HOUSE OF COMMONS

# Foreign Affairs Committee

## Oral evidence: Tech and the future of UK foreign policy, HC 201

Tuesday 2 November 2021

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

Watch the meeting

Members present: Tom Tugendhat (Chair); Chris Bryant; Neil Coyle; Alicia Kearns; Stewart Malcolm McDonald; Andrew Rosindell; Henry Smith; Royston Smith; Graham Stringer.

Questions 81 - 162

### Witnesses

I: Katie O'Donovan, Public Policy Manager, Google UK.

II: Joe Westby, Deputy Director, Amnesty Tech, Amnesty International; David Sullivan, Executive Director, Digital Trust and Safety Partnership; and Jason Pielemeier, Deputy Director, Global Network Initiative.

# Examination of Witness

Witness: Katie O'Donovan.

Q81 **Chair:** Welcome to this afternoon's session of the Foreign Affairs Committee. Thank you very much, Katie O'Donovan from Google, for joining us. I will ask you to introduce yourself very briefly and then we will get going.

***Katie O'Donovan:*** My name is Katie O'Donovan. I am the director for Government affairs and public policy at Google, covering the UK.

Q82 **Chair:** Thank you very much for joining us this afternoon. Does Google have a corporate foreign policy, and, if so, what does it look like?

***Katie O'Donovan:*** Thank you for your question. I do not think we would describe ourselves as having a corporate foreign policy, but we certainly have a system of principles and approach both to the way we operate globally and in individual countries, and also in the way that we think about the internet and the way we think the internet should be governed.

Q83 **Chair:** Do you do foresight and horizon scanning? Do you have in place anything to anticipate global social, economic and political changes, and other disruptive or unforeseen events?

***Katie O'Donovan:*** Yes, we do. I am not sure again I would quite characterise it like that. Part of the role that someone like me would do is look at the country that it operates in, to understand the politics, and understand what is on the horizon there. I have worked at Google for the last six or seven years, and it is my job to advise the company: "We have a referendum on Brexit coming up. This is what people are thinking. This is what people are doing. This is what the pollsters are saying. Will it have an impact on our operations in the UK?" I would have those conversations with the UK leadership of Google but also think about it in the global setting and have conversations with my colleagues in the US. We have a team of people like me in different countries around the world.

Q84 **Chair:** Clearly, you have transnational operations. Do you have much engagement with foreign Ministries or other Ministries in the jurisdictions in which you operate?

***Katie O'Donovan:*** It depends country by country. In the UK most of our engagement with Government is through DCMS. We have a bit of engagement with BEIS and other Departments. We probably have limited direct engagement on the ground in the UK with the Foreign Office, but the UK Foreign Office, similar to other countries, has a special envoy for technology, who is the Consul-General based in San Francisco, so through his office and him we would have engagement with the Foreign Office and its processes.

Q85 **Chair:** As part of that engagement, have you had much conversation with people like the UK's tech envoy, Joe White?

***Katie O'Donovan:*** Yes, with both Joe White and his predecessor. That role is physically located in San Francisco, so in proximity to our company's headquarters and other companies' headquarters. Obviously, he would be good at describing his own role, but from our perspective his role is to help the UK tech industry out in California and have an inward investment role there, but also to engage with companies like ours to understand what we are thinking about issues of the day, what we are thinking about UK operations, and to help the engagement along those lines.

Q86 **Chair:** Do you find his position useful?

***Katie O'Donovan:*** Yes, I think I do.

Q87 **Chair:** Have you had much engagement with others—the Danish tech envoy or other countries' envoys?

***Katie O'Donovan:*** My colleagues will have done. There is a Danish tech envoy and perhaps one in New Zealand, too. They are useful roles. Generally, and it will not surprise you to hear this from somebody who does a role like mine, where there can be increased engagement between Government and technology companies, or companies with emerging technology, it is helpful to understand Government priorities and Government challenges, and the scrutiny they might want to put on us, but also for us to be able to explain emerging technology and the way we operate, and some of the considerations we might think are relevant to current conversations.

Q88 **Chair:** Are there any Governments you do not talk to?

***Katie O'Donovan:*** I would not have a comprehensive list.

Q89 **Chair:** Perhaps not Governments you avoid talking to but ones you specifically do not talk to.

***Katie O'Donovan:*** I do not think so. There are countries that we do not operate in. I am sure the Committee is aware that we do not operate in China. I am not up to date with whether we have any regular or infrequent conversations there. I would have to talk to colleagues. Generally speaking, and you asked at the beginning of the session about our approach to foreign policy, we absolutely think there is value to us as Google and a shared value to society and the Governments to turn up, to engage and to have live dialogue with Governments, regulators and legislators. That does not mean they are necessarily easy conversations all the time, but I think there is shared value, and there is also a responsibility on our behalf to be part of those conversations.

Q90 **Graham Stringer:** The Electronic Frontier Foundation claims that 92% of the UK and global search market is controlled by Google. One of your ex-employees said that means, in effect, that Google determines what 92% of the world see and what they do not see. What sorts of policies do you have to deal with that extraordinary responsibility?

***Katie O'Donovan:*** Thank you for the question. It is an extraordinary responsibility. We were not the first search engine to market, but we are proud that customers come to us and users use us, because they find out through experience that they get trusted and authoritative results through the Google search engine. Unlike other technologies, you do not have to have a Google account to use our search engine. You can swap very easily and very frequently to other search engines. Often, when people are looking for different types of information, they might start their journey online. For example, if you are shopping you might go to a commerce platform, or if you are looking for sports results you might go somewhere else. That said, we are a very frequently used search engine. We are very proud of that and we take that responsibility incredibly seriously.

Inherent to what makes Google a success is our preference and dedication to making sure that you get relevant, trusted and authoritative results when you use Google Search. If you did not, you would quite quickly swap to a different search engine. When I typed in this morning "Foreign Affairs Committee, UK Parliament", I got taken very quickly to the website not of the UK Parliament, not of a different foreign affairs committee but exactly this session. That is what I wanted and that is why I will go back and use Google Search.

We need to make sure that the information we are using is what people expect. We publish our 200-page search quality rater guidelines, which are used by people across the world who test the search results to make sure they are meeting the expectations we set out. We will look for relevance, for authoritative information and for trusted sources to make sure you do not get surprising, unhelpful or indeed irrelevant search results.

We also add features to Search where we know there might be contested information, or where it might be of real importance to get that information very quickly. For example, at the beginning of the Covid pandemic we worked in the UK with the NHS. If you type in "Covid-19" or a similar term, you will get what we describe as a knowledge panel, which will tell you the up-to-date information. When we had lockdown restrictions it would tell you that, it would tell you the symptoms and it would tell you vaccine information, because we know when people are receiving information through Google it is really important that they see trusted, authoritative results.

Q91 **Graham Stringer:** That is very much a market-based answer. I understand that. Some of the decisions you are taking would previously have been taken by Governments. Do you talk to Governments about how you respond and how you provide that information?

***Katie O'Donovan:*** We do. A product like Search is the index to the world's information, so we do not host that information ourselves. We help people discover it, and it is hosted by—

Q92 **Graham Stringer:** You prioritise it, don't you?

***Katie O'Donovan:*** We do because people want relevant information. They need to know the answer to their question. We do that in line with our search rater guidelines rather than editorialising and saying, "I much prefer the Parliament website to another website." We will talk to Governments, and we will work with Governments. Some of the interesting questions this Committee has been raising are how tech companies can work effectively with Governments. There have been some good examples, particularly around child abuse material and terrorist content, and building the right multisectoral approaches and bodies to tackle those by working closely with Government to make sure we are keeping our users safer.

Q93 **Graham Stringer:** Is it advice on what the law is in these areas or what Government think is appropriate in that case for keeping children safe?

***Katie O'Donovan:*** That is a really good question and a question that Parliament is looking at and scrutinising in the Online Safety Bill at the moment. If you take the video platform we own, YouTube, as a company we directly host the millions of videos that are on there, and we have what we call community guidelines, which go above and beyond the law. You will have content that is legal but is not allowed on YouTube, and we are very clear about that. In some instances it might be because it is pornographic, or it might be because it is Covid misinformation, or because people are making threats or something like that.

On Search, because we are indexing the world's information, we return the results that people are looking for, but we work with Governments where there are areas of real high harm. For example, on child abuse material, that content is clearly illegal, and it is illegal in all jurisdictions. It is not a political decision and it is not made for political reasons. There is global acceptance that such material is abhorrent and should not be on the internet. We work with institutions in the UK like the Internet Watch Foundation, and institutions in the US, to identify that content. We have built technology that is relatively successful in identifying that content and then blocking access to it.

Q94 **Graham Stringer:** You mentioned contested information in your first answer. We are in the middle of an epidemic. There are a lot of contested issues about the number of infections and, in some cases, whether Covid in fact exists. We also had the very divisive EU referendum. Can you tell the Committee how you went about dealing with contested issues in those two areas?

***Katie O'Donovan:*** That is really at the heart of building a successful search engine, because if people perceive or feel there is bias in our search engine they will not trust us and they will not use it, so it is really important.

For the pandemic, for example, we have the knowledge panels that come from authoritative information because we give particular attention to

making sure we have authoritative results, particularly in areas that might impact health. Obviously, that is one of those. We have seen examples where, particularly in some of the scrutiny or some of the debate about the origin of the pandemic, our systems have looked to be exploited. About 15% of the searches we see every day are new on Google Search. While you can search for some things and there will be hundreds of thousands of answers, you can search for other topics, and either they are not yet a news story or no one has chosen to write about them online. We have seen these things called information vacuums, where people have sought to exploit that by creating content and using search terms to proliferate conspiracy theories.

We have made a number of product changes to guard against that. Now, if you do a Google search, you will see three dots next to the search result. You can click on that and it will tell you why you got this result, and it will tell you who the publisher of that result might be. Is it a Government news agency or an established news agency, or is it something more informal? When there is a breaking news story, we say, "Look, the results are changing quite quickly on this topic. You might want to come back," or on both Search and YouTube we will direct traffic searching for topical events that are just happening to authoritative news organisations, because quite often, particularly with topical events, there is a race to be the first person to write or blog or film or produce content, and not all of those actors are authoritative.

Q95 **Graham Stringer:** Do you have anything to say about the EU referendum, where many of the contested issues were more subjective than even in Covid?

***Katie O'Donovan:*** We have sought to ensure the search engine works as directed. People will type in a search query and the content that is most relevant to that will be returned. Often with something like an election you will return news content because it is topical and you want something that is relevant today. Often the search term that people use is really important. If I type in "EU referendum", that is very different from typing in "Why should I vote yes?" or "Why should I vote no?", or an allegation of misuse of funds or whatever.

We look carefully at the EU referendum and we look carefully at elections more generally. We have in place a procedure around elections to make sure that, again, we are giving authoritative information. In some countries we have seen misinformation campaigns on polling day, "Your polling station is shut," or giving the wrong address—really sinister motives like that. We work with local partners to ensure we can provide that information with confidence and great visibility, and also have transparency in any elections ads that we allow on our platform.

Q96 **Alicia Kearns:** On data voids, at what point did you become aware of the vulnerability we saw? I think you called them information vacuums.

***Katie O'Donovan:*** I do not know, I am afraid, so I will have to get back to you on that. Both on YouTube and on Search it is something we have seen happening in different instances quite quickly, and often as much as one person is trying to do something, we are being alerted to it, and it is being reported in that instance. I am not quite sure of the timeline, but we have a permanent threat analysis group, which is a cross-functional group of security experts, ethicists and other specialists who are responsible for that work. I can find out the timeline on that.

Q97 **Alicia Kearns:** You said it is handled by the threat group, so does that mean you recognise it as primarily being undertaken by hostile state actors and by terrorist actors?

***Katie O'Donovan:*** In that specific case I do not know. Speaking more generally, you see, for example, YouTube content on a breaking news event that is not sinister; it is just that someone has got it wrong and they are either reporting in a ridiculous way or they are free and loose with the facts. If you want to come to YouTube and you want to find out what is happening, that is not a good user experience. That is where we will default to trusted news organisations. The motivation of the actor is neutral for us. What we want to do is give people the most relevant information, and that remains true for Search, too.

Q98 **Alicia Kearns:** It is interesting what you say about the motivation of the actor being neutral but, obviously, from our perspective that is the opposite of what we are concerned about as legislators. It would be interesting to hear more, and I do not know if your threat group could come and give evidence before the Committee. When it looks at the threat, it will not be looking at just the operational aspect. It will also be looking at where it emanates from. If you are unable to talk to us about whether it is hostile states or terrorists groups, do you think it would be able to come before us and talk to us about that?

***Katie O'Donovan:*** Yes, and what I was trying to explain is that on YouTube you have a product solution and the product solution does not need to understand the motivation of the actor. The threat analysis group's objective—and it publishes a quarterly report, which is available online—is to keep our products and users safe, and to share that information with the wider ecosystem. It will look at who is perpetrating those acts and report on that, because attribution within the security community is so important. We have sent about 50,000 reports in the last year, and that is up about a third on the previous year. Partly that is because we saw a big, concerted effort by a Russian actor, and we have reported on that, attributed on that and made that very explicitly clear. We have also given examples of other foreign actors that we have attributed that information to.

Q99 **Alicia Kearns:** I recognise you are trying to put the line of being reasonably politically neutral as an organisation. You mentioned that you do not look at the intent of the actors carrying out the activity and you look purely at the impact it is having on the product, but surely only by

understanding their intent will you be able to recognise further ways in which they might try to exploit YouTube.

***Katie O'Donovan:*** Let me clarify that. The threat analysis group will absolutely look at the intent of the actor, the origin of the actor and why they are doing it, and that provides the sophistication for us to make the right judgment and take the right act. When we have a product like YouTube, if you are at a football match, I am filming you and we are having good fun, it does not really matter if what we are saying is accurate or reliable, but if we are at a breaking news event, our users are coming to us for authoritative information. We might not be being sinister in uploading our original footage, but it is important that our product responds appropriately. To be very clear, the threat analysis group will analyse the threat and look at the intent, and we will act on that intelligence and share it within the tech sector and the broader law enforcement community.

Q100 **Alicia Kearns:** In terms of data voids and things like that, do you think we need a counter-disinformation Bill in the UK to protect our citizens from the threat of disinformation?

***Katie O'Donovan:*** What was the name of the Bill?

**Alicia Kearns:** I am happy to have many names for it.

**Chair:** "The Alicia Kearns Bill".

**Alicia Kearns:** Counter-hostile state disinformation, counter-disinformation, information protection, however you want to go about it but essentially looking specifically at the tools and techniques used, whether it is troll farms, data voids or manipulation of information, something to protect the public.

***Katie O'Donovan:*** I would be very open to looking at that and seeing what could be achieved with legislation. A lot of my work is looking at the Online Safety Bill. The discussions about that have spanned a number of years, and it will probably be a number of years before the legislation comes into force. What is equally important in considering legislation is thinking about what tools we have now as a company that we should be acting on, and we certainly should not wait for legislation to do that. But also much of what is challenging online is already illegal and we should be making sure that organisations, whether in the UK or elsewhere, have the resources and the expertise to tackle that.

Q101 **Alicia Kearns:** Do you think the Online Safety Bill in the current amalgamation that has been pulled together does enough to protect us from hostile states who are undertaking disinformation activities, or do you think it is too focused on abuse and other things such as that?

***Katie O'Donovan:*** I do not have a particular expansion that I would recommend in terms of foreign states. It clearly is not its stated primary

intention. Its primary intention is to think about the systems behind addressing content that is either illegal or harmful but legal.

Q102 **Alicia Kearns:** Obviously when people think of big actors in the tech space they think Google, they think Facebook and they think Twitter. Facebook and Twitter both declined to give evidence to this Committee on the basis that it would put their staff at too great a risk in country and due to commercial sensitivities, I think. I am sure the Clerks will correct me if other reasons were given. Do you recognise those concerns, or do you think perhaps Twitter and Facebook should be rightly stepping forward and recognising that they have a role to play?

***Katie O'Donovan:*** Perhaps I should have considered my safety before giving evidence. We discussed this in the Chair's question at the beginning. I cannot speak for the other companies, but I think it is entirely appropriate. In fact, it is my job, and as a company we see it as a very important responsibility to come and engage in dialogue like this. Sometimes questions will be challenging, or sometimes we will have disagreements over what we think the right path forward is, but it is absolutely our responsibility to be here, and to be part of this dialogue.

**Alicia Kearns:** Dialogue to aid our vision. Hopefully Facebook and Twitter are listening in and will reconsider.

Q103 **Chris Bryant:** Thank you very much and apologies for being late; I was on another Committee.

This is not directly a foreign affairs question, but lots of people when they get serious medical concerns go to Google. Google doctor is really dangerous, or can be really dangerous, because it does not sort out for you whether the material that you look at is up to date or is from your country. I have had people with a cancer diagnosis say to me, "Oh my God, I am going to die in the next fortnight according to Google doctor," but that is because they are looking at statistics from 25 years ago but did not realise. Is there anything we can do, or you can do, I guess, to improve the performance of Dr Google?

***Katie O'Donovan:*** Certainly we want to be able to give really reliable and authoritative search results. We all instinctively Google things when we have a diagnosis or when we are worried about things. We believe that can be a real asset. Twenty years ago if you had a diagnosis or you were concerned about something, you would have a 10-minute or 15-minute consultation with your doctor and you might be given a leaflet to read on the way home. We know that direct, qualified, high-quality medical information is relevant and accessible via Google, and importantly so is peer-to-peer support communities and organisations where you can talk to other people with similar conditions.

As I mentioned earlier, we prioritise queries on what we describe as "your money or your life." For health queries it is super-important to us that we are returning quality information. If we know where your location is, we might return NHS information. We are very lucky in this country to have

such a significant bank of information on the NHS website. Not every country has that on such a wide number of clinical areas. We have the rater guidelines and we test information against that.

You will sometimes find a knowledge panel on some illnesses, as I described earlier with Covid, but there is definitely more that we can do on that to keep working.

Q104 **Chris Bryant:** Isn't one of the difficulties that, if you google most conditions in the UK, the first five or six answers that come up will be paid stuff from the United States of America from people trying to sell procedures or healthcare products?

***Katie O'Donovan:*** Not necessarily. We have particular restrictions around who can advertise pharmaceuticals. I would expect, but it is always dangerous—

**Chris Bryant:** It is mostly clinics—the Mayo Clinic and places like that.

***Katie O'Donovan:*** I do not know enough about the Mayo Clinic and its business operation. I have definitely read some of its content when I have looked for health queries on Google, but you will often get NHS information that is authorised by the UK and is relevant.

Q105 **Chris Bryant:** Normally around 12 or 15 would be my anxiety in the UK. Poor old doctors—I know everybody has a different view about their own GP—now tell me everybody comes in and says, "No, you're wrong. Google tells me x."

***Katie O'Donovan:*** More information can be challenging. We seriously believe it can be really helpful for our users, certainly speaking from personal experience and more broadly, to be able to supplement the advice they get from a GP by looking for information on the internet—

**Chris Bryant:** They have done their own second opinion.

***Katie O'Donovan:*** That is not necessarily a bad thing, always.

Q106 **Chris Bryant:** Not necessarily always, yes. On the different subject of co-operation with the police and prosecuting authorities, I am conscious that quite often the police will complain when there is a threat against somebody that they find it very difficult to get information out of Google and your associated companies.

***Katie O'Donovan:*** Yes, and that is something we are conscious of. We have an improved system in place internally, a law enforcement request system, which streamlines that process and enables people to request that information. We have also worked with the UK and US Governments to make that process more efficient. There is something called the CLOUD Act, which has been passed, but we are waiting for the agreement between the two countries to come into force. We work with both the NCA and with local law enforcement to improve understanding of how to

request information from us. There is definitely more we can do, because we see both anecdotally and in practice not every—

Q107 **Chris Bryant:** Do you co-operate with the others in this field? Twitter is appalling. You can never get anything out of them, and it takes months and months and months.

***Katie O'Donovan:*** I just cannot speak for them. On areas like counter-terrorism we work through the GIFCT and on child abuse content we work with organisations like the IWF, and Twitter is also a member of those. It is our responsibility to make sure law enforcement can come to us to request that information and that we are dealing with it in a timely and effective fashion. We work hard to do that, but it is an area of developing, emerging and evolving policing that needs ongoing dialogue and support.

Q108 **Stewart Malcolm McDonald:** Thank you, Katie, for your time this afternoon. May I take you back to some of the stuff you said in response to Alicia Kearns's questions? You talked about the threat analysis group. Who is that and what do they do?

***Katie O'Donovan:*** They are a part of Google. They are made from different disciplines. We will have some engineering and security folk, some legal and some policy folk, some people who understand foreign policy and some of the live dynamics, and they work to look for live threats. Often both for our own systems and for other organisations' systems there will be vulnerabilities that the system is not aware of. We look for those vulnerabilities and identify them. We offer a reward system for people who—I was going to say phone up, but obviously I am very out of date—get in touch to say, "We have noticed this vulnerability in your system or elsewhere."

We also look at, as I described earlier, actions from foreign actors. One of the recent reports we published was around an Iranian-based actor that had, among other things, targeted a UK university to use its infrastructure as part of a phishing account.

Q109 **Stewart Malcolm McDonald:** That would include YouTube, I take it, as well—

***Katie O'Donovan:*** Yes.

**Stewart Malcolm McDonald:** If people see something on YouTube that is a potential threat to someone—

***Katie O'Donovan:*** Yes.

Q110 **Stewart Malcolm McDonald:**. I ask this from admittedly quite a personal standpoint because a few years ago my constituency surgery was targeted by—I will not name the name because it will flare up again if I do—a very high-profile, right-wing activist, and you probably know who I am talking about.

***Katie O'Donovan:*** I do not, I am afraid.

**Stewart Malcolm McDonald:** It was livestreamed on Facebook and Facebook deleted it, but it is still on YouTube to this day, and I get a ton of abuse for it. As I said to a colleague of yours whose name escapes me, if the video is not there, I don't get the abuse and the threats. It is still there and I was told it couldn't be taken down. What process would the threat analysis group go through when a video like that is up there, which encourages far-right supporters to attack and threaten me even to this day? Talk me through the process by which they have gone through a video like that—and I am perhaps unfairly putting you on the spot here—and decided that it can stay up.

***Katie O'Donovan:*** I am sorry if this is semantics, but it would be a different bit of Google and YouTube that looks at that video. The threat analysis group would be looking at external threats and that would be our YouTube trust and safety team, just so you understand a little bit of the difference.

As I mentioned earlier, on YouTube we have our own terms and conditions that go further than the law, and that enables us to take action on content like that. I am very sorry, I have not seen the video, so I will speak generally, but we can obviously review the video.

We have policies at YouTube against harassment and against inciting or inspiring real-life violence or harm. From the sound of it, it would need to be reviewed under those criteria. I am not talking specifically about this video because I have not seen it, but we also have criteria that we call EDSA. If something is educational, documentary, scientific or artistic, we might allow it to stay up. I said earlier that Covid misinformation is not allowed on YouTube, but if I were to create a news report and said, "Look at this damaging Covid misinformation. Here is somebody talking about Covid misinformation," that would be allowed to stay on YouTube. If I just clicked the video with no context, it might be removed.

It might be, and again I want to stress that I have not seen the video, there was a public interest element. What we can do is make sure our trust and safety team, who are the experts on our community guidelines, review it. I am very happy to do that.

Q111 **Stewart Malcolm McDonald:** Thinking of the external or the foreign side of it, YouTube recently banned RT Deutsch from its platform, which I was delighted to see. When are you going to do it in the UK?

***Katie O'Donovan:*** Every channel on YouTube is subject to the same guidelines and the same terms and conditions. We have a system where our community guidelines are very well published and it is the responsibility of the channel to meet them. We have what we call a "three strikes and you're out" policy. Occasionally, in very serious instances, if you do something very seriously wrong, we will remove the

channel immediately. If you receive three strikes for breaking our community guidelines, we will terminate the channel.

Q112 **Stewart Malcolm McDonald:** It was done, I believe, in Germany. I am not sure if there were three strikes or if it was one, on Covid disinformation. They pump out the same stuff here, just in English. So where are they? Have they had two strikes here in the UK?

***Katie O'Donovan:*** I do not know that, I am afraid, off the top of my head. On every video and channel on YouTube there is a flag icon. Users can flag that content. We have our own systems in place to detect violations of our community guidelines and we will remove those. We adhere to those policies for everyone equally on the platform.

Q113 **Neil Coyle:** Thank you, Katie, for being with us today and being more open and transparent than, as has been pointed out, Facebook and Twitter have chosen to be, given their more secretive stance.

I want to start by asking about the UN guiding principles on business and human rights, which state that, where a company finds itself in conflict between state jurisdiction and international human rights law, businesses are expected to respect international rights law to the greatest extent possible in the circumstances and to be able to demonstrate their efforts in this regard. How do you handle those kinds of conflicts, and do you publicise where those conflicts occur?

***Katie O'Donovan:*** Thank you so much for the question. It is a really good, important question. It sometimes feels a bit cheesy, a corporate representative coming and explaining a company's mission, but it is worth dwelling on here. Google's mission is to make the world's information universally and freely available. That is our reason to get up in the morning and it is how we judge our success, if we are able to do that. We want to be accessible to as many countries as possible. That way a student in Delhi has access to the same search engine and content as a professor in Oxford might have.

Where we seek to operate around the world, we operate in some very complicated and complex environments. We have our own human rights systems in place for our operations. We have developed, particularly around our AI practices—

Q114 **Neil Coyle:** Are they global? I am sorry to interrupt, but with regard to the extent to which you might uphold a particular bit of human rights law, is there no differentiation between which country you are in?

***Katie O'Donovan:*** Let me come on to that, if I may. Those guide our work. We have AI principles that have established that we must trust for safety and that we must ensure they have a positive impact on society. We have committees in place to review those and to make sure we are adhering to them.

Where there is a challenge sometimes is where we operate in local jurisdictions. For example, we were just talking about a piece of content on YouTube. The first thing we do if content is flagged to us is review it against our own community guidelines, and if that content falls foul then we will remove it. If it does not, we will require a legal request for it to be removed. In some countries we are compelled under local law to remove content that would be described as being sometimes challenging. We would fully scrutinise that legal request and make sure we really understand the law, the letter of the law and any impact it might have on our systems. We will also look at factors on the ground. We will look at the safety of the staff and how this will impact our users. If we are present in a country, and if we are legally compelled to remove content, we will have to do that.

If that is the case, we publish a quarterly transparency report. It is very worth while looking at this if you are interested in it. It publishes by country the requests that we have had to remove data, what we have done with those requests, and it talks through case studies in different countries where we have taken down content and where we have not, and where we have accepted the request because it is absolutely grounded in local law and where we have been able to reject it.

Q115 **Neil Coyle:** May I follow up on that, because I think this comes back to the other question? You mentioned the threat analysis group for YouTube specifically. Why should the Met here in London, for example, have to make requests? It says it has made hundreds of requests to take down YouTube videos that are about threats to life, intimidation of witnesses in legal cases or homophobic cases that have led to attacks on individuals. Why should the Met request that comes down and not require it?

***Katie O'Donovan:*** It is probably about legal jurisdiction, and if they are able to require it they might require it, and if they have to request it they might request it.

Q116 **Neil Coyle:** Are you telling me we need to give them that power?

***Katie O'Donovan:*** That is the decision of the legislators of a country. That is where you get tensions because some countries choose to give more powers to requests for information to be removed than others.

Q117 **Neil Coyle:** Coming back to the first answer, this is where your quarterly review will outline which cases the Met has put in and it will say why you have chosen to keep up a video that the Met has said could lead to the threat against an individual's life.

***Katie O'Donovan:*** Yes. We do not list every single case but we list a good illustration of cases from different countries. We work very closely with the Met here. There are some cases where it is able to request information or content to come down, and it is very clear-cut. There are others. For example, we did a big piece of work with the Met police around drill music where there is quite often a threat to life. We do not want that sort of content on our platform, and we want to remove it

when it is flagged to us. At the same time we want to be, and we are proud to be able to be, a home for drill music, which is giving young people a chance to express themselves. We cannot use technology to identify all drill music and remove it, because we would be removing freedom of speech from a group of people who need it and can exercise it responsibly.

Q118 **Neil Coyle:** It would be worth seeing some of these quarterly reports, because I think the videos the Met has identified have had specific threats and in some cases have led to attacks.

Stepping back up to that state-level conflict, you say you have teams of people on the ground to make these decisions. Talk me through how, for example, in Russia the Navalny case came up where Google acceded to taking down tactical voting advice and information. Talk me through the process that led to that outcome, because I think it surprised a lot of people.

***Katie O'Donovan:*** I was not closely involved in that process, so it might be more helpful if I talk in general terms. Certainly the first thing we will do is look to see if content or applications break our own community guidelines, or our own terms and conditions, which was not the case in this instance. Depending on the country and depending on the legislation in that country, there might be a legal request. Where we choose to operate in a country, we have to abide by local law. We will fully scrutinise that and really test it. We will make sure there is no option but removal. We will also consider the conditions on the ground and the implications for local staff and for users, and other considerations.

Q119 **Neil Coyle:** Are you suggesting that, if you had not acceded to that demand, your staff could have been at risk from what—state actors in Russia?

***Katie O'Donovan:*** This is something I would be very happy to discuss in private with the Committee. Speaking in general terms, this is how we usually approach systems. There is a tension, and you have heard from other witnesses at this Committee, where countries decide to have a stronger approach to the internet and requesting information, or on creating the legal framework to demand that information or applications are removed from the internet. That is a real challenge for not just companies like ours, but for our users, citizens and voters, and it is why we believe very firmly that the free and open internet that has enabled us all to benefit from access to the internet is being challenged at the moment and needs really careful, concerted international co-operation to defend it.

Q120 **Neil Coyle:** You mentioned China specifically, but perhaps you could tell us what bearing a country's domestic approach to human rights has on Google's decision whether to operate in a country or exit the market.

***Katie O'Donovan:*** I have spoken a bit about our mission, and that is very important to us. Our not being present in a market is not a neutral

act. If you are not able to access Google Search—at the moment in China you cannot access Google Search or use Google Maps or Docs, or any of our features—that is not helping us achieve our mission. Our mission, we hope, benefits people, so it is to the detriment of local citizens if they are not able to access a plurality of information or search the internet.

In China at times, I think it was about 2010, we had a search engine. We were not happy with the conditions that were put on us to operate that search engine. An international version was then blocked and we now have no operations in China.

Q121 **Neil Coyle:** But you were developing Dragonfly, weren't you? Talk me through the process of the decision even to consider operating a site that is not the same as Google in the rest of the world, because you said you wanted information freely accessible wherever you are, but you were developing a product that was not to that standard for China. When was it realised that it did not meet Google's aspirations?

***Katie O'Donovan:*** I do not have the precise timeline or detail on that. We very clearly are not in China at the moment. We have no products and services that we offer there.

Q122 **Neil Coyle:** Human rights advocates have said that the surveillance-based business model of Google is fundamentally incompatible with human rights. I think they would choose to link that to the tracking on phones, for example. How do you respond to the suggestions that you are undertaking probably the biggest amount of data surveillance of any country or corporation on the planet?

***Katie O'Donovan:*** We operate an ads-funded model and we do not apologise for doing that. That makes our product freely available, but we want to make sure all our users have confidence that their data is secure and private, and that they are in control of it. I mentioned at the beginning that around half of Google searches are not from signed-in users. Unlike many tech products these days, you do not need to have a Google account to use Google, and we truly believe that is a very powerful tool.

We then make sure when we serve adverts, and we were the first company to give people access to their own ads profile, that people are in control of that. Some people like Google to know they are in the UK or even in their neighbourhood because when you search for things you get relevant information in response. Some people absolutely do not like that. You have control over your ad settings. We never sell data to any third party. We never use sensitive information to serve advertisements.

I absolutely understand that there is scrutiny in this place. We also respond to changing expectations. For example, Google has announced that we will phase out the use of cookies through our ad servers. That is a significant change to the internet infrastructure.

Q123 **Neil Coyle:** This is in response to the *Washington Post*, I think it was,

calling Google Chrome the biggest spy software.

***Katie O'Donovan:*** I do not think it was in response to that.

**Neil Coyle:** An article, I should add, I found on Google Chrome.

***Katie O'Donovan:*** We aim to give you what you are looking for. It is in response to user expectations, essentially. Phasing out cookies is a really significant change. It is significant not just for the user, not just for technologies, but for those platforms, too. We have given long-term advance notice of that. We are working with industry experts. In the UK, the Competition and Markets Authority is closely reviewing this, which we welcome, to ensure we progress to a system that is successful in the long term.

Q124 **Neil Coyle:** You mentioned you are proud of the fact that you are an advertising-funded model. I am glad you are proud of that, but you are not very transparent about it. I wonder why you are not transparent about advertising revenue. It genuinely concerns me that, if someone searches for a piece and they find it, and they are looking for a local or national newspaper article on the subject, Google can keep 86% of the advertising revenue against that article even though they are going through to that article. I am wondering why it has taken the Australian Government to intervene, for example, to get more transparency on this issue, and whether we need to move to that model in the UK.

***Katie O'Donovan:*** I do not recognise that figure, and I would be happy to follow up. We drive about £500 million-worth of revenue to news organisations. People search for stories like you did and end up on a newspaper website.

Q125 **Neil Coyle:** If you are happy to follow up, perhaps a meeting with Reach on this would be a welcome step forward, and others who are interested.

***Katie O'Donovan:*** Yes, we are very happy to do that.

Q126 **Stewart Malcolm McDonald:** May I ask about Governments who want you to censor things? I won't pick on a specific country or a specific issue, but if a Government want you to censor an article on something, or whatever, how would a Government approach that, and how do you assess that request?

***Katie O'Donovan:*** I cannot give you an exhaustive list of examples, but often we will have content that is flagged by a user or by a Government. That can be in many different ways. The Met police might be saying it is interested in something, or, in the UK, a non-governmental organisation might have a specialist area of interest or concern. When we receive those requests, we will judge them by our stated and published terms and conditions and community guidelines. Often, a Government will feel very strongly about something. Often, we will understand why a Government feel very strongly about that, but if it does not break our community guidelines we will not be able to remove the content and we will ask for legal reason to remove it.

Q127 **Stewart Malcolm McDonald:** Globally, are you seeing an increase in the number of Governments, and I am thinking specifically of Governments, seeking censorship of some description?

***Katie O'Donovan:*** Absolutely, and you can look at the quarterly transparency report, which is available online. If you google the transparency report for Government take-downs, you will see we plot Government removals over time. Obviously, some of that increases because more people are doing more things online, but you will also be able to see by individual countries how they take things down—for example, how they request for things to be taken down. For Russia we receive about 20% of the requests from them on national security grounds. For the UK it is 2%. In the UK we receive much more requests for removal on something like copyright grounds.

Q128 **Stewart Malcolm McDonald:** Perhaps with the pandemic you will have seen an increase in stuff related to that, I would have thought.

***Katie O'Donovan:*** Yes, we design our systems, particularly on YouTube, to catch relevant content, but that would be one area, yes.

Q129 **Stewart Malcolm McDonald:** What would you say are the main challenges in handling those requests? Was that one fifth of all requests are from Russia or one fifth on national security grounds from Russia?

***Katie O'Donovan:*** One fifth of requests from Russia are on national security grounds.

Q130 **Stewart Malcolm McDonald:** What are the main challenges for Google in handling those requests? Talk me through how that would be kicked around. I know you have the guidelines you referred to and there will be legal channels and all the rest of it, but how do you kick that around and reach a decision?

***Katie O'Donovan:*** In some cases it can be very straightforward, particularly where we have clear, established content guidelines where the content clearly fits one description and falls within that. That does not necessarily need to be a controversial process. We might say, "We have received a request. We have reviewed the content. It doesn't meet our terms and conditions, so we'll remove it."

In more contested areas it can obviously be more challenging, and we find people who understand how to create content that goes right up to the line but does not cross it. That can be challenging and we think about how that content is discoverable on our platforms, and make sure that we are perhaps reducing the recommendations of that content so people are not exposed to it accidentally.

Q131 **Stewart Malcolm McDonald:** If you are unwilling to bow to the request of a Government, and I will pick on the Russians just because we have mentioned them, what kind of kickback do you get from the state in that case, and how do you deal with that?

***Katie O'Donovan:*** It depends very much on the content and on the country. In some cases you can have a very respectful exchange, "Okay, we have reviewed the content. We understand the concern, but it does not break our community guidelines," and there is no legal request that follows it up. Sometimes we get a lot of public scrutiny about not removing content, and in some cases the easiest thing to do would be to remove the content and ask for a quiet life, but we take very seriously our responsibility to allow people to have free expression and to access free information.

Q132 **Stewart Malcolm McDonald:** Do you have an example of where it would be easier to do that but you have chosen not to?

***Katie O'Donovan:*** I cannot think of one immediately, but you have news cycles about different types of content that come up, and it can be controversial. We will look very carefully against our community guidelines. Drill music is a good example. Drill music, which is very heavy rap music that is popular in London and across the UK, has some fantastic artistic credentials. It gives a voice to young people who want to express themselves and is now a really successful industry in the UK. Several years ago, we saw some really challenging content where some people made threats to life in their drill music videos that they then carried out in real life. We have community guidelines to enable us to remove that content, but we had calls at the time to remove more drill music and remove lots of drill music without the sophistication of linking it to an offline case of violence and threats. We felt very clearly in that instance that we wanted YouTube to be a home for young people to create music that they enjoy and share, and they have been able to go on and successfully monetise. I certainly had lots of representations from different people that we should take a broader approach and remove content where we did not find that it violated our community guidelines.

Q133 **Stewart Malcolm McDonald:** Going back to states and Governments for a minute, when a Government ask you to remove something on whatever grounds it might be, do you think international law is strong enough at the moment in terms of how Google responds? Could it be strengthened?

***Katie O'Donovan:*** There is absolutely a role for the international community here. I touched on it earlier. Free and open internet sometimes covers a multitude of sins, but it is such an important principle to enable us all, whether it is education, social or economic opportunities, to realise those online. At the moment, we see different countries taking different approaches to internet regulation and we recognise that sovereign states will do that, but the norms can be established by Governments like the UK. We have seen this in some of the G7 work the UK has done. Or, for example, the EU and the US have just established the Trade and Technology Council, which has real potential to set what are acceptable norms, and to enable organisations like ours to offer what we think is a good service that enhances the free and open internet, but to do that in a way that is responsible, yes, but

also protected from some of the challenges and threats we see to our operations in some countries.

Q134 **Stewart Malcolm McDonald:** Lastly, you will be familiar with Brad Smith from Microsoft and his grand idea of a digital Geneva convention to codify more of people's rights and what they can expect from the internet, and also the way that the internet and online is regulated. We have the chemical weapons convention, but we do not have similar treaties for cyber-attacks and all the rest of it.

Can you very generally give a view on that idea—a lot of people roll their eyes when they hear the words "digital Geneva convention", call it what you like—in terms of where it could seriously be beefed up?

***Katie O'Donovan:*** What I am interested in is what works. Sometimes things that start small can be incredibly effective. Making partnerships within the tech sector or having a multisectoral approach that is sponsored by Government can be incredibly powerful.

If you look at something like GIFCT, which is the Global Internet Forum to Counter Terrorism, that started off as a partnership between us and some of the other tech companies. The US and UK Governments very much encouraged it. It has since gone on to become a free-standing organisation with permanent staff and is demonstrably helpful to us as a company but also to Governments—the G7 scrutinised its work most recently—in tackling terrorism and the interplay between terrorism and technology. I prefer to focus on practical solutions that we can use today.

Q135 **Stewart Malcolm McDonald:** It sounds like a thumbs down from Google for a digital Geneva convention.

***Katie O'Donovan:*** I think all ideas are worth discussing.

Q136 **Alicia Kearns:** I have a very quick question. I was just looking at my Google Maps after Stewart's questions. Maps are one of the most controversial things. I was just looking at Donetsk, which, rightly, is labelled as being in Ukraine by Google Maps, which is fantastic, or there is a dotted line. How do you look specifically at map policy because it is highly controversial for many?

***Katie O'Donovan:*** It is highly controversial and it is an excellent question I would love to come back to you with a bit more detail because I know there have been challenges with changing borders and jurisdictions. It is something we invest a lot in to get right, but certainly it can be a very lively discussion.

**Chris Bryant:** And Scotland is in the United Kingdom.

**Stewart Malcolm McDonald:** For now.

**Chair:** We will move on from that.

Q137 **Graham Stringer:** You are out of China. You have had a fight with

Australia. Do you think that is the future, that the internet will splinter and there will be different regulatory authorities over the internet in different countries? How do you view that? What is your policy response?

***Katie O'Donovan:*** There are different regulatory environments for the internet already. For example, the European Union created GDPR and data protection. We are a global company with a global mission and we want that to be rooted in established norms. We also recognise that individual countries will pass legislation. What is important is coming back to the principles that guide that legislation and that that legislation protects.

There are challenges to a free and open internet at the moment. That does not mean nothing should happen and that we take no responsibility. Actually, companies like ours can and should take a very great degree of responsibility, and we do. That can be framed and done in conjunction with Governments, and Governments will set their own local legislation, but it is really important to think carefully about what that legislation does for the citizens of that country and also the precedent that it can set for other countries.

We have seen cases where democratic Governments have created legislation on internet policy that has been almost copied and pasted by more nefarious or less democratic states. We need to be careful about that challenge. It is a somewhat unfashionable point to make, but when we create legislation we need to make sure that we are setting a good example globally.

There was a question earlier about the role of the Foreign Office in tech policy, and I think that is a really important role that the Foreign Office can play.

Q138 **Graham Stringer:** It comes back to the very first question I asked. With the Australian situation, you are in direct conflict with a democratic Government that wanted a particular tax regime. How do you deal with that conflict in general? What is your policy attitude to that? I do not just mean Australia but where demographic Governments take decisions that are not within your company's interest.

***Katie O'Donovan:*** I think part of a role like mine is to represent what we think is in the interests of Google and what is in the interests of our users. We can make representations, for example, and think about how the Online Safety Bill might impact us but also impact the wider tech community and our users. In a democratic country like the UK, sometimes our thoughts can be listened to and accepted; sometimes they can be challenged and rejected. Obviously, the Government then go on and shape the legislation and pass it through Parliament. There will be instances where legislation is passed that we find challenging, and if it requires us to do more we will do more. I think there is a difference between requiring companies like ours to do more within the democratic framework, which is absolutely part of the world that we live in, and

something we would not shy away from, and passing legislation that challenges the ability to access and benefit from the free and open internet.

Q139 **Graham Stringer:** I am not sure where the difference is there. Let me pose the question a different way. You presumably pay for opinion polls to be carried out that MPs fill in. Apple, Alphabet, Amazon, Microsoft are all interested in what legislators think of them. What my constituents and I often say is that you frighten me, not you personally but Alphabet and all these huge multinational internet companies, because you can take decisions that take on democratic Governments; you can take decisions that individual citizens find difficult to deal with. What is your answer to that criticism? How can you reassure elected politicians and the electorate?

***Katie O'Donovan:*** I think that is part of the reason why I am here today and part of the reason why we want to engage with legislators. We realise the responsibility we have and we realise the importance that we play in people's lives. People use Google to run their businesses. They use Google to educate their children, or to prepare for exams. They use Google to enjoy and get more out of life. It is really important from a user point of view that we are seen as helpful. We know our users choose to use Google because we deliver against what our products help to do.

We also know that the world of work is changing; the way people make money is changing; and the way people access information is changing. Change is always disruptive, and I think it is absolutely right for you, this institution, the Government and other organisations to challenge and scrutinise us. It is right that we then absorb that feedback, listen to it, calibrate against it, and think, "This is where they've got a point. We could change things. We could do things slightly differently," or think, "Actually, this is what we think is important and we believe in," and we will respectfully make that case, too.

**Chair:** Thank you very much indeed. I think we have covered everything we were hoping to cover. You have been extremely kind with your time. There were a few areas where you indicated that you would write to the Committee. I would be very grateful if you would do that. Clearly, there may be follow-ups and I would be very grateful if you would take those on board.

I note in passing that you were able to cover Google's policy on international affairs and on dealing with Governments around the world without putting at risk any of your staff in many countries. I am slightly surprised that others feel they would not wish to appear before a Committee inquiry when the power of your organisation, and indeed of Twitter and Facebook, is now at least equivalent to or, indeed, greater than most states in the world.

Witnesses: Joe Westby, David Sullivan and Jason Pielemeier.

Q140 **Chair:** Welcome back to this afternoon's session of the Foreign Affairs Committee. We have three new witnesses on this panel. I invite them to introduce themselves briefly, starting with Mr Westby.

***Joe Westby:*** My name is Joe Westby. I am deputy director of Amnesty International's technology and human rights programme. Thank you for the opportunity to speak to you today.

***David Sullivan:*** I am David Sullivan and I am executive director of the Digital Trust & Safety Partnership, an industry effort to create a safer and more trustworthy internet. It is great to be with you today.

***Jason Pielemeier:*** I really appreciate the opportunity to be with you. My name is Jason Pielemeier and I am deputy director at the Global Network Initiative. We are a multi-stakeholder initiative that brings together leading academics, civil society organisations, investors and technology companies to work collaboratively around freedom of expression and privacy.

Q141 **Chair:** Thank you. Are civil society organisations being engaged enough in Government and private sector efforts to counter human rights abuses through technology?

***Joe Westby:*** Thanks for this question. What we would like to see is greater engagement with, in particular, marginalised groups that are often disproportionately impacted by technology around the world. That includes racial justice groups, migrant rights groups and groups in the global south. We have already made submissions to the FCDO about the steps it could take to further support human rights defenders. I am happy to set out and share those recommendations.

One thing I would add on this question is that we have concerns about the corporate lobby power of big tech companies and the influence they have on states all around the world. Recently, there was a major report on the role of tech companies lobbying in the EU, setting out the scale of the investment and efforts to influence EU digital regulation. That is relevant to this question in so far as it exposes a disparity between the extent to which states are engaging with civil society compared to some of the big tech platforms and the inequality of arms between big tech and civil society when it comes to engaging on human rights issues.

***David Sullivan:*** I would certainly say, first, that the kinds of challenges we see at the intersection of technology, foreign policy and human rights are too challenging for any single constituency or stakeholder group to address. I would certainly want to see more collaboration between states, companies and human rights organisations, human rights defenders and the voices of affected communities.

The Digital Trust & Safety Partnership, where I work, is an industry effort. It is a group of companies working together to articulate best practices

for trust and safety online, and then to have an assessment process of those practices.

Across the areas of commitment that our companies have made, when it comes to things like product development, how services are governed, enforced and improved, and how transparency can work, we have articulated best practices for working with human rights groups, civil society organisations and voices from under-represented communities. I would highlight the importance of those kinds of channels for both corporate responsibility and foreign policy in the role of the UK Foreign Office.

Q142 **Chair:** Perhaps I can push this forward, Mr Pielemeier. How much do you work with big tech companies to inform their human rights policies? Have you been engaged in those conversations?

***Jason Pielemeier:*** Indeed. The Global Network Initiative has a set of principles and more detailed implementation guidelines that were developed collaboratively between civil society and tech companies across the information communication technology sector, academics and investors. These seek to guide those companies as they interact with Governments around the world, and to address some of the scenarios that this Committee has heard about in the first panel and previous panels.

It is not only a static set of principles and guidelines but an ongoing conversation that we facilitate among our members, including through a periodic assessment process, whereby we structure an independent assessment of how those companies are implementing the principles and guidelines, which is evaluated by our civil society, academic and investor members. The idea is not necessarily to point out only where companies are falling short in their implementation, but also to identify where good practice exists and can be replicated across different companies, and where opportunities for collaboration exist between these different stakeholders, again recognising the point that Mr Sullivan made about the need for actors to work collaboratively to address the concerning threats in this space.

Q143 **Chair:** Mr Westby, perhaps you would like to pick up on some of that. Have you been co-operating or helping to inform big tech companies?

***Joe Westby:*** I think our role is slightly different. We are a global human rights organisation, and it is very important that we maintain our role as an independent watchdog. We seek to hold those in power to account, and that obviously includes the extremely powerful tech companies.

Having said that, of course, we have open channels of communication to most of the major tech companies. We have frequently spoken to the platforms on human rights issues over the years, and we seek to make recommendations for ways in which they can take steps to improve their

policies and processes to make sure they are more rights-respecting and are in line with international standards on business and human rights.

Q144 **Chair:** We have had some recent exposure to some of the data aspects of control and privacy in Afghanistan, for example, where the US Government, and indeed others, have left data behind, or in some cases actually handed over data of different individuals to organisations that may not—almost certainly do not—share the same respect for privacy or personal safety.

Would there be any avenue for looking at a new way of controlling it, perhaps a Geneva convention for data, so that those signatories to it were responsible for maintaining data privacy as well as the security of cultural objects, for example, or indeed any other of the Geneva rights?

***Joe Westby:*** I think it is a really interesting proposal. It is not something we have investigated in a huge amount of depth. I would obviously have a question mark because, whenever you centralise data, it provides a honeypot target for attackers, be it nation states or others. There would obviously need to be a lot of thought into how that data was held and who was responsible for it, but I would certainly be interested in looking into that further.

Q145 **Chair:** Mr Sullivan, is that something that has come across your radar?

***David Sullivan:*** It is not something we are directly focused on. There are good practices out there. The UN guiding principles on business and human rights were mentioned in the previous session. The practices of risk assessments and human rights impact assessments are things that are not limited just to private sector corporations but, whether it is development organisations, Governments or humanitarian projects, all of these types of projects can be thinking about potential unintended consequences and risks to people's data and safety that could perhaps be mitigated on the front end so that you do not wind up playing catch-up in these very critical situations.

Q146 **Chair:** Is there more that Governments could do, particularly Foreign Ministries, in working with social media organisations and data companies to counter hate speech and disinformation?

***Jason Pielemeier:*** Undoubtedly. The majority of companies operating at scale today see the real challenges and risks that hate speech, disinformation and other types of harmful content present. Many of them are making good faith efforts to try to address those concerns, but there is a real need for stronger collaboration, particularly with countries that respect the democratic rule of law, to ensure those countries are operating in a way that is transparent, responsible and accountable, but also that they are getting the necessary guidance and clarity from Governments as to how they should be prioritising their efforts.

There are differences in different regions and countries as to which issues the public and elected lawmakers want to focus on in any given period

and there are also, unfortunately, countries where Governments seek to use those same legitimate concerns as a pretext to stifle political opposition or to disadvantage minorities. So there really needs to be strong collaboration and co-ordination.

The Foreign Office has taken positive steps over the years. The UK is a founding member of the Freedom Online Coalition, which I believe is now a group of 34 rights-respecting countries around the world that work together, including through a multi-stakeholder advisory network of which I am a part, to promote human rights principles in the online space.

There are lots of opportunities for improvement. Joe mentioned, for example, the need to increase support for civil society organisations, particularly those in the most repressive environments. There are opportunities to bring civil society and industry voices into relevant forums, whether that is the ITU or some of the relevant committees of the UN General Assembly, to ensure their voices and their expertise are represented. I know the UK has done that in the past through its delegations, and there is room for further expansion of that type of facilitation as well as co-ordination with other states on that kind of engagement.

Q147 **Royston Smith:** How realistic is it to expect companies to compromise their market access? It is a contradiction frequently, isn't it, to be somewhere but to have to behave in a certain way? How realistic is it for us to expect companies to give up that market access? What can Governments do to help them bridge the gap of that contradiction?

***Jason Pielemeier:*** That is a really important and weighty question. The reality is that if all the large western, for lack of a better term, technology companies were to choose to avoid operating in challenging jurisdictions, that would create a situation on the ground that might not be better for the types of users and communities that we are all interested in supporting.

At GNI, we work very carefully across our membership to help companies consider questions of both market entry and market exit. Obviously, we are seeing a disturbing trend at the moment of more and more countries moving more aggressively to put repressive measures in place, which can make these challenges more difficult.

You will have likely seen in the news recently the decision by LinkedIn to remove the social networking aspects of its service in China. Earlier this week, Yahoo also announced that it is making its services unavailable to users in mainland China following changes in the regulatory framework there.

On the one hand, we want to continue to support an open, interoperable internet where users have as much access to free information and services as possible—free in the sense of open, not necessarily in the

sense of gratis—but, on the other hand, we also recognise that companies need to make difficult decisions and at times will have to stand on principle.

A good example of this is GNI member company Telenor, a mobile network operator that had been operating in Myanmar for the last several years. It has recently decided to exit that market after the military coup that occurred in February. That is a decision it has made on principle. It has laid out the reasoning behind it, but it has been criticised by many in civil society in Myanmar who saw Telenor providing, compared to other operators in that market, a more trustworthy and more open service.

These are real challenges, and I think the UK Government have an opportunity of working with democratic partners and allies to improve co-ordination with companies that are facing these types of questions, to stand up and push back in a co-ordinated manner against these more assertive and rights-infringing regulatory and policy actions, and also to be understanding of the sometimes very challenging dynamics that companies can face.

Q148 **Royston Smith:** Something that was challenging, I suppose, was the decision of Google and Apple to remove Navalny's smart voting app after pressure from the Kremlin. You have touched on it, and perhaps Mr Westby might want to go first on this. What advice can you give to companies like that? It was a difficult position for them to find themselves in, and in the end they capitulated. What advice would you give them?

***Joe Westby:*** I acknowledge that these are difficult questions, of course. Tech companies find themselves in difficult positions. The tech companies say they are committed to human rights, including of course freedom of expression and privacy. For those commitments to have any value, they have to be applied throughout the company's operations and not only when it happens to suit their commercial incentives. That sometimes means making difficult decisions. We campaigned for Google not to re-enter China's search market because there was no way to do that without being complicit in the Government's surveillance and censorship architecture.

The case you point to is a slightly more complex one. In so far as I understand it, there is the added complication that the local staff members of Google were under an unspecified threat from the Government. Of course, in making a decision, these companies have to be sure that they are taking the safety of their staff into account.

In practice, what this means is carrying out human rights due diligence and identifying ways to prevent or mitigate against harms linked to their conceding to Government demands, but, yes, it does have to be on a case-by-case basis. In that particular instance with the Navalny app, I would like to see a lot more transparency around the decision making that Google and Apple carried out in relation to that obviously very problematic request from the Russian Government, which amounted to

censorship and a clear violation of freedom of expression. I saw that the Google representative on the previous panel did not speak directly on this particular case, and that the other tech companies did not engage, but I think, as a first step, there has to be much greater transparency around decision making.

Q149 **Royston Smith:** What more can the UK Government do to help companies try to counter incitement and hate speech by Governments? Twitter, for example, was temporarily banned by the Nigerian Government.

***David Sullivan:*** The complexity of these issues is increasing very significantly. The authoritarian Government censorship demands we were just speaking about continue to be incredibly important, but the example you cite is one that shows a different trend, which is that, as companies are seeking to enforce the rules for the use of their services around the world, they are running into situations where Government actors or actors affiliated with the Government are the ones that are actually misusing their services, including through things like dangerous speech that could incite violence or information operations conducted by malicious actors linked to Governments or political parties.

Companies are experiencing blow-back from trying to enforce the rules of their services when it comes to Governments. Diplomatic support from the UK Foreign Office, whether it is private, public or through bilateral or multilateral means, is going to be important in trying to reinforce norms that Governments should not be blocking or throttling services or disrupting networks in retaliation for efforts by companies to enforce their rules.

One specific potential path forward that the UK and other like-minded Governments could support is to make the point that the blocking and censorship of services by Governments could constitute a barrier to digital trade and could be part of the trade agenda of the UK and other Governments.

Q150 **Royston Smith:** Where is the line? When is it an attack on free speech and when is it upholding human rights? I know there is a different level, and wherever you are people will see those two things differently perhaps, but what is the line between protecting free speech and upholding human rights in tech?

***Jason Pielemeier:*** I think the international human rights law framework is the best, most comprehensive place to look to answer that question. That framework, which was established in the wake of the second world war, has a generally permissive approach to speech, in the sense that the assumption is that expression should be allowed and tolerated, even if it is offensive or sometimes harmful, unless it fits into certain clear categories that the UN member states have endorsed through the relevant treaties and identified as being appropriate for regulation. Those are areas such as public order and national security. Even then, when a

legitimate purpose is found, the restrictions on speech must be carried out pursuant to law, and those laws need to be developed in an open and transparent manner so that users, as well as anyone seeking to enforce the law, which is sometimes Government entities but increasingly Governments are looking at companies to enforce these laws, know what the rules are so that people can adjust their behaviour accordingly.

Finally, those measures need to be necessary and proportionate, which is to say they must be the least restrictive means possible. There must be a clear articulation of why this particular type of speech is being restricted and under what circumstances.

To get back to your earlier question, in addition to all the things that my colleagues on the panel have said, the UK can also lead by example. The Online Safety Bill is a clear opportunity for the UK Government to demonstrate how a democratic Government can put in place a regulatory process that is consistent with those international human rights principles. There are aspects of the process so far that have been commendable. There are elements in the proposal that also raise significant concern because they may not meet those proportionality and necessity principles. In particular, they may create precedents that make it more difficult for the UK Government in their foreign policy, as well as actors like those of us represented on this panel, to advocate in other countries around the world, to be able to push back on things like requirements to put staff in local offices and make them criminally liable for any perceived non-compliance with the regulatory regime.

We are seeing countries around the world, including authoritarian Governments and nominally democratic ones like Turkey, use those kinds of measures to turn the screws on international communications and technology companies to restrict speech in ways that we see as inconsistent with international human rights principles, and they are pointing to European examples to justify those actions.

Q151 **Chair:** How well are the international principles that guide the ethical practice of companies actually being implemented in reality? What are the main stumbling blocks to the implementation of principled engagement?

***Joe Westby:*** Fundamentally, the main problem is a lack of finding requirements. Voluntary principles and multi-stakeholder initiatives like the GNI are important and can go a long way, but ultimately what we have seen, particularly when it comes to the tech sector, is a clear failure of corporate self-regulation in managing the human rights impacts of their operations. For example, as was alluded to in the earlier panel with Google, a lot of the problems that we are seeing—and we have spoken about hate speech and freedom of expression—have at their root the business model of companies like Google and Facebook, which relies on invasive surveillance of our data and online behaviours in order to track and profile us for the purpose of selling ads.

Currently, there are not enough regulations to hold that business model in check and to really challenge those root causes of the problem. We would like to see the FCDO support a corporate duty to prevent law that holds companies to account when they fail to protect human rights, and that should include mandatory human rights due diligence to identify and prevent harm from a company's operations. That should be all companies, but when it comes to the tech industry it is vital that that kind of human rights due diligence is applied to the core functioning of business models that are themselves driving human rights abuses in many instances.

Q152 **Chair:** Among your members, Mr Pielemeier and Mr Sullivan, are there certain types of technology companies that appear to struggle more in meeting their human rights obligations or that face more pressure from authoritarian Governments?

***Jason Pielemeier:*** Each company faces different risks depending on its business model, its size and the degree to which it has been operating in particular markets for some time. Interestingly, it is not always size that is the leading indicator of risk or the challenge to a company being able to implement human rights principles responsibly.

The extent to which a particular product or service is new and is on the so-called bleeding edge of what is being offered is often where most potential risk may come, because neither that company nor any of the other users or stakeholders in this broader community who are thinking and concerned about these issues has had an opportunity to see how that product or service will necessarily impact the existing power arrangements and risks, and how it may create new risks.

It is important for Governments, as they think about how to support and empower companies to do better in terms of implementing their human rights responsibilities, to appreciate that each company is going to be slightly different in both the risks that it faces and the potential mitigations and solutions that it can put in place.

***David Sullivan:*** Our members at the Digital Trust & Safety Partnership include a range of companies including big social media companies like Google, whose representative was speaking earlier, as well as smaller companies that have a range of products, services and business models, not just advertising but subscription services and e-commerce providers, and they are all struggling with the issues that in the industry are referred to as trust and safety.

We think it is key to take a proportionate and risk-based approach, building on what Jason was just describing. We have started this process of making an industry contribution to these efforts by articulating some best practices and starting a process of self-assessment and ultimately independent third-party assessment to have an objective look at how companies are implementing these practices. We are developing a process of assessment that uses this kind of risk-based approach where

you look not just at the size and scale of a company but also at its particular products and services and the risks that they present, to have differing levels of scrutiny for companies that face different risks. We hope to share and make public the methodology for those self-assessments in the near future, and I would be keen to provide that to the Committee when it is available.

Q153 **Chair:** Thank you very much. We would be grateful to get any supplementary information.

Do you think existing international guidance, such as the UN principles on business and human rights, is sufficiently future proof? There are some gaps that many have commented on, and I was wondering what you feel is appropriate.

***Joe Westby:*** The main gap in the UN principles on business and human rights has been their enforcement in practice. Again, it is my earlier point that these need to be put into binding laws, including mandatory human rights due diligence. That is the first step.

There are some really interesting questions on the framework of the UN guiding principles in relation to the obligations and power of states and companies, because, particularly now with the tech companies gaining power over our digital world and our information architecture, which is really unprecedented, it raises some real questions about the extent to which their human rights obligations should be extended to protecting human rights as well as just respecting them. I think there are question marks on that. That is not necessarily Amnesty's position, but there are interesting discussions to be had in terms of updating that framework for the digital age and acknowledging the power that these companies have established.

**Chair:** Mr Sullivan, I presume your organisation might have some views on this as well.

***David Sullivan:*** This is something I would probably want to talk to my members about before developing a position, but it is certainly a provocative and interesting question.

**Chair:** Okay, we will let that pass. Mr Pielemeier, do you want to comment?

***Jason Pielemeier:*** Joe is right that the guiding principles are only one element. The guiding principles were set up to be a floor, not a ceiling, as Professor John Ruggie, the recently passed author of those principles, put it. The development of the scaffolding and the infrastructure on top of that floor has been slow to date, in particular on the states' side, and I think there is more that can and should be done there.

I would caution a bit against reopening the guiding principles to negotiation or calling for any new sets of guidance or principles, simply because the geopolitical conditions at the moment might not be

particularly auspicious, and I think the guiding principles provide a very carefully and intelligently designed framework that is flexible and can evolve.

The Office of the UN High Commissioner for Human Rights has a project ongoing called B-Tech, which is focused on evaluating and developing further guidance specifically for how the UN guiding principles framework applies to the tech sector. There is some very good work being done there, and GNI is very happy to be partnering with the B-Tech project and others on that kind of work.

Q154 **Henry Smith:** Thank you for joining us today. As companies in more authoritarian countries develop their own surveillance technologies, how concerned are you about the export of those technologies to other countries? What do you think the UK Foreign Office should be doing to address such concerns?

***Joe Westby:*** I would slightly turn around the question, because we have focused more of our research on looking at the export of technologies from countries, including the EU, to states that present a high risk to human rights. I think there is also work to be done in relation to the UK and other western countries' export regulation controls and making sure that those are much stronger.

We did a report last year on the export of digital surveillance systems, including facial recognition technology, to key players in the Chinese mass surveillance apparatus, not from the UK but from companies based in the EU. That was despite the very high risk of those digital surveillance technologies being used against Uyghurs and other Muslim ethnic groups throughout the country.

Similarly, through our work on Pegasus, we have repeatedly pointed to and called for stronger export controls in Israel, which is the home state of NSO, in order to prevent the export of surveillance tech that can be used to target human rights defenders, journalists and others around the world through technologies such as Pegasus.

When it comes to the UK, we would urgently call for intrusion software and other surveillance technologies to be moved into category A of the UK's current trade controls system. We have also called for a moratorium on the use and export of surveillance technologies, particularly given the findings of the Pegasus project, and the extent of the use of NSO Group spyware.

Q155 **Henry Smith:** By mentioning the Pegasus spyware scandal, you have anticipated my next question. Do you feel, and I think I probably know the answer, that the NSO Group has been properly held to account? What are the main lessons that the UK Foreign Office can learn from the Pegasus spyware scandal?

***Joe Westby:*** Indeed there has not been enough done as a result of the findings. The scale and breadth of the harms that were exposed across

multiple countries warrant an urgent response. There has been some progress in various jurisdictions. An investigation was recently ordered by the Supreme Court of India, and there is an investigation in Hungary by the data protection authority, but it is not enough and it is why we are calling for states to support an immediate moratorium on the sale, transfer and use of surveillance technology until human rights-compliant regulatory frameworks are in place.

We need the international community to get behind this call. Of course we would love to see the FCDO and the UK Government support this call for a moratorium, which is backed by the UN special rapporteur on freedom of expression.

In addition, we would like to see the Foreign Affairs Committee use its bilateral relationships with the 11 client countries where we found or it was revealed that NSO had been used to improve domestic regulation and conduct investigations for victims. Again, as per my earlier point, we need to improve export controls and checks. That would be on the client countries and certainly on Israel as the home state of NSO.

You ask what the main lessons are from the Pegasus scandal. One thing we would say is that NSO is one bad actor. It is really the tip of the iceberg. There is an entire unregulated industry providing similar technologies. That is why we need a moratorium urgently, and we would love to see the FCDO support that.

Finally, given it was revealed that UK citizens and residents had been targeted by NSO Group spyware, we are also calling on UK authorities to conduct an immediate, independent, transparent and impartial investigation of any cases of unlawful surveillance linked to the Pegasus spyware, including, where possible, providing remedies to victims.

Q156 **Henry Smith:** Thank you very much for that comprehensive response. Are there any observations or comments from other members of the panel?

***David Sullivan:*** First, this is a clear case of the point made by the other panellists of the importance of Governments like the UK leading by example. The best thing in terms of trying to shape the international environment is to regulate their own domestic industry and to provide an example worthy for other Governments to follow.

I also think this is an issue that demonstrates the potential of coalitions of the like-minded where we can disagree significantly on other issues in the tech policy space. It is fair to say that Amnesty and Facebook, for example, disagree about quite a number of things, but here you have a case where WhatsApp, owned by Facebook, is engaged in a lawsuit against the NSO Group in the United States that has been supported by amicus briefs by both the tech industry and human rights organisations. Let us not let disagreements about one set of issues prevent collaboration and co-ordination across Governments, companies and industry to

address some of these issues that are so critical for human rights around the world.

Q157 **Stewart Malcolm McDonald:** Thank you, gentlemen, for your time with us this afternoon. I am not sure if you were all listening to the first panel with the Google rep, but she told us there had been an increase in Governments requesting censorship or restrictions of some kind of what is online. Just a quick yes or no: does that surprise you?

***Jason Pielemeier:*** No.

***David Sullivan:*** Not at all.

***Joe Westby:*** No.

Q158 **Stewart Malcolm McDonald:** It does not surprise any of you. In response to questions from my colleague Alicia Kearns about map policy—and maps are obviously very controversial—she offered to write to us about that. Do any of you want to offer any reflections? For example, I believe it is the case, or it certainly was the case, that Apple Maps and Google Maps show Crimea as part of Russia, when, in reality, there is an illegal annexation and occupation taking place there. There will be other examples, I am sure. There is a line down the map on Google Maps showing the contact line of the war in eastern Ukraine, for example. It is obviously a sensitive area for tech companies like Google to wrestle with. Do you have any observation or remarks on that particular point? Don't all rush at once.

***Joe Westby:*** We would not have a specific position on that question, I am afraid, but it illustrates a point I made earlier about the power and control that many of these tech companies have over core pieces of internet infrastructure, on which we all rely to enjoy and realise our human rights in a digital age. Really, it just emphasises, if anything, the importance of ensuring that those companies are carrying out their operations on a rights-respecting basis, including in relation to their business model. I would have more things to say on that, but I realise it is slightly tangential to your original question.

Q159 **Stewart Malcolm McDonald:** That is all right. If there is nothing from the other two guests on maps in particular, I want to move on. I hope to hear something positive, and I will start with you, Mr Westby, if that is all right. How are you and your organisation using new technologies to support and protect human rights?

***Joe Westby:*** In our technology and human rights programme, of course one of our main priorities is to hold tech companies and Governments to account when they use technologies, but we also see the value in the use of technology to advance human rights goals. We use technology extensively in our own work. We have a security lab that led a lot of our work on the Pegasus project. We were a technical partner in that project. As part of our work, the lab developed a tool to enable people to check whether or not they had been compromised by Pegasus. That is an

example of the kinds of technologies we have been developing to help activists and others with digital security in order to defend their human rights through the use of technology.

On a different note, we have a long-established project that enables digital volunteers to crowdsource our research and to uncover human rights abuses called the Decoders project. That has been running for a number of years on various different issues, including a recent project to identify, through the help of thousands of volunteers, surveillance cameras across New York City to reveal where people are most likely to be tracked by intrusive facial recognition technologies. There are other—[*Inaudible*.].

**Chair:** I am afraid we have lost Mr Westby.

***Jason Pielemeier:*** I am happy to pick that up.

Q160 **Stewart Malcolm McDonald:** My next question was to both of you, so let's move on to that. If you could talk a bit about how organisations in your network are using tech to protect citizens, that would be really useful.

***Jason Pielemeier:*** First, I want to take my hat off to Amnesty and groups like Access Now, CitizenLab and others, which are doing incredible work, helping both to mitigate risks for human rights defenders and other vulnerable actors in the ICT space but also proactively getting technology out to them that they can use affirmatively to advance their agendas. That is really important work and it is work that I hope the Foreign Office can increase its support for.

To your follow-up question, a number of members of the Global Network Initiative are working both individually and collectively to try to provide technology solutions to human rights defenders and other activists. I will give just a couple of examples. Google has rolled out an advanced protection programme where it has identified users who are at particular risk of being targeted. Those kinds of additional protections might not be necessary, and in some cases they can be a bit cumbersome for regular users, but they are important for users who face hostile state and non-state actors on a regular basis because of the work they do.

Cloudflare, a company that provides content delivery services around the world, has a very unique, bird's eye view of connectivity around the world. It has rolled out a new service called Radar, which helps it identify where services are being disrupted in a very timely manner so that activists and users on the ground can see where perhaps the state may be pressuring or demanding that companies cut network access, for instance, around protests or elections, or other critical democratic moments.

There is a lot of good stuff happening and it is important to underscore that for all the challenges that these technologies have, and the risks that they create, which are real and deserve our focus, there is also a lot of

good use that is being made of these same services, and we need to ensure that, as we work to resolve the challenges and address the risks, we do not create additional burdens or restrictions for the positive use cases.

***David Sullivan:*** As I mentioned earlier, for our partnership, which is a partnership of companies, we have articulated five commitments around how companies develop products, govern their services, enforce their rules, improve over time and are transparent. We have articulated best practices underneath those for how companies can work with and support human rights organisations and civil society organisations. As we examine those best practices, there are going to be opportunities that come out of that and ways that technology can support human rights.

I would add one other thing. I remember years ago, when I was working for a humanitarian organisation, that in training our finance team asked whether our humanitarian NGO was a business. There was silence and then they said, "This is a business, because if you don't treat it like a business you're going to go out of business." I have taken that over the years to mean, when it comes to things like the UN guiding principles on business and human rights and risk assessments, that these kinds of things are just as applicable to efforts, whether it is from Governments or NGOs, to use technology for good to try to anticipate any unintended consequences and mitigate those. I think everybody can take advantage of these kinds of approaches, regardless of whether you are in a company, in civil society or in Government.

Q161 **Stewart Malcolm McDonald:** We will publish a report at the end of this inquiry. What do you think the Foreign Office does well in ensuring that technology is not used in an abusive way as far as human rights are concerned? Where do you think there is perhaps room for improvement?

***Joe Westby:*** Apologies for dropping off the call. I have alluded to a few specific recommendations for the FCDO. I agree with Jason on the importance of supporting efforts to give training and digital security advice to HRDs and activists.

More widely on HRDs, we have been calling for a UK Government strategy to support protection for human rights defenders. Work with HRDs and civil society should be woven into the strategic narrative of the recently formed open societies and human rights directorates.

Aside from that, I have mentioned some of the recommendations already but I will briefly reiterate them. We would love to see the FCDO support a moratorium on the sale and exports of surveillance technologies. We are also calling for a ban on the use of facial recognition technologies in surveillance contexts. Finally, we are also calling for a ban on surveillance advertising to challenge the harmful business model of companies like Google and Facebook, which underpins many of the harms we have seen.

Q162 **Stewart Malcolm McDonald:** Do either of you want to add anything?

What does the FCDO do well, and where is there perhaps room for improvement?

***Jason Pielemeier:*** I would second all Joe's points, but I would add that, having worked previously in the human rights office at the US State Department, I am aware of some of the bureaucratic challenges that sometimes face those who sit within a Foreign Ministry environment whose job is to consistently bring up the challenging bilateral issues that may at their core be about human rights issues. Anything this Committee can do through its oversight and forthcoming report to highlight and underscore the importance of those functions, not just within the FCDO but within the whole-of-Government approach to technology specifically, would be very worthwhile and very important.

The ability to implement things like export controls effectively hinges not only on the right regulatory classifications, as Joe said, but having people sit in the room where an individual export control licence application is reviewed, who can speak articulately and effectively and will be listened to when they present a compelling case for why a particular licence might need to be rejected or limited because of human rights concerns. That is not always easy to do, I can say from experience.

***David Sullivan:*** I would add one to the great points that have already been made, which I would second, and that is the importance of not always trying to reinvent the wheel with new initiatives. There are things that have already been mentioned like the Freedom Online Coalition that can be elevated. The importance of supporting existing efforts is something that merits attention. I would also point to the support the UK Government and the Foreign Office give to the development of industry-driven technical standards. Those can also be places where human rights can be advocated for by the UK Government internationally.

**Chair:** Thank you very much indeed to all three of you for your contributions this afternoon and for your time and insight. I am particularly grateful for your work in supporting so many of the movements that we will need to see succeed if we are to maintain freedom and democracy online as well as offline. Thank you very much indeed. On that note, I am going to close the session.