody should be in charge of this at the social media platforms. Would you agree with what he was saying there? If it is global, surely there should be somebody at Facebook in charge of X.

Dr Mulhall: Yes, absolutely. I agree with Danny. We need direct penalties to executives at these platforms. This is why the duty of care thing is useful in this argument. We have a duty of care to users in the United Kingdom. If the platforms are breaking, and consecutively breaking, that duty to people in Britain, there should be a legal consequence for the people at the platform. For example, if somebody can sit in Australia and send racial abuse or engage in harmful behaviour constantly that is affecting people in the United Kingdom, the platform should still be liable for that and should be facing consequences for their failure to protect people in Britain from that harmful behaviour.

Ruth Smeeth: I am really nervous, though, that we would prosecute not the people who are undertaking the abuse but the people who work for the platforms. The perpetrator will get away with whatever they want to: there is no criminal liability, they do not go to prison and they do not get fined. The platform is a neutral entity. Unless we can prove and demonstrate that it is their algorithms and their AI, or it is structurally set up to facilitate people threatening to kill me, I am genuinely nervous that we are focusing our efforts on the wrong element of this. We are ignoring the people who are actually breaking the law.

Q37 **Chair:** Is it not about challenging both, though? The platforms have a duty to take on the perpetrators and deal with them. If they fail to do so, it is the platform that ultimately has that responsibility.

Dr Mulhall: Nobody is arguing for either/or; the argument is very much for both. We should be tracking down individuals, users and content that break the law, but this legislation will go beyond illegal content. If it were to be effective, it would need to go beyond illegal content. It is also algorithms; it is also AI. Part of the reason this content causes so much harm is because it is amplified by the nature of these platforms through algorithmic recommendation, et cetera. I would sleep better at night if the far right still had to radicalise people on a one-to-one basis in the pub rather than people opening their phone and having the information handed to them and sent to them. These are the things where we go after the platforms.

If people are engaging in sending death threats to MPs, that is absolutely a legal issue and we should be going after them and those pieces of content as well. No one is arguing that this is either/or.

Ruth Smeeth: It is just that this legislation puts more onus on the platforms than it does on the perpetrators. The balance of that is skewed in this legislation.

Q38 **Tonia Antoniazzi:** The platforms are not neutral entities, are they?

Ruth Smeeth: Mark Zuckerberg does not care about me; he is not interested one way or the other about me. He did not establish his platform to give people a pathway to threaten me, you or anybody else. That may be incredibly naive, but I do not think that is why it was set up.

We have to step back. It is a very emotive area, especially because all of us, and especially the groups that you heard from earlier, have experienced horrendous things on social media. Some 10% of what I received came via telephones and letters. If we had been Members of Parliament 30 years ago, it would have been green-ink letters. We would never have threatened to ban green ink. We need to be really careful about how we do this and who we are blaming for it. As someone who has sat on your side, I do not want it taken away from the perpetrators and I do not want us to forget about the education and cultural element that goes alongside this.

Q39 **Martyn Day:** On the subject of content that is not illegal, looking at the Government's draft Online Harms Bill with the requirement on platforms to enforce their own rules, does that strike enough of a balance between tackling the abusive content and avoiding unnecessary state intervention?

Chara Bakalis: This is a really difficult one. When I first read that, I was horrified. I thought, "I cannot believe they are doing this. How can these platforms have control over harmful but legal content?" I have thought about it a little bit, and I guess there are two things that are making me change my mind.

One is that the platforms are already doing this. The platforms are already making a decision about what goes on or does not go on. If you look at community standards—I appreciate that they are not properly implemented—and you look at their description of hate speech, for example, it is far wider than what the law describes as hate speech. That illegal content is already being taken away. You then have to think, "Who do I trust more? Do I trust Facebook more to decide what I get to see? Do I trust the Government?" It is difficult, but I am veering towards an independent regulator, where you have lots of different people involved and so on. That is preferable to Facebook.

There is another thing that is also important. When we are thinking about this balance of freedom of expression and protection of victims, looking at this from a human rights perspective, the penalty imposed on somebody is absolutely crucial in determining whether or not you have achieved that balance. Having this category of harmful but legal content may well mean that we are keeping that balance much better. What is the alternative? The alternative is that we increase what we consider to be illegal content. That is the alternative. If we think there is stuff going out that we do not want to be out there but we are limited to what the law says, we will just change the law, make the law really broad and come out with broad offences that can cover all sorts of material.

At least this way it can be the Secretary of State that lays out what constitutes "harmful". If we can see the detail of exactly how those decisions are going to be made and how people can feed into that, it would make me less concerned.

Dr Mulhall: The first thing to say is that on the duty of care thing around freedom of speech, the best thing to stop overreach will be to concentrate on platforms and the duty of care rather than content. There is a paradox in arguing it the other way around.

I absolutely agree around the "legal but harmful" thing. There are a few things to say. One is that "legal but harmful" is not a new phenomenon. People often talk about it in the sense that it is this new huge threat to freedom of speech. It is already in numerous pieces of legislation. The Communications Act 2003 places a duty of care on Ofcom to deal with legal but harmful content on broadcast. As you mentioned earlier, there is a whole host of ways in which we curtail speech that is legal in certain places, because of the harm it can cause. It is absolutely possible to say that we should be expanding that to social media in the same way as we do under the existing communications legislation.

Ruth Smeeth: I do not agree. I understand where the principle and the duty of care element come from. As a definition, "legal but harmful" is extremely dangerous, especially because there is not a proper definition of what "legal but harmful" could be. There could be a level of political interference. The Secretary of State will always operate in a non-political way, but the Secretary of State getting to define what is legal but harmful means that it can be politically manipulated. I find that very disconcerting. It will also end up in court because of that.

Again, this touches on the psychological harm conversation. I would suggest that people who have experienced a level of targeting have ended up much more resilient than others, unfortunately. What would be psychologically damaging for me at this point? I have a higher threshold because of what I have seen than other people may. If that is the definition, it is really difficult.

It also goes to something that we have not touched on, which is the exemption clauses, with politicians and political speech being exempt and journalists' speech being exempt. We have never been able to define what a journalist is in the UK for very good reason. That is even more complicated on an online platform, because of citizen blogging and citizen journalism. For example, someone might video something awful and it then might go viral. If they have witnessed something, they almost become a journalist because of what they have put up and what has gone viral, as was the case with George Floyd's murder. We have to be really careful about what we are doing.

In terms of the political definitions, I would say this. I am a former elected official. I may or may not stand for office again. I am the chief executive of an organisation that publishes a quarterly magazine. I could make a case that I should be exempt on many different grounds, except I am also just a normal human being. I hate to step on HOPE not hate's toes—forgive me, Joe—but Tommy Robinson has stood for election; Laurence Fox has stood for election. Are they exempt for everything that they have said even when they or others have incited violence? Would you then stand for election, and pay the deposit for a general election, in order to say whatever you want with complete protection from the law? We know that people stand at a general election and pay £500 in order to get the free post to have menus delivered. It is not beyond the realms of possibility that that would go further in other cases. We have to be really careful with definitions. That is key within all of this.

Dr Mulhall: On the first bit of that, I would say that the duty would be on Ofcom to come up with what is harmful—

Ruth Smeeth: Who is going to be their chair, Joe?

Dr Mulhall: I know, but Ofcom is currently the organisation that comes up with what is offensive and harmful for broadcast. The onus would be on an ostensibly independent body. I would just like to reiterate that the two sections of the legislation around democratically important speech and journalistic speech are extremely problematic for exactly the reasons Ruth has said. A huge number of the individuals who we monitor now class themselves as citizen journalists.

Of course, one of the things we are most concerned about in the legislation is that we have spent many years trying to convince tech platforms to de-platform incredibly dangerous and toxic individuals. Take Nick Griffin for example, the former leader of the British National Party. Would his speech be classed as democratically important if he stands in an election? Is Tommy Robinson a journalist? There are all of these questions. We need to do a huge amount more—maybe it is one for the philosophers—to come up with some serious definitions around those two terms. At present, they feel as though they have been somewhat thrown in. The danger is that they are going to hugely undermine the Bill.

Chair: I am conscious of time. I am going to go to Christina, last but not least, and hopefully we are going to end on a positive note.

Q40 **Christina Rees:** Yes, hopefully. You are probably going to say yes to this question. Should the Government be doing more to try to drive cultural and behavioural change amongst social media users to reduce online abuse alongside possible legal and regulatory changes? I would like to know what that would look like in practice, particularly in terms of education in schools and efforts to reach adults.

Ruth Smeeth: Google does an amazing education programme. They come into a school and take it over for the day. They now teach other people how to teach. One of the reasons why they are so good at it—they came to a school in Kidsgrove—is because they know their users really well and they are very aware of the problem. As was suggested earlier, we can work with the platforms to develop programmes.

Chair, you were talking about "polluter pays". That is definitely one of the things that they could and should be paying for, but this is wider than just children. The original drivers behind this piece of legislation were around young people, safety and security. All of us live a far too big chunk of our lives online now. In its broadest sense, how do we educate and empower people at every level? That is why I mentioned getting the WI involved and getting community groups involved, as we did when the internet first arrived. We got every level of community engagement to educate people so they knew how to use the internet and how to use computers. We have to go through that process all over again.

Some of it can be statutory. As we are upskilling the country, we are going to do things. We are currently sitting through COP. There will be an education programme that comes out of COP that touches all ages in terms of how they can be better green citizens. There is nothing to stop us doing digital citizenship at the same time. In terms of what the Government could do, if you want to access some of these sites, you could have to do an online training module before you did. That could be a really easy way to do it.

Dr Mulhall: I do not have a huge amount to add. We talk a huge amount about how we need things in primary schools. We absolutely do, but I used to be a lecturer at a university and a student gave me an essay that was full of holocaust denial. When I challenged him on it, he was utterly appalled and he could not believe it. His ability to differentiate sources that he had found online versus ones he had found in the library was not there. This was a guy at a red-brick university.

There is a thing about education. When we think about Covid misinformation and people engaging in the conspiracy scene, this is people of all genders, all ages and all backgrounds. A society-wide educational programme is required. We absolutely should start in primary schools, but we should also start with my aunt.

The only other thing that I would say on top of that is that people are engaging in abusive behaviour online partly because of the nature of those online spaces, but people engage in online hate because they hate people. We have to root our online education in much wider programmes of attempting to deal with hate and discrimination across society. It is not an abstract; it is just a different way that this manifests itself.

Tonia Antoniazzi: On the final points that you were making there, Mark Zuckerberg—I am sorry to use his name—has failed to allocate resources to police the online space. He has enabled the proliferation of misinformation and abuse. That is what we have seen on our platforms. Thank you for your time. That is where the problem lies. We should not be that naive. That is why it is important that we do call them out as well.

Chair: Thank you so much for all the evidence you have given today. Thank you to our current panel and our previous panel. It has been a very rich discussion and will hopefully contribute to making a better online and offline world.