House of Commons

# Foreign Affairs Committee

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

Tuesday 11 January 2022

Ordered by the House of Commons to be published on 11 January 2022.

Watch the meeting

Members present: Tom Tugendhat (Chair); Chris Bryant; Liam Byrne; Alicia Kearns; Andrew Rosindell; Bob Seely; Henry Smith; Royston Smith; Graham Stringer.

Questions 163-230

## Witnesses

I: Sarah Spencer, Digital Specialist Consultant and Digital Threats Advisor, International Committee of the Red Cross; and Balthasar Staehelin, Director for Digital Transformation and Data, International Committee of the Red Cross.

II: Miranda Sissons, Global Director of Human Rights, Meta; and John Hughes, Global Head of Geopolitical and Economic Public Policy Strategy, Twitter.

House of Commons

# Examination of witnesses

Witnesses: Sarah Spencer and Balthasar Staehelin.

Q163 **Chair:** Welcome to this afternoon's session of the Foreign Affairs Committee, in which we are looking at the effect of technology on the future of the UK's foreign policy. We are very fortunate to have with us Sarah Spencer from the International Committee of the Red Cross. Would you care to introduce yourselves briefly?

***Sarah Spencer:*** My name is Sarah Spencer. I am the Digital Threats Adviser for the ICRC, and I am based in Jordan.

***Balthasar Staehelin:*** Good afternoon. My name is Balthasar Staehelin. I am ICRC's Director for Digital Transformation and Data.

**Chair:** Thank you very much indeed. Ms Kearns, you wanted to make a quick declaration.

**Alicia Kearns:** Yes, I worked with Sarah Spencer in my role at the Foreign Office and in my other work as a civil servant.

Q164 **Chair:** Thank you very much. Sarah, in what ways have new and emerging technologies changed the way the ICRC works? What are the main changes that you have seen?

***Sarah Spencer:*** Technologies have not changed the ICRC's exclusively humanitarian mission to protect the lives of the communities affected by armed conflict and provide them with assistance, but they are really changing the nature of armed conflict and of the ways in which wars are waged in maritime, cyber, space and the means and methods of conflict resolution.

The ICRC remains deeply concerned about the threats and challenges that new technologies pose to civilians and humanitarian operations. We have tracked some of those across the past decade, and we are also exploring ways in which new technologies can help us to improve our reach and the impact of our work, including by helping us to identify missing persons, by analysing large amounts of data, and by providing a digital space to allow people in humanitarian crises to store their most important documents. Perhaps I can turn to my colleague Balthasar to make additional comments.

***Balthasar Staehelin:*** Thank you, Sarah. As we are an exclusively impartial, neutral and independent organisation with a mission to protect the lives and dignity of victims of armed conflict, and to provide them with assistance, we of course look very much at the new digital threats and challenges that technologies pose to civilians, to NGO operations and to the body of humanitarian law under which we operate internationally. It is true that these new and emerging technologies are changing the nature of armed conflict and environments in which the ICRC works.

A couple of issues that we are particularly concerned about—I think much of our discussion today will bring an armed-conflict perspective into the Committee's deliberations—are the cyber incidents affecting civilian infrastructure; I mean mainly, but not exclusively, if they happen in situations of political tension and armed conflict. Criticality of civilian infrastructure is absolutely important. If you think of possible disruption to medical facilities or the interruption of energy or water supplies, those are significant risks to civilian populations that we really have to look at.

We are also seeing lethal autonomous weapons systems that select and apply force to targets, possibly without human intervention. We feel that that loss of human control and judgment raises serious concerns and—I can perhaps come back to this later—really asks for new clear and binding rules on how autonomous weapons systems can be used.

A third point that I would like to mention in my introductory remarks is about information. That has been very much at the centre of previous discussions. It is really about how people can access information and how disinformation, misinformation and hate speech can have important consequences. The difference, of course, is that situations of armed conflict are exacerbated by the vulnerability of the population, so information can really lead to violence in real life. In extreme situations of vulnerability, with people depending on information, it very rapidly becomes survival-critical.

Q165 **Chair:** You mentioned three areas: autonomous weapons or specific forms of weaponry, civil infrastructure, and hate speech. They cover a large area of technology. As you know, we will be speaking to two social media companies later. I do not want to get into the data question, because we will come to that in a second as well.

The question of targeting civilian infrastructure is something that has changed radically. The ICRC—or rather, the Geneva convention—has formerly had target indicators, or target disindicators, as it were, to identify cultural and civilian property that should not be targeted by military conflict. Are there the beginnings of a conversation about civilian infrastructure that should not be targeted by technological conflict?

***Balthasar Staehelin:*** I think civilian infrastructure is already protected under the existing humanitarian law. What we see now is cyber operations against critical civilian infrastructure, which can cause significant economic harm, disruption to society and tension among states. In that sense, we need to address how we implement existing rules under international humanitarian law and apply them when cyber capacities are added to the traditional kinetic way of waging war. I do not know whether Sarah would like to build on that.

***Sarah Spencer:*** I would just echo that and say that the adherence to international humanitarian law should apply to all the new modern domains in which wars are waged, including cyber. In all the policy that is being developed—foreign as well as technology policy—the protection of civilians needs to remain paramount, so that new and emerging technologies that are being developed for national security and defence capabilities must necessarily take into account humanitarian impact. That requires really effective, trusting partnerships between Governments, humanitarian actors and technologists.

Q166 **Alicia Kearns:** Thank you both very much for appearing before the Committee. You touched briefly on maritime, autonomous weapons systems and cyber. Starting with Sarah, can you talk us through the cumulative effect of the many new and emerging technologies that we potentially hear less about, such as quantum, gene editing, nanotechnology, AI and battery storage, and how you think they are shaping conflict and conflict zones?

***Sarah Spencer:*** That is a great question. New technologies in themselves are not necessarily good or bad. What is important is how they are being used in the context in which they are deployed. Most important is to try to think about looking at these new technologies collectively, particularly ones that are coming of age, either at the same time coincidentally or linked to each other, and the context in which they are deployed.

It may not be enough, as you said, to explore the potential challenges and opportunities related to AI, but it is much more insightful to look at the development of AI alongside more affordable and accessible internet access, better battery life and access to quantum computing, particularly what that could do to change conflict dynamics or narratives in active conflicts. For example, bots and more affordable AI could industrialise the production of synthetic media. I am not sure we are in the best position right now to figure out how best to address that trend, should that play out, as a humanitarian community or, more broadly, as an international development community. That is something that is certainly important to watch.

The other really important thing to consider about new technologies and how they play out is to ensure that those developing the technologies are adopting a conflict-sensitive approach. They should be really clear, if they are used and deployed in active conflicts, that they are already identifying the potential harms that the technology could fuel. I will admit that it is very difficult to do so when we are trying to look so far in advance into the future and when it comes to something like technology, but if we cannot conceptualise those harms very specifically, it is very difficult to try to mitigate those risks and put in the right protective measures. I am not sure if Balthasar would like to add anything to that.

***Balthasar Staehelin:*** I would also say that it links to how we use technology. We could not just preach and opine on how technology should or should not be used without taking a very hard look at how the humanitarian actors are also using technology.

In a way, what digital technology inherently brings about is a massive data trend. People used to say, and still do, that data is the new oil, but data at the same time is the new asbestos. It is actually both. What matters is how data is being used. In that sense, we are very much trying to walk the walk but also impress on the humanitarian community in its globality the need to have very strict data protection rules. We have our own rules, which are public and to which we are held to account by an independent commissioner who oversees how we do it. We also try to ensure that the technology sector as a whole applies these data protection standards.

Why is data so important? I think in a country of peace, a breach of data may be essentially seen as an issue of privacy, whereas in a conflict zone, if your data is falling into the wrong hands, it can become an issue of survival, of life and death. I think in this sense we have to reflect on how we use the technology that we have, go beyond it and think about how technology is more generally used: what are the kinds of due diligence requirements that technology providers should apply? In a way, armed conflicts are showing these issues under a magnifying glass. The issues are the same, but they come up against a backdrop of vulnerability. In this sense, they sharpen the issue considerably.

Q167 **Alicia Kearns:** Very briefly, because other colleagues want to come in, within the humanitarian community and when you talk to HMG and the UN, for example, how commonplace is discussion about these new and emerging technologies, and how capable would you say they are in terms of deploying them, defending and understanding them? The understanding piece is the key question for me.

***Sarah Spencer:*** I think the learning journey for humanitarians is early. In some respects and for some agencies, technology is seen as a separate component to the critical work that humanitarian agencies deliver. I would argue that most humanitarians need to gain, at a minimum, proficiency in technological language and capabilities, to better bridge that divide between technologists and humanitarians. Equally, that responsibility falls on the shoulders of technologists.

I have spoken to countless numbers of techno-enthusiasts and optimists who see data-driven solutions or new technologies as a panacea in some ways for the crises and dilemmas that face humanity, including humanitarian crises, without really understanding the ways in which conflicts play out, and the ways in which the humanitarian industry is already addressing humanitarian need and really trying to have problem owners, like conflict-affected communities and the civil society actors who are present in those communities, trying to identify what critical problems could be addressed and supported through the deployment of technology.

**Chair:** Thank you very much.

Q168 **Andrew Rosindell:** Following on from that question, though some of it may have been answered, could you tell us the importance exactly of data protection in a conflict zone or humanitarian arena? Could you take us through why it is so important in that context?

***Balthasar Staehelin:*** To build on what I alluded to, it is that data could be used against the people. It is particularly important that humanitarian organisations ensure that that is not the case. Our whole operation is to protect them, but it is also based on trust. It is incredibly important that humanitarian actors responsibly use the kind of data they collect.

That may be personal data, which is very much at the centre. If you visit prisoners, people talk about the abuse they have suffered. There are also data on, say, observations of the conduct of hostilities by belligerents. There is personal data but also confidential data in the hands of an organisation such as the ICRC. We have to do whatever we can to ensure that the data is not used in any other way than to further the humanitarian impact, and the benefit and trust that must exist with all the affected communities and the belligerents that allow us to operate as humanitarian organisations.

There is perhaps a link to be made with regard to what that means for states. States should strive to ensure that humanitarian data that is collected by organisations is not used for any other purposes. They should not lean on humanitarian organisations to share that data for other purposes, such as security because that could undermine the trust and access that humanitarian organisations enjoy.

That means, of course, that we need to have rules. Organisations have to be very transparent and clear about how they go about it and how to be held accountable. Those issues around data protection in situations of armed conflict are exacerbated by certain technologies. As my colleague, Sarah, said, humanitarians need to become technology savvy to understand where the data goes.

You can't just take any off-the-shelf products and use them. You should know where the data goes and how to protect it against unlawful and lawful access. How do you ensure that an organisation, such as the ICRC, can uphold the privileges and immunities that also shield it in the physical world against any unauthorised access to the data that we have collected?

Q169 **Andrew Rosindell:** It is hard enough to protect data in a normal setting, but how do you approach it in a conflict zone? This must be incredibly challenging to deal with in a war zone or a place where there is conflict taking place.

***Balthasar Staehelin:*** Absolutely, and I think it also affects the kind of technology solutions that we use. We have a very strict policy on biometrics. It is all about going about the use of technology responsibly. You can't just rush into technology without understanding it, without understanding where the data goes and without being sure about the people who can have access to the data—that this is okay with regards to the category of data. Is it confidential? Is it public? Is it very confidential?

It means there are limits to technology. We have quite an elaborate approach to cloud solutions, which ensures that confidential information does not go on public cloud solutions, because we cannot get the assurance that we need on controlling the data. Without going too much into the technological solutions, it imposes upon us a very rigorous look at how technology actually plays out, how you ensure that you master it, and forward-thinking about the implications for people. Humanitarian actors should do that, but technology providers should do it too. If they go into a conflict zone and deploy their tools, we can expect them to give consideration to what the impact of that technology could be in a situation of acute vulnerability.

Q170 **Chair:** The challenge of data control in conflict is one that we saw recently in Kabul, where the UK Government was accused of having lost control of some of its data—and, indeed, there are other parties who may have left some documents behind. Has there been any consideration given to adding protocols to the Geneva conventions on the security of data?

***Balthasar Staehelin:*** I am not aware of that being regulated at the level of the Geneva convention and additional protocols, but in terms of the practice that we develop and deploy, both as humanitarian actors and as states, we need to give very serious consideration to any kind of technology and how it could involuntarily cause harm to civilians. However, I am not aware of an attempt to regulate the issue of data through an additional protocol to the Geneva convention.

It is important that we talk about the Geneva convention and the digital space, and that we clearly delineate the fields that the people who propose a digital Geneva convention would like to be covered. We do not need a convention that covers a field that is already covered. As we mentioned earlier, attacks on civilian infrastructure are already banned. Attacks against civilians are already banned regardless of the means used to cause that harm.

This is partly about reaffirming the key principles and tenets that are absolutely vital to the protection of civilians and are proven over time, and ensuring that they are applied, but we should also start to unpack new digital threats that may require new measures, and that is what I alluded to when I talked about autonomous weapons systems. We feel that we have one path where current rules do not provide sufficient clarity and protection, and we hope that countries such as the UK, which take a leading posture in thinking about the protection of civilians, can play an important role.

**Chair:** I get your point on digital weapons systems as a different form of technology, and we will be coming to elements of that in a moment. May I push you on the security of data? I must be clear that I do not just mean the security of the data that you collect—on prisoners, displaced persons, or whatever the ICRC happens to be working on—but the actual security of data within a structure in the community, and its position in the conflict. Quite rightly, we have any number of protocols on the use of various weapons, including chemical, nuclear, biological and so on. Given the weaponisation of data and information in recent decades, it would seem that this is a new form of weaponry that can do equal and perhaps in some ways greater harm than some initial triggers; it can divide communities and lead to extreme violence.

I take your point on civilian sites requiring a clarification or an emphasis, and on adjusting the protocol to clarify that targeting a place of worship, a dam or whatever includes not just direct physical attack, but technological attack. Is there not a place for an extra protocol on the security of data? I don't know whether Sarah would like to express any views.

***Sarah Spencer:*** I have a broader question around data protection that I think is relevant to the Committee, so I will leave commenting on an additional protocol on data protection to Balthasar.

If you take a helicopter view or back out of the question around data protection, there is a really important question for the Committee to ask: why is the data being collected in the first place by humanitarian agencies? If you argue that there are hundreds of millions of people displaced by conflicts and crises or in need of humanitarian assistance, you could equally argue that hundreds of millions of people are having their personally identifiable information collected by a range of agencies. What measures are needed to protect that data?

I guess a conversation should be happening between the donors that fund humanitarian agencies, as well as the agencies, about what data it is absolutely necessary to collect, and for what purpose. Some of that is about accountability of ODA spend. Some of it is about trying to verify that one person is a family member of another person. Unpacking that is a knotty problem, but it is one that deserves a bit of attention. The complexities around that problem are part of the drivers for the data race—this race for increasing amounts of data. Equally, there should be some measures for deleting and removing data, and there should be guidelines that say, "When the data no longer serves the intended purpose, we in the humanitarian community agree that it will be destroyed." It is about embodying that right to be forgotten.

***Balthasar Staehelin:*** I would be happy to build on that. The ICRC President Peter Maurer has convened a global advisory board on the international legal and policy framework to protect civilians from digital threats during conflicts. That will bring people with different perspectives together—Government representatives, tech representatives and academics—and they will try to unpack exactly the kind of questions that you just raised. They try to identify whether there are gaps in the regulatory framework that we need to close, and how we would frame it afterwards. That board is trying to think about these digital threats you alluded to, and the way data is possibly used against people is an important dimension.

Q171 **Bob Seely:** If you don't feel able to answer my next question, that is fair enough. I hear what you are both saying; it is very interesting. I am just thinking about how what you say applies to recent conflicts. I am wondering whether you have any insights on how the use of data, either in refugee camps or among fighting groups—paramilitary or militant groups—worked in a place like Syria, where you had an awareness of digital security. Quite a lot of people did not like the regime, which was quite totalitarian in its nature. You also had refugee camps, and not only was there word of mouth going around those, but quite a digitally literate younger generation.

***Balthasar Staehelin:*** I am not sure we would like to delve into specific contexts, but one of the issues we are particularly concerned about, in terms of how technology creates a risk, is around misinformation, disinformation and hate speech, where we see manipulation that exacerbates hate. That can lead to physical violence against people. I would say that the issue of misinformation, disinformation and hate speech seems almost a greater risk for civilians than the misuse of data, which is very important, and which we are trying to address in how we manage our own data.

Data that falls into the wrong hands could lead to people being targeted. It could lead to oppression, killing and discrimination, but I would say that this data, be it humanitarian or from other stakeholders, creates very important risks. We humanitarian actors need to start to manage our own data in the most responsible and transparent way possible. Our president recently said that misinformation, disinformation and hate speech are one of the biggest problems characterising our conflict. That is almost an equally important concern for me.

**Bob Seely:** Thank you.

Q172 **Royston Smith:** Talking of misinformation and disinformation, to what extent are social media giants responsible for having policies that protect affected populations from hate speech, misinformation, disinformation and other forms of incitement to violence?

***Balthasar Staehelin:*** Sarah, do you want to take that?

***Sarah Spencer:*** Sorry to rephrase the question, but were you talking about the social media giants and their policies for protecting conflict-affected populations?

**Royston Smith:** Yes.

***Sarah Spencer:*** I cannot speak to the specific policies that they have and employ. I would say that there does seem to be a trend, similar to Government, where we tend to fight the wars we have already fought—we tend to build battle plans for the wars we have already fought. There is a real need for us, in the future, to look at how new technology and the increasing availability and ubiquity of data can create and industrialise synthetic media—or industrialise MDH in ways that we have not yet seen.

I would question whether the policies that exist today with regard to the—*[Inaudible.]*—and technology firms writ large are sufficient to address that future threat. There is the fog of war and the fog of information; the information environment has been a critical factor in how conflicts play out for hundreds of years. What is different now, and what will be different in the next several decades, is how technology can make it far easier—and with far less cost, both human and financial—to really shift conflict dynamics and narratives in favour of some or all parties to the conflict. It would be interesting to hear how social media companies and technology firms are looking ahead at how their technology may play out in future conflicts.

Q173 **Royston Smith:** I do not expect you to know the ins and outs of their policies—I would not dare to ask—but what accountability mechanisms do we need for big tech companies? I do not know what their policies are either; perhaps we will get more information about that in the next session. What do we need to do?

***Sarah Spencer:*** With regard to regulation, the ICRC is really concerned about the risk that MDH creates for the security and fundamental rights of populations affected by armed conflicts. The ICRC would encourage the UK Government—and all states—to take measures to ensure that information or influence operations are carried out in line with, or compliant with, IHL, and to ensure that technology firms in conflict settings take a conflict-sensitive approach to the deployment of their technology. I would be curious to know whether they do—not just from a human rights perspective.  I would also be curious about whether they have conflict experts in their teams and organisations, in the same way that the FCDO has conflict advisers looking at whether interventions abroad are conflict sensitive and not inadvertently increasing harm to conflict-affected populations. A similar approach could be taken with technology firms and social media giants, I would suggest.

***Balthasar Staehelin:*** The ICRC engages in a dialogue with a number of these tech actors. There is an interest on their side in adding a specific armed-conflict perspective into their thinking and practice. Clearly, the debate for us is around doing business in a conflict-affected environment. That brings about an enhanced responsibility, because the population has a vulnerability that makes it different from the population in a country that is at peace. That means also understanding the context. How do you follow what happens with your tools? Do you speak the local language? Do you know the local dynamics? How much do you invest? How do you react? In previous panel discussions that I listened to, I heard a lot about the transparency around the effort; I found it very interesting that these companies are very clear about how they go about deploying their technology to new conflicts and how they lift their due diligence. They are quite transparent about the balancing act that they undertake in these conflicts. I think that would already be—and is, where it has been done—an important step in the right direction.

Q174 **Royston Smith:** You mentioned that tech companies have an enhanced responsibility; I think that most of us would agree with that. Do you think that they live up to that responsibility?

***Balthasar Staehelin:*** I think it is difficult to give a one-size-fits-all answer. I would answer with the question, do we have all the necessary data and transparency, in terms of how they go about it? Many of these companies have an interest in finding the right approach, but it will require far more debate and scrutiny between lawmakers, local actors and these organisations to come to a conclusion on where they feel that they are.

Are they in the right place, in terms of these trade-offs? Where do we feel more needs to be done?

Q175 **Royston Smith:** Finally, do you think there is a contradiction between what they say and what they actually do?

***Balthasar Staehelin:*** Sarah, did you want to come in?

***Sarah Spencer:*** Perhaps this is an answer to your question, but I was going to say that it is important to remember that in responding to conflict, humanitarian agencies are doing so as part of a broader humanitarian mandate that is rooted in international humanitarian law, protected by the Geneva convention and focused on neutrality, impartiality, independence and humanity. It is really about protecting lives.

That is not the vision or the main ambition of technology companies, nor do I think they purport to uphold that. I suppose the challenge for regulation is trying to work out how to bridge the difference in the mission statements between technology firms and humanitarian actors. They do not have mutually exclusive, clashing or competing visions, but it is not necessarily the same vision.

Q176 **Chair:** Thank you very much. Can I go on to the question of values? One of the key roles that the ICRC has had, and indeed the Red Cross has had since its foundation over 150 years ago, is trying to bring values and a certain order to areas of chaos and conflict. Clearly, this raises a lot of questions when we look at the development of technology.

Mr Staehelin, you have already mentioned the question of artificial weaponry of different kinds, and Ms Spencer, you have spoken about various different forms of technological change. How do you see the injection of values into technology? Do you see ethical considerations being conducted in any way by different organisations? Do you see it either in the arms makers, which are going into autonomy more and more, or in the technology companies that are designing the systems on which they run?

***Balthasar Staehelin:*** It is a very broad question because of the number of stakeholders that you mention and how they would relate to values. That makes it difficult to give you a pertinent answer.

If I may bridge to the issue of autonomous weapons, it is important that we believe in human control of technology and policy, with all its faults. Human control does not mean that people come down on the side of values and do the right things, but we believe that elements of human control are very important. That informs our stance on one important technology that is emerging—autonomous weapons.

We feel that unpredictable autonomous weapons systems should be expressly ruled out, because it is human control that allows values and, hopefully, the right decisions to be made, which would be in conformity with IHL. Play out should be ruled out, which is why, for instance, people have said that autonomous weapons systems should not target people—

human beings—and that, when we define the use of autonomous weapons systems, we should have a combination of limits on types of path, duration, geographic scope and situation of use.

I give that as an example to say that the human element, underpinned by values, must remain a dominant force in the way we use technology. What I say here about autonomous weapons could probably be transposed to other emergent technologies that we may not even know yet. The question is whether we just let them out in the open and see what happens or whether we feel we need to keep that human control and the values that we hopefully share. On some values, we may also disagree, in terms of how they are implemented; look at the state of the world and how belligerents behave in different parts of the world. That is a debate that will need to go on as technologies of which we are not even aware yet emerge and provide and represent new challenges.

***Sarah Spencer:*** I will add two points, if I may, on the issue of ethical principles and regulations. One is that the established humanitarian principles are really important, and they do not only apply to humanitarian actors. Technology companies could easily integrate those into their work, codes of conduct and ethical frameworks as a critical component of how they do business and their due diligence processes for where they do business and whether they should engage in business in fragile or conflict-affected areas. The issues around impartiality, independence and neutrality are really interesting when you think about social media and how social media tools play out in conflicts today and in future conflicts.

The other point to raise is that, particularly in conflict-affected areas, domestic legislation and the regulation of new technologies may be embryonic or non-existent, and equally, not entirely enforceable. While it is incredibly necessary for technology companies to think about the impact of their new tools and systems and how they use data and how they deploy their technologies in conflict-affected scenarios, the accountability angle of that will be a challenge, given the actual nature and operating environment in which humanitarian agencies operate.

Q177 **Chair:** Thank you very much. On the ethical principles that relate to the technology that shapes the Committee’s work, how do you have the discussions on the legal points that go into it? Do you have an ethical team within your organisation? How do you approach it yourselves?

***Balthasar Staehelin:*** The most mature part, in terms of the kind of policy that we have set, revolves around data protection. It may sound a little bit technical, but as I tried to underline earlier, data protection and the way we manage data are very much at the heart of many of the vulnerabilities that we see in our use of technology. In this sense, through the data protection angle, we capture most of the risk that the use of technology could represent for the people we try to protect and assist.

Beyond that, we also have an ethical committee that grapples with typical operational ethical dilemmas that may be linked to new technology or to other issues. We try of course to have an ethically responsible approach to our work. Our work is based on trust. We go to war zones, we cross frontlines, we speak to states, we speak to nearly 500 non-state armed groups. We need all these different belligerents, stakeholders and communities to accept our work, and that means that we have to be extremely smart about how we can best ensure not to inflict any harm and to really have a positive humanitarian impact according to the principles of impartiality—serving as per need—independence and neutrality.

In foreign policy in a broader sense, to connect this to the work of your Committee, we will need to think collectively about the long-standing principle of humanitarian action of doing no harm. We probably have to rethink it to include doing no harm in the digitised world and what that actually means, and then to transpose it. I think the principle stays the same, but the questions that it triggers are very new; they are emerging as we speak. Clearly, we will need to grapple with them for years to come.

Q178 **Chair:** Talking about technologies in a wider context, one of the things that has become increasingly clear is the gap in technological ability between different states or different armed groups. For example, if you look at the Armenian-Azeri conflict, the Ethiopian conflict or, indeed, the Ukraine-Russia conflict, you can see major technological gaps between parties. How do you see the effects of that challenge in your work and the ability of the international community to maintain at least some norms, such as those set out in the Geneva protocols?

***Balthasar Staehelin:*** I do not think we would comment on the imbalance of means between belligerents, and who has the best technology. That would not be within our remit. What we would be most concerned about is how these technologies, when they are used, are impacting civilians, the ones who do not actively partake in hostilities. Our key concern is ensuring the protection of civilians, the wounded and those who are detained and do not actively partake any longer—prisoners of war and so on—so that these protected categories remain as well protected as possible in spite of the addition of new ways of waging war.

One dimension that comes to mind is again the issue of civilian infrastructure. How can we ensure that civilian infrastructure remains standing in a world where cyber-attacks become a very potent way to disactivate them? Often the civilian and the military use of such infrastructure give rise to debate in some states. They would argue that the capacity is also used by the military, and we are in very important policy discussions in which we need to be absolutely sure that we do not flippantly forsake the essential services for the civilian population that need to be preserved in situations of armed conflict.

I understand that your Government is building cyber-capacity in growing economies and that is an interesting avenue for looking at the resilience of critical civilian infrastructure. Perhaps it needs to be more defendable and separate, where possible, from any military use to reduce the argument—which I personally take issue with—that because it may be dual use it can be taken out. There is an important issue around how we can ensure that in tomorrow's wars, which may be kinetic and cyber in a mixed way or in grey zones where we may not even know whether there is a conflict happening and how it will play out—we may be in murky waters—what should be our obsession is what it means for civilians and how can we ensure that critical infrastructure remains standing.

Q179 **Chair:** Looking at what the British Government are doing, you have already mentioned autonomous weapons. Perhaps, Ms Spencer, you might like to touch on this, given your prior experience with the British Government and perhaps your greater understanding of what the British Government are doing. You may be following it more closely. How do you view the work that the FCDO is currently doing to promote and defend vulnerable populations from the abuses of technology? Where do you think we are doing well and where do you think there are gaps?

***Sarah Spencer:*** I think all Governments should be doing more to think about how technologies are fomenting conflict and playing out in areas of conflict, and how the humanitarian sector as a whole could be using technology to improve impacts—deepen or broaden the scope and the scale of humanitarian action, as well as mitigate those risks. I think we are in the early stages of those conversations, and making sure that we better integrate the development of new technologies, which tend to sit in national security and defence circles, so that they are equally brought in to the development, ODA and humanitarian parts of Government, to make sure that there is more joined-up discussion.

Equally, we need to ensure that in those national security and defence conversations there is a humanitarian voice and someone there to ensure that recommendations on cyber-security capacity building, or cyber-governance efforts with partners, are conflict-sensitive and primarily prioritise the minimisation of harm to civilians. I think we are still in the early days, and more could be done. The British Government are leading some really notable efforts to that end, but this is a fast-moving agenda, and the ways in which technologies are evolving and conflicts are playing out against a backdrop of rapid geopolitical transitions and changes means that it is really worth improving the joined-up conversations and problem solving of Governments.

Q180 **Chair:** How do you think the FCO could be working more with tech companies to change the way in which this is being achieved?

***Sarah Spencer:*** There are some really interesting movements on the part of technology companies increasingly to influence foreign policy and engage in what used to be the sole sphere of development and humanitarian efforts that, as we have previously said, had a very focused mandate: on poverty reduction if you are in the development world, and—crudely speaking—on life-saving humanitarian assistance if you are on the humanitarian side. It is interesting to see technology firms move into that space and partner increasingly with member states to play a quasi-duty bearer role in those contexts.

I think those conversations need to be thought through very carefully on both sides, and Governments need to be clear-eyed about the incentives that corporations may have in conflict and non-conflict environments. They are very open and frank about those priorities and those visions, and the FCDO—as well as other Governments—is probably in a good place to broker some very good conversations between technology firms, humanitarian actors, civilian actors and states to think about ways to amplify and capture the real benefits of technology to accelerate progress against the sustainable development goals, or improve access to humanitarian assistance. That starts with having proficiency in our different languages and understanding one another's industries, world views and perspectives, but I think Government could be a good convener for that conversation.

Q181 **Chair:** Thank you very much. The last point I was going to ask about was about other Governments. Whom do you think the British Government should be learning from? If you look around the world and see who is engaging in the defence of data, or rather using data as defence—both ways, perhaps—which Governments are doing well? We hear about tech ambassadors from countries such as Denmark. Are they particular examples, or are there others you can think of?

***Sarah Spencer:*** I am not in a particular position to comment one way or another on the capabilities or expertise that other Governments lend, only because I have not really looked into it, but I can say that from a humanitarian perspective, it is nascent. It is very nascent, and there are some interesting partnerships happening between tech firms and humanitarian organisations directly that are helping to test and trial safe ways to use technology, to increase access and to improve impact. Those are funded and supported by other nation states—those in Europe particularly—but I could not speak specifically to the foreign policy-type policy agendas of other nation states, I am afraid.

***Balthasar Staehelin:*** I could perhaps add that on our side, of course, we really believe that in order to understand conflict dynamics and all the relevant actors that have a direct impact on the situation of civilians on the ground, the big tech companies will now be natural partners for dialogue and engagement for the ICRC. They have influence in these contexts, and we need to engage with them because their behaviour can have an impact on the situations of people. Since 2018, we also have an ICRC representative in the bay area to engage with America-based companies, but from an ICRC perspective, we really want to enlarge that dialogue to tech companies. I went to St Petersburg and had engagement with Russian tech companies, and I think we will want to engage with Chinese tech companies.

From the ICRC's perspective as an organisation, we need to understand how the technological landscape evolves and how the digital risks evolve. We need to understand the different perspectives, and we need to try to influence and engage with different companies that, via their technology, will probably have an increasing impact on the situation of the populations that we try to protect and assist.

This is a learning process. I would not be able to point now to one country that has found the optimal way of doing this, and I feel that is also the advantage of being able to exchange and learn from each other and find the best ways. But it is true that tech companies—through their transparency, the accountability, the data minimisation, the way they handle personal data, the way they improve their practices, the way they live their due diligence, which is enhanced in conflict zones, and the way they walk the talk on corporate responsibility—will be important partners to ensure that populations in a situation of armed conflict have the best possible protection in the decades to come.

Q182 **Chair:** Thank you very much indeed. You raise interesting challenges. May I express personal thanks for the work of the International Committee of the Red Cross in conflicts around the world? My first encounter with you was in Yemen in 1995—a while ago. The work that I have seen you do around the world has been pretty phenomenal—what you have achieved. Thank you very much for that. Thank you for appearing before the Committee this afternoon. If there are areas that you think of in the coming days that you think we should be thinking about, I would be very grateful to hear.

***Balthasar Staehelin:*** May I express our deep gratitude to the UK Government, the UK Parliament and the UK people for the strong support that they have traditionally provided to the ICRC, both financially but also by upholding and striving to improve international law and make it a relevant and strong body of law? Thank you very much.

**Chair:** Thank you very much. We shall move straight on to our next panel of witnesses.

## Examination of Witnesses

Witnesses: Miranda Sissons and John Hughes.

Q183 **Chair:** I would be grateful if you would briefly introduce yourselves with a name and a brief description. For simple reasons of alphabetic appearance, Mr Hughes, why don’t you kick off?

***John Hughes:*** Thank you for the opportunity to be here today with you all. My name is John Hughes; I am the Global Head of Geopolitical and Economic Public Policy Strategy at Twitter.

***Miranda Sissons:*** Good afternoon, Chair and Committee members. My name is Miranda Sissons and I am Director of Human Rights Policy at Meta. I am from Australia, and I lead the team that has responsibility for creating and implementing our human rights policies. I joined Meta two and a half years ago, after a career as a human rights defender, transitional justice advocate and diplomat. I have also worked in social impact tech.

Q184 **Chair:** Thank you. Mr Hughes, how does your company view its global role when it comes to matters such as protecting privacy and human rights? Where do your responsibilities end and Governments' responsibilities begin?

***John Hughes:*** Thanks for that question; I think it is a really important one. Twitter's purpose is to serve the global public conversation and that is what we are focused on every day. What we do as a company is this: we enable people to have a voice online, and we want to make a conducive environment around the world to make sure that as many people as possible are able to do so. The responsibility does not just lie with us, of course; this is why we published an open internet paper last October, in which we talked about many of these issues. In particular, the one that I would highlight is that we think it is quite important that the private sector and Governments work together on these issues, and in particular on creating a regulatory environment that allows for that speech to happen online.

Q185 **Chair:** Ms Sissons, how would you answer that?

***Miranda Sissons:*** Obviously, similar to Mr Hughes, our company's mission is voice community and social impact. We apply and seek to uphold our responsibilities through applicable law, our terms of service, the UN guiding principles on business and human rights, which are the UN rules that relate to human rights conduct by companies, and also by our corporate human rights policies. We seek to express those through a variety of different rule sets in the organisation, including our content policy.

Q186 **Chair:** Thank you. You both have huge control over how people across the world communicate with each other, and over the kind of information that they are able to access and share. How comfortable are you with being put in the position of having to make decisions that would typically be the responsibility of Governments? May I start with you, Mr Hughes, and with this specific example? Former President Trump cannot tweet, but Ayatollah Khamenei can tweet. That is quite a political decision. How comfortable are you with making such decisions, rather than leaving them to Governments?

***John Hughes:*** Thank you for the question. Of course, that is something we certainly do not take lightly. That is why, as my Facebook colleague has mentioned, we have a number of rules in place on the platform, including our terms of service, which we enforce every day—we have people focused on these issues 24/7 around the globe.

In answer to your specific question, we do think that it is important for people to hear what world leaders, in particular, have to say, and for citizens to be able to hold their Governments to account. We think this is quite important, which is why we err on the side of keeping tweets up in that sort of situation, particularly if a world leader is speaking to other Governments around the world. We think it is quite important that people are able to hear those comments and respond to them. In answer to your question, that is how we look at it. I am happy to go into more detail, if you would like.

Q187 **Chair:** Perhaps you might go into a bit more detail. It is one of the areas where traditionally a Government would have a view. Some people in the United Kingdom will remember that in the ’80s a rather unwise policy was followed whereby members of the IRA—a terrorist group operating in Northern Ireland—were not allowed to have their voices broadcast, so you would see an image of Gerry Adams speaking, for example, and there would be a voiceover. Clearly there are other ways in which people can communicate—Twitter is not the only site—but it is interesting that such decisions on silencing or hearing individuals would traditionally have be taken by a Government. I am thinking specifically of democratically elected Governments here. This decision has been taken by Twitter, and indeed Facebook—I mean Meta; forgive me—has taken similar decisions in slightly different ways. Up to where does your responsibility go, do you think?

***John Hughes:*** Let me go into a bit more detail. First, as I said, as a private company we do have in place terms of service, which we enforce on an ongoing basis around the world. Almost a third of our company is focused specifically on this issue, looking at tweets that might violate our rules. If we find that those tweets do violate our rules, we take action, and this is really one of the highest priorities for our company.

That said, on issues such as world leaders, frankly, we don’t think that this is something we should be doing on our own. In fact, we think that there is a role for Governments and others. This is why last year we launched a public consultation on this very issue, where we asked people—experts, NGOs, civil society, academics and others—to comment on our world leaders policy and how we should proceed with it. We are currently in a process of looking at those answers and at how our policy should react to those, but there are a couple of points that I should make now.

First, it is quite important that when you look at something that is in the public interest, in our view—and we saw this clearly in the survey—that should be not just be focused on world leaders; I think public interest is a broader term, so that is something we should take into account.

Secondly, we think it is important to be transparent about our decisions—why we take them, when we take them and what the consequences are. This is something we are quite focused on as a company. For example, we publish blogs all the time that talk about these different issues and how we approach them, and this is an approach that we will continue to take.

Q188 **Chair:** Ms Sissons, I am going to press you on a similar issue. I know that a few years ago you set up a board that was designed to make some of these decisions. These decisions that come under your terms of service and are effectively decisions of your own—they are not Government requirements to accept or to silence some people; they are decisions taken by Meta, its board and its staff—are these not the decisions of a publisher?

***Miranda Sissons:*** If I can briefly touch upon your previous question, we do take our responsibilities very seriously, but we are not comfortable with the roles that we are currently playing. That is why we have supported and continue to support regulation and developing regulation that is aligned with human rights standards across many of these questions.

Indeed, the application of our rules to any individual, including a Head of State, is based on whether or not that person has breached our policies. There are a variety of policies, including content policies, that seek to uphold norms of international law. Freedom of expression is not unlimited, although there is a great deal of discussion about where those limits actually lie. That is why, in enforcing these policies, we did so on the basis of the content of the speech in question and referred that to our oversight board, which made decisions and recommendations based further on international human rights norms.

Q189 **Chair:** I get your point. Forgive me; our focus is very much on the foreign affairs aspect of this and the impact it is having on foreign policy, as I am sure you will understand. The tricky thing about this is that your reach is not national, almost by definition; it is much greater than that. I do not know how many active users each of your sites have, but it is numbered in the hundreds of millions, if not billions, rather than in the normal realm of a nation state or citizenry, so we are not dealing with the normal application of law.

Many countries already have laws that cover what you can and cannot broadcast and the ways in which you can communicate. The US first amendment is a particularly famous example, but there are many other different examples around the world. I know Australia and the UK have their own versions of it.

The challenge we have got is that the decisions you take as a company have quite major foreign policy implications. I mentioned earlier Ayatollah Khamenei of Iran, who some people may support and others may criticise, but he has made on Twitter, and no doubt on other platforms as well, statements in Persian and sometimes in English that, politely put, are incendiary and call for acts of violence against groups or targeted individuals around the world.

I hear your point about world leaders having views and their people having a right to hear them, and clearly democratic accountability is an important aspect of what we would see leadership to be. However, once you have taken the decision not to recognise the first amendment rights of a former President, why should another President, or Head of State in this case, have the authority and the ability to communicate in ways that are problematic? This raises a challenge. I know both of your companies call themselves platforms, or variants on that description. Are you not just publishers, and therefore should you not just simply be bound by the publishing laws, or the broadcast laws, that apply to the jurisdiction in which you operate?

***John Hughes:*** Thank you again for that, Chair, and I really appreciate you focusing on this very important issue. I will just say a few things. I already told you what our world leaders' policy is and that we are looking at that now, and we are happy to follow up with you and the Committee as we continue to do so.

The second point is that, as my colleague from Meta already said—this is true for Twitter as well—human rights are fundamental to our platform and to having free speech on the platform. This is quite important to us, and we understand that this does not mean unlimited speech, and that sometimes there are problematic issues on the platform that we have to address. This is why we have, like I said, our terms of service. This is why we have multiple channels for Governments, law enforcers and others to raise issues to us. This is also why we are proactively looking at technological and other issues so that we can identify abuse on our platform without people having to raise it with us.

I would make a broader point here: going back to the open internet paper that I mentioned earlier that we published back in October, this is something where we really think that Governments, the private sector and others all need to work together to come up with global norms and standards. In particular, if you look at laws in places like the UK and elsewhere, that could be working on implementing laws that protect free speech, that look at abuse but that also have adequate safeguards in place. Quite frankly, Governments around the world are looking at this. We are continuously seeing concerning trends in countries around the world where they are attempting to force us to make content decisions through potential internet shutdowns, throttling of our service and things like that. That is why I think it is really quite important that we as a company continue to engage on this, continue to advocate against these sorts of policy and continue to advocate for the open internet. But we think it’s quite important also to work together with Governments, in the UK and elsewhere, to set those norms, so that others will see that and be able to follow behind.

Q190 **Chair:** Ms Sissons, the challenge we’ve got here is that, to come back to the point I made earlier, many nation states have already made these decisions. The challenge that Meta has is that it operates across jurisdictions. Which jurisdiction is supreme for you?

***Miranda Sissons:*** Chair, I think there are perhaps two or three points I would like to raise. First of all, you alluded to a number of different actors, as we call them—individuals active on the platform. We make our decisions around the content of those actors based on our policies and rules, which are developed with extensive expert and civil society input, and with strong reference to human rights law, and also obeying applicable sanctions law. I think it’s important to convey that.

Secondly, we do seek to fulfil our terms of service and applicable law in jurisdictions where we operate, but rule making around the internet—and particularly about social media, as a form of technology—is in its infancy, and that is why we have sought to call for regulation and support regulation in this area.

Q191 **Chair:** I do understand that, but China’s regulation is not the same as the

US's regulation, and therefore calling for international regulation is not quite the panacea that some may believe. Indeed, the difference in concepts of free speech even between the United Kingdom and the United States—two countries that have a very long tradition of free speech and indeed civil rights—means that this is a very difficult decision. Forgive me; I don't mean to gloss over it. This is a very difficult decision for platforms like yours that operate on a cross-jurisdictional basis. But the challenge surely remains. If you are going to operate on a cross-jurisdictional basis, which you do, because that is your business model, you have to work out ways in which you obey national legal requirements. You also have to work out ways in which you have responsibility that is different from Governments'.

So may I ask a slightly different question? To whom are you accountable? Are you accountable to Governments, the democratically elected—in the best circumstances—expressions of the sovereign wills of sovereign peoples? Are you answerable to your users? Or are you answerable to your shareholders?

***Miranda Sissons:*** At the heart of your question is how we handle the protection of freedom of expression, privacy and other key human rights internationally. It is very important to let you know that there are essentially three key pillars that provide and guide our behaviour globally. The first is that we are a long-standing member of the Global Network Initiative, which we joined in 2013. That is an information and telecommunications sector multi-stakeholder initiative that includes telecom companies like BT or Vodafone, Meta and other companies—Microsoft, for example—academics, NGOs and others. The companies that join commit to upholding freedom of expression and privacy according to the world's leading human rights treaties, and they have specific implementation guidelines globally and also in what they call difficult jurisdictions.

Company members are assessed against how they operationalise those requirements on a regular, periodic basis. We have been assessed twice and will be independently assessed again, with results communicated in 2022. That is the bedrock of our operational work. When we receive requests for user data or Government takedown requests, we must scrutinise them under both local law and international human rights standards, and seek to minimise or mitigate any gaps between the two.

**Chair:** I am going to ask you to hold your thoughts while I suspend, because we have to go and vote. We will be back in about 10 minutes. I do apologise, Ms Sissons.

***Miranda Sissons:*** No problem.

*Sitting suspended for a Division in the House.*

*On resuming—*

Q192 **Chair:** Welcome back to the Foreign Affairs Committee. I apologise for the interruption. Ms Sissons, you were telling us three points, and you covered point one. Would you mind carrying on?

***Miranda Sissons:*** Not at all. Briefly, the second thing that I wanted to note is that another way in which we uphold our responsibilities to the many different sectors of society that seek to hold us accountable is through our human rights policy, which is formalised and is enterprise-wide. It embodies the glue that links Meta to the global human rights framework, and to accountability for oversight of our human rights functions.

The third point is on the UN guiding principles on business and human rights, which are the developing glue that businesses are supposed to use in knowing and showing their human rights risks, and in undertaking best practice in human rights protection. We use all three of those things, as well as our other policy development processes, to try to ensure that we hold ourselves accountable to Governments and regulators on rights, and to our users and populations around the world on our norms and principles.

Q193 **Chair:** Forgive me, but you raise different forms of international oversight that are—I do not say this pejoratively—self-constructed. They are therefore accountable to those who constructed them, who are a collection of international firms, of which yours is one, and you cited Microsoft; I don’t know if Twitter is part of the same outfit, but there are various elements that feed into it. As you are no doubt aware, you run into the problem that your accountability certainly has the appearance of being compromised, on the grounds that you are selecting the judges for your own hearings. How do you feel that you can get genuine oversight?

Look at the criticism that your firm has received on, for example, the fall of Afghanistan; people were not full of praise. Look at the criticism that Meta received over the behaviour in Myanmar. It seems that the language barrier masked sins; were things to have been conducted in English, there would have been a whole lot more evisceration of the policies that you claim defend human rights. Can you see the challenge here, Ms Sissons?

***Miranda Sissons:*** Absolutely. It is extremely challenging, but that is why these emerging and existing frameworks are of great importance to the company in individual nation states and around the world. It is vital that those frameworks not only enact systems-based accountability and transparency but seek to hold, implement and embody human rights standards related to expression, safety, privacy and other rights.

Q194 **Chair:** I will go back to this, I am afraid, because it is such a key point. We talk about the discussions that our diplomatic service should be having on how we structure these international rights, whether they are international rights as set out in the ’47 declaration of human rights, or whether they are updates to the WTO in the last few weeks and months. One of the challenges is bringing people together to try to structure an international process that allows for various kinds of accountability. In the ’47 example, those are overarching rights, and in the WTO example, they are very specific rights. You are trying to do something in between, which has very different implications in different cultural circumstances.

Do you not think that it would be more sensible to pick a jurisdiction—for example, the one that you are headquartered in: the United States—and say that you are simply going to apply the law as it comes from there?

***Miranda Sissons:*** As director of human rights, I work on some of these aspects, but of course I cannot speak for the defined legal analysis. What I can say is that, yes, obviously we apply applicable law, and the applicable law in the jurisdictions in which we are headquartered is extremely important, but as you have noted, as we are a global company offering services in many different jurisdictions, there is a very difficult question as to how we model our adherence to regulation and to human rights standards. It is a very complex question.

One thing I would like to note to you in your capacity as Chair of this Foreign Affairs Committee is the importance of supporting the UN Secretary-General's strategy and road map for digital co-operation, because that is one of the few multilateral strategies and opportunities to articulate further detailed global rules, with input from many different sectors of society and many different nation states.

Q195 **Chair:** Mr Hughes, do you want to address this? You face exactly the same challenges. I have highlighted Ayatollah Khamenei, but there are many other examples of threats of violence, the organisation of acts of terror, and vile human rights abuses. There is the Rohingya example in Myanmar that Meta has been accused of being part of. Would it not be wiser for you to say that, except for where there are very specific local jurisdictional changes, you will not operate under any law except the laws of the United States? You would therefore not, for example, find yourself being bullied out of China, because you will recognise immediately that while you are not allowed to operate in China, you carry the imprint of the global times and the various spokespeople of the Chinese state.

***John Hughes:*** Thank you for this question, Chair, and I completely agree with you—these are not easy issues. I will make a few points. First, if you are pointing to the United States, I would just point out that, like Meta, we are a global company; in fact, the majority of our users are outside the United States, so I don't think that following the laws of the country where we are headquartered is the right frame.

That said, there are a few different ways that we look at this. The first is this: as I think my Meta colleague said, our processes are grounded in fundamental human rights, and in particular the UN convention on business and human rights and other similar frameworks; we look at these things and apply them consistently and globally.

The second point is on our responsibility as a platform; I think there are two points there. One is that we try to be as consistent as possible in how we enforce our rules around the world. That is why we make sure that we have people who speak different languages and who are aware of the cultural context, and that we are able to take action on a 24/7 basis. This is quite important for us. Similarly, we want to be as transparent as possible. I made this point earlier: we don't always get it right, but we certainly want to make sure that we are transparent with our users, who are the public, and with Governments on what we do and why we do it. We put all that information on our websites; we want to make sure that people are aware of that.

There is a third point that I would make—I have made it before—about our Open Internet paper. We think it is quite important for companies and Governments to work together on these issues, because there is a role for both of us. There is also a role for civil society. We think that it is quite important to set those norms and standards around the world, because as I said, other Governments are watching.

The last point I would make is that if you avoid this—this goes to your point on choosing just one jurisdiction to comply with—it leads to a fragmentation of the internet. You are looking at, essentially, a race to the bottom, where companies are just looking to comply with different rules, Governments are trying to force compliance, and companies are just going to spend more money and resources to do it, and that doesn't really take into account human rights or freedom of speech. We think it is actually a much better approach to look at this as a global issue, and to work on developing those norms together.

Q196 **Chair:** I'm going to bring in somebody else in a minute, but forgive me: I want to come back on this. The challenge we have is that the internet is already fragmented. The great firewall around China means—I believe I'm correct in saying—that neither of your companies operates in China. I think that is true, although various dictatorial states that don't allow you to operate within their jurisdictions are quite free about using your platforms to operate outside their jurisdictions; that is an irony that hasn't been lost on many. The idea that we are going to get some sort of great global agreement on what it is to be a global publisher in 2022 seems to me aspirational at best.

Would it not be more sensible to decide that you will work with those countries that can at least agree on your terms of service, as it were, or that at least have the ability to regulate, as you claim you wish, rather than leaving it to you? I understand why you have set yourselves the exam questions in various different ways, and then sought to answer them. The challenge we have is that the regulation you have set leaves people rather uncomfortable. You will know that the accusation against Meta of—how can I put it?—failing to counter hate speech in Myanmar in 2018 was matched by a similar accusation in 2021, there having been no obvious lessening of harm. There is a real concern for many of us that while you call for Governments to act—those are bold words—you profit from the suffering that your product causes. Would that be fair, Ms Sissons?

***Miranda Sissons:*** I'm afraid I don't agree with that characterisation, Chair. Indeed, my team and I have worked extensively on mitigations in Myanmar in preparation for its election, and also post coup. I would be delighted to share some of the detailed information we released about our activities there with you and the Committee.

There are obviously a number of different questions within that question. It is clear that regulation is desirable and that rights-respecting regulation is key in this internet that has already splintered, so that the different regimes that emerge are systems-based and seek to uphold rather than destroy norms. There is no magic solution—no solution other than the co-operation to which my Twitter colleague alluded. Indeed, while in principle the selection of rules in one particular jurisdiction is attractive, the realities of the service provision around the world make that neither desirable nor possible, in many senses. Thus the mitigation is to seek to uphold these key human rights standards and best practices around transparency, wherever we are.

On the question of profiting from hate, I want to be very clear: it is not in our interests, or those of our company or our users, to allow hate to flourish on the platform. This is one of the most contested and difficult areas of social media. We have very strong rules about it, and I would be delighted to brief you and the Committee on our prioritisation and company-wide work to reduce the risk of harms in at-risk countries.

**Chair:** Perhaps I can bring in my colleague Bob Seely.

Q197 **Bob Seely:** I want to develop some of Tom's points, if you don't mind. The general point here is that freedom of speech is incredibly important. Arguably, now that we have the rise of authoritarian states in Russia and China and a splintering, as we say, of the internet, it is actually more important than ever that we stick to our freedom of speech values and freedom of debate. There is a growing sense that the big media giants and social media giants, such as the firms that you represent, are becoming part of the problem, not part of the solution.

For example, over Christmas, I was reading the book "Viral", by Alina Chan and Viscount Ridley, about the origins of the covid virus. In an interview, they made references to the way that Facebook had tried to shut down the debate about the origins of the virus, saying that it was a conspiracy theory, which it was not. Clearly, there are conspiracy theories about covid and there is an unhelpful conspiracy theory debate, but at the same time there is a genuine debate about the origins of the covid virus, which is very important. I will read you a quote from Alina Chan: "It is hard to ask whether covid originated in a lab without being shouted down or censored by social media platforms as a racist, a conspiracy theorist or anti-science."

How would you defend that? That is over and above the recognised damage that Instagram does, for example, to teenage girls. Parking the social angst caused by social media platforms, can you talk about why people are concluding that you are a bad thing, not a good thing, for freedom of speech sometimes? Sorry about the long question.

***Miranda Sissons:*** I am happy to speak to that.

**Chair:** Please do. That would be lovely, thank you.

***Miranda Sissons:*** Obviously, one of the great and very underdeveloped—in a human rights sense—questions of our time is how social media platforms should cope with and develop rules relating to misinformation, which has a variety of definitions. I note that freedom of expression can be limited under the global human rights regime and the relevant treaties for reasons of public health. At the outset of the virus, we sought to develop misinformation rules that looked at verifying accurate information and allowed information to be verified by third-party fact checkers, or, under a different area of policy, to strike misinformation that leads to real-world harm. Because misinformation is a spectrum, those areas are extremely difficult to calibrate. We therefore approach that area of rule-making with very great care, and continual calibration. I would be more than happy to take your specific question to my misinformation colleagues and to give you an answer in writing. However, the answer will be that this fell under the set of rules that we developed early on and have since iterated and developed to combat virus-related misinformation, and vaccine and health misinformation.

Q198 **Bob Seely:** I understand what you are trying to say. This is on a spectrum of nuttiness, ranging from intelligent debate to full-on crazy conspiracy theory. However, what you say is quite chilling; effectively, you are saying that algorithms control freedom of speech. That is quite worrying. Do you accept that Facebook censored the "lab leak" theory—certainly at first—and that Meta, or Facebook, was part of the problem by limiting the debate about something that may turn out to be true? You held back that debate and censored it, and because of that, there is an incredibly serious charge that people can make against your company—one that shows the damage to freedom that algorithms can do, considering that many millions of human beings had and were dying of covid at the time.

***Miranda Sissons:*** First of all, it is important to understand that this is not censorship by algorithm, but rather a very detailed and constantly evolving rule set, develop by our content policy team and other experts, with strong consultation from human rights and public health experts and public health organisations worldwide. I am very happy to follow up on this and get you specific information about what may have occurred and the relevant part of the rule set that this book is examining, but I am afraid I am not familiar with that particular text.

**Bob Seely:** That is the problem. I know this may not be entirely your patch, but you are here as a reasonably senior representative of your company, and it is frustrating when you say, "Well, I can't possibly talk to that point and that point," because I would have thought freedom of speech is really a very important part of your role in the human rights agenda.

You have put warnings on 50 million pieces of content relating to covid, and those warnings were very successful in discouraging people from going further and exploring the information, when that information was actually part of an intelligent debate, very often by scientists and scientific students and researchers, about the cause and origin of covid, which is probably the single most important debate that has been going on in the public domain in the past 24 months. I mean, we haven't even had an apology from your company that shutting down that debate may have been a very damaging thing for human freedom and for freedom of speech globally.

**Chair:** I think they are maybe waiting for a question.

Q199 **Bob Seely:** Do you have any comment on that, apart from that you will give me an answer in writing?

***Miranda Sissons:*** I think what I have reiterated is that it is important to realise that freedom of expression under international law and human rights treaties can be limited very carefully for reasons of public health, and that there has been a great deal of public commentary and voices—health authorities and others—first of all, arguing and supporting measured policy frameworks against covid and vaccine misinformation, which are essential components of the public health campaign to minimise the terrible impacts of this disease.

On the specific question of a specific policy area that may have originally limited people's ability to discuss this specific theory of viral development in a lab, I will be happy to get back to you with the most up-to-date and correct information that I can.

Q200 **Bob Seely:** That would be nice, and it would be nice if one of your representatives would like to talk to us about it, because it is a pretty serious issue and goes to the heart of what human freedom and freedom of speech means in practice.

Can I ask Mr Hughes if he has anything to say on this issue? Clearly, on one hand, you are shutting down some people on Twitter who you disapprove of, such as President Trump. On the other hand, to be fair to you, you have a cleaner bill of health when it comes to being able to debate the origins of covid and indeed some of the initial academic debate that was discussed used your platform to have an international discussion about the origins of it. Do you have anything you would like to say here, Mr Hughes?

***John Hughes:*** Thank you for that question. As my Meta colleague said, this is a really challenging issue and one that we certainly don't take lightly. I would say a few points to this. First, similar to what my Meta colleague said, we certainly take many different viewpoints into account here, and in particular talk to experts on our trust and safety council, which is made up of NGOs and others around the world, including 10 members here in the UK, when we develop policies like this, to provide that expert advice and to make sure that we are thinking about various issues when we do so.

Beyond that, we also think that this takes innovative solutions, given the broad challenge of misinformation. That is why we have been experimenting with a number of different things on our platform that would either potentially put labels, as you said, on certain information, to provide people some additional context or to direct them potentially towards an authoritative Government source to provide that additional nuance so that they are able to take everything into account.

We are also right now experimenting with something that we call Birdwatch, where we are getting community input on these policies and how we should think about them, to try to get as wide an alliance as possible. For us, it is important to provide this context.

To your question, it is not that we are necessarily limiting it—it is that we are providing the proper context so that people are able to make their own decisions.

The last point I would make is that, to us—and I have said this before—transparency is really key, with both misinformation and disinformation. We publish all of these policies on our platform. When it comes to disinformation, we have specifically put out a series of things on our platform on where Governments have been trying to put state-backed information campaigns on the platform—we have called those out in detail. So we will continue to do so. We think it is important that we are accountable to these, but also that we are telling our users and others how we approach them.

Q201 **Bob Seely:** Mr Hughes, you are saying that you are giving guidance and context. That is fair enough, but if the context and the guidance you are giving is, "Don't listen to this person because we do not approve of what they are saying", that is more is than guidance—it is a form of quasi-censorship. Indeed, you are shutting down some people as well. The problem is, trying to test the truth and opinions, such as the origins of covid, becomes a very contentious issue.

***John Hughes:*** I certainly appreciate that. That is why, as I said, we take into account various viewpoints, including talking to experts. That is all grounded in human rights and working with our trust and safety council.

I certainly appreciate your question, but there are tweets on the service that are in clear violation of our rules and we will take action, just like we will against any tweet that violates our rules. We certainly are not hesitating to do that if necessary, but when it comes to misinformation specifically, we acknowledge it is challenging and there can be varying viewpoints. That is why we are trying to provide a range of different ways that people can interact with the platform, thinking about how we can limit the spread of abuse or harms, but also making sure that we are not unnecessarily stifling free speech.

Q202 **Bob Seely:** Just one more general point for you both. Clearly, there are risks involved, but is the best way to arrive at a better public debate not to have full freedom on your sites? The best way to defeat an idea is to air it in the public domain. When people see how truly stupid an idea is, because it is racially cretinous or hate-based, rather than you making judgments on ideas, is freedom of speech not the best defence against good debate? Does it not weed out bad, unethical and evil, arguments, because human beings are fundamentally good and they have the ability to make judgments themselves without having judgments made for them? Do you buy that? Is that still credible in this day and age? I am almost testing your reaction.

***John Hughes:*** I am happy to start; you are hitting on a really important point. As I said at the start, free speech is fundamental to our platform—it is what everything is built upon. That said, free speech does not mean unlimited speech. We recognise, just as I am sure our Meta colleagues do and others around the world, that there are limits. For example, if someone is trying to use hate speech or online abuse that can lead to offline harm, those are things we take quite seriously. That is why we have our terms of service and why, if there are tweets that violate those rules, we take action.

Q203 **Royston Smith:** Much of what I was going to ask has been covered, but I would like to pick up on a few points. How do you evaluate and handle Government requests to censor posts, tweets or accounts? Have the origin and frequency of those requests changed in recent years?

***Miranda Sissons:*** I am certainly happy to take that. We evaluate Government requests for removal of content based on very defined procedures. Fundamental to that is our membership in this global network initiative, which, as you remember, requires us to uphold freedom of expression and use of privacy, as defined by key provisions of the international covenant on civil and legal rights.

When requests are made through the relevant channel, each one is scrutinised for lawfulness under local law, and tested for its compatibility with international human rights law. If a request is not lawful under local law, it is rejected. If it is lawful and it is consistent with human rights principles, we may seek to restrict it in the jurisdiction in which it is locally unlawful. We do not take it down globally. If we scrutinise a request and it does not appear to be consistent with global human rights principles, we may undertake a variety of actions, such as requesting further information, pushing back or failure to comply.

We communicate about these trends and individual requests twice a year in our global transparency report. While numbers vary from year to year, it is clear that these requests are increasing over time.

Q204 **Royston Smith:** And who is the arbiter of a human rights transgression? Is it Meta itself or is there someone else?

***Miranda Sissons:*** That’s a wonderful question but, in this sense, the answer would be that we would work to operationalise the principles that are defined in global treaties, and our legal teams and law enforcement teams seek to do that. We are assessed against our behaviour and operational process by independent assessors, who are accredited by the Global Network Initiative. That reporting is then scrutinised by members of the initiative. That, in a nutshell, is how the systems work, but they are framed around, and absolutely seek to be consistent with, global human rights law and practice.

Q205 **Royston Smith:** If a Government asks you to censor a post, and then you check to see whether it contravenes local law, wouldn't the Government that asked you to censor that post know that already?

***Miranda Sissons:*** Governments are made up of many different entities, and how we organise our interactions with those entities through our law enforcement channels and Government request channels is key. We find that requests come in that may, for different reasons, fail to qualify as lawful under local law.

Q206 **Royston Smith:** Have you had any requests to censor anything in Hong Kong, where Meta does operate, although it doesn't operate in mainland China?

***Miranda Sissons:*** We would indicate that in our transparency reporting. While I cannot comment on any specific countries here, I am certainly happy to provide answers in writing to the Committee.

Q207 **Royston Smith:** And could you provide answers in writing to the Committee about who requested the censorship of President Trump, for example?

***Miranda Sissons:*** I think that that is not, as far as I understand it, based on a Government take-down request. That is to do with the application of our content policies to an individual for extraordinary breaches of those policies, but I am certainly happy to provide that information. There is quite a lot of useful information, which I am very happy to share, that was available through the oversight board's consideration of this issue. That case was referred to and considered by our independent oversight board.

Q208 **Royston Smith:** Thank you. May I ask you about Government surveillance and how frequently Governments request private data on your users?

***Miranda Sissons:*** Again, that is an area where we seek, through robust operational processes, to uphold the Global Network Initiative principles, and where Government requests for user data are scrutinised in exactly the way I mentioned to you earlier.

Again, we report on that in quite some detail on our transparency centre twice a year. Those requests for user data are increasing in frequency but, again, I want to stress that we will assess the lawful nature of those requests, and their conformity with human rights law, before determining whether to comply.

Q209 **Royston Smith:** Would you be willing to accept losing access to markets with authoritarian Governments?

***Miranda Sissons:*** I'm sorry; I don't want to cut off my colleague from Twitter, who looked as though he was about to reply.

***John Hughes:*** I'm happy to take a first crack at that—thank you very much for the question. First, I would say that certainly we have been blocked in countries in the past, and we are currently blocked in some countries. That is a decision taken by Governments, not us.

As I said at the beginning of this session, we exist to serve the public conversation, and we continue to engage with Governments around the world in order to explain the benefits of the open internet and why we think it is important for people to have a voice online. This is not just because they are able to access Twitter; there are also economic opportunities in being able to access the open internet, being able to do commerce across borders and so forth. These are things that we are also reiterating.

As I also said before, and as we say in our open internet paper, this is why we think it is quite important for Governments and the private sector to work together to come up with norms to push back against these principles. I think it is no secret, but this is a concerning trend that we have seen, whereby, as you asked, there really is an uptick in Government pressure on throttling our service or shutting it down.

One thing that we have also seen are so-called hostage laws, whereby Governments are trying to hold local employees accountable for content decisions made by headquarters, and those local employees do not necessarily have any say in what the content decisions are. We think that this is quite concerning. We have some of these criminal liability laws, and we think it is important that Governments recognise this, are careful when they put them into legislation, and work together to create these norms, so that authoritarian Governments do not copy the norms and say that, because this or that Government did something, it is therefore okay.

Q210 **Royston Smith:** Finally, it was only in March last year that Facebook published its first corporate human rights policy. Why did you do that then, and why did it take so long?

***Miranda Sissons:*** It is very important to note that, through its membership of the Global Network Initiative since 2013, Facebook did have and sought to uphold explicit human rights commitments regarding due diligence and protection of freedom of expression and privacy. The corporate human rights policy that was adopted enterprise-wide in 2021 is the codification of a broader set of commitments and much more reflects current practice and evolving business and human rights practice.

I would be happy to speak to any particular aspect of the policy, but you will see that it connects us to a broader set of global human rights standards. It clearly defines oversight, and it seeks to uphold the support and protection of human rights defenders online and offline.

Q211 **Liam Byrne:** Thanks so much for the thorough evidence so far. You are sometimes accused of being first-amendment businesses, but what we have basically established today is that it is first amendment minus adjustments for particular countries. You have pleaded the case today for global consensus on what those adjustments might look like and for more robust shared frameworks for the future. I think we have agreed that that plea falls somewhere on a spectrum between aspirational and naive. What we have definitely got here in Europe are two important norms that have emerged from the legislation over the last four or five years that we have seen.

In Germany we have seen the NetzDG laws. Here in the UK, we now have the framework of duty of care, which I first proposed three or four years ago. It is now slowly making its way on to the statute books. How do you see the success of NetzDG and the duty of care legislation? Do you think those are principles that actually could be part of an international consensus as we try to make sure that speech is both free and good? Can I put that question to Meta first?

***Miranda Sissons:*** Thank you. I might respectfully note that the guiding standard among all of the nations you have mentioned is the International Covenant on Civil and Political Rights and other global human rights treaties that hundreds of countries have signed and share responsibility for. I would note that.

I think the important thing about the legislation that you have mentioned is that, whatever specific local concept is used, they seek to take a systems-based approach, a rights-compliance approach, and they emphasise transparency and thoughtful regulation adhering to human rights norms. Rather than any individual concept or system, those are very positive elements of a regulatory approach that is relevant to all countries.

Q212 **Liam Byrne:** When you say a positive approach, you would badge the NetzDG proposals, for example, as something that was a positive development?

***Miranda Sissons:*** As human rights director, I don't have the primary oversight of our regulatory response in different countries, so I cannot, unfortunately, give you the detail you are looking for. I can say that we see efforts by countries to enact rights-respecting regulation. They all have challenges of different kinds.

We have spoken a lot today about speech, but there are significant challenges in national legislation about the proactive requests for data sharing. In democracies—in all countries—it is important that they have independent oversight, which is something that the majority of proposals that I am aware of in my role fail to address. So let me back up and say that the system-based approach of seeking systemic transparency, systemic adherence to rights and norms and systemic complaints and appeals procedures for users are broadly positive, regardless of the strengths and weaknesses of particular legislation.

Q213 **Liam Byrne:** Okay. John Hughes, what is your perspective on that?

***John Hughes:*** Thanks for that question. I would reiterate one point made by my Meta colleague, and maybe make another. We agree that a systems-based approach is best, not least for the reasons that my Meta colleague already said. There is another element that we think is important, and it is something that we published in our white paper back in October, where we talk about how content should really be more than just a "leave up or take down" construct. Not only does that have limitations on free speech—we think it is better to have a range of interventions, such as those I mentioned earlier around certain labels or context around a tweet, so that we are not just necessarily taking it down—but I also think that there is a competition issue here. This is where I think we probably differ from our colleagues at Meta. Frankly, the more that you focus on individual content requests, that takes time and resources from companies to do so. I think that larger companies are able to do that better, and so that does disadvantage smaller companies, including companies that are even smaller than Twitter. We think that has a direct impact on the open internet; more competition allows for a better open internet.

A second point I would make is around what I already said before on criminal liability. You mentioned the UK Online Safety Bill. Of course, I am not an expert on the Bill itself—our UK colleagues are happy to follow up with you on the specifics—but I would say that the issue of criminal liability is one that we are quite concerned about in general around the world, for the issues I already stated. Authoritarian Governments do look at this and they say that if a country like the UK or Germany or anywhere else is doing that, then it is okay for them to do the same. But they have very different ideas on what it means for content that is problematic and trying to force companies like Twitter to take that down.

Q214 **Liam Byrne:** I am glad you have raised that, and I will come back to that in a second. Let me first ask where you think there are international organisations that are going to make the most progress the fastest on establishing some of these norms and consensus. We have recently seen the UNESCO convention on AI, for example. UNESCO has done a magnificent job in actually getting that framework agreed. In Europe, we have organisations like the Council of Europe that are able to agree conventions that bite on member countries. Where do you see the multilateral institutions that are potentially going to build the coalitions of the willing?

***Miranda Sissons:*** In my experience to date, and in my experience prior to Meta in international affairs, obviously global innovation can come in a variety of ways, and it can be bottom up or top down. The creativity and focus of original bodies in Europe or in other areas can be extremely important to set precedent, big or small. Having strong networks of knowledge, stakeholder consultation and information exchange, whether at ministerial level or regional level, is very important here.

I mentioned earlier in the session the potential importance of the UN Secretary-General's work on the road map for digital co-operation. I would like to emphasise that that is a process that is genuinely multilateral, with many different competing interests, but where there does appear to be a framework that will allow for a broad conversation, but with a strong focus on rights.

***John Hughes:*** There are a couple of points from me on top of that. I think this starts at the highest levels, with, as my Meta colleague already referenced, the international covenant on civil and political rights and the universal declaration of human rights, stemming from the UN and all member states—working together on these issues is quite important.

As I have already mentioned, it is important for individual Governments to think about this. That is why the public policy team at Twitter, of which I am a part, has many people who, like me, have long careers in government. I worked for the US State Department, and we have others who have worked for other Governments around the world. Our entire job is to engage Governments around the world on these issues, and both provide our viewpoint and, more importantly, understand their viewpoints.

On individual pieces of legislation, I think it is quite important for Governments to understand the international context around what they are doing and what the implications could be in other Governments around the world. I think it is about individual Governments, as well as working together, not just at the UN, but also as other international groupings such as the G7, the G20 and so on, all of which play a role.

Q215 **Liam Byrne:** My final question is about enforcement. You have different moderation resources in different countries, and those resources are no doubt geared in part towards the nature of the local legislative environment. That is obviously very frustrating for us as parliamentarians when we see, for example, incitement to violence affecting our colleagues who are elected to this place, because there has been inadequate enforcement of norms that you profess to implement. Perhaps you could say a word about that now, and perhaps it might be something that you could follow through on. How do you judge the level of moderation resources that you deploy in each country?

***Miranda Sissons:*** First of all, it is important to note that our moderation resource is global. We operate 24/7 systems at 20 sites globally in some 70 languages, and we have brought on an additional 12 languages in the last year alone. So rather than thinking about the systems as country-specific, it is probably more important to think about them as language-specific.

I think the prospect of perfect moderation is something that one can pursue endlessly, but the very important thing to know and to acknowledge is that the key question in moderation is about the rules that we apply and the controversy over that rule set. There are greatly differing resources depending on the complexity and breadth of the language, and the diglossia or other technical aspects of the language.

***John Hughes:*** I will say something similar. Enforcement is really a top priority for our company. As I mentioned earlier, a little more than a third of our staff is focused just on enforcement, which I think is a measure of how seriously we take it. Like my Meta colleague, we have people around the world looking at this 24/7 in a number of a different languages. We also have people like me, in the public policy team, who are in those various jurisdictions and are able to provide some of the local context that is needed to make some of those decisions.

On top of that, we have really focused on proactively surfacing, through technology, some of those issues on the platform, and removing them before they even need human review. That is something that we will continue to do.

That said, I want to make clear that abuse has no place on our platform. That is something that we take quite seriously. You mentioned potential abuse towards political figures in the UK, and that is also something that we take quite seriously. We understand that abuse towards public figures in particular is quite challenging, and it is something that we are quite focused on. We continue to look at ways to better ensure that that does not happen.

Q216 **Alicia Kearns:** Thank you both ever so much for appearing before the Committee. I want to bring together a few threads of conversation. Miranda, you mentioned operating in 70 languages and the importance of looking at moderation as language-specific rather than country-specific. May I ask you both how many languages you have moderators working in?

***Miranda Sissons:*** I shared that number earlier because at the moment we have language support for some 70 languages. I should add that we have some 40,000 people working on trust and safety. We are, I believe, on track to spend some US$5 billion on this topic in 2021.

Q217 **Alicia Kearns:** So 70 languages are currently being moderated. How many languages are currently used on your platform?

***Miranda Sissons:*** Given the many thousands of languages in the world, there will be a reflection of that number on the platform, because users can—and frequently do—choose to use the platform in the language of their choice and the script of their choice, regardless of whether we officially support it.

Q218 **Alicia Kearns:** How have you chosen which 70 languages you choose to moderate in?

***Miranda Sissons:*** Internationalisation is an extremely complex and long-term topic. Broadly speaking, we have sought to provide service in the official language, optimised to cover the largest proportion of the world's population and other countries' population. I can get you quite specific information on that in writing afterwards, because obviously there is a lot of detail in that strategy of decisions. For example, in the last year, we have consciously adopted and sought to bring on languages that are lesser spoken, but are extremely important to reducing harms in the countries that we prioritise, that are most at risk of societal harm of conflict. Those include 12 languages in the last year, such as Kinyarwanda.

Q219 **Alicia Kearns:** Those languages that are not moderated, then, are essentially a gangland for abuse, recruitment and anything else you might want to look at, because there is essentially no moderating of any form of those languages and the content that is on your platform.

***Miranda Sissons:*** That is not quite correct. As my Twitter colleague mentioned, we, like Twitter, have invested extremely heavily in the development of proactive detection technologies that rely, certainly, on speech, but also on video, graphic images and hashes, as well as other means of behavioural or network analysis that would allow us to understand, assess and act against risks.

Q220 **Alicia Kearns:** So you have algorithmic assessments of risk within those languages. You just do not have any human assessment.

***Miranda Sissons:*** No, what I am saying is that we have a variety of different technical techniques, not all of which are algorithmic, and human investigative and analytical techniques that we employ to forecast, manage and mitigate risks in any particular area or issue.

Q221 **Alicia Kearns:** You must therefore at some point have somebody who speaks that language, if you are bringing in someone human to look at that.

***Miranda Sissons:*** That would be the case if we purely dealt in written content, but obviously a great deal of internet-based content is in fact visual. For example, if we look at the work of the GIFCT—the Global Internet Forum to Counter Terrorism, of which we are a member—the databases and procedures of the GIFCT are premised on image hash matching, as they are for StopNCII, which is anchored by a key UK NCII prevention partner. Facebook and Instagram participate, as well as 50 other CSOs, and again, it is premised on hash matching technologies.

Q222 **Alicia Kearns:** Before I come to you on Twitter, John, in terms of looking at foreign influence operations and counter-disinformation, do you have a top 10 countries—or a top 10 languages, shall I say—that you are currently monitoring because you are concerned about a particular issue? Rather than a thematic concern, a linguistic focus.

***Miranda Sissons:*** We prioritise across a variety of different problem sets. We have, for example, our policy on co-ordinated inauthentic behaviour, where adversaries may use assumed or fake identities in order to seek to manipulate public opinion. That is a well-developed enforcement area where we report on our takedowns monthly, and indeed, last year we published a three-year look back report that is very useful. We also enforce against cyber-espionage by states and cyber-surveillance by companies: for example, in December, we published details of a major surveillance as a service takedown that targeted individuals in more than 100 countries. I am happy to provide further details of that in follow-up.

We have a variety of different policy areas where we will then address problems. An additional area that I did not mention is our state media labelling policy, when we label media entities that are judged to be entirely or substantially under the direction of a national Government.

Q223 **Alicia Kearns:** I think there was an investigation for Meta's "Surveillance-for-Hire" global threat report. Were any UK targets identified within that report, and which Governments were the main perpetrators?

***Miranda Sissons:*** The report on surveillance as a service took down the basis of actions by companies. We have detailed analysis in that report which I am happy to share with you. The surveillance targets were widespread and, as I noted, went across 100 companies. The firms identified operated—if I can remember rightly—in India, Israel and two other countries. I am happy to follow up after the sitting to give you those details.

Q224 **Alicia Kearns:** Thank you. John, how many languages does Twitter moderate in?

***John Hughes:*** Thanks for that question. Twitter is available in more than 40 languages around the world. We provide 24/7 content moderation on all those languages that we serve on Twitter.

I want to make a couple of additional points beyond just the raw numbers. One point to make is that this is an evolving situation. This is not a static world. We are always looking at new developments around the world and how we may need to adjust activity on the platform, for example.

Also, as I have said a couple of times now, we consult experts on these issues. As I said before, we have our trust and safety council, which is made up of leading international NGOs around the world that we consult on human rights and other related issues such as this. For example, if there is a crisis around the world, we are able to bring in resources quickly and talk to relevant experts to understand the context—in addition to the work that we are already doing—and make sure we are taking all the steps necessary on the platform.

Q225 **Alicia Kearns:** You mentioned there a crisis breaking, and I am interested. Over the past 24 hours, I have watched video after video of Ku Klux Klan-style attacks and threats against Bosniak Muslims in Bosnia to mark the anniversary of the creation of the Republika Srpska, of which one of the first priorities was, in essence, the extermination of Bosniak Muslims. I have not seen anything on Twitter about having those videos removed, even though they talk about and glorify genocide and celebrate war criminals. I have seen no sort of counter-narrative or removal of content. The videos are still up of people being intimidated, threatened and surrounded with giant flaming pieces of equipment—clearly an orchestrated activity. Would Twitter consider that to be a crisis, when there is a big independence day celebration that essentially glorifies ethnic cleansing? Has there been any action at all on that in the past 24 hours?

***John Hughes:*** Thanks for that question. Of course, I am not able to comment on these specific issues—I am not aware of this specific issue that you are talking about—although I am happy to have my team follow up in writing after this to give you more detail.

That said, in general, as I said before, that sort of activity—incitement to violence and harassment—has no place on our platform. That is why we have a number of resources in place to make sure that we can take action. We have channels available to Governments, law enforcement and others to proactively surface potentially problematic content to us, so that we can take action. As my Meta colleague already referenced, in Twitter also we have really invested in technology to try to surface some of those issues—

Q226 **Alicia Kearns:** May I ask specifically about this? We know that your platform was overwhelmed with genocidal narratives—videos supporting it and videos celebrating war criminals—for at least a 48-hour period. Who within Twitter will it have been escalated to, the fact that your platform was suddenly being overwhelmed with this sort of activity?

***John Hughes:*** Thanks for that. Again, you are raising very important issues and using the sort of things that we want to be aware of. That said, there is not really a specific person who this gets escalated to at the company. As I said before, more than a third of our staff are focused specifically on content moderation, which again I think shows how seriously we take this issue. They are not the only ones who are working on these issues. As I have mentioned, we have myself as a public policy colleague and others of my colleagues around the world who are looking at these issues and discussing them with our colleagues. We also have our legal colleagues and others internally who are looking at these issues and, as I said, we often and always consult outside experts, including primarily our trust and safety council, who are able to bring these sorts of perspectives. Whenever this comes up, we aim to take action at speed and at scale, but also to make sure that we understand the context and that we are able to take action as quickly as possible.

Q227 **Alicia Kearns:** But surely there is somebody who—I find it very hard to believe. You might have individual moderators looking at individual videos and individual posts, but surely at some point someone would say, thematically, "Oh, FYI, we need to be aware that there are a load of people going around and saying, 'Let's commit ethnic cleansing again in this country,' and perhaps we as an entity need to take a responsible approach in managing this and monitoring it to make sure we don't see that." Supposedly with Trump, you took him off because he was inciting violence. If we are seeing mass amounts of inciting of violence from one specific country, that should flag up on your system that there is something going on on your platform, which is being used to facilitate that.

In the same way, when I used to work on counter-terrorism operations, we would monitor the situation in Iran and say, "Oh my God, all of a sudden we're seeing a lot of chatter that everyone is going to go to McDonalds's at 11 o'clock tomorrow morning. Why is everyone going to McDonald's at 11 am? Oh wait, McDonald's is actually at the American embassy." And we would therefore alert that up the system and make sure someone was paying attention. We prepared and protected the embassy staff and they knew not to come in that day. Something somewhere surely has to go to a person, rather than just being dealt with on a really small, low level.

***John Hughes:*** Yes, I completely agree with you on that. As I said before, there's a couple of different things we would do there. First, I would cite our terms of service. Now, those are not just a static document; we are constantly looking at our terms of service, making sure that they reflect the realities on the platform and updating them as necessary.

Certainly, key for us also is being transparent, so if there was a certain issue that happened on the platform, we would want to make sure that people are aware of it. We are transparent and publish those issues on our website. But to your specific question—again, I can't talk specifically about Bosnia, but I would just say that certainly if that sort of thing does happen, we would want to look at it and would want to take action in that or any other crisis. We do have processes in place to make sure that we have the right people looking at it—to bring people, resources, internally together to talk about it and to make sure that we are able to make quick decisions. Key to that is also making sure that we are getting expert advice from the outside to make sure that we understand the context and are able to move quickly.

Q228 **Alicia Kearns:** I am going to move on to my final question, because you are going back to things like terms of service. Essentially, rather than a quantitative assessment, I am asking about an individual looking one to one at the micro level—someone who sits there and looks at what is going on and has an ability to provide an assessment of what that means, and of the fact that there is clearly something concerning going on on the platform. They would not be saying, "They're breaking our service terms." They would be saying, "What does this tell us about what's going on on our platform, and do we suddenly need to escalate staff to look at the fact that there is clearly something concerning going on and our platform is facilitating it?"

My final question is to both of you. You mentioned earlier—particularly you, Miranda—that you are always keen to work with Governments on legislation that helps you to better do what you want to do to protect users. Can I ask you both what legislation you are asking the British Government to bring in to help you to better tackle hostile influence and disinformation?

***Miranda Sissons:*** I understand that, first of all, Meta has made a submission on the Online Safety Bill, and obviously there will be a great deal of detail in that. But I think, for online and hostile influence operations, the question is less the legislation and more the practical framework and the practical actions that the Government seeks to implement, because they are very difficult issues. We have, certainly in my own experience at Meta—in this time, I would like to emphasise the value of the ABC framework, which is the actor, behaviour and content framework. Again, if one takes a systems-based or behaviour-based approach to disinformation, one would look less at arguments and standards relating to content and more at analyses and initiatives focused on restricting or limiting the impacts of certain kinds of behaviour from certain kinds of actors.

Q229 **Alicia Kearns:** John, is there any legislation that Twitter is asking for that we as legislators are not giving you to allow you to better protect users?

***John Hughes:*** On the UK specifically, I would be happy to have my colleagues based in the UK follow up with you on that. I know that they, like Miranda said, are closely following legislative activity in the UK and, also like Meta, have submitted some written responses to the proposed Online Safety Bill, so I will leave it to them to give you the specifics.

That said, there are some issues that I have raised previously that I am happy to reiterate. Like Miranda said, systems, processes, rather than just leaving up or taking down content, are quite important for us and, I think, are something that we look to see in legislation. Also transparency—we are already being quite transparent at Twitter when it comes to state-backed disinformation, and we have been publishing those things repeatedly and making sure that the public are aware of them. I think it's important for Governments to also take that into account. As I said before—this is a little bit different than your specific question—there are then the issues around creating the norms, for example around hostage laws and internet shutdowns. We think it is quite important to push back against those and to create an environment, with legislation, that promotes a free and open internet.

Q230 **Chair:** I am very grateful for the time you have given us, and I will close in just a minute, but may I have a very brief answer from both of you on tech ambassadors? Have you any experience of working with them? Do you find the position useful, or is it just another layer of bureaucracy that gets in the way of you and the Government you are negotiating with?

***John Hughes:*** I am happy to take that first, Chair. Thank you for the question. As a former diplomat myself, I think it is quite important to have those sorts of positions. As a company, we place a premium on engaging with Governments around the world, to exchange ideas and make sure that they understand our position—that is as important as understanding the Government's position—and to try to work together on what are really challenging issues. To your specific question, having tech ambassadors as part of that process is certainly helpful; it provides a point of contact that we can talk to.

**Chair:** Thank you. Anything to add, Ms Sissons?

***Miranda Sissons:*** No, nothing to add.

**Chair:** Thank you very much—that is the best answer of the evening. Thank you very much indeed for your help this afternoon. I am extremely grateful, and I apologise again for breaking for the vote in the middle. Thank you very much for spending the time with us. I look forward to receiving your follow-up letters—I know you have both committed on various levels to follow up with other members of your teams in different jurisdictions, so I look forward to receiving those.