DÁIL ÉIREANN

AN COMHCHOISTE UM CHUMARSÁID, GNÍOMHÚ AR SON NA HAERÁIDE AGUS COMHSHAOL

JOINT COMMITTEE ON COMMUNICATIONS, CLIMATE ACTION AND ENVIRONMENT

Déardaoin, 7 Samhain 2019

Thursday, 7 November 2019

The Joint Committee met at 9 a.m.

Comhaltaí a bhí i láthair / Members present:

Teachtaí Dála / Deputies	Seanadóirí / Senators
Timmy Dooley,	Terry Leyden,
James Lawless,	Tim Lombard.
Michael Lowry,	
Eamon Ryan.	

I láthair / In attendance: Senators Mark Daly, Aidan Davitt, Alice-Mary Higgins and Lynn Ruane.

Teachta / Deputy Hildegarde Naughton; Seanadóir / Senator Hildegarde Naughton sa Chathaoir / in the Chair.

International Grand Committee on Disinformation and 'Fake News'

Chairman: Good morning. I welcome all our foreign parliamentarians and witnesses to the International Grand Committee on Disinformation and 'Fake News'. I have received apologies from our delegation from Argentina. Unfortunately, our UK colleagues, Damian Collins, Ian Lucas and Jo Stevens, are unable to attend because of the UK elections. Our Canadian colleague, Bob Zimmer, is unable to be here either due to the Canadian elections. I am sure they will stay tuned in here throughout the day and we wish them well. Our parliamentary representatives will each give their name and state the country they are representing. We will go briefly through the group. We might start with Australia.

Ms Carol Brown: I am a representative of Tasmania in Australia. I am part of the Joint Standing Committee on Electoral Matters, of which I am deputy chairperson.

Mr. Milton Dick: I am a Member of the House of Representatives in Australia. I also serve on the Joint Standing Committee on Electoral Matters.

Ms Keit Pentus-Rosimannus: I am Member of Parliament from Estonia.

Mr. Tom Packalén: I am Member of Parliament from Finland.

Ms Nino Goguadze: I am a Member of Parliament from Georgia.

Dr. Janil Puthucheary: I am Senior Minister of State from Singapore.

Mr. Amrin Amin: I am a Senior Parliamentary Secretary of Home Affairs, Singapore.

Lord Puttnam: I am a Member of the House of Lords from the UK.

Mr. David Cicilline: I am a Member of the House of Representatives in the United States of America.

Session 1: The Evidence

Chairman: In our first session we will hear from Dr. Karlin Lillington of *The Irish Times*, Dr. Johnny Ryan from Brave, Mr. Roger McNamee, an investor and author, and Mr. Ben Nimmo from Graphika. It is hoped that Ms Carole Cadwalladr of *The Observer* will be joining us shortly.

I need to read out some formal notices. I draw the attention of witnesses to the fact that by virtue of section 17(2)(*l*) of the Defamation Act 2009, witnesses are protected by absolute privilege in respect of their evidence to this committee. However, if they are directed by the Chairman to cease giving evidence on a particular matter and they continue to so do, they are entitled thereafter only to a qualified privilege in respect of their evidence. Witnesses are directed that only evidence connected with the subject matter of these proceedings is to be given and they are asked to respect the parliamentary practice to the effect that, where possible, they should not criticise or make charges against any person, persons or entity by name or in such a way as to make him, her or it identifiable. I also advise witnesses that their submissions and opening statements to the committee will be published on its website after this meeting.

I remind members of the long-standing parliamentary practice to the effect that members should not comment on, criticise or make charges against a person outside the Houses or an official by name or in such a way as to make him, her or it identifiable.

The format of the meeting is that witnesses will be invited to make an opening statement of no longer than five minutes. I will signal when they have one minute remaining. I will be strict on time with both witnesses and parliamentarians because we are on a tight schedule.

I invite Dr. Lillington to make her opening statement.

Dr. Karlin Lillington: I have been a technology journalist and columnist for more than 20 years, primarily with *The Irish Times*. I am grateful to the committee for this opportunity to offer my perspective on these issues.

The existing business model of social media and search platforms, which is based on extracting and monetising as much personal data as possible from users while encouraging them to engage addictively with and return to the platforms, is a foundation for the serious problems we are discussing today. It is a vicious but highly lucrative circle in which clickbait material of hate, outrage, conspiracy and tribalism proves the most engaging, while the micro targeting of ads and content means only a select receptive audience may ever see material that becomes impossible to refute.

Too often, policy discussions focus on the risks posed by social media in established democracies, but the most vulnerable victims are, ironically, those who fight most courageously on behalf of democracy, namely, human rights defenders. For them, online threats can swiftly descend into violence, arrest, torture or death. Activists do not wish to leave the platforms because, despite their serious flaws, they are a major tool of democracy. They allow anonymity, communicate helpful information or help spread irrefutable evidence, and offer easy-to-use encrypted messaging. Many of the proposed solutions and interventions to social media problems, such as the banning of online anonymity or account registrations being tied to formal identity, only exacerbate the problems. If we better understood and more adequately addressed the serious risks and harms to human rights activists, we could better resolve the problems for all of us because studies indicate human rights activists are the outriders for these dangers.

In 2017, Front Line Defenders, an Irish-based international human rights NGO, analysed data on the murders of 312 activists. In 84% of these cases, the activists had received threats, often made online. As the organisation noted, the world's worst regimes know well that attacking the legitimacy and credibility of human rights defenders softens the ground and lessens the reaction when they are arrested, imprisoned or murdered. Women activists are regularly the recipient of some of the most loathsome and sexually explicit threats. In a survey of eight countries carried out last year, Amnesty International found that more than 40% of women who had been abused online feared for their physical safety and 24% feared for their family's safety because online mobs often issue graphic threats against their children.

Facebook has been particularly implicated in human rights reports, ignoring anti-democratic campaigns on the site and inexplicably viewing despots as opportunities to extend platform reach. For example, in the Philippines, Facebook eagerly helped the Duterte campaign learn more about social media use and considered him to be, in its own words, a king of social media engagement, even though his vigilante drug squads were already well-known for carrying out summary executions. The UN harshly criticised the company for its failure for many years to shut down co-ordinated threats that scaled into violence in Myanmar. One Myanmar legislator

concluded that Facebook had been dangerous and harmful to the country's democratic transition. Avaaz, a human rights organisation, recently condemned the company for similarly failing to curtail violent threats to vulnerable minorities in Assam. Similar difficulties arise with Twitter, YouTube and any other platform that can carry a message, photo or video.

Human rights organisations have stated that platforms regularly back down in the face of government requests to remove posts by or accounts of journalists, activists and organisations. Acceding to a request of the Indian Government, Twitter recently took down 1 million tweets relating to Kashmir. Activists have been deplatformed in Vietnam. Algorithms that encourage and promote engagement also enable co-ordinated hate and disinformation campaigns such as a fake accounts broadcast propaganda campaign in Sudan to commend military generals who massacred demonstrators last summer.

The platforms need key reforms that will protect pro-democracy activists and start to remedy abuses elsewhere. They should work more extensively with trusted regional and local NGOs to better understand the context of government requests for content and account takedowns. They need to be more aware of and vigorous in assessing possible future harm and interference caused by their actions and promotional programmes. Governments and regulators should foreground risks to activists as they consider ways to manage online problems. Too many proposals undermine grassroots movements toward democracy and are as much a threat to democracy as the online harm they hope to combat. States and regulators will not address these broad problems unless they terminate the core surveillance capital business model of platforms and reduce their operational size to a level such that platforms can begin to manage and fix these problems.

Dr. Johnny Ryan: I thank the Chair and the distinguished members of the international committee. I represent Brave, a private web browser. Our CEO, Brendan Eich, invented JavaScript and co-founded Firefox. Since those early days, as all members are aware, the web has become grimy. Millions of people use Brave to make the web safe, fast and private. The problem of disinformation arises because of what happens every time one loads a web page. As the page loads, a broadcast of information about the user is sent to tens or hundreds of companies. This is intended to allow technology companies that represent advertisers to compete for the opportunity to show the user an ad. That sounds fine, but the broadcast data includes an inference of the user's sexual orientation, political views, religion, and any health issues from which he or she may suffer. It generally includes the precise thing the user is watching, listening to or reading at that moment, as well as where he or she is located. These data are bundled with identification codes for the user that are as specific to the user as his or her social security number. All the data I described can be put into a dossier about the user, whatever age he or she may be. This is a description of the multibillion dollar real-time bidding, RTB, industry. The broadcasts occur hundreds of billions of times per day. My written submission contains plenty of footnotes with evidence for this. This relates to perfect information from micro-targeted disinformation. I should say that I did not set a timer, but I will not filibuster.

It is almost certain that every voter in every election has been profiled based on almost everything they watch, read and listen to online. That is problem number one. The second problem is that the real-time bidding industry, which involves advertising, is a cancer eating at the heart of legitimate media. That works in at least two ways. If a person visits the website of *The Irish Times*, for which I used to work and for which Dr. Lillington currently works, and reads about a luxury car, and then later in the day that person goes to a less reputable website, it is very likely he or she will be targeted with an ad for a luxury car because the companies

that received the information profiling that person as a high-value *Irish Times* reader interested in cars can now, at a significant discount, show him or her the ad on the poor quality website.

That happens even if one is not human. What about an ad for a bot? Not only does audience arbitrage, as it is referred to in the industry, commodify a worthy publisher with a unique audience, it also allows a criminal to operate fake people who pretend to view and click on ads. This diverts an estimated $5.8 billion to $42 billion per year from worthy publishers out of the wallets of real advertisers and into the pockets of criminals.

There is a glimmer of light, though. I admit that it comes from my company. We have been pioneering a new system of private ads that are opt-in. The engagement rate has been sky high over the past six months. We are proving that privacy can be good business.

We at Brave urge the grand committee's distinguished members to take a single specific action, that being, to pressure with their intergovernmental weight the two entities that control this global system. The first is called the Interactive Advertising Bureau, IAB. Its largest members are Facebook and Google and it controls the rules about how real-time bidding, RTB, works and what can be in a broadcast. The second is Google itself, which has its own proprietary version. We have given detailed evidence to 16 regulators through colleagues across Europe and we have seen investigations triggered under GDPR into both entities. This is good. Twelve months later, though, we are still awaiting enforcement.

If there is one thing we can leave the grand committee with, it is a plea to stop the business model of the bottom of the web and starve the data brokers who enable micro-targeted disinformation. There is an easy way to do that.

Chairman: I thank Dr. Ryan for concluding on time. I now call Mr. McNamee.

Mr. Roger McNamee: It is a great pleasure to be here and to address the grand committee. I will reinforce everything that Dr. Ryan said. Everyone should think of that as the fundamental backdrop to what I am saying.

In the US and other countries, the institutions of liberal democracy are losing their ability to serve the needs of constituents. Many factors contribute to this. Historically reduced funding has been a major one, but, increasingly, the dominant role of technology in society is undermining the ability of liberal democracies to operate. Internet platforms have exploited the weaknesses of democratic institutions and accelerated their weakening. Platforms have positioned themselves to replace democratic institutions with initiatives such as Alphabet's Sidewalk Labs waterfront project in Toronto, Facebook's Libra cryptocurrency, Amazon's efforts in law enforcement and Microsoft's services for governments. The success of Internet platforms has produced harm to public health, democracy, privacy and competition on a global basis. The driver of that is the algorithmic amplification of hate speech, disinformation and conspiracy theories as well as micro-targeted advertising based on massive surveillance. Similar to the chemicals industry of the 1950s and 1960s, Internet platform profits are inflated because the industry does not pay the cost of the harm it causes. This is important. As Professor Shoshana Zuboff has noted, Internet platforms are gradually displacing democracy and consumer choice with algorithmic processes.

To protect competition, governments have an existing anti-trust toolkit. To protect public health, democracy and privacy, however, they need new tools. They need to constrain the business model of surveillance capitalism. The best way to do this is to declare that personal data

are a human right, not an asset. This would limit business models to first party intended uses of data. There would be no third party commerce or use of private data, no predictive models based on personal data, no web tracking and no corporate surveillance. In this, I would like to go beyond the Brave solution.

Internet platforms behave as though governments lack the tools and political support necessary for meaningful regulation. Our challenge is to prove them wrong. We have to be prepared to shut them down for periods of time when they misbehave, given that they are clearly defying democratic governments and will persist in doing so until there is an incentive to change. I have spent 34 years as a technology investor. At one time, I was a mentor to Mark Zuckerberg and Sheryl Sandberg. I cannot be absolutely certain that I am right, but I am very confident that I am not wrong. I thank the grand committee for its time.

Chairman: I thank Mr. McNamee. I call Mr. Nimmo.

Mr. Ben Nimmo: I thank the grand committee for the opportunity to attend. I will focus my comments on electoral interference and large-scale disinformation operations because these are what I study on a regular basis.

This is a vast and fast-moving problem set. According to the Oxford Internet Institute, 70 countries are now reported to be running organised social media information operations, up from 48 last year. We do not have enough data to prove whether this stems from a rise in operations, a rise in reporting or both. Either way, it indicates a global phenomenon. Most of these operations are aimed at domestic audiences, but we must remember that the Russian operation that targeted the US from 2014 onwards also started out by targeting the domestic opposition.

The evidence suggests that a state that has the capability to run domestic information operations can quickly pivot to external targets if the political need is there. Russia did so in 2014. Saudi Arabia did so after the murder of Jamal Khashoggi. China did so when the Hong Kong protests began. Nor is this limited to state actors. We saw the far right in Britain and America trying to interfere in the French presidential election in 2017. These operations do not solely play out on social media platforms. They also include websites and television stations. They can include on-the-ground events and local activists, some of whom are unaware of the role they are playing.

All of these problems are underpinned by a perception that online information operations are easy, cheap, effective and profitable. Since 2016, the narrative has emerged that Russia managed to tip the balance in the US election by running social media trolls. That narrative is significantly flawed, but it has caught on.

Unscrupulous marketing companies around the world are promising to "change reality" for their political clients through social media campaigns. Fake amplification on social media is very cheap. One can buy a three year old YouTube channel with videos already uploaded for just $1. Domestic actors on both sides in the US have experimented with Russia's playbook.

However, we also know that the environment in 2019 is much less permissive than it was in 2016. The platforms, law enforcement and open source researchers are all actively hunting influence operations online. The rate of takedowns has accelerated dramatically since early 2018. Over the past 12 months, we have seen more than 50 takedowns just from Facebook, covering operations from some two dozen countries. That has forced interference operations to sacrifice engagement to stay concealed.

In this environment, I bring four urgent needs to the committee's attention. These are not the only four, but they are the areas where parliamentary work can have most immediate impact. First and of most direct relevance to elections, parliaments and political campaigns must urgently improve their own cybersecurity to prevent the sort of hack-and-leak operations that Russia used to such devastating effect in 2016. This is not a duty that can be passed on to the social media platforms. Every parliament and every campaign should ensure that all its staff have cyber training and contingency plans in place. This is expensive and many campaigns will argue that the money would be better spent on ads, but it is much less costly than seeing their emails leaked to the press a week before the election.

Second, we do not yet have a deterrence system in place. We have seen individual nations react to interference attempts, but we do not have a credible system for imposing unacceptable costs on foreign actors who attempt to interfere in elections.

Third, we need legislation that imposes systematic costs on the commercial operators who sell fake accounts or hire out their interference campaigns. Two weeks ago, we saw the first case of the Federal Trade Commission fining a US company for selling fake engagement. Social media companies can, and do, ban such operators from their platforms, but they cannot impose a direct financial cost. The black market in fake accounts is the easiest place for hostile actors to buy their assets, as China demonstrated over the Hong Kong protests.

Fourth, parliaments should lead discussions on how to reduce polarisation online, both through regulation and through education. This is a long-term challenge, but we should always remember that if we did not have domestic trolls, the foreign trolls would not have anyone to pretend to be. Such discussions will require technical analyses of how the platforms' algorithms suggest friends and content for users, but they will also require social analysis of how users select their online identities and tribes and how they can be encouraged to broaden them. Every human has a complex pyramid of identities in real life, but the dynamics of social media often reduce that to one-dimensional tribalism. If our parliaments can work across party lines and lead the debate on how to reverse the spiral of ever narrower partisan groups online, that would mark a step towards reducing the scope for online polarisation and online interference.

Chairman: I thank Mr. Nimmo. Our final witness is Ms Cadwalladr. She has five minutes, and I will indicate after four to let her know she has one remaining.

Ms Carole Cadwalladr: I thank the grand committee for inviting me to attend and for the focus it is bringing to these important issues. When I accepted the invitation, I thought that its British MP members would be in attendance. The fact they are not here today because Parliament was suspended two days ago in preparation for a general election is profoundly disquieting on many levels. The UK Digital, Culture, Media and Sport Committee, DCMS, has painstakingly detailed the risks to our elections, and yet the Government called this election having done absolutely nothing to address them. It has failed to undertake any of the committee's recommendations, which is a gross dereliction of its duty to protect the British public.

Nobody can be in any doubt about the risks to our democracy that are posed by these Silicon Valley tech platforms. I have spent three years investigating these risks and we now know many facts. We know the Brexit vote was fraudulently and illegitimately conducted. We know the tech platforms, particularly Facebook, facilitated multiple campaigns to break the law. We know the authorities have entirely failed to hold these perpetrators to account. We know that Britain is set to leave the European Union on the basis of this fraudulent and illegitimate vote. The failure to reckon with these crimes has led to a situation where the man who led one of

these campaigns, Vote Leave, which carried out the single biggest electoral fraud in my country for more than a century, is now the Prime Minister, and the man who masterminded this scheme is his chief adviser. This is not a situation that should exist in any well-functioning democracy. Britain is now a warning to the rest of the world because what happened in our country could happen in this country too. The vast unchecked power of the Silicon Valley technology companies represents a truly global risk, and it is not even clear that democracy will survive them.

It is absurd that I am here today but another invited witness, Mark Zuckerberg, is not. The contempt he has shown to the nations represented here is extraordinary. We are in a truly staggering situation where a single company plays an absolutely central and pivotal role in elections in almost every single country across the world, yet it is answerable to none of them. This cannot and should not go on. I urge Congressman Cicilline to invite the committee to Congress for its next hearing. Mark Zuckerberg needs to be subpoenaed by this committee. He needs to answer proper, rigorous and informed questions. I believe Mark Zuckerberg has deliberately misled Congress. Two weeks ago, Representative Alexandria Ocasio-Cortez asked Mark Zuckerberg when he and Sheryl Sandberg learned about Cambridge Analytica. He said he could not remember but he thought it was in March last year. This simply does not bear scrutiny.

The entire story that Facebook has told about Cambridge Analytica, including who knew what and when, is crumbling. Throughout 2017, I and other journalists were writing about the company and we now know, thanks to the SEC report, that Facebook had being lying to reporters, including me. That, essentially, means it was lying to shareholders. We know that Facebook employees knew about Cambridge Analytica abusing Facebook data before even the very first report by Harry Fox Davis in *The Guardian*, again thanks to the SEC report. Mark Zuckerberg claims to have known nothing until March last year. This defies belief. Yesterday, we learned that the California Attorney General had tried to subpoena emails between Mark Zuckerberg and Sheryl Sandberg that would clarify all of this, but Facebook has repeatedly refused to hand them over. One has to ask why and what exactly it is that Facebook is trying to hide.

Facebook cannot be trusted to run the world's elections. No company can. I hope the company moves towards a total ban on micro-targeted political advertisements and that it seeks to obtain the forensic evidence of what actually happened on Facebook's platform in 2016 in the US election and the EU referendum. This information cannot remain the private property of a private company.

Chairman: I thank Ms Cadwalladr. I acknowledge Lord David Puttnam, who will be representing the UK on this committee today and we are delighted to have him here. I will go through the list in alphabetical order. Every country has five minutes and I will indicate after four so speakers know they have one minute remaining. That includes the answers, so if witnesses keep their answers short and to the point, it will allow other countries to come in with their questioning. I call Ms Carol Brown of Australia.

Ms Carol Brown: Dr. Ryan talked about stopping the business model and said there is an easy way to do it. Would he like to elaborate?

Dr. Johnny Ryan: I would. This is part of the business model. When we are talking about hundreds of billions of broadcasts leaking data, one would imagine there are thousands of companies involved and one would imagine correctly, but there are only two standards that decide what data are being leaked around the place. One can act against the two entities that control those standards.

Ms Carol Brown: To follow up, I want to talk about obstacles but, given the testimony today, and Ms Cadwalladr highlighted her belief around the British Prime Minister and his chief adviser-----

Ms Carole Cadwalladr: It is not my belief. That has been documented by the Electoral Commission.

Ms Carol Brown: Is Ms Cadwalladr saying there is no political will in Britain to change the way the system is currently working?

Ms Carole Cadwalladr: In terms of changing our electoral laws, that depends on the Government. The recommendations have come from the Electoral Commission, from the DCMS committee and from the Information Commissioner's Office, ICO. There is a whole suite of recommendations that say our electoral laws do not work, are completely inadequate, are not fit for purpose, and are placing our elections at risk, and the Government has failed to act upon any of them. That is why calling an election in these circumstances is so particularly troubling.

Ms Carol Brown: What would the panel like to see come out of this hearing?

Ms Carole Cadwalladr: The committee is in this leadership position because it has collective power in terms of countries acting together. There have been these very strong recommendations from bodies, such as the Institute of Practitioners in Advertising, IPA, on a total moratorium on micro-targeted political advertisements. At the moment, we know these elections are not safe, and that has been documented. Until the platforms can prove they are safe and prove they will stay within the confines of the law, I think it is perfectly reasonable to have a pause, for which the Information Commissioner in Britain has asked, or a moratorium to give a chance to assess and to gather in the expert evidence, and see if the current situation is beneficial to our respective democracies.

Mr. Milton Dick: I am interested in Ms Lillington's evidence about the impact of social media platforms on democracies and elections. I am glad everyone in this room is committed to that, but it is really the people outside of this room who we are having a conversation with. In regard to the anti-democratic pro-regime nations where social media is used for freedom of speech, if we were to have a set of rules or guidelines around the globe about what is a standard set of procedures, how would that impact struggling democracies?

Dr. Karlin Lillington: For electoral processes?

Mr. Milton Dick: Whether in regard to truth in advertising, standards or media panels.

Dr. Karlin Lillington: The note of the Myanmar legislators is one to keep in mind in that we do not want platforms destabilising elections. There needs to be a recognition that many of these countries are in a transitional period and are fighting for greater democracy. In regard to decision-making around processes, the NGOs and the activists are best placed to define by country the greater specifics of what might need to happen. We need to keep in mind that the remedies we try to take in established democracies for many of these problems, or to bolster elections, can work against the human rights defenders and emerging democracies.

Mr. Milton Dick: We do not want a situation where an election panel set up to observe elections in a struggling democracy is counterproductive in a nation where there could be an electoral commission or an independent body overseeing that process. It would be counterproductive to have that placed on pro-democratic reform or reformers.

Dr. Karlin Lillington: Yes. My message would be that the people to talk to would be the NGOs and the human rights defenders who would know this area in much greater detail than I would in terms of specific remedies.

Chairman: I thank Dr. Lillington and Mr. Dick and I now call Ms Keit Pentus-Rosimannus.

Ms Keit Pentus-Rosimannus: I thank all of the witnesses for an excellent start to the meeting. My first question is to Mr. Ben Nimmo. I admire his dedication and his previous work in the Atlantic Council's DFRLab. I echo Mr. Nimmo's comment that disinformation operations are not some sort of innocent, so-called meddling. Rather, they are blatant attacks against the core of democratic states. In Russia, as we know, they are part of the military doctrine. They are used as weaponry tools, and should be treated as such. Hence, a proper co-ordinated international response is definitely needed. It is something we have been missing thus far.

There have been recent examples of how Russia-backed influence networks and the manipulation techniques were used in Africa. They did not use faked profiles created in the St. Petersburg troll factory on that occasion: they hired locals. They basically bought their locals' profiles. I ask Mr. Nimmo to comment on whether this is something we can expect in upcoming big elections and to elaborate on the next things we should be waiting for?

Mr. Ben Nimmo: I thank Ms Pentus-Rosimannus for the question. I would nuance the African finding slightly. There was a combination of fake profiles and genuine profiles and they were using some genuine people on the ground. It also looked like they had bought accounts from people. One of the problem sets here is the black market in recycled accounts. Something that we have seen consistently over the last three or four years is information operations taking more steps to try to hide because they are being hunted more. The latest take-down of probable Internet research agency accounts was announced approximately one week before the African announcement. They were going to extraordinary lengths to try to hide their traces. Mostly, they were copy-pasting genuine American comments. This means that one has to be looking for signals that are not content based because the content is all coming from somewhere else. It also means that they are getting much less engagement because if all they are doing is parroting somebody else's words then they do not have their own voice.

I think what we will see is more attempts to masquerade as other people. We have already seen many attempts to co-opt local activist groups. Part of the challenge is going to be communicating with activist groups ahead of the elections and teaching the broader electorate the type of cautionary steps they need to take before engaging with somebody else's Facebook group, which is asking them to take action on the ground. We need to teach them how to verify who is behind that. There are basic steps that one does in real life that people seem to forget online. Much of this is about teaching normal users the same wariness online that they would have in real life.

Ms Keit Pentus-Rosimannus: I thank Mr. Nimmo. On the deepfakes and synthetic reality, one can find the source when it comes to ordinary fake news, but it is so much more difficult when it is about the deepfakes. What developments are happening in that regard?

Mr. Ben Nimmo: In the long term, deepfakes have the potential to be a problem but they will be the greatest problem in communities which are predisposed to believe them anyway. Those communities will be predisposed to believe cheap fakes as well. The simplest way of faking is to repurpose a video from some other time and place and say that this is happening right now. That kind of content still goes viral. In the long term, deepfakes are a challenge but

they are secondary to the problem of emotional engagement and the virality which is driven by outrage. If we start looking at outrage-driven virality, then we will have a good chance of dealing with the deepfakes fake problem at the same time.

Ms Keit Pentus-Rosimannus: I have a similar question for Dr. Johnny Ryan in regard to deepfakes fakes because he also highlighted micro targeting, which is definitely a problem. Lies tend to spread very fast even without targeting. How does Mr. Ryan see the deepfake developments?

Dr. Johnny Ryan: My focus is on the bottom of the web, that is, on the websites that are operated perhaps by a crank conspiracist. Once upon a time, he or she would done this in a shed in the bank of his or her garden but now we have a business model that allows this to become a viable business. Instead of it being a single crank, there is an incentive to host and operate whatever content, including deepfakes. My suggestion, in addition to everything we have already heard, is a focus on undermining the business model, the source of data and the source of cash.

Chairman: I thank Ms Keit Pentus-Rosimannus, Mr. Nimmo and Dr. Ryan and I now invite Mr. Tom Packalén to put his questions.

Mr. Tom Packalén: I thank the witnesses for their excellent presentations. It is interesting to be here and to listen to all of them. I thank Ms Cadwalladr and Mr. McNamee for their great job of work in regard to Facebook and the Cambridge Analytica issue in particular, which was very bad for artificial intelligence, AI. It showed both sides of what AI can do. We had thought AI could be used only for good but it can be used as a weapon to do bad things.

There are many problems that need to be addressed by way of regulation, including hate speech, fake news, identity bubbles, election influence and interference. There are also many algorithmic problems. What is the biggest problem? Where should we start to solve this problem?

Chairman: To whom is Mr. Packalén's question directed?

Mr. Tom Packalén: It is for all of the witnesses.

Chairman: I ask Mr. McNamee to respond first.

Mr. Roger McNamee: The danger on a global basis is that each country experiences a different manifestation of the problem and so the tendency is to attack the symptoms. The problem could be with young people, teen suicide or bullying or, perhaps, elections and democracy or privacy. All of those problems derive from the underlying business model. It is a business model based on capturing and maintaining attention. Please do not be distracted by what in the United States we call First Amendment issues or free speech issues. Algorithmic amplification is a business choice. It is completely independent of speech. One can put all voices onto social networks without harm. Where the harm comes in is that the amplification looks to the most basic elements of evolutionary psychology, specifically , flight or fight. That is why outrage is so effective. The problem with outrage is that it is politically asymmetric. One does not see outrage being equally effective across the entire political spectrum and so it has resulted in a uniform shift to the far right globally. My observation is around how to stop this stuff happening. It is very important to go after both algorithmic amplification and micro targeting because they together are what create the problem. The great, unique opportunity of the committee is that it is the only place where we convene people and bring together all the different experiences. It gives the opportunity for the political will to migrate to the root causes. I truly hope

the committee will flourish and that we can do everything in our power to support it.

Mr. Tom Packalén: How to regulate posits a great challenge because it is so complicated and the technology in the companies is in their hands alone. Mr. McNamee knows about Facebook. Ms Cadwalladr stated Mr. Zuckerberg knew about Cambridge Analytica last year. It is deep inside what such companies do. It is a matter of algorithms.

Ms Carole Cadwalladr: Mr. Packalén is correct. There are multiple very complex issues but there are also some simple, straightforward issues. A foreign company played a central role in all of the representatives' elections and is unaccountable to any of their parliaments. It is wrong to consider it in any way a political issue. In the context of the national security of countries, this foreign company is playing an absolutely pivotal role. Politicians have no idea what role it plays in their elections and it is beyond the reach of any of their laws. That is completely unacceptable and profoundly worrying.

Politicians have the power. All of us are helpless and powerless in the face of such massive companies but politicians have come together, as a collective body of 12 parliaments, and have the ability to make a stand and say it is unacceptable, which I hope they do.

Chairman: I thank Ms Cadwalladr and call Ms Goguadze.

Ms Nino Goguadze: I thank the witnesses for their presentations. My first question is for Mr. McNamee. Most online information is provided by consumers. Are people aware of the web data collection process? Do customers have a clear understanding of how data provided by them could be used in the future?

Mr. Roger McNamee: There is a grave misunderstanding of the data sets involved. My estimate, which is by no means precise, is that less than 1% of the data that Google and Facebook have are the data contributed voluntarily by consumers. The vast majority are acquired in the third party marketplace, either by tracking people online or by acquiring bank statements, credit cards, location from mobile vendors or purchase history from various companies and products. The core issue is that the surveillance takes place largely outside the awareness of people and without their direct participation. In the case of credit card processing companies, for example, which sell their customers' information, no consumer has a direct relationship with any of the companies or has any control over them.

One of the challenges is making people aware that the data being given up are not used to improve their experience, except to a small degree. Most of the data are used in a way that has social impact. In Myanmar, one would not have needed to be on Facebook to be dead but just to be a Rohingya, while in Christchurch, one did not need to be on Facebook or YouTube to be dead but just to be in the mosque. That is the problem we face. It is no longer an interpersonal, one-to-one relationship. Data are being used against whole populations, which is why the committee is so important. They are being used against populations globally.

Ms Nino Goguadze: Which entity could be responsible for informing people properly?

Mr. Roger McNamee: I do not know. I do my best every day, as does everyone on the panel. I know many of the people in attendance. Representative Cicilline, who is a friend of mine, has done an amazing job of making people aware. I attended a meeting two nights ago for 2,300 people in Florida, and I am sure 95% of them did not know what I have just stated. Making people aware remains the challenge. This is an opportunity for governments to educate citizens and in countries such as Georgia or Estonia, an effort has been made to do that because

there is a clear threat to their viability.

Ms Nino Goguadze: I thank Mr. McNamee. My second question is for Dr. Ryan. In Georgia, any possible electoral interference is considered a managed process that could have been orchestrated or linked to forces outside the country. Russia is often a suspicious country, not only in Georgia. To address the problem properly, do we need to reveal who stands behind the orchestrated process and how they operate and get access to data collected on social networks?

Mr. Ben Nimmo: In general, I am in favour of transparency in respect of information operations as an educational tool. If people can be shown how it worked on the previous occasion, it will inoculate them against how it will happen the next time, and put pressure on the information operator to change its ways because it will have to find a new tactic. There have been at least four generations of takedown of content from the Russian Internet Research Agency, RIRA, and every time it has had to change tactics precisely because the previous attempt has been caught.

The more transparency, the better. The challenge is the attribution. We do not want people to say an instance must be the Russians because those behind the content behave the way the RIRA did on the previous occasion. The attribution very much comes down to how much the platforms can attribute. Transparency is important and educational but there is a limit beyond which attribution will probably not be able to go. We are in the space where one tells what one can but one has to accept that, sometimes, if the threat actors are clever enough, a hard attribution will not be possible. We want to avoid hysterical attributions to the effect that it is one bot online and that, therefore, it must be a Russian operation. Sadly, there has been much of that in this space recently. Part of what needs to happen is a realistic assessment of what we see, rather than an overexcited one.

Deputy Eamon Ryan: I thank our guests. We might agree that political micro targeting can be dealt with by national legislatures but that is only one aspect of a very complex problem. If we look more deeply at the business model, given that Dr. Ryan, Dr. Lillington and Mr. McNamee all advocated going to the source of the problem, the main question, if we can get agreement today, is where the governance is and where the collaboration is in the international regulation to make it work. It is hard to do it as a nation state. Is it at the European Union, the UN Internet Governance Forum, some version of ICANN or the IAB, which Dr. Ryan mentioned? What has the best structure to make the business model change?

Dr. Johnny Ryan: In the case of real-time bidding, strangely, this city is the crucible, along with Brussels. The IAB is regulated, under the general data protection regulation, GDPR, from Belgium, and Google is regulated, under the GDPR, from Dublin. The two regulators have appropriate law and massive legal authority. The Belgian data protection authority is investigating the IAB, while the Irish data protection authority is investigating Google. The Irish regulator received my complaint in respect of the issue well over a year ago. I understand she is hard pressed and it is difficult to process a large amount of work. Nevertheless, elections are approaching in various parts of the world and these are essential, life-and-death matters.

I suggest that the forum is, in fact, in this House, in the Chamber. That is because our regulator can be scrutinised by no one other than Members of the Oireachtas. I can sue the Data Protection Commissioner if she does not effectively act on the complaint and evidence I have given her. That is something we have in reserve. A far better way of forcing action is to provide resources to regulators in both jurisdictions and to make sure there is appropriate scrutiny of the regulator for these critical things. I realise I am going over time. The whole idea of this regu-

lation was that it was risk-based. We would focus on the key and important players and leave the greengrocer, for example, alone. In that case, this biggest data breach we have ever had in digital history should be the number one item and it does not seem to be.

Chairman: Mr. Nimmo would like to contribute. I ask him to be brief.

Mr. Ben Nimmo: I do not have an answer but I will make a nuanced point here. So far, we have been talking about the Silicon Valley tech giants and the social media platforms. We are already in a world where those are not the only major platforms around. We are also seeing major platforms from China, for example. Whatever we build in we will have to do so with a sense that we will not just be regulating for companies based in democratic countries but also for large social media platforms located in non-democratic countries. How we address that in the regulation will be a big question.

Deputy James Lawless: I thank the witnesses for their contributions and attendance. I have two questions which I will tie together and try to keep as brief as possible. The first relates to an incident from social media yesterday. As we know, the British general election is under way and we miss the presence of our British colleagues, with the exception of Lord Puttnam who is with us. The official Twitter account of the Conservative Party sent out a tweet with a mock-up of the Opposition Brexit spokesperson, Keir Starmer, poised to answer a question he was not asked. This is possibly the first time the headquarters of a mainstream political party has run fake news. We have seen this from many fringe actors but this is probably the first time I have seen a mainstream party officially engaging in fake news. It is probably no surprise because the main protagonist in that party is on the vote leave side.

Have we reached peak social media difficulty? The flipside of that question is that, as legislators, we have to anticipate the counter-arguments and play devil's advocate to some extent. With every new technology, from Gutenberg's printing press to the Pony Express when riders crossed the United States on horseback delivering telegrams, come those who will exploit these technologies. We were discussing this issue last night. Regulators and legislators have always tried to clamp down and sometimes it takes a while to get on board. Sometimes the public get on board faster and apply their own filter by taking fake news or, previously, a bogus telegram with a grain of salt. I fervently believe legislation and regulation are needed. To what extent have we reached a peak? Are people moving off the platforms already or will they remain an ongoing threat for some time?

Dr. Karlin Lillington: I would like to make a quick point that we need to recognise that democracy, as a global aspiration, will be undermined when the political leaders of the countries that are supposed to be the central democracies are themselves using social media to lie, spread disinformation and question and undermine elections. That emboldens and gives comfort to the dictators and autocrats in the most repressive nations and undermines activists. We are leaching our own democracies of any moral authority. I know this is a broader social issue that goes beyond concern about the platforms. However, these problems are tied together and this is something to think about.

Chairman: If we have time at the end, I will come back to witnesses as I know there is more than one speaker from some countries.

Mr. Ben Nimmo: On the foreign threats, we have not yet hit peak activity because the idea is out there that this is effective but we are already past peak vulnerability. In 2016, nobody was looking for this and now people are.

Chairman: I will bring in our guests from Singapore next. We have Mr. Amrin Amin and Dr. Janil Puthucheary.

Mr. Amrin Amin: I will touch on the point of business models that was mentioned by many members of the panel. I direct my question to Mr. Roger McNamee. The underlying issue is the business model. Mr. McNamee spoke about surveillance capitalism. If we dig deeper, the issue is that the more engagement, the better sensational news sells. Mr. McNamee spoke about stuff that triggers a fight or flight reaction as well as hate speech, conspiracies and disinformation. Given the various technological solutions at hand, there is little or no incentive for social media companies such as Facebook to prevent these harms as it would affect their bottom line. Is that correct?

Mr. Roger McNamee: It is worse than that. If one thinks about it from the perspective of the social media companies, they would like to appear to be co-operative without going after the business model. When they put in place measures like moderation to try to capture things after the fact, the thing to understand is there is latency, that is, a lag between when content goes up and when moderators can take it down. Almost all the harm from this stuff happens very quickly. It is not just that they have no incentive to do it. They have no technological way to solve these problems. The scale is so great that moderation cannot work. The business model has to be changed.

To respond to the previous question because these matters are related, we must remember that these companies are not sitting still. The business model is migrating from advertising-based businesses to taking over the functions of liberal democracy.

Mr. Amrin Amin: The key issue is they have community standards to appear to be helpful but in fact there is inaction. This is evident in various incidents we have seen around the world, for example, in what happened in Sri Lanka where there was a refusal to take down a post that could clearly qualify as hate speech and a refusal to fact-check political advertisements. There is clearly a profit motive. They like to have community standards to give a veneer of co-operation and certain code words that appear to be helpful, but in fact the underlying purpose is the insatiable thirst for profits. Is that right?

Mr. Roger McNamee: That is correct. I would like to reiterate what Mr. Nimmo said a moment ago, that is, that we have passed peak ignorance on this issue. The problem is the technologies are evolving and the surveillance is becoming so much deeper with technologies such as Alexa, Google Home and the ubiquitous facial recognition that is going around the world. We should keep in mind that because these companies control information flow - people get their information by searching Google and Facebook - they have the ability to use the data they have, the voodoo dolls they have created of each person which are a digital representation, to control search results and, therefore, control the choices available to people. That business model is the reason they can migrate from advertising into replacing government functions.

Mr. Amrin Amin: Because of this, Mr. McNamee would advocate for governments to have powers and effective levers to intervene swiftly to prevent harms, including requiring corrections, curbing the spread of disinformation by taking out bots and protecting people against foreign interference. Would that be correct?

Mr. Roger McNamee: I would answer that question by saying that, right now, there are no disincentives for bad behaviour so we need to scale up the punishments by perhaps two orders of magnitude. The punishments need to be measured in trillions not millions of dollars. The

companies need to understand that undermining democracy should be punishable by extermination of the company. There is no reason any company should have the right to be an enabler of the destruction of the society in which it lives.

Mr. Amrin Amin: In short, there have to be laws that ensure social media giants do not just focus on profits and are accountable to governments and the people.

Mr. Roger McNamee: If I may, I would like the focus to be on their business models to prevent the problem from happening in the first place.

Mr. Amrin Amin: Correct.

Mr. Roger McNamee: If we try to do it in the way we are doing it now, by attacking symptoms, we will always be playing a loser's game because they will migrate away from this business model to new ones that are even more harmful, using the same underlying framework.

Mr. Amrin Amin: The regulations have to target the underlying business models to require them to adjust, change and adapt to ensure they meet-----

Mr. Roger McNamee: If personal data is made into a human right and is, therefore, not an asset that can be traded, that will take care of this problem.

Chairman: We will move to the United Kingdom and Lord David Puttnam.

Lord Puttnam: I should explain I am here in a personal capacity because our parliament was dissolved yesterday. I bring apologies from Damian Collins, MP, for whom I was supposed to act as sidekick. Suddenly, I have become the main part of the show. One point I would like to get across is that my select committee would very much like to take evidence from the witnesses. We have a problem because unless we get that evidence, either in writing or orally, I cannot use it in our select committee report. The witnesses will definitely receive invitations and we will find a way of circumventing those obstacles. There is a wonderful irony here. I am an unelected politician, yet the one security I have is that I know our select committee will be reformed in January, whereas if I was in the House of Commons, I would have no such certainty. It is a rather bizarre situation in which to find oneself. As I see it, we are on the horns of a major dilemma. The bad actors - Russia, China and whoever else - have no real interest in achieving specific outcomes, which is very unusual. They do not, for example, really care who wins the British election. What they care about is seeding confusion, disharmony and disrespect for democracy. The very worst that could happen - I suspect it might happen on 12 December - is that there would be a contested election. That would be a massive win for the people who wish to deal in disinformation. I have no idea what the result will be. Likely as not, it will end up in the Supreme Court. There is irony in all of this. The more one can create confusion, the more one justifies the sovereignty of the social media companies because, in their competence, they begin to look as if they are almost a safe haven, as opposed to the incompetence of plural democracy. That is a very serious problem and the problem is amplified by the fact that within our own nation states, going by all of my experience of 20 years of legislation and as I am sure Mr. Cicilline will confirm, if a government wants to defeat something that is coming at it, it will try to split ranks and sow confusion. What is happening is that each nation state is looking at the benefits of employment, the tax take and so on versus its own security and the security of democracy. That becomes an internal discussion within each country. It is certainly true in the United Kingdom, Ireland and other countries. It further confuses the entire issue.

We are looking at various possible solutions. I totally support everything Ms Cadwalladr

said. What she did not mention that is bang up to date is the suppression of the Grieve report. We have a report that has been right the way through all of our institutions, but the Prime Minister personally has refused to release it. We had a question in the House of Lords on Tuesday when the Front Bench spokesman, the Minister, confirmed that it was a personal decision of the Prime Minister. That is outrageous. Our entire democracy relies on what is termed the "good chap" principle, that the Prime Minister of the day, man or woman, behaves like a good chap. I am sorry about the gender inflection, but that is the way it is. We are going through a process, whereby all norms are being defied. That is playing to the benefit of the major social media companies, which is very worrying.

We have had one suggestion made to us as a committee by which I am intrigued, namely, the possibility of having a Euro SWAT team of high competence that could be moved around in situations where there was palpable vulnerability to democracy on the grounds that the problem was so enormous no one country would be able to put together the permanent competencies to deal with it. Having a European SWAT team that would be constantly looking for it and that could be moved around might be one at least temporary answer to the problem we are discussing. Does anyone have a view on it?

Mr. Ben Nimmo: On having a SWAT team, absolutely, what we need is far more investigators in this space who would do this work all the time. There are probably more countries committing to information operations than there are people who are studying them; therefore, there is a massive problem. I would not, however, want to see a Euro SWAT team run by governments because giving governments the right to decide what goes up and what comes down is fundamentally something to which I would object. One nuance on information operations is that quite a lot of the time they do have an interest in achieving a specific outcome. We could see, for example, that the Russian operation in 2016 was very definitely about stopping Hillary Clinton from being elected. There are outcome-specific cases. A lot of the information operations we see are about increasing polarisation. That is where we need to have a conversation, not so much about the operations but about the underlying social dynamic of why polarisation happens in the first place.

Chairman: We will move to Congressman David N. Cicilline from the United States of America.

Mr. David Cicilline: In the wake of the scandal of Cambridge Analytica, the committee has undertaken really important work to advance our understanding of data privacy, threats to democracy around the world in the digital age and the role of anti-trust and competition in the digital economy. These problems are not confined within geopolitical borders. They are real and affecting our democracies in fundamental and lasting ways. It is essential that we work together to find solutions to restore the Internet's promise. The committee was established to work out some solutions to these problems, as Chairman Bob Zimmer noted during the last meeting, and I strongly support that goal. To quote one of our panellists, Ms Cadwalladr, democracy is not guaranteed and not inevitable. We have to fight and we have to win as we cannot let the tech companies have this unchecked power. I want to begin with a question to Ms Cadwalladr. I thank her for the incredible work she did in her extensive investigation and reporting on the impact of Facebook on elections and our democratic institutions. Her work reinforces why a free and vibrant press is so critical to our democracy and holding those in power to account. One of the challenges we face in the United States is having people understand the impact of this one-on-one micro targeting of politicals and issue advertisements and how they work. I wonder if Ms Cadwalladr could speak to this for one moment, particularly about micro

targeting in the political context.

Ms Carole Cadwalladr: What is most troubling about it for me is that individuals have no idea why they are being targeted or on the basis of what data they are seeing an advertisement. Somebody who lives in the same house might be targeted with a different advertisement and people would not be aware of it. This happens in darkness; therefore, it is influence being brought to bear on individuals based on unknown information that is being collected on them across the Internet. It is a really different idea about politics and elections from those we have had at any other time. It seems to be completely incompatible. We previously had a situation where parties and politicians would come up with ideas and place them in the public domain. We would have had a discussion about them and then voted on them. Now they are finding out information on you and in what you are interested, crafting a particular policy that somehow might speak to it and showing it to you in darkness, as it were. That is just not known to the rest of society at all and it is profoundly anti-democratic.

Mr. David Cicilline: Dr. Lillington has made some public criticisms of Facebook's decision to allow false political ads on its platform, as have I. There was an open letter published by hundreds of Facebook employees who have criticised this policy. Can Dr. Lillington see any defence for it?

Dr. Karlin Lillington: No. That is the very brief answer. It connects directly to what Ms Cadwalladr is speaking to also. On the idea that one can be allowed to micro target people with advertisements and then justify letting politicians or campaigns state anything they like about issues in these secretive advertisements that the entire Commons does not get to see means that Facebook's defence that it is a free speech issue and that people should be allowed to say what they want and then the voters can decide, the thing is if I am highly targeted with a single advertisement that appeals to ways in which they understand, I can be persuaded owing to micro targeting and how does anybody else dispute it? How do people have a discussion at the dinner table with their family if they have not all seen the advertisement in the newspaper or on television? There is no defence.

Mr. David Cicilline: I thank Mr. McNamee for his brilliant work and leadership on so many of these issues. I wonder if he would spend a moment speaking about the implications for the proposal he has suggested to recognise data privacy as a human right. Would it solve the problem in a way that some of the things like purpose specification and a number of other approaches might not?

Mr. Roger McNamee: At the end of the day, when we think about the current model and the end point, in the United States there are 220 million registered voters. In principle, there could be 220 million campaigns, each completely isolated from the next. The metaphor I use is imagine going to the doctor with a broken arm. Imagine if the doctor repaired the arm and then said, "I own your arm now." That is what happens with data. Any corporation that touches a piece of data claims ownership and the ability to do whatever it wants with it. Because there is a free market, they can create what Tristan Harris calls a data voodoo doll, a complete representation of a person's life in all respects. It is effectively part of one's body. The notion that they are allowed to unilaterally exploit it to predict and manipulate a person's behaviour strikes me as being profoundly inappropriate. We can attack this by going after symptoms or we can attack the problem. In my mind I would like to reset and go all the way back to where we were 25 years ago and say data cannot be used in any way. There would be no models or anything else. We could then have a reasonable conversation about what uses of data were appropriate and which were not. That is instead of starting with the assumption that all things are good and trying to

subtract from it. Such a process has brought us to a bad place. The implication is very simple. In the short run both Google and Facebook would lose profoundly in their earnings, but they would both have massive opportunities to rebuild them. To my mind, their profits should not be the first consideration of society. As somebody who has been involved with that world my whole life, I look at this issue while knowing the creative forces around the world will replace those functions instantaneously. It would be only a matter of weeks before one would have a global standard for alternatives based on good business models if they were willing to do it.

Chairman: We have some more time if others wish to comment.

Mr. Tom Packalén: Mr. McNamee has mentioned that moderation is not possible before damage may be done. It is possible and to artificial intelligence questions, the solutions are artificial intelligence ones. It is impossible to handle those amounts of data manually, as Facebook is doing. It does not really want to do it. If there was a willingness to pursue these solutions, it would be possible. With respect to business models, there are identity bubbles; therefore, why does it not do "pre-moderation" with artificial intelligence?

Mr. Roger McNamee: Honestly, I do not know the answer to that question. Speaking philosophically, Mr. Mark Zuckerberg and the founders of Google believe efficiency is the most important goal in the universe; therefore, they are trying to eliminate friction. Everything needs to be automated and scalable. As many things as possible would be ignored. The notion of regulations and criticism is a form of friction with which they would not like to deal. If Mr. Zuckerberg puts in place an AI-based moderation system that can find 98% of child pornography, the problem is we would be dealing with billions of transactions and being only 98% right still means there would be tens of millions or hundreds of millions of failures. In the context of democracy, that is completely unacceptable. As much as I believe artificial intelligence will evolve eventually to having very powerful capability, today it is far more limited than the people who are pushing it are willing to admit.

Deputy James Lawless: One of the weaknesses where the platforms get around existing obligations and we need to legislate for new obligations is the platform-publisher chestnut. They say they are just a dumb terminal displaying binary code which is throwing up content and that in that way they are just a carrier. To my mind, the companies are curating content and selling advertisements based on personalised content. They are moderating content and making decisions about what can be taken down or left up. They have many of the attributes of a publisher. What do the delegates think?

Mr. Roger McNamee: Algorithmic amplification involves a business decision that should be treated completely separately from the publisher versus platform decision. It is a business choice and they should be liable for the consequences of predictable failure.

Dr. Karlin Lillington: We are well past the time when perhaps these platforms need to be termed as being some kind of hybrid between publisher and platform, with existing laws applying to them and making much of this work in a simpler way.

Lord Puttnam: To whom should a European SWAT team be accountable, if not governments? I agree on the point, but we must create an accountability framework.

Mr. Ben Nimmo: I am sorry, but I may have been unclear. I distinguish between accountability in terms of who is paying for it, who is organising it and how it is organised. I envisage having something almost like a police force which would be subject to and accountable to the

law but not directly run by the political parties.

Lord Puttnam: Would it be like a specialist Interpol?

Mr. Ben Nimmo: It could be a specialist Interpol and there are many hypothetical models that could be used. We would want to have a body that would have to report to the government and law enforcement agencies but which would not be controlled by any political grouping or party. A government could not tell it what to do.

Ms Carole Cadwalladr: Lord Puttnam spoke about Mr. Boris Johnson personally blocking the report on Russia. I was wondering if he had any idea why Mr. Johnson would be personally invested in blocking a report on Russian interference in British politics. I could offer a couple of suggestions as to why that might be the case, but perhaps Lord Puttnam might like to comment first.

Lord Puttnam: The Hansard debate is very interesting. My belief is the report is being blocked because it begs real questions about the legitimacy of the original referendum. The last thing in the world Mr. Boris Johnson wants is a debate about the legitimacy of that result.

Ms Carole Cadwalladr: Mr. Johnson was British Foreign Secretary after the referendum in 2016 during, for example, the period in which we know that Mr. Arron Banks and Mr. Andy Wigmore were continuing to visit the Russian embassy in London, while they were also campaigning for Mr. Donald Trump in America. That is the Russian ambassador who was named in the Mueller report as being a conduit between-----

Chairman: We need to be careful about naming people at this committee.

Ms Carole Cadwalladr: It is the Russian ambassador to London who was named by Mr. Robert Mueller as an intermediary between the Trump campaign and the Kremlin.

Dr. Janil Puthucheary: One of the problems for the committee is that this industry is not adequately regulated. In no other industry domain have we tried to have a global set of standards prior to the industry adhering to national laws or national sovereignty in regulation in the first instance. The tension arises as there is an issue about the accountability of platforms and the varying measures of accountability different countries and jurisdictions use in of the strength of democratic institutions brought to bear on the problem. I just want to get a sense from the delegates, on the work of the committee, of how we can balance the tension in arriving at some transboundary set of standards and norms versus solving the very practical problem of getting tech companies to adhere to local laws in the first instance.

Dr. Karlin Lillington: I suggest the GDPR as a model in the European Union. I have been covering technology issues for 20 years and there was always a very dismissive attitude taken towards privacy issues, that the European Union would never do anything and that the United States could do whatever it wanted. The GDPR forced everybody to rise to the level of privacy offered there.

Dr. Janil Puthucheary: I appreciate that, but the GDPR only covers the European Union.

Dr. Karlin Lillington: Yes, but it has forced countries outside it to rise to a level of oversight. It can form a basis to bring more to that level.

Dr. Janil Puthucheary: Yes.

Chairman: We will shortly suspend the sitting as we are approaching the end of the session. Perhaps Senator Higgins might be brief.

Senator Alice-Mary Higgins: I will go straight to the business model and looking at some of the key intersecting issues. Are there issues about data points and special categories of personal data being allowed to be used in micro targeting or algorithmic construction? To what extent do we economically and algorithmically reward the giving of misinformation? What is the intersection between Google Ads rewarding misinformation sites and advertisements appearing on trusted sites? Is there space to be exploited by publishers in trusted national spaces like national newspapers?

Dr. Johnny Ryan: The answer is "Yes". The GDPR makes personal data privacy a fundamental right. We have over 51% of global GDP if we consider all of the jurisdictions with GDPR clones on the way. There is a question about special category data, which is very sensitive information about people. If one were to ask Facebook what it thinks about the fact that I might attend a Catholic church and read about Catholic issues, the response would be that that is an interesting collection of interests but it will only accept as special category data the word "Catholic" if written in the box next to religion. We have to be careful with these industries, even when there are tight, legal definitions. Where the enforcers are asleep in the middle of systematic infringement of this new regulatory framework which is emerging as a *de facto* global standard then this place being the home of that framework will show that the framework is not sustainable.

Senator Alice-Mary Higgins: I am not sure if that data is key in that regard. What they call "observed data" can be personal data. In terms of the ring-fencing-----

Chairman: I apologise for interrupting, but I have to cut Senator Higgins off. We are on a really tight schedule. I thank the witnesses for being here. We will suspend for 15 minutes to allow our parliamentarians to take a break before we commence the next session.

Sitting suspended at 10.31 a.m. and resumed at 10.45 a.m..

Session 2: Industry Perspective

Chairman: I welcome Dr. Monika Bickert, vice president of content policy at Facebook; Mr. Jim Balsillie, chair of the Centre for International Governance Innovation; Mr. Marco Pancini, director of public policy at YouTube EMEA Google; Ms Karen White, director of public policy at Twitter; and Mr. Ronan Costello, public policy manager at Twitter.

I advise witnesses that by virtue of section 17(2)(*l*) of the Defamation Act 2009, they are protected by absolute privilege in respect of their evidence to the committee. If they are directed by the committee to cease giving evidence on a particular matter and they continue to do so, they are entitled thereafter only to a qualified privilege in respect of that evidence. They are directed that only evidence connected with the subject matter of these proceedings is to be given and they are asked to respect the parliamentary practice to the effect that, where possible, they should not criticise nor make charges against any person, persons, or entity by name or in such a way as to make him, her or it identifiable. Any submissions or opening statements made to the committee will be published on the committee website after the meeting.

Members are reminded of the long-standing parliamentary practice to the effect that they

should not comment on, criticise or make charges against a person outside the House or an official by name or in such a way as to make him or her identifiable. I will give witnesses an indication when four minutes are up to let them know they have one minute left. We will start with Dr. Bickert.

Dr. Monika Bickert: I will not read my entire submission. I will just hit some high points. I thank the Chairman and the members of the Oireachtas Committee on Communications, Climate Action and Environment for inviting me to speak to it and the other International Grand Committee members today. I am the vice president of content policy at Facebook and based in our Menlo Park headquarters in California. I joined Facebook in 2012 after serving 11 years as a US public prosecutor and as regional legal adviser at the US embassy in Bangkok, Thailand. I now lead Facebook's global content policy team. My team's responsibilities include developing and enforcing the rules for how people can use our services. My remit also now includes work to further our company's goal of facilitating appropriate regulation of content on social media platforms and the broader Internet.

Facebook welcomes governments and regulators taking a more active role in addressing harmful content online. Protecting the people who use our services is a top priority, to which we continue to dedicate a great deal of time and resources, but we do not believe any company should tackle these issues alone. This is why we work together with governments, civil society, experts and industry peers to develop rules for the Internet that encourage innovation and allow people the freedom to express themselves while protecting society from broader harms.

The aim of the committee's session today is to advance international collaboration in the regulation of harmful content, hate speech and electoral interference. Facebook shares this goal and I am grateful for the opportunity to share our thoughts on how to meet it.

Freedom of expression is a core value of our company. Facebook exists to give people a way to connect and express themselves. At the same time, we want to make sure that people using our services are safe. That means we must make decisions every day about what is and is not acceptable among our community of 2.8 billion people. Some of these decisions are clear but many are nuanced and involve balancing competing principles like voice, dignity, safety and privacy. We work hard to get these decisions right and we have community standards that define what is acceptable content. Those standards are informed at every turn by relationships with hundreds of civil society groups and experts around the world.

We invest heavily in technical solutions to quickly identify potential violations of our rules. For example, more than 99% of the terror propaganda we remove from the site is content we identify ourselves using technical tools before anybody has reported it to us. We also have more than 10,000 people working around the clock to assess whether content is violating our rules and removing it if it is. We respond to the overwhelming majority of reports of potential violations within 24 hours. We publish transparency reports about how effectively we remove harmful content. These documents, which are publicly available, show how much content we are removing in each category and how successful we have been in trying to identify that content before it is reported to us. Nevertheless, we know that with such a diverse community, the lines we draw will never please everyone and we will never be perfect in enforcing these lines. To address these challenges, Facebook is creating an independent body called the oversight board to which people can appeal our decisions on content they have posted but we know that this too will not solve all of the challenges we face. We believe that a more standardised approach would be beneficial. Regulation could set baselines for what is prohibited and guide the development of systems to better address harmful content.

In the area of elections, regulation could address important issues such as the definition of political advertising, who is allowed to run political advertisements and what steps those persons must take before doing so. Regulation could also address how political parties can and cannot use data to target political advertising. We believe that Facebook and companies like it are central to solving these complex challenges but it is clear that we cannot and ought not do this alone. In that spirit, we look forward to collaborating further with governments, civil society, industry and all of the people who hold a stake in creating rules for a safe and innovative Internet.

Mr. Jim Balsillie: I thank the committee for the opportunity to present to it today. The committee's leadership on issues related to data governance inspires many well beyond Ireland's borders. I am the retired chairman and co-CEO of Research In Motion, a mobile data services firm we scaled from an idea to $20 billion in sales. My expertise is the commercialisation of technology, specifically for multi-sided platform business model strategies and their network effects.

In the attached appendix, I list the six recommendations I made at the IGC meeting in Ottawa in May. Today, I will explain three foundational elements that underpin all of my recommendations because a stable, long-term solution to the current challenges lies in confronting them systemically.

The current business model is the root cause of the problems the committee is trying to address. Its toxicity is unrelenting. It is not a coding glitch that a legal patch will fix. Data at the micro-personal level gives technology unprecedented power and that is why data is not the new oil. It is the new plutonium - amazingly powerful, dangerous when it spreads, difficult to clean up and with serious consequences when improperly used. A business model that makes manipulation profitable is a foundational threat to markets and democracy. Democracy and markets only work when people can make free choices aligned with their interests, yet companies that monetise personal data are incentivised by and profit from undermining personal autonomy. Whistleblowers inside platform companies told us that "the dynamics of the attention economy are structurally set up to undermine the human will." That is why we need to outlaw the current business model and reintroduce responsible monetisation, such as subscription-based models. Strategic regulations are needed to cut off the head of this snake. Anything less means governments will be perpetually coping with its slithery consequences turning policymaking into a losing game of regulatory whack-a-mole.

Silicon Valley's business plans are not political programmes. The contemporary technology sector is an industry that celebrates engineering as an alternative form of governance. It distrusts the political process and disregards the public interest. Its concentration of power is owed to the features of the modern knowledge-based and data-driven economy that tip markets through its steep economies of scale, powerful economies of scope, pervasive information asymmetry and network externalities. Technology is not governance; it must be governed. The choice we face in 2019 is not between Facebook and China, which paradoxically borrow from each other the tools and tactics that encode their grip on power. The option we face is either a social choice mediated by democracy or social outcomes engineered by unbridled, unethical and unaccountable power.

A global digital stability board is needed to institutionalise co-ordinated responses and underwrite a progressive digital future. Cyberspace knows no natural border. The Cambridge Analytica scandal involved Canadian technology on a US platform paid for by Russian and US money to interfere in a British referendum over its future in the European Union. The busi-

ness model that enabled this, nourished by discredited neoliberal policies, turns customers into products. If left unaddressed, it will render liberal democracy and free markets obsolete. The timing is urgent. In North America, record-setting lobbying expenditures by data-driven platforms resulted in chapter 19 of the United States-Mexico-Canada Agreement, which includes provisions that lock in the current advertising-driven business model and prevent lawmaker oversight of algorithms. The current US Administration is working to entrench these rules globally through the World Trade Organization negotiations on the trade-related aspects of e-commerce. We have arrived at a new Bretton Woods moment where new or reformed rules of the road at the international level are needed. They should be rules that preserve an open global trading system yet, at the same time, respect a nation's sovereign ability to regulate the data-driven economy's profound cross-cutting economic, security and social effects. I have proposed the creation of an organisation that would be akin to the Financial Stability Board that was created in the aftermath of the 2008 financial crisis. Industry can be part of the solution by acknowledging the toxicity of the current business model and migrating to responsible revenue generation for services.

Mr. Marco Pancini: I thank the committee for the opportunity to join its deliberations today. I lead YouTube's public policy work in Europe, the Middle East and Africa. I have over a decade of experience in online safety issues and I am centrally involved in our work to keep our users safe every day. This committee's work over the past year has addressed a range of critical topics, including privacy, misinformation, election integrity and more. In our testimony before this committee previously, we outlined Google's commitment to information quality and how continued collaboration improves the ways we all address harmful content online. Today, I will focus on YouTube's efforts and outline improvements we have made to address misinformation on that platform. I will also highlight opportunities for greater collaboration among companies, government and civil society to tackle this challenge.

YouTube is an open platform where anyone can upload a video and share it with the world. The platform's openness has helped to foster economic opportunity, community, learning and much more. Millions of creators around the world have connected with global audiences and many of them have built thriving businesses in the process. At the same time, YouTube has always had strict community guidelines to make clear what is and is not allowed on the platform. We design and update our systems and policies to meet the changing needs of both our users and society. Videos that violate those policies generate a fraction of 1% of total views on YouTube, and we are always working to decrease that number. In fact, over the last 18 months, we have reduced the number of views of videos that are later removed for violating our policies by 80%.

Our approach towards responsibility involves four Rs. We remove content that violates our policy as quickly as possible. We raise up authoritative voices when people are looking for news and information, especially during breaking news moments such as elections. We reduce the spread of borderline content and harmful misinformation. We set a higher bar for what channels can make money on our site by rewarding trusted, eligible creators. Over the past several years, we have used those four approaches to address misinformation.

While we remain vigilant against new threats, we are proud of the progress we have made. We have raised up quality content by, among other things, implementing two cornerstone products, namely, the top news shelf in YouTube search results and the breaking news shelf on the YouTube homepage. These products highlight authoritative sources of content and are now available in 40 countries. We have worked especially hard to raise up authoritative and useful

information around elections. For example, earlier this year, we launched information panels in YouTube search results. For example, when users were looking for information about official candidates running for seats in the European Parliament in May we showed them authoritative information. We have continued our strict enforcement of YouTube's policies against misleading information and impersonation. From September 2018 through to August 2019, YouTube removed more than 10.8 million channels for violation of our spam, misleading and scam policy, and more than 56,000 channels were removed for violation of our impersonation policy. We have also undertaken a broad range of approaches to combat political influence operations, which we have regularly reported over the course of the past two years. For example, in September, we provided an update about disabling a network of 210 channels on YouTube when we discovered they behaved in a co-ordinated manner while uploading videos related to the ongoing protests in Hong Kong. We have also worked hard to reduce recommendations for content that is close to a policy line but does not violate it, including attempts to spread harmful misinformation. Thanks to changes we have made over the past year, this type of content is viewed as a result of recommendations over 50% less than before in the United States. YouTube has begun experimenting with this change in other countries, including Ireland and the UK, and we will bring it to other European markets soon. We know that this work is not done. That is why we continue to work with law enforcement, industry and third-party experts around the world to continue to evolve our efforts.

I will conclude by discussing opportunities for greater collaboration. The EU code of practice on disinformation is an important foundation that we can all build on. Launched just over a year ago, the code was developed in light of work that we and others had been pursuing with experts and publishers around the world to elevate quality information and support news literacy. As part of the process, we have provided regular reports on our efforts to address disinformation and we have highlighted the work that we can do collectively in this regard.

We must continue to support collaborative research efforts. For instance, we have invested in research on the detection of synthetic media, often referred to as deep fakes, and have released data sets to help researchers around the world to improve audio and video detection. We have also made the data about our election advertising efforts available in the transparency report. This information is available to everyone, including governments, industry and experts. We can work together with this data to improve matters. We strongly believe that addressing harmful content online is a shared responsibility, which is why we are so committed to meetings and collaborations like these. We are committed to doing our part and we look forward to answering members' questions.

Ms Karen White: I thank the committee for the invitation to participate in today's session. I am the director of public policy for Twitter in Europe. I am joined by my colleague, Mr. Ronan Costello, public policy manager for Twitter in Europe. We are pleased to be here with the committee today for this session which aims to focus on how industry can be part of the solution. Twitter is committed to improving the collective health, openness and civility of the conversation on our platform. Our success is built and measured by how we help to encourage more healthy debate, conversations and critical thinking. Conversely, abuse, malicious automation and manipulation detract from it.

I will use this opportunity to briefly walk through three specific areas where Twitter has been doing critical work to prioritise online safety and election integrity. These include our investments in proactive technology to better enforce the Twitter rules, our policies on political advertising and synthetic or manipulated media, and our focus on state-backed information

operations. I will also share some insights into the structural and operational changes Twitter has made since 2017 to protect conversations on the platform during elections while building partnerships that promote a better understanding of our online environment.

It would be instructive at this point to re-emphasise the public commitment made by our CEO, Jack Dorsey, in May 2018 to prioritise the health of public conversation on Twitter above all else. He recognised that the platform had come to be used in ways that were harmful and unforeseen and he said Twitter would hold itself accountable towards progress. Since then, we have leveraged a combination of policy, people and technology to yield positive results. It is our view that people who do not feel safe on Twitter should not be burdened to report to us, so we have significantly ramped up investment in proactive technology and tools to better tackle issues such as abuse, spam and automation, which detract from people having healthy experiences on our service.

More than 50% of the tweets we remove for abuse are surfaced proactively for human review by technology, rather than relying on reports. This is an increase from 20% last year. While we will strive to improve this further, it is a significant enforcement milestone and a positive indicator that our investment in technology is helping us to tackle abusive behaviour at scale. Figures released just last week in the latest edition of our biannual transparency report further outline the trends and progress we saw in the first half of this year. We have increased by 105% our rate of action on violating content. We took action on 133% more accounts for violation of our hateful conduct policy. We took action on 68% more accounts for violations of our policies on abuse. Taken as a whole, the progress I have summarised reflects Twitter's mission and commitment to enhance the health of the public conversation on our service.

The scale, speed and targeting effects of online political advertising have been widely discussed lately. Last Wednesday, our CEO announced that Twitter had made a decision to stop all political advertising. This policy is global, includes all candidate and issue advertisements and will come into effect in the very near future. We continue to update our rules and policies in response to evolving threats and technological challenges. We share the public concern regarding the use of disinformation campaigns that rely upon the use of manipulated and synthetic media, commonly referred to as deepfakes.

On Monday, 21 October, we publicly announced that we have been working on a policy to address comprehensively synthetic and manipulated media on Twitter. In the coming weeks, we plan to open a public feedback period to get input on this from the public. We want to listen and consider a variety of viewpoints in our policy development process and we want to be transparent about our approach and values.

We appreciate that some of the threats on our platform can be urgent, and our expertise and analyses can be bolstered by partnerships with external researchers, journalists and academics. One area where we have unlocked these valuable partnerships to help provide more transparency on our platform is in the area of state-backed information operations. For more than a year, we have been publicly disclosing comprehensive datasets of tweets and related media information we identify on the platform that we have attributed to malicious state actors. We launched this initiative to empower academic and public understanding of these co-ordinated campaigns around the world and to enable third-party expert analysis of these threats and tactics. Using our archive, these researchers have conducted their own investigations and publicly shared their insights and independent analyses.

Since January 2017, we have launched numerous election related product and policy chang-

es, expanded our enforcement operations and strengthened our team structure. We further expanded our enforcement capabilities for global elections by creating a dedicated reporting feature to allow users to report content that undermines the process of registering to vote or engaging in the electoral process. This reporting feature was first used this year for the Indian and European Parliament elections.

The challenges we face as an online society are complex, constantly evolving, and often without precedent. Industry and Twitter cannot address these issues alone. Nor is our industry monolithic in its approach to these issues. Each of us has different services, varying business models, and often complementary but distinct principles. This should be recognised as we continue our engagement. Every stakeholder in this conversation has a role to play. We propose a whole-of-society approach to improving the health of online conversation and citizenship. We all need and deserve a thoughtful approach and long-term perspective in this discussion, and Twitter very much welcomes the opportunity to participate.

Chairman: We will start with Australia and I ask the witnesses to try to keep their answers as short as possible to give the parliamentarians time to question them.

Mr. Milton Dick: My first question is for Dr. Bickert. My colleague, Ms Carol Brown, and I, are Members of the Australian Parliament. In Dr. Bickert's written submission, she states Facebook does not believe:

> ... that a private company should be determining for the world what is true or false in a politician's statement. This doesn't mean that politicians can say whatever they want on Facebook.

I appreciate Dr. Bickert will not know every nation's issues to do with her company and I am happy to speak further offline to her about the matter I am about to raise. In our recent election in May this year, in which I was a successful candidate, a campaign was waged anonymously through Dr. Bickert's platform against the party I represent with regard to a death tax and inheritance tax. This campaign was false and misleading. Advertisements were posted and anonymous statements were made. Despite our nation's complaints to Facebook executives, no action was taken. Why was this?

Dr. Monika Bickert: With respect to the specific advertisements mentioned, I would have to talk to colleagues to understand them. I am happy to follow up. In 2017, we introduced an advertisement library whereby we have brought unprecedented transparency to political advertising. Now when somebody runs a political advertisement on Facebook, people can see who is running the advertisement and we verify identity. We also make public the audience for that advertisement, the dates it ran, and any other advertisements that party is running.

It is not a free game for political advertisements. They must adhere to our advertisement standards, which are a step above our community standards. The community standards have measures such as a prohibition on hate speech and threats. The advertisement standards go higher and they are the standards that are applicable to any of the political advertisements that are run.

Mr. Milton Dick: In terms of advertising, in her statement Dr. Bickert said Facebook does not believe a private company should be determining for the world what is true or false in a politician's statement. How does that intersect with the standards?

Dr. Monika Bickert: From what Mr Dick has just described, it sounds like the advertisements mentioned were not run by a politician, so let me explain the difference.

Mr. Milton Dick: They were. They were run and sponsored by elected representatives of the Parliament. Anonymous fake accounts were set up to support them. Videos were collated with the unrelated and irrelevant words "death tax" and "inheritance tax", as said by my colleagues, spliced and put into advertisements that were sponsored and paid for on Dr. Bickert's platform.

Dr. Monika Bickert: Any account run under a false name or inauthentically violates our policies and should come down. We also have a mechanism for sending to third-party independent fact checker organisations, certified by the Poynter Institute, information that is likely to be false. They can rate that themselves. We also have tools and user reporting systems that will send information to them. If those fact checking organisations rate something as false, we put that information next to the information that is being seen and we do not run the advertisements. If something is directly from a politician and if the politician refers to something such as a link or an image that has already been debunked by a third party fact checker, the advertisement will not run. However, if the politician himself or herself is engaging in direct speech, he or she is held to our advertisement standards but we do not police whether the information is true. We do not believe we are the right entity to do this and we do not believe it is something we could do to the satisfaction of all involved.

Mr. Milton Dick: Does Dr. Bickert think more needs to be done in the area of fact checking on Facebook?

Dr. Monika Bickert: This is a primary area where we have actually called for regulation. We think the purpose of this hearing today to see how we can collaborate further is entirely appropriate and we are very open to discussing what regulation in that realm could look like.

Mr. Milton Dick: What, in Dr. Bickert's opinion of the company's position, does she see as appropriate regulations?

Dr. Monika Bickert: Especially in the area of political advertising, definitions would be very helpful, such as defining what a political advertisement is, when it is appropriate to run the advertisements, who are the appropriate parties to run them, and what are the appropriate verifications. I will say the verification process has proved to be not simple. We mail people if they want to run a political advertisement. Part of the authorisation process involves us mailing something to them to confirm their identity because we do see the upload of false documents. These are challenging areas, but we are very open to regulation.

Mr. Milton Dick: Will Facebook look at the Twitter model that was announced on 21 October about political advertising? Is Facebook considering this?

Dr. Monika Bickert: We are very open on what the next steps are to improve our political advertisements and how people encounter them on Facebook. We think it is an important part of the political dialogue. It is an important part of the way policy makers often communicate with their constituents and we want to try to preserve that. We also want to make sure we are acting responsibly, and we are very open to that dialogue.

Chairman: We will now move to Estonia and I invite Ms Keit Pentus-Rosimannus to ask her questions.

Ms Keit Pentus-Rosimannus: I thank the witnesses for their statements and for the work they have already done to increase preparedness for fighting disinformation. My first question is for Facebook. I want to use this opportunity to get a better understanding of the principles behind its policy on political advertisements. I have understood from the previous answer that the current state is still that Facebook does not fact check political advertisements. Is this correct?

Dr. Monika Bickert: Not exactly. We do not send to our fact checkers advertisements containing direct speech from politicians. Other political advertisements may be sent to our fact checkers. I should point out the fact checking framework we have is relatively new. We only developed a process for sending advertisements to fact checkers in August 2019. Prior to August 2019, this was not something that would have been a process. We have never sent direct speech from politicians in advertisements to fact checkers. We thought it was important to make this clear, so recently we publicly reiterated it.

Ms Keit Pentus-Rosimannus: Will Dr. Bickert explain why Facebook does this? Why is it for all other Facebook users there is no right to lie on Facebook and Facebook does not take money from those advertisements but for politicians it is okay to lie and Facebook accepts money for the advertisements that spread the lies?

Dr. Monika Bickert: Let me be clear. It is not that we think it is okay for people to lie. We think that when people come to Facebook freedom of expression is one of the best ways the truth comes out. The fact we do not think Facebook should be the truth police for the entire world and that we should not determine for citizens what they shall and shall not see in terms of truthfulness from their politicians does not mean we dismiss the importance of combating disinformation. There are several things we do to combat false statements on Facebook. First, we go after fake accounts that the data have told us time and again are disproportionately more likely to be sharing disinformation. Second, we disrupt the financial incentives. Most disinformation, and this includes political disinformation, is shared to make a profit. It leads to ad farms. We have gotten much tougher on that. Finally, for content that is around the border and run in somebody's real name, we now have a process for allowing third party fact checkers to check that information. When it comes to the direct speech of a politician, we do not think it is appropriate for any private company to interfere between that politician's speech and the citizenry and saying this is true and this is false.

Ms Keit Pentus-Rosimannus: Is it still all right to interfere in all the other ads except politicians' ads?

Dr. Monika Bickert: Sorry, could Ms Pentus-Rosimannus repeat that?

Ms Keit Pentus-Rosimannus: In any other ads, Facebook still interferes and does not let the false advertisements run on its service. However, it does not interfere when it comes to politicians and, therefore, it is all right for politicians to spread lies on Facebook.

Dr. Monika Bickert: To be clear, we are not the truth police for the world. We do not remove content simply for being false outside of a couple of small areas such as if there is an immediate threat to safety and a safety partner has confirmed for us that there is an imminent risk of harm or if somebody misrepresents voting times, locations and processes. Generally, when we use those third party fact-checking organisations, we do not remove content they say is false; we mark that as having been rated false by the fact checker and we put the information from the fact checker next to it.

Ms Keit Pentus-Rosimannus: That does not necessarily make it much better. A few people have said the change in Facebook's policy, where it refuses to take down false political ads, has happened because it allows Facebook to accept millions upon millions of dollars from upcoming large and important campaigns and spread information that is knowingly false as political ads. How does Dr. Bickert answer those accusations?

Dr. Monika Bickert: These ads represent a very tiny portion of our ads' revenue.

Ms Keit Pentus-Rosimannus: Can Dr. Bickert be specific on that? In 2016, for example, what was Facebook's approximate earnings from political ads versus all other ads?

Dr. Monika Bickert: I believe Mark Zuckerberg clarified this publicly. I do not have the exact statistic on hand. We can follow up with Ms Pentus-Rosimannus on that but suffice it to say financial motivations do not lead us to have this policy. We make very little from these ads. That is because we do not believe that it is appropriate for a private company to decide for the world what is true or false coming from their politicians and we do not think we could do so effectively.

Chairman: I will move to Finland next and call Mr. Tom Packalén.

Mr. Tom Packalén: I thank all the guests for their presentations. Many of them have done a good job and we are going in a better direction. It is important companies take on their responsibilities beforehand. We must have tight regulation with respect to what is bad and difficult for everyone.

My question is for Dr. Bickert. With respect to false information, I understand it is very difficult to say what is false. Something is false for one person and means something else to another person but hate speech is a much easier target to discuss. For example, in Sri Lanka, people were burned alive because of the hate speech spread through Facebook. In Myanmar, there was violence against the Rohingya minority. I refer to what Facebook has done to prevent this. It has more than 10,000 moderators, as Dr. Bickert mentioned, but what can it do with them? The only way to address this is with an artificial intelligence, AI, solution. Mark Zuckerberg told the US Senate in April 2018 that it might take five to ten years to have this kind of technology but that is not true. A Finish company, Utopia Analytics, has offered to build Facebook a model in two weeks to get rid of the hate speech content originating in Sri Lanka but Facebook was not interested in it. Many companies do AI moderation. Will Dr. Bickert explain a little why Facebook will not go deeper into tackling hate speech and why it believes, with more than 10,000 moderators, it can handle billions of messages?

Dr. Monika Bickert: I very much agree it is important to tackle hate speech. It is, and has been, a focus for us and, like Mr. Packalén, we think that technology is an important part of that solution. We do not allow hate speech on our service. We have very strict policies against it. Our transparency report indicates that the majority of speech we remove for violating our hate speech policies is flagged by our automated systems before anybody has reported it to us. That number is now is in excess of 65%. Interestingly, Myanmar, is one of the areas where we have made the most progress. Back when our detection efforts removed approximately 50% of the hate speech we found with automated technology, in Myanmar, our detection rate was at 63%. We have focused on hiring people who are native language speakers and on building relationships with organisations on the ground that can help us spot trends. Those are very helpful but we also think technology is very important. We partner with others to improve that technology but we also invest significant resources ourselves.

Chairman: I now call Ms Nino Goguadze from Georgia.

Ms Nino Goguadze: I thank the guests for showing their openness to work together to address the challenges we face today. Facebook is the most broadly used social network in Georgia. It is the main source of information, especially among the younger generations. That is why I have question for Dr. Bickert on Facebook's operational system. In 2008, with Russia military intervention, Georgia experienced a severe cyberattack, which blocked critical digital infrastructure in the country. Our citizens were denied access to Facebook. In 2009, a similar cyberattack took place. We had no access to Facebook and Twitter and one can imagine the effect of that when Facebook is most important source of information for the country. That fact was brought to international attention and even *The New York Times* pointed out how vital web tools and services are becoming to political discourse and how vulnerable they are to disruption. My question is whether, in 2019, Facebook has a policy to protect its users from political bullying or whether the company has a policy or any deterrent measures against countries which undertake attacks on Facebook users.

Dr. Monika Bickert: There is much to address in this question. We think, however, that it is very important to maintain open access for the public to Facebook. We have a team devoted to cybersecurity and that includes preventing hacking and cyberattacks, perhaps of the sort mentioned. We also focus on disrupting what we call "co-ordinated inauthentic behaviour". These are networks of accounts, sometimes state-run and sometimes not, trying to abuse our platform to share things such as divisive messaging, political messaging or intimidation. We have a team focused on identifying and removing those instances. It is not something we can do alone, so we partner closely with researchers, academics, security firms and others in the industry.

Sometimes we will get a lead from somebody else, we will do the investigation and then we will remove that network. When we do that, we are transparent about it and in our newsroom, we publish blog posts about the actions we have taken. That has been a major area of investment for us. Going after fake accounts has also been an important part of disrupting bad activity that may, or may not, again come from state actors. Our automated tools have got so much better that in the first quarter of 2019, we removed more than 2 billion fake accounts. Not all of those were designed to share disinformation but we were removing the vast majority of these accounts within moments of their creation. These are definitely areas of interest for us. We believe people should have access to Facebook.

Ms Nino Goguadze: Is this information about the policy available somewhere? Can I find it?

Dr. Monika Bickert: Yes. I will follow up with Ms Goguadze on this issue.

Ms Nino Goguadze: That is very good. Has Dr. Bickert every been in Georgia?

Dr. Monika Bickert: I have not been to Georgia.

Ms Nino Goguadze: That is fine. I invite Dr. Bickert. That would be a great opportunity not only to explore an amazing country but also to learn what kind of challenges such relatively small countries are facing today. It is important that small countries should be the focus of big social networks. The presence of Dr. Bickert in Georgia and her personal experience of the problems in small countries would be very important for Facebook, as well as for us. It should be a part of the policies of big social networks to take care of the challenges and problems faced by small countries.

Dr. Monika Bickert: I thank Ms Goguadze. Although people think of Facebook sometimes as an American company, more than 87% of the people using Facebook are outside of the United States. Ms Goguadze is correct that getting policies right in smaller countries is important for us and we are committed to building those relationships. We have a public policy team based around the world and my team is based in 11 offices around the world. I look forward to following up with Ms Goguadze.

Ms Nino Goguadze: I thank Dr. Bickert and I look forward to seeing her in Georgia.

Chairman: I will start with my own questions briefly. In its written statement, Facebook proposes to create an oversight body. Who will be on that oversight body? How independent will it be? Will those members be paid employees of Facebook? Will the body be funded by Facebook? It also appears that this body will be an appeals mechanism for people who want content removed by Facebook. We are here to ensure that social media platforms are safe environments and this does not seem to be helpful in ensuring we are working in a safe environment. This oversight body is instead going to allow people who have their content removed to appeal to Facebook to have that content restored. That is the opposite of what we are discussing. I invite Dr. Bickert to talk to us about that oversight body and those questions first.

Dr. Monika Bickert: We are launching the oversight board and while we do not think it is the perfect answer to all of these challenges, we think it is important to give people who have had content removed from Facebook the opportunity to appeal to an independent body. To go quickly through the questions posed by the Chair, we put out a charter in September 2019 that was the result of nearly a year of consultation in many countries with many stakeholders from different backgrounds. The result is that the board will have up to about 40 members. Those members will be chosen through a collaborative process between the co-chairs of the board, who will be initially selected by Facebook. Those co-chairs will then choose the additional members, with input from Facebook. That said, the decisions made by those members will be independent and binding. They will be paid by a trust that Facebook will fund, but those funds will be held and administered independently.

I will clarify the way that cases will get to this board. We have millions of cases every week where we make decisions. This board will be able to choose from among the decisions appealed to it by users. If Facebook finds a case where it is hard to make a decision, we will also be able to proactively send something to the board for it to make a decision.

Chairman: The board, therefore, will be essentially funded by Facebook and Facebook will essentially be choosing who is on this oversight body. Is that correct?

Dr. Monika Bickert: We are not choosing the individual members of the board. We have chosen the co-chairs in a collaborative process. There is far more information in the charter that we published and I am happy to follow up with the Chair on the details.

Chairman: There would be questions and concerns regarding the independence of the board. I highlight that from looking at this proposal initially. The perception is that this board would not be independent.

Dr. Monika Bickert: This is one of the challenges we face and one of the reasons that we had such a long consultation. We want the board to exist, which means that we have to pay for it in some form, although we are certainly open to other models of funding. We also, however, want to make it an independent body and that is why we have created the trust, or are in the

process of creating a trust, to fund the board.

Chairman: Facebook, however, is creating the trust.

Dr. Monika Bickert: We fund the trust and the trust will be administered.

Chairman: That is a concern.

Dr. Monika Bickert: The board members, who will be chosen by the co-chairs, will serve three-year terms and cannot be terminated because of their decisions. They have that independent authority and they are paid by the trust and not Facebook.

Chairman: My colleague from Estonia asked about political advertising. Twitter has announced that it is not going to allow any political advertising anymore. Mr. Zuckerberg has stated, however, that Facebook has no intention of implementing such a ban. Following on from that, how much revenue did Facebook earn in political advertising during the last presidential election in the United States and how much does it expect to generate in next year's presidential election?

Dr. Monika Bickert: I do not have specific figures to answer that question. I believe that Mark Zuckerberg has talked about electoral advertisements and how they have been and continue to be a very small, percentage of our advertising revenue. These decisions are not financially motivated. They decisions to allow political advertising are because we think that this is an important way that politicians are able to interact with their constituents.

Chairman: Would Dr. Bickert be able to provide those figures to us on the revenue?

Dr. Monika Bickert: I will follow up with the Chair. I know statements have been made on this issue and I apologise for not having those figures to hand. I will follow up on them for the Chair, however.

Chairman: That would be very helpful for the committee. I will come back to my Irish colleagues, but I will start with the representatives from Singapore. I call Dr. Puthucheary.

Dr. Janil Puthucheary: I apologise to the other members of the panel, but I am directing my questions to Dr. Bickert, as have all of my colleagues. I welcome her comments concerning Facebook being committed to addressing the issue of co-ordinated inauthentic behaviour. I would like to clarify that my understanding of how this functions is correct, however, and perhaps we could use the example given by Ms Cadwalladr and some others this morning concerning the upcoming British elections. I refer to a situation where the authorities are potentially concerned about co-ordinated inauthentic behaviour as an attempt to alter the British elections in the near future and Facebook is made aware of this information through the security services, government agencies, think tanks, academics and-or voluntary organisations. Ultimately, however, it would be Dr. Bickert's team that would then decide whether to act on evidence of co-ordinated inauthentic behaviour. The execution and timing of that decision might affect the British election. Is that correct?

Dr. Monika Bickert: Our policy against co-ordinated inauthentic behaviour is laid out publicly and those are the rules that we follow, so if-----

Dr. Janil Puthucheary: I understand. I have a very simple question. Ultimately, does Dr. Bickert's team decide to act upon this evidence?

Dr. Monika Bickert: Yes. We do so often in consultation with security firms.

Dr. Janil Puthucheary: Absolutely, but ultimately the decision is her team's, the timing and execution is her team's.

Dr. Monika Bickert: Yes. These are our policies; we apply them.

Dr. Janil Puthucheary: She can imagine the concern in the execution and timing. That may well have an effect on the election outcome.

Dr. Monika Bickert: Certainly, we will remove abusive content that we find and we are very public when we do that.

Dr. Janil Puthucheary: However, my understanding about the process is correct.

Dr. Monika Bickert: They are our policies and we apply them, absolutely.

Dr. Janil Puthucheary: Can I extend that perhaps to Irish law? I imagine Facebook has employees here and in Singapore. They are subject to Irish law surely.

Dr. Monika Bickert: Yes. I cannot speak to the direct applicability of which country's laws apply to which individuals.

Dr. Janil Puthucheary: Let me give an example. The Minister, Deputy Bruton, has suggested an online safety Act. There is been some public discussion here in Dublin about that. If it comes to pass, he has proposed an online safety commissioner. That may, for example, provide directions requiring the removal of content after adjudication, perhaps even court injunctions to enforce. Presumably, these would be served on Facebook employees here in Ireland. Would they need to check with Menlo Park and Dr. Bickert's team before complying with Irish law?

Dr. Monika Bickert: While I cannot speak to the specifics of Irish law, I can tell the committee that we have a process for evaluating and complying.

Dr. Janil Puthucheary: I understand that. The person subject to Irish law would not, therefore, in Facebook's view be required to comply with a direction constituted through Irish law.

Dr. Monika Bickert: No. My answer is that we have a legal team and a process in place for evaluating when we receive a request for a Government as to what is appropriate for us to do in terms of compliance.

Dr. Janil Puthucheary: I understand.

Dr. Monika Bickert: In our data use policy, we explain how we evaluate requests from governments with our processes.

Dr. Janil Puthucheary: I ask Dr. Bickert to explain the employees' letter that was circulated widely. Why are Facebook employees concerned about the company not observing election silence in compliance with local laws?

Dr. Monika Bickert: I cannot speak to the opinions of those individuals. I can say with that policy, as with all of our policies, we of course hear views across the spectrum - indeed we solicit them. When we refine our policies, part of that process involves talking to people across the company, but also civil society groups and experts outside the company. We want that diversity of thought.

Dr. Janil Puthucheary: I understand. This is my final question. Dr. Bickert's comments and assessments do not address any of the issues that are happening in end-to-end encrypted platforms such as WhatsApp and perhaps what is being proposed for other messaging services. They centre on Facebook's newsfeed-based products. In places like India and Brazil, there is good evidence that WhatsApp has been compromised, weaponised and exploited for the purposes of disinformation as well as affecting elections. Have any Facebook employees in its safety team or otherwise expressed serious concern about the weaponisation and use of WhatsApp and other closed platforms for this purpose? Does Facebook have plans to address some of our concerns, as legislators and regulators, that these closed platforms would be used for these purposes?

Dr. Monika Bickert: Absolutely, safety on WhatsApp is a priority. In fact, my team is responsible for safety and security, and has on it people who have spent their careers in safety. They did not just get assigned to it in Facebook. These are people who came to Facebook because they cared about safety and security. We cover WhatsApp as well. So, we are focused on ensuring that this service is safe. As we think about encryption on WhatsApp or on other services, part of that is figuring out the ways we can offer superior safety in an encrypted world. Some of that means focus on behaviour, trends, using artificial intelligence. However, absolutely this is an area of focus.

Chairman: I now call the US representative, Congressman David Cicilline.

Mr. David Cicilline: Facebook's CEO, Mark Zuckerberg, recently said that Facebook should not fact-check political ads as Dr. Bickert has defined them, because political ads are already subject to public scrutiny and it is not the role of a private company to censor politicians. Does that accurately reflect Facebook's position?

Dr. Monika Bickert: Yes, it does.

Mr. David Cicilline: As we learned from our first session, politicians can use Facebook to micro target specific audiences with tailored ads, such as men between the ages of 55 and 75 who drive a pickup truck and watch Fox News. Micro targeting on Facebook allows an advertiser to limit the distribution of an ad to a very particular group of people. Is that correct?

Dr. Monika Bickert: There are limits on how specific that can be and limits on how one can use targeting, but yes, generally.

Mr. David Cicilline: If I were to pay for a false political advertisement and then seek to target audiences on Facebook who are susceptible to disinformation, would that be possible?

Dr. Monika Bickert: When Mr. Cicilline says audiences that are susceptible to-----

Mr. David Cicilline: I mean audiences I determine I want to micro target that may, in fact, believe the false representation I make in my ad. That is not prohibited by Facebook; in fact, that is its practice.

Dr. Monika Bickert: There are limitations in our policies and in the targeting criteria that we offer.

Mr. David Cicilline: However, within that we are allowed to micro target and we can pick the population that we think is susceptible to the false representation we are going to make in a political ad.

Dr. Monika Bickert: Mr. Cicilline can pick his population and he can target the ad within our policy.

Mr. David Cicilline: Would the person who saw or engaged with that advertisement know they were being targeted by false information?

Dr. Monika Bickert: They would know that they have been targeted in an ad. I can click on the ad and see why I am seeing this. Also, significantly-----

Mr. David Cicilline: No. Would they know they were being targeted by false information?

Dr. Monika Bickert: As Mr. Cicilline knows, our policy is if something is direct speech from a-----

Mr. David Cicilline: I take that as a "No". They would not know they are being targeted with false information.

Dr. Monika Bickert: Our policy is that we do not fact-check direct speech from politicians. However, if somebody receives an ad, they can click on it and see why they are seeing it. Our ads library shows not only the ad, but also the audience, including-----

Mr. David Cicilline: However, my question is in respect of the veracity. They would not know they are being targeted with false information. They would know why they are being targeted as to the demographic, their race or whatever, but not as to the veracity or falseness of the statement.

Dr. Monika Bickert: The reason that is hard to answer is political speech is so heavily scrutinised. There is a high likelihood that somebody would know if information is false and there is robust conversation around political speech so people may well-----

Mr. David Cicilline: With all due respect, Mark Zuckerberg's theory that sunlight is the best disinfectant only works if an advertisement is exposed to sunlight. However, as hundreds of Facebook employees made clear in an open letter last week, Facebook's advanced targeting and behavioural tracking tools make it "hard for people in the electorate to participate in the 'public scrutiny' that we're saying comes along with political speech. These ads are often so micro targeted that the conversations on our platforms are much more siloed than on other platforms."

It seems clear that micro targeting prevents the very public scrutiny that would serve as an effective check on false advertisements. Does the entire justification for this policy not completely fall apart given that Facebook allows politicians both to run fake ads and to distribute those fake ads only to people who are most vulnerable to believing them? This is a good theory about sunlight, but in practice Facebook's policies permit someone to make false representations and then to micro target who gets them. This big public scrutiny that serves as justification just does not exist.

Dr. Monika Bickert: Respectfully, I say there is great transparency in how the targeting happens. That is why we have the ads library, which is unprecedented. We literally show them. One can look up any ad in this library and see the breakdown of the audience who have seen the ad. Many of them are not micro targeted at all. In no way did this impair. We saw this recently in the press coverage of political advertisements. There is in the US and elsewhere robust conversation about whether political statements by politicians are accurate.

Mr. David Cicilline: When rolling out this recent public policy allowing politicians to pay Facebook to spread lies, Mr. Zuckerberg said it was not appropriate for one company to decide what political ads can appear on Facebook and what cannot. If the problem here is that Facebook should not be exercising this kind of power, is the problem not that Facebook has too much power? Should we not think about breaking up that power rather than allow Facebook's decisions to continue to have such enormous consequences for our democracy? Dr. Bickert said that Facebook does fact-checking for a number of other things but does not do fact-checking for political ads. The cruel irony is that her company is invoking the protections of free speech as a cloak to defend its conduct, which is, in fact, undermining and threatening the very institutions of democracy it is cloaking itself in. That is the cruel irony: the idea that it is only generating a small part of its revenue. Its CEO said it is 0.5%, which is €330 million in revenue. That may seem insignificant to a company of Facebook's size but it is a substantial revenue source.

Does Facebook currently prohibit the payment of political advertisements in foreign currency? Can a politician or someone else in the US use rubles, or any foreign currency, to pay for a political advertisement?

Dr. Monika Bickert: In terms of any political advertisements that are run in the country, we verify the identity of the person-----

Mr. David Cicilline: That is not my question. My question is whether Facebook has a policy in place that prevents it from accepting foreign currency.

Dr. Monika Bickert: I cannot speak to the payments tools. I can tell the Congressman that when we have political advertisements that are offered in the United States, we have a process through the mail by which we verify that the advertisement is coming from an actor within the United States.

Mr. David Cicilline: I am told in public reporting that Facebook accepts foreign currency. It would seem to me that, as a minimal first step, Facebook might want to adopt a policy that it does not accept foreign currency in payment for domestic political advertisements. Since foreign interference in an election is prohibited by law, it might want to consider doing that.

Dr. Monika Bickert: Again, we do ensure that through our authorisation flow where we actually require-----

Mr. David Cicilline: Did Facebook accept rubles in connection with the American presidential election in 2016?

Dr. Monika Bickert: The measures I am speaking about were put in place after the 2016 election in part because of the lessons we learned there. What we do now is-----

Mr. David Cicilline: The lessons are not to prohibit foreign currency. Facebook still takes that.

Dr. Monika Bickert: Respectfully, the concerns the Congressman and others have expressed are about foreigners - people from outside one country - running political advertisements in the country where the election is happening. We get to the heart of that by requiring identity verification from the advertiser himself or herself.

Chairman: I call Deputy James Lawless.

Deputy James Lawless: I will share time with Deputy Eamon Ryan. Staying with Face-

book and to follow up on the previous speaker's contribution, was the Libra cryptocurrency an attempt to circumvent the issues we just talked about in terms of currencies from multiple jurisdictions coming in?

Dr. Monika Bickert: I am sorry. Could the Deputy repeat the question?

Deputy James Lawless: I refer to the Libra cryptocurrency that Facebook was rolling out. Was that an attempt to in some way address some of the issues around rubles and many other currencies being used in multiple jurisdictions? Was the Libra currency geared towards circumventing some of the traceability and auditing issues Dr. Bickert has just been talking about with the previous speaker?

Dr. Monika Bickert: No. The Libra product is unrelated and is about access to financial services. That is not something I work on. It is a separate project.

Deputy James Lawless: If I understand the position correctly, Libra may assist in concealing some of the issues that have just been discussed. I will move on.

Is it the case that, essentially, the only way for political messages to get across on Facebook is by advertising? The algorithms were changed about two years ago because there was a growth of negative news or, to an extent, spam on Facebook. My understanding is that the algorithms were rejigged so that family and friends type content was primary in people's newsfeeds. This means that the organic reach for political advertisers was so small, the only way they could get into newsfeeds again was by paying for it. While it may or may not be a small percentage of Facebook's revenue, it is a constant guaranteed source because the only way to get political messaging into newsfeeds is by advertising. Is that not the case?

Dr. Monika Bickert: It is certainly not the only way to get into feeds. If we look at the major politicians, some of them have very large page followings. The Deputy is right that the friends and family posts have been elevated in the past year or so but it is certainly not the only way that something would get into somebody's newsfeed.

Deputy James Lawless: Two allegations have been made against Facebook. One is that it promotes addictive behaviours in order to keep users on the platform. The second is that it has exploited its dominant position in some ways. An example that brings those two behaviours together is Facebook's advocacy for video content in recent years. I am told that the statistics for video content supplied by Facebook internationally and in various reports were such that the primacy of video content was exaggerated and boosted to the extent that it was way over the scale in terms of what was actually being seen. Video content was being reported as having such a humongous reach that newsrooms and media organisations began to recalibrate their offering, packages and reporting to model this trend but the video statistics, as reported, were a gross exaggeration of the reality being experienced on the platform. Is that the case?

Dr. Monika Bickert: I am sorry. I do not have any information on that but I can have the relevant team follow up on it with the Deputy.

Deputy James Lawless: Dr. Bickert might come back to me on that.

I have a final question. What percentage of Facebook's moderation team globally is made up of company employees and what percentage is made up of outside contractors?

Dr. Monika Bickert: I do not have an exact percentage for the Deputy-----

Deputy James Lawless: Approximately.

Dr. Monika Bickert: -----but we certainly use both. What I can tell him about our contract force is that they go through the same training and are subject to the same privacy and accuracy audits and controls.

Deputy James Lawless: They are not subject to the same conditions. I have met some of them in Ireland and elsewhere, and I have read the stories. They are certainly not subject to the same conditions. There have been many stories about the harshness, the pay inequality, the difficult conditions they work in and the psychological trauma and mental health issues that have arisen afterwards. They may be subject to the same training but they are certainly not subject to the same pay and conditions. What is the balance in that respect? Is it 50-50 or two thirds to one third? Is it primarily contractors that form the moderation team or is it Facebook employees?

Dr. Monika Bickert: The Deputy is right that these jobs can be very challenging. That goes for the full-time employees as well as the contractors. I want to acknowledge that. I was a criminal prosecutor for more than a decade. I worked a lot on child exploitation cases so that focus on making sure that we are providing resources is a major one. I, too, have toured many of our contractor workforce locations, including in Ireland. I have found them to be nice places to work. I know that there are counselling and other wellness resources for them and I have talked to the employees there. They always have challenges in their jobs but, generally, our attrition rates are very low and our family and friend referral rates are very high.

Chairman: I will bring in Deputy Eamon Ryan.

Deputy Eamon Ryan: How would Mr. Pancini answer the point made by Mr. Balsillie? We heard it yesterday when we were deciding on a workshop on this entire issue. Extensively, leading academics and researchers in the area agreed that the basic business model here is the core of the problem we face. I refer to the use of algorithms seeking to attract attention. I see it with YouTube in that one is immediately brought down a tunnel of confirmation of one's particular view. This issue is very commonly discussed but Mr. Balsillie and others argue that we have to look at the business model. What does Google say in that regard?

Mr. Marco Pancini: I would make two points. First, we believe that the open Internet has created an unprecedented opportunity for everyone, both on the user side but also small and medium enterprise creators from Ireland and across the world, to have a voice and find an audience to which to make their message, speech or, on occasion, economic message available. There is a value in these and in creating a business model that makes this possible. That is a key point. There are different business models. There are subscription models and advertising. Advertising still represents a way to make these services available to the vast majority of people.

Deputy Eamon Ryan: Can I ask another question?

Mr. Marco Pancini: Sure.

Deputy Eamon Ryan: Mr. Pancini is Italian. I refer to the atmosphere for public debate. The town hall debate in Italy changed in the past ten or 20 years. Has it become more or less civil?

Mr. Marco Pancini: I grew up in a country where television was the media that influenced public opinion on political speech for a long time. The Internet, in the specific Italian context,

has opened up different voices - new parties to find and audiences to get out their message.

Deputy Eamon Ryan: Most politicians have a sense that the world has become more divisive and polarised. The reason for a large part of that is because the business models of the social networks are driving divisive communications. Does Mr. Pancini refute that?

Mr. Marco Pancini: I agree with the expert from Graphica when he said it was a much more complex issue which also includes the role of the single communities that are sometimes radicalised or are very strongly convinced about the political message in spreading this political message to the echo chamber. That is part of the problem. Also, education and digital literacy are part of the problem. The business model is-----

Deputy Eamon Ryan: When I am putting in a selection for YouTube, is what was said earlier true, namely, that in terms of the activities I carry out in a range of other areas, including how I use my credit card, Google knows more than I know about myself? Is it true that all that data is used to influence the videos that are put in my feed?

Mr. Marco Pancini: I respectfully disagree with that statement. It is very different when we look at content like music in that what the Deputy has seen before, other people have seen the same music and liked it. When we look at the news, the only element that is really important in making sure that we are doing a good job in providing a recommendation to the user is if the source is authoritative. That is why we want to work for news and political speech with authoritative sources that can help us to ensure that the 80% of the result that the user finds on the platform comes from authoritative sources. It is not engagement that counts as news.

Deputy Eamon Ryan: I will put the same question to Dr. Bickert. She has been focus of all the questioning because Facebook is probably the most toxic political platform. Our Georgian colleague invited her to visit Georgia. I would invite her to visit my Facebook page and see the nature of the commentary that is increasingly prevalent on the platform. It is not a community, it is war. For whatever reason, the algorithmic model, not just in recent advertising but in the 95% of other organic content, is leading towards political dialogue which is abusive. I have yet to meet a politician who does not think that is what is happening. To refer to the question Mr. Balsilli put, it is the business model, not just in respect of political advertising but the whole organic commentary model that is leading to political discourse which is not community, it is hate speech and abusive. It tends towards that. It is the experience of every politician I have met. Are we all wrong?

Dr. Monika Bickert: I echo what Mr. Pancini said. I do not think this is related to the business model, which is largely a very good thing. There is abuse but the data suggest that polarisation has been increasing since the 1970s. That is a separate topic. We take abuse of politicians or others very seriously. We do not allow harassment, threats or hate speech. We are not perfect at enforcing that line but we are committed to getting it right. I welcome feedback from the Deputy.

Senator Terry Leyden: I welcome our guests. I have been a member of the Seanad for 17 years. I welcome Dr. Bickert, particularly she is the vice president of content policy at Facebook. She is resident in Menlo Park, in Galway I presume, not California.

Dr. Monika Bickert: I am in the Menlo Park, California. I am in new Menlo Park.

Senator Terry Leyden: Contrary to what Deputy Eamon Ryan said, my daughter, Councillor Orla Leyden, launched a campaign to try to retain the Cuisle centre for the Irish Wheel-

chair Association, IWA, in Donamon in County Roscommon. The general media has literally ignored this issue. On Facebook, its service users, people in wheelchairs, and others who have difficulties and so on, have responded. There have been 35,000 hits. RTE has not responded to this issue; it has ignored it completely. The people my daughter and I represent are voiceless without Facebook. Whatever about hate speech, I do not have Facebook, I do not read Facebook and I do not want to know what people are saying about me on Facebook, that saves me any concerns. I am, however, concerned about an issue which is of such vital importance that, last Friday, the chief executive of the IWA told the 45 members of staff that they would be sacked on 29 November. They had no voice and Facebook is the face and voice of the voiceless.

Senator Aidan Davitt: I am delighted to welcome our esteemed elected members and our esteemed associates from the social media. Like most politicians in Ireland, I have seen content put up on social media and all the rest that is not correct. I accept that there is legislation coming in Ireland. If people say things on Facebook or some other social media platform and it is incorrect, the law of the land must bring them to account. To expect Facebook, which we have dealt with a lot today, to police itself about something an elected representative says is not a good enough standard for us. It has been thrashed out here several times. The Minister for Communications, Climate Action and Environment, Deputy Bruton, is considering legislation and I am well aware that this has been discussed in our own parliamentary party and it will I am sure make different amendments to it, like several politicians here. We have to be serious as politicians. There are different formats, guys pay for advertisements and say stuff but if they are saying stuff that is incorrect the court is the place they deserve to be grilled.

Chairman: I do not know if there were any particular questions there. I might let witnesses in at the end. I am also chairman of the Joint Committee on Climate Action and I would like to raise the issue of Twitter banning political advertising.

Senator Terry Leyden: I thought we were going to get a response from the witnesses.

Chairman: Yes, I will let them back in again. I am just conscious of the time and that Twitter-----

Senator Terry Leyden: I thought I might get a quick response.

Senator Aidan Davitt: They should come to Menlo in Galway, it is a much nicer place.

Chairman: I will let them back in again. I just want to put a question.

Senator Terry Leyden: The Chairman might lose track of a situation where I am saying that Facebook is the voice of the voiceless. In this regard, let us put the positive spin as well as negative spin.

Chairman: Absolutely. The Senator has had his time. I will let the witnesses in.

Senator Terry Leyden: I would like the response. That is all.

Chairman: The Senator will get a response. I am conscious of time and I want to get a question in to Twitter which has not had an opportunity to answer.

It would appear that, under Twitter's new advertising rules, environmental groups will not be able to pay for advertisements promoting green policies or pro-climate policy content after 22 November but, on the other hand, there appear to be over ten current Exxon Mobil tweets

relating to climate change that Twitter does not classify as political issue advertisements. Will they be classified as political advertising after 22 November?

Ms Karen White: We are very aware that this issue was raised in the past couple of days in the United States. We are still working out the details of that policy with regard to political and issue advertisements that would encompass issues of national importance. We hope to be in a position next week to provide more details of what types of advertisements will and will not be allowed under these new policies and I would be very happy to follow up with the committee then and to share more details. Towards the end of the month, advertisers will have a chance to become familiar with, and educated about, that new policy. It will take effect from later in the year.

Chairman: I would welcome interaction on this because the concern is that there are environmental groups working positively to help people and governments take positive action to tackle climate change whereas oil companies which are allowed pay for advertisements talk about climate change too and there is a contradiction there and a real concern about how Twitter will enforce this ban and who will and will not be allowed to place political advertisements. We will all be watching that space.

Does Dr. Bickert or anyone else on the panel want to reply to Senator Leyden or Senator Davitt?

Dr. Monika Bickert: We do not want abusive actors, we do want a voice for others, and we can follow up with the Senator on specific concerns.

Senator Terry Leyden: I am actually praising Facebook. I said Facebook is the voice of the voiceless. The national media have ignored this issue but Facebook has not.

Chairman: I thank the Senator. We have only six minutes left. Will the next speakers just stick to asking a question?

Deputy James Lawless: My next question is to Google and I am going to keep it tight.

Chairman: Just a question.

Deputy James Lawless: Yes. I understand that Google is a search engine and it performs as a directory but I also understand that any content, illegal or otherwise can be retrieved by the search engine because Google's view is that it is a directory. I was perturbed by this when I met Google recently, that it applies to disturbing content, freedom of speech, violent and pornographic content and illegal content. All it does is pull things back from the web and show them. Is that acceptable?

Mr. Marco Pancini: If I can correct the statement, the point is that Google as a search engine is indexing content and providing a link to content that is not hosted on Google. The same content on YouTube can be taken down because we host the content. The content that we link from Google, since it is not hosted on our networks, cannot be taken down by us. What we can take action on is the link. We can make sure that when somebody is searching something on Google, he or she cannot find the link that is leading to the illegal content. For illegal content that is hosted elsewhere, we do not have any technical possibility to take action. Of course we can work together with law enforcement and the technical community to solve the problem.

Ms Carol Brown: I want to go to Facebook in terms of what Dr. Bickert said about fact

checking and that a correction would sit side by side with the original ad. That means that anyone who accesses the ad in the future would see the original statement and the fact-checked correction. What about those who have already seen just the original statement or ad?

Dr. Monika Bickert: If content has been fact checked, we do not allow it to run in an ad. With the organic presentation of it, just on a page, we do put the fact checkers' information by it. For somebody who has, say, already shared that content in the past, we send them a notification that the content has now been fact checked and rated false.

Ms Carol Brown: Why does Facebook not send the correction to all those who have seen that ad? One of the criticisms is around the lag time between the ad being fact checked and all those people who have already seen the original, and the fact that the correction is not sent to those who have already viewed the original ad.

Dr. Monika Bickert: When we send notifications, we do share a link to the fact-checking material, which may render as a thumbnail depending on where the person views it. We agree there is room for thinking about how we can improve this process. I welcome Ms Brown's feedback and thank her.

Mr. David Cicilline: When the Twitter CEO made the decision to ban political advertising, he stated:

> A political message earns reach when people decide to follow an account or retweet. Paying for reach removes that decision, forcing highly optimized and targeted political messages on people. We believe this decision should not be compromised by money. [...] This isn't about free expression. This is about paying for reach. And paying to increase the reach of political speech has significant ramifications that today's democratic infrastructure may not be prepared to handle.

Is that an accurate statement of the CEO's position?

Ms Karen White: Yes.

Mr. David Cicilline: This argument that this is just political speech, which we heard Dr. Bickert make, and that it is really not about money but about free expression, has been completely rejected by Ms White's CEO. He spoke of significant ramifications for today's democratic infrastructure. Does Ms White know what he meant by that?

Ms Karen White: I think when it comes to political advertisements on Twitter, what he meant by that was that when they are targeting individuals and placing a targeted message within their feed, it removes the choice from that. We would, moving forward, much prefer to be in a position where that political reach is earned through retweets and various other means.

Mr. David Cicilline: I applaud Twitter for that.

Ms Keit Pentus-Rosimannus: According to advertising analytics and Cross Screen Media, which is a company that analyses advertising markets, the predicted spend on digital video ads will be around €1.6 billion during the 2020 election cycle. It was very good to hear from Dr. Bickert that despite that amount of money, financial incentives do not play any role in the decision to refuse to take down false political ads. She has repeatedly said that her company, Facebook, is not in a position to decide if a lie is a lie or not. If that is the case and if financial motivation does not play any role, I am still struggling to understand what exactly prevents

Facebook from deciding that it will not run paid political ads and that it will not be a platform that can be used for amplifying the lies.

Dr. Monika Bickert: With regard to the revenue number, I think Mark Zuckerberg has put our revenue estimate out there and that is the figure I would use. It is a very small percentage of our revenue and is not-----

Ms Keit Pentus-Rosimannus: If that is the case, why does Facebook not say that since money does not play any role, it can easily give it up and say it will not be the platform that will amplify the lies?

Dr. Monika Bickert: We think that ads are an important way for politicians to be able to share their platforms and-----

Ms Keit Pentus-Rosimannus: I am a politician and I share my ideas without paying for it. It does not mean that Facebook has to kick out the politicians. The question is if it will allow itself to amplify lies for money.

Dr. Monika Bickert: We think that there should be ways that politicians can interact with their public, and part of that means sharing their views through ads. I will say that we are here today to discuss collaboration in this area with a thought towards what we should be doing together. Election integrity is an area where we have proactively said that we want regulation. We think it is appropriate. Defining political ads and who should be able to run them when and where are things for which we would like to work on regulation with government.

Ms Keit Pentus-Rosimannus: Yet Twitter has done it without new regulation. Why can Facebook not do it?

Dr. Monika Bickert: We think that it is not appropriate for Facebook to be deciding for the world on what is true or false. We think politicians should have an ability to interact with their audiences so long as they are following our ads policies. We are very open to how, together, we could come up with regulation that could define and tackle these issues.

Chairman: I thank everyone. We are going to have to suspend our meeting for 15 minutes. I thank all our witnesses for coming before us this afternoon.

Sitting suspended at 12.17 p.m. and resumed at 12.30 p.m.

Session 3: The State of Play in Regulation

Chairman: This is the third session of the International Grand Committee on Disinformation and 'Fake News'. I welcome to our meeting this afternoon Ms Helen Dixon, Data Protection Commissioner for Ireland; Mr. Paolo Cesarini of the Directorate General for Communications Networks, Content and Technology, DG Connect, of the European Commission; Mr. Marc Rotenberg, president and executive director of the Electronic Privacy Information Centre, Washington DC; and Deputy Richard Bruton, Minister for Communications, Climate Action and Environment in Ireland. I thank them all for coming here today.

I draw the attention of witnesses to the fact that by virtue of section 17(2)(*l*) of the Defamation Act 2009, witnesses are protected by absolute privilege in respect of their evidence to the committee. However, if they are directed by the committee to cease giving evidence on

a particular matter and they continue to so do, they are entitled thereafter only to a qualified privilege in respect of their evidence. They are directed that only evidence connected with the subject matter of these proceedings is to be given and they are asked to respect the parliamentary practice to the effect that, where possible, they should not criticise or make charges against any person, persons or entity by name or in such a way as to make him, her or it identifiable. I also advise our guests that any submission or opening statement they make to the committee will be published on the committee's website after this meeting.

Members are reminded of the long-standing parliamentary practice to the effect that they should not comment on, criticise or make charges against a person outside the House or an official either by name or in such a way as to make him or her identifiable.

The format of the meeting will be the same as previous sessions. All witnesses are asked to give a five-minute opening statement and I will give a ding on my glass after four minutes to let them know they have a minute remaining. I ask Ms Helen Dixon to give her opening statement.

Ms Helen Dixon: I thank the Chair and members of the committee for inviting me to be here today. I am pleased to have the opportunity to share details of the role of the Irish Data Protection Commission, DPC, and position in relation to the regulation of online platforms.

There is no doubt that despite the great benefits and access to more and more information the Internet has provided all of us with, it also presents significant challenges to our rights and freedoms in how it now operates. The challenge of combating disinformation in many contexts, such as during electoral cycles or in, for example, public health scenarios is a pressing issue of our time given the negative consequences for democracies and societal well-being.

Issues of harmful and-or illegal content and disinformation are issues that stretch well outside of the scope of the data protection legal framework. Data protection is predicated on a fundamental right of individuals to have their personal data protected and, as a result, the remedies individuals may avail of under the general data protection regulation, GDPR, require the personal data of that specific individual to have been processed.

The DPC is very pleased to have an opportunity for interaction during this panel with the Minister for Communications, Climate Action and Environment as the DPC has this year responded to his consultation on the regulation of harmful online content and the implementation of the audiovisual media services directive. In the context of making a submission to that consultation, the DPC clarified that it supported the Irish Law Reform Commission's recommendation in their 2016 report on harmful communications and online safety that a dedicated office with a statutory responsibility to promote online safety and to oversee and regulate a system of takedown orders for harmful digital communications should be considered. The DPC, however, has responsibility for a number of areas of regulatory activity that relate directly to the theme of the hearing and are relevant to the panel.

First, it is possible that content relating to a specific individual posted online may be harmful to the individual or may contain false information about the individual. In such circumstances, the individual may be able personally to exercise his or her data protection rights, in particular to erasure and rectification. In circumstances where a platform does not comply with a request to exercise data protection rights by an individual, the individual may make a complaint to the DPC, following which we will take the matter up as appropriate on his or her behalf. Equally, however, it is worth recalling that Article 85 of the GDPR requires a reconciliation of the right to freedom of expression with the exercise of data protection rights, and therefore they are not

absolute rights. The majority of complaints the DPC receives in respect of platforms are complaints about erasure.

Another issue of significance is the role that personal data play in a social media context through facilitating the so-called micro targeting of individuals with specific content, thereby amplifying any harmful effects of disinformation. In such a scenario, the profile a platform has created of a user and the categorisation of that user as being of a certain lifestyle, passion or habit may allow an undecided voter in an election context to be pushed in one direction or the other. All of this may happen without the user being aware his or her data are being deployed to reinforce the individual's existing viewpoint rather than the individual being in a position to take an objectively informed stance based on an understanding of both sides of an issue. Given the rates of online users who consume their news exclusively on social media, this is a concern. As a data protection authority, we have a number of ongoing investigations into how the online behavioural advertising system operates and whether in all respects it is in compliance with the GDPR, especially in respect of lawfulness and transparency to users. In this regard, we have investigations open into platforms, data brokers and advertisement exchanges, which will conclude in 2020.

The issue of children and other vulnerable Internet users being subject to disinformation and harmful content somewhat overlaps with the protection of children's personal data in an online context. To protect children, whether in respect of their personal data or to protect them from harmful content, presupposes that children can be identified as such on the Internet. To date, a systemic solution to age verification online that protects younger users but leaves the Internet open and accessible to all has been elusive. The DPC has watched with interest the attempts in the UK under the Digital Economy Act 2017 to impose age verification measures for access to legal online pornography. That the legal provisions have not proceeded to implementation simply underlines how difficult it is to find a solution that meets all requirements. The DPC has run a consultation over the past year on the protection of children's data, including a consultation directly with children through their schools and youth centres. The DPC will next month publish a guidance note based on the outcomes of that consultation, proposing ideas and criteria that data controllers need to take into account when implementing mechanisms to identify and protect children online.

Finally, I raise an issue of interest to the committee, namely, that of how to foster international collaboration. As an EU data protection authority, the commission is bound in close legal co-operation with all other European Economic Area data protection authorities. Indeed, we meet in Brussels weekly. In addition, the DPC is a member of the Global Privacy Assembly, has signed memoranda of understanding with a number of global data protection authorities, and this year we have been visited at our Dublin offices by a large number of other commissioners, including the New Zealand, Icelandic, Australian and UK commissioners. The dialogue and the opportunity to discuss regulatory approaches and solutions to issues of common concern are invaluable in shaping better outcomes in our regulatory role.

I look forward to the panel discussion and questions from committee members.

Chairman: I thank Ms Dixon and invite Mr. Cesarini to give his opening statement.

Mr. Paolo Cesarini: I thank the committee for inviting a representative of the European Commission to this important event. I am head of the unit responsible for media convergence and social media policy at DG Connect. Respect for democracy, fundamental rights and the rule of law are core values of the European Union. They bind us together and underpin

the functioning of our institutions. President-elect Ursula von der Leyen has announced that protecting European democracy will be a priority of the new Commission and underlined we must do more to protect our democratic processes and institutions from external interference. Disinformation poses major challenges to our democracy as new technologies can be used, notably through social media, to disseminate disinformation on a scale and at a speed that are unprecedented. They can create personalised information spheres and become powerful echo chambers for disinformation campaigns, polarise the public debate, and create tensions in society. Media manipulation, however, and the strategic use of disinformation are not the exclusive prerogative of foreign actors. Domestic actors, too, can exploit digital technology to interfere in electoral processes and, increasingly, to manipulate policy debates in areas such as climate change, migration, public security, health and finance.

While the conduct of free and fair elections is primarily a responsibility of member states, the cross-border dimension of efforts to manipulate democracy, as well as the importance of joined-up efforts to address such threats, make a European approach necessary. What affects one member state affects us all. The Commission, along with other EU institutions, has put in place a robust framework for co-ordinated actions against disinformation, with full respect for European values and fundamental rights. We often mention free speech, freedom of association, press freedom, and pluralism, which are fundamental principles that need to be kept in mind.

Our work on combating disinformation has evolved over three major, interlinked initiatives. Last December, the Commission adopted an action plan against disinformation, a plan that builds on the communication on tackling online disinformation and was adopted in April 2018. Furthermore, in September 2018, the Commission put forward a comprehensive election package, setting out a variety of measures, with a focus on what were then the upcoming elections to the European Parliament.

Broadly speaking, the work carried out in recent months centred on the strength of action. First, we improved the EU capability to identify and counter disinformation via our strategic communication task forces and the EU hybrid fusion cell, which operates within the European External Action Service. Second, we supported member states by setting up a rapid alert system to facilitate the exchange of information between member states and the EU institutions. The system has become a reference point for national authorities and a mechanism for strength and co-operation with platforms. It also links up and facilitates co-operation with other international partners, not least the G7 and NATO. Third, in the run-up to the European Parliament elections, we closely monitored the implementation of the code of practice on disinformation, to which the major online platforms signed up in October 2018. The platforms, in particular Facebook, Google and Twitter, were subject to a programme of targeted monitoring that required them to report each month from January to May, inclusive, on the progress made on the implementation of their commitments under the code.

The monitoring was carried out in co-operation with the audiovisual authorities of the member states, the ERGA. It focused on those actions that held particular relevance to the integrity of elections, namely, actions to disrupt the advertising and democratisation incentives for purveyors of disinformation; to ensure the integrity of the platform services against inauthentic behaviour, including fake accounts and malicious bots; and to ensure the transparency of political advertising. In the final respect, searchable political advertising libraries were created and they resulted, for the first time insofar as online political advertising is concerned, in a better view of the identity of the sponsors, the amount spent and the basic targeting criteria used in

the campaigns.

The fourth strand of actions included a number of initiatives directed to improve societal resistance to disinformation. One of the aspects on which I wish to focus is the effort to promote media literacy, which is important to enable citizens to evaluate the credibility of information they encounter online and access alternative points of view when they navigate on social networks. In the long run, media literacy initiatives may prepare users of online platforms and social media to better understand the effects of disinformation and the malicious actors with which they may be confronted.

We are facilitating the creation of a European multidisciplinary community of fact checkers and academic researchers. The programme will arrive in 2020. The Commission has supported investments in new technologies for content verification and network analysis through social media. It has also launched a new platform, the Social Observatory for Disinformation and Social Media Analysis, SOMA, to facilitate networking, knowledge exchange and best practices among independent fact checkers. The Commission will follow this up by founding a new digital infrastructure entitled the European Digital Media Observatory, which will offer tools and networking possibilities to link fact checkers and academic researchers to improve their understanding of the phenomenon and to exercise better oversight of the dynamics that disinformation shows online.

Disinformation is a multifaceted phenomenon, which requires a multidimensional response. Our preliminary view is that all the efforts I mentioned have contributed to narrow the space for malicious activities online. On 29 October, we published a report that takes stock of the self-assessment reports prepared by the signatories of the code of practice. Our initial view is that it is a mild kind of assessment. After all, the recent elections to the European Commission were not free from disinformation and malign actors constantly change their strategies. As such, we need to strive to be ahead of them. The evolution of the code is ongoing. When the full evaluation has been carried out, we will see what further actions are necessary.

Mr. Marc Rotenberg: My organisation, the Electronic Privacy and Information Centre, EPIC, was established 25 years ago to focus public attention on emerging privacy issues. More than a decade ago, we worked with an organisation entitled Facebook Users Against the New Terms of Service. It was an international campaign joined by more than 150,000 people on the Facebook platform to oppose changes in the company's policies that would diminish personal privacy. As a consequence of the campaign, in 2009 Facebook gave commitments to its users that it would allow them to actively participate and vote on changes in its business practices. At the time, this was viewed as a great success and a demonstration of how Internet governance could promote democratic principles. However, Facebook reneged on its commitments and backed off on its agreement to allow users to vote. Chillingly, it shut down the political organisations, including the Facebook Users Against the New Terms of Service group and prohibited the use of the company's name in any user group on the platform. I bring this story to the attention of the committee because there has been much reference to Facebook and free expression. I know from ten years ago the company's view on free expression.

Thereafter, EPIC and a group of consumer privacy organisations in the US went to the FTC and laid a charge that the changes in the company's business practices violated US trade law and, specifically, were unfair and deceptive. We spent two years persuading the FTC to act on our complaint. We provided evidence, legal analysis and the blueprint for the remedies that the FTC announced in November 2011. Once again, we thought we had obtained a victory. The then chairman of the FTC pointed to the settlement with Facebook and stated the company

would be held to account. When FTC commissioners appeared before the US Congress and in Europe, they pointed to the Facebook settlement as evidence that the US had effective protection for personal data. However, we almost immediately became aware of a problem, namely, that the FTC was unwilling to enforce its legal judgment.

In a related case, Google changed its business practice in violation of a consent order. We sued the FTC and stated that it must exercise its enforcement authority to protect users. The judge was sympathetic to our case but concluded that she did not have the authority to force the commission to take the action it should have taken in 2012.

We have spent many years trying to get the FTC to act against Facebook. During that time, complaints from many other consumer organisations and users have increased and include complaints about the use of personal data, the tracking of people who are not Facebook users and the tracking of Facebook users who are no longer on the platform. A request lodged by EPIC under the US Freedom of Information Act uncovered that 29,000 complaints were pending against the company. The FTC issued a judgment in June of this year against Facebook, accompanied by a historic fine of €5 billion. However, the FTC left Facebook's business practices in place and the users of the service at risk.

My message to the committee is simple: it must act. It must not wait ten years or one year to take action against this company. The terms of the GDPR must be enforced against Facebook and that should be done now. Facebook should be required to divest of WhatsApp not because of a scheme to break up big tech but, rather, because the company violated its commitments to protect the data of WhatsApp users as a condition of the acquisition. Until adequate legal safeguards are established, Facebook must be prohibited from engaging in political advertising. Its recently stated views on political advertising and the US First Amendment, which are not shared by US legal scholars, are reckless and irresponsible. Advertising revenue from political candidates should instead flow to traditional media organisations, which would help to support independent journalism.

Minister for Communications, Climate Action and Environment (Deputy Richard Bruton): I congratulate the committee members and other parliamentarians on this initiative. The background to the regulatory environment in Ireland is very much set in our broad plan on online safety. It involves several Departments, including the Departments of Communications, Climate Action and Environment, Justice and Equality, Health, Taoiseach, Children and Youth Affairs, and Education and Skills. I am a former Minister of the latter Department, which provides strong online support mechanisms for students and schools. The plan has a broad base. The principles of what we are trying to do are clear and well set out in the committee's documentation. They include transparency, accountability and protecting citizens while also respecting freedom of expression.

The devil is in the detail when it comes to regulation. There are several main regulatory developments under way in Ireland. I could name at least six. The regulation of harmful online content, to which I will return, is being pursued by my Department. The Department of Justice and Equality is facilitating a consultation on the regulation of hate speech and hate crime. Regulation of transparency of political advertising has been developed in the context of an electoral commission that is being drafted and that will deal with the regulation of elections, including funding, which is another element. Private Members' legislation supported by the Government has proposed the creation of new criminal offences relating to images displayed without consent. Stronger protections relating to cybersecurity and cyberattacks are also relevant to my area. The approach we are taking to online safety, for which I am directly responsible, is

not dissimilar to that being taken in Australia. We propose to define harmful content, require companies to have a code of practice and put an online safety commissioner in place to oversee the delivery of those codes of practice. That online safety commissioner would receive third party complaints and could, on his or her own initiative, require takedown or notify companies that their code was inadequate. Non-compliance with the directions of an online safety commissioner would be a crime and the commissioner could publish details of non co-operation. That legislation is in development and we have had consultations on it, as Ms Dixon indicated.

Consultations are also ongoing on the area of hate speech. There are issues around that and the characteristics of certain groups that have been defined. Some argue that the bar is very high under the existing incitement to hatred legislation. The definition of "hatred" in that legislation stipulates that an intention or likelihood to stir up hatred must be demonstrated. We are also considering whether such laws adequately deal with online content. Those issues are being developed.

This week, the Government announced the initiation of legislation to deal with political advertising, which will define political advertising, require its clear identification and labelling, and require the disclosure of any targeting or engagement metrics being used. There is quite a bit of legislative initiative under development. We also need to educate people and equip them with the right tools to help them be discerning in their use of the Internet. That balance is very strong.

There is no doubt that the power of the Internet is accelerating. When I was Minister for Jobs, Enterprise and Innovation, we discussed aspects such as social, mobile, the cloud, and big data. It has now moved on to the Internet of things and AI. Principles of operation will be embedded within those areas, which should be subject to regulation. This is a very tricky area for governments and it is absolutely essential that we work together across countries. Media and politics are at the front line of this invasiveness, but it will start to move into other areas of our lives. We need to decide the principles underpinning the roles of artificial intelligence, big data, micro targeting and so on. This is a challenging area and this initiative is worthwhile in bringing countries together to be a part of this group.

Chairman: I thank the Minister. I call the representative from Australia.

Ms Carol Brown: My first question is for Mr. Cesarini. Does he have any communication with Facebook as part of his fact-checking projects?

Mr. Paolo Cesarini: The digital service infrastructure that will bear the name, European Digital Media Observatory, must be understood as an independent, academic-driven structure that will exercise oversight of the social media platforms. This initiative is aimed at building up co-operation and constructive relations, particularly as regards access to the data that are necessary for analysing disinformation trends and threats, and better understanding the impact of policies on the phenomenon. As such, the platforms must be external to this co-operation.

Ms Carol Brown: Mr. Cesarini mentioned in his presentation that one would be able to click on an ad in this proposed library and see where it is coming from. We heard evidence earlier that when an ad is fact-checked, there is no mechanism for getting back to people who have viewed something that may contain lies or disinformation. The fact check does not go back to the people who have already viewed that ad. Is there an avenue to request or put pressure on Facebook to take that very simple step? It is really extraordinary that it has not done so.

Mr. Paolo Cesarini: I understand Ms Brown's question. This should apply not only to sponsored content or political ads, but to all information that has been fact-checked and discovered to be false. This is not a question of public authorities - much less private companies - exercising censorship; it is a question of duly informing consumers. This mechanism should enable users' awareness of the type of content to which they have been exposed. Consumer empowerment is part of the fourth pillar of the code, which is now being implemented. Priority was given to other parts of the code during the first months of this year as they related more directly to the integrity of the elections. Those include the fight against bots and fake accounts and other malicious or co-ordinated actions. For the first time, a transparency space will be created for political ads where the question is not the veracity of the ads. The question is who is paying for them, how much they are paying, and what the targeting criteria are. It will also monitor and track advertising revenues to avoid the monetisation of bad actors.

Chairman: Did Ms Brown want to come back in?

Ms Carol Brown: I wanted to ask Mr. Rotenberg a question. In his presentation, he gave a snapshot of what has happened with the various decisions and rulings that have been handed down, which Facebook and others that should be in a position to enforce seem to have simply ignored. Based on the discussions I have been having over the past few days, that view seems to be shared by many. Mr. Rotenberg spoke of his own recommendations. Does he think the business model needs to be changed?

Mr. Marc Rotenberg: I certainly think the business model needs to be changed. Facebook should be prohibited from using the platform for political advertising today. That is a concrete action that is supported by plenty of evidence. Other companies are already doing it.

I will make a further point, in partial response to Ms Brown's first question to Mr. Cesarini. A good friend of mine, the former European Data Protection Supervisor, Giovanni Buttarelli, who recently passed away, addressed the issue of election integrity last spring. He made a very important point. He said that, in his view, transparency and content management will not be sufficient to solve this problem. This is about the collection and use of personal data. If our aim is to safeguard the integrity of elections and to limit fake news, we must enforce these privacy obligations. Transparency will not be a substitute for doing so. Mr. Buttarelli was exactly correct on that.

Chairman: I will bring in Ms Pentus-Rosimannus, who is from Estonia.

Ms Keit Pentus-Rosimannus: I thank the Chairman for all the introductions. The urgent need to forbid Facebook from accepting political advertisements has been mentioned. It has been suggested that there is a need for regulation in this area. I wonder how it is envisaged that it would be possible to make such a distinction. If we say that political advertisements are not allowed on Facebook, should we proceed to say the same in respect of television and newspapers? How can this distinction be made? As lawmakers, how can we forbid political advertisements in one case by regulating, as opposed to their own self-regulation?

Mr. Marc Rotenberg: I can speak to our position in the United States. By tradition, we regulated political advertisements. We required people in print and broadcast media to identify the source of their advertising. Facebook quite brazenly claimed it was unnecessary for Internet companies to be bound by the same obligations that apply to print and broadcast media. It removed itself from what traditional journalists and news organisations were required to do. I believe this accelerated the trend towards fake news and disinformation. My view at this point

is that the time has long since passed for Facebook to come before this committee to say what type of regulation it thinks it will find acceptable. There is enough reason now to say this is one place where we no longer need political advertising, which is a source of significant revenue. It could help to support independent media, which needs the support.

Ms Keit Pentus-Rosimannus: My understanding is that there is no need to have a new regulation in this area. During a previous session, we heard from representatives of Twitter, which has decided - without any new revelation - that it will no longer allow political advertisements to run.

I would like to put some questions to Mr. Cesarini. Before the European Parliament elections, the EU worked with online platforms on the basis of the code of practice. How can that be evolved? What is the conclusion? Shall we continue with a similar formula? What were the main problems with the code of practice?

Mr. Paolo Cesarini: I will express my personal view.

Ms Keit Pentus-Rosimannus: Sure.

Mr. Paolo Cesarini: I think the code of practice was a necessary step. It remains to be seen whether it is sufficient. We are in the process of evaluation. I cannot anticipate the conclusions that will be known to the next Commission, which is now carrying out caretaking duties but is unable to take political decisions on the next step forward. This moment will come very soon, early next year. My view is that today we are in a better place than we were a year ago. It is clear that much more needs to be done as well. There are several areas we may need to consider. I will not mention them all. As we are focusing in today's debate on political advertising, I remind the committee that the devil lies in the details. I refer, for example, to the definition of "political advertising". What would the ban be about? What about sponsored content that communicates on social, political and economic issues that do not come within electoral contests and, therefore, escape the definition? We are well aware that such content can influence and shape public opinion artificially and in a much more pernicious way in the long term. These complex questions need to be taken in their integrity and in their totality.

Ms Keit Pentus-Rosimannus: I agree with Mr. Cesarini. If I am correct, the rapid alert system that was put in place before the European Parliament elections was never triggered during the campaigning period. Was it not needed because there were no disinformation campaigns? Does Mr. Cesarini envisage that we will continue with a rapid alert system that will alert us if something bad is happening on social media?

Mr. Paolo Cesarini: The rapid alert system was put in place in March of this year, less than two months before the European Parliament elections took place. It had the merit of creating links and connecting dots that had been completely separate and did not communicate between one another at the level of the different member states. Each member state has a different authority that deals with issues concerning electoral integrity and disinformation attacks. While it is true that the rapid alert system has issued just one alert, an increasing flow of information is being exchanged. This shows and demonstrates the usefulness of the tool. It certainly needs to be developed, especially in terms of agreeing common methodologies, discussing the thresholds for triggering an alert and having better ways of co-operating with platforms, particularly when disinformation leads to investigations into groups that co-ordinate their behaviour and, therefore, require the intervention of specialised authorities within the structures of member states.

Chairman: I will move on to Mr. Packalén, who is from Finland.

Mr. Tom Packalén: I would like to ask Mr. Cesarini about the work of the European Commission. Fact-checking is an important part of the growing problem of false media and fake news on the Internet. It is a difficult question when there is clear fake news and when we should somehow verify where the limit is. There is no one truth in the world when it comes to difficult and controversial questions such as climate warming. It is very difficult to say what is fact and what is not. I ask Mr. Cesarini to speak about what the SOMA project is doing. How are the things it is working on chosen? I would like to open up this question. How is the project seen in the European Commission?

Mr. Paolo Cesarini: I agree fully that fact-checking is not a silver bullet. Nevertheless, there is a need to create more clarity about the trustworthiness of the information space within which we experience our access to news on a daily basis. Fact checkers can make an important contribution that has to remain independent from any public interference. The initiative must come from the media sector. The SOMA project is helping fact-checking organisations that have been growing over the past couple of years, having entered this newly emerging market, to work together to avoid duplications, to learn from one another and to develop fact-checking in a proper way. Mr. Packalén's question raises the important question of where to draw the limits between news and views, or between what is false and what is real. It would be a dangerous move to concentrate on the idea of regulating content. We have to focus much more of our attention on detecting, analysing, preventing and, where necessary, sanctioning online behaviours that are systematically directed towards the amplification of certain stories and narratives and that use the vulnerabilities that exist in the current digital media ecosystem to mislead the users of such media by making them believe that a certain story has popular support when, in fact, it does not. We need to hide the authors and vectors that have been helping this manipulation to happen. In other terms, we should be much more focused when we talk about regulation and much more concerned about the conduct than the content, although the content FactCheck has provided and the analysis it has carried out are important in order to provide leads to identify the kinds of conduct that could be reprehensible in a regulatory framework.

Mr. Tom Packalén: I thank Mr. Cesarini. Those are very good answers. How much co-operation does DG CONNECT have with these big companies such as Google and Facebook? Are they trying to solve this problem with DG CONNECT? Is there communication? If so, how much?

Mr. Paolo Cesarini: There is an arm's length relation. The code of practice is their own code of practice; the Commissioner has acted as a facilitator. Without the intervention of the Commission, the code of practice probably would not be there. However, the implementation of these principles remains entirely within the responsibility of the signatories to the code. The Commission has the very precise role of an independent oversighter - I do not know whether that word exists - to exercise oversight over the actions taken and then to take the appropriate steps on its own, using the powers that can be used in this tricky field, in order to ensure that the objectives that underpin the code are actually achieved.

Ms Nino Goguadze: Ms Dixon mentioned in her presentation that there is active co-operation between data protection agencies, that she has a permanent platform of co-operation and that they meet regularly. Could she explain the level of co-operation she has with big social media companies?

Ms Helen Dixon: Regarding the co-operation between data protection authorities, we have

excellent fora but there is huge room for improvement. For example, the general data protection regulation provides for something new called joint enforcement operations. We have not really got them off the ground yet in the EU in terms of data protection authorities lending resources to one another that can be authorised on investigations, so there is lots of room for improvement there. Regarding co-operation with the big platforms, the relationship is one of regulator to regulated entities. The regulated entities are obliged under the GDPR to co-operate with investigations conducted by the data protection authority. To date, the 21 big tech organisations in respect of which we have large-scale investigations open are engaging and co-operating. With equal measure they are challenging at every turn and seeking constant clarifications on due process. They are obliged under various measures under the GDPR, for example, to conduct data protection impact assessments in certain circumstances and to consult with us as a data protection authority where they identify high risks they can mitigate and so on. Again, that form of co-operation with, or submission to, the regulator is already in effect. What remains to be seen is how the investigations we currently have open will conclude and whether there will ultimately be compliance with the outcomes of those investigations or whether they will be subject to lengthy challenge and so on. The big question of whether we will be able in the near term to drive the kinds of outcomes we want is still open and awaits us as a data protection authority to put down the first final decisions in a number of cases.

Ms Nino Goguadze: Are those big companies flexible and open to co-operating with the Data Protection Commission on preventative measures? Preventative measures are very much important and sometimes it is much more important to prevent new harmful actions on social networks. To what extent are they flexible, and are they willing at all to co-operate actively on effective measures?

Ms Helen Dixon: On practical measures, did Ms Goguadze say?

Ms Nino Goguadze: I mean preventative measures.

Ms Helen Dixon: I think Ms Goguadze is well familiar with the fact that the GDPR is a high-level, technology-neutral, principles-based law. From our point of view, it is a very good platform over which we can regulate. All organisations, including the platforms, despite how large they are and the resources they have, have an issue understanding with any degree of certainty how these principles should be applied in specific scenarios. For example, the GDPR for the first time now in the EU calls out that children merit specific protections in a data protection context, but it really gives us no clues as to what those specific protections should look like. I mentioned earlier the challenge of even knowing how to identify children on platforms without limiting the rights of adult users or making platforms inaccessible. It is a challenging question. We find when we engage in exercises such as the consultation we have run on protections for children's data that the platforms are willing to come forward, make submissions and engage in ideas to ultimately find solutions that work across the board and drive up the levels of protection.

Ms Nino Goguadze: Is my time up?

Chairman: Ms Goguadze has 30 seconds.

Ms Nino Goguadze: I will ask one last question. I asked it during our morning session and I will ask Ms Dixon the same question. Some items of information collected by big social platforms are provided by consumers themselves. I believe that in many cases people are not aware when they provide and share information of the possible usage of that information in the

future. I am very much interested in Ms Dixon's opinion on this. What does she think? Should social platforms and the big social media companies be responsible for informing people before they share their personal data on a network?

Ms Helen Dixon: Probably the first large-scale investigation we will conclude under the GDPR is one into the principle of transparency and involving one of the large platforms. We will shortly make a decision spelling out in detail how compliance with the transparency obligations under Articles 12 to 14, inclusive, of the GDPR should look in that context, but it is very clear that users are typically unaware. For example, some of the large platforms do have capabilities for users to opt out completely of personalised ad serving, but most users are not aware of this. There are also patterns in operation that nudge users in certain directions. Aside from the hard enforcement cases we will take, we also published guidance recently on, for example, that issue of how users are being nudged to make choices that are perhaps more privacy-invasive than choices they might otherwise make if they were more aware. There is a role for us as a regulatory authority in regulating the platforms as well as driving awareness among users. It is an uphill battle, though, given the scale of what users face.

Deputy Eamon Ryan: I thank Ms Dixon. She put very well some of the concerns a number of people have articulated about the business model when she said in her testimony, "All of this may happen without the user being aware his or her own data are being deployed to reinforce the individual's existing viewpoint rather than the individual being in a position to take an objectively formed stance based on an understanding of both sides of an issue." In other words, this is having the consequence of an increasingly self-reinforcing polarisation. Ms Dixon went on to say her office is looking at "whether [the online behavioural advertising system] is in compliance with the GDPR, especially in respect of lawfulness and transparency to users". In coming to conclusions on this, is any decision the commission makes binding on all of Europe? Is the decision the commission has to make an all-Europe one? Ms Dixon made the point that the GDPR is a very good, broad, principles-based regulation. Does it give her the powers to address some of these issues if she feels there is a real lawfulness or transparency issue in the consequences of this characteristic of the platforms?

Ms Helen Dixon: Any decision we will ultimately make is binding only on the data controller, against which we make the decision. However, I did mention in response to the last question that there is a demand from controllers of all types for more certainty as to what the correct objective standard in application of the principles looks like. We anticipate that any of the decisions we make in these larger scale cross-border investigations will serve as a precedent and will be followed by others, not least because they will wish to avoid enforcement action subsequently being taken against them on similar issues. It is important to be aware that when we are applying the principles to something like online behavioural advertising, we must go back to what Mr. Rotenberg was saying about underlying business models. The GDPR is not set up to tackle business models *per se* but to apply principles to data processing operations. When we come to look at something like advertising technology or online behavioural advertising, there is, therefore, a complexity in that we have to target multiple actors. I mentioned earlier that for that reason we are looking at publishers at the front end that start the data collection from users. It is when we first click on a website that the tracking technologies such as pixels, cookies and social plug-ins start the data collection that ultimately ends up categorising us for the purposes of sponsored stories or ad serving. We are looking at the advertisement exchanges, the real-time bidding system, the front-end publishers and the advertisement brokers that play an important part in all of this in combining offline and online sources of data. We will rigorously apply the principles against those data processing operations. When we conclude we will

then have to see if that adds up to a changing of the underlying business model. The jury is out on that until we conclude.

Deputy Eamon Ryan: I have a question for Mr. Cesarini. On that issue, if the GDPR directive does not sufficiently address some of the underlying principles or approach in the business model, is the European Commission looking at how the e-commerce directive might provide further support if there is a desire within the European Parliament and Council for that sort of approach? This spring the Spanish data protection agency temporarily banned micro targeting in political advertising, although the decision has been withdrawn pending an appeal. From the European Commission's perspective, has any individual data protection regulator taken action to initiate a ban on micro targeting, whether in political advertising or another sector? Is there a fundamental difficulty with doing that?

Chairman: I ask Mr. Cesarini to keep his answer as short as he possibly can because we are conscious of time.

Mr. Paolo Cesarini: The two issues are separate. What can be done in the perspective of the review of the e-commerce directive would point more towards the issue of fairness in a commercial relationship than to the legitimate use of personal data for micro targeting purposes, which is within the realm of the GDPR. One point I would like to stress is that micro targeting is only one of the possible vulnerabilities of the ecosystem. When we talk about disinformation, clickbait, which works by directing traffic into a malicious website, operates in a different way. Micro targeting is typical for sponsored content and that is certainly an issue that needs to be addressed. Then there are other issues that are not necessarily data-driven or are not so linked to the use of personal data. For instance, the manipulation of media for amplification purposes where bot accounts behave in a co-ordinated manner and the trade of engagement indices or signals in the black market are not necessarily linked to the manipulation of personal data. Another issue about personal data may appear in the area of algorithmic bias. When the recommendation system operates in order to provide the user with certain recommendations, there we have an issue again with the usage of personal data.

Deputy James Lawless: I will be as succinct as possible. I have two questions, one for the Minister, Deputy Bruton, on the Irish environment and the new proposals, and one for the panel as a whole on regulatory enforcement. I welcomed the announcements this week and the Minister alluded to a number of other proposed measures. I look forward to reviewing the details of those when they are published. One of the findings of the committee in its discussions today and in some of the preliminary discussions yesterday has been that we should not delay because, as Mr. Rotenberg said, delay only suits the platforms. There is an urgency about all of this. Our Canadian colleagues told us yesterday that we must not let the perfect be the enemy of the good but must plough on and take steps. That point was well made. We may not take the final step but we must take the first steps and every step forward is progress. In that vein, on the proposals the Minister mentioned, two Private Members' Bills that deal with these matters are before the committee. These are the Digital Safety Commissioner Bill 2017 and the Online Advertising and Social Media (Transparency) Bill 2017, which I proposed. Both of these Bills have undergone detailed scrutiny on First and Second Stage in the Dáil. It would be prudent to consider these as vehicles to make progress, even if they are superseded by Government legislation. That would certainly fit the theme we discussed of making rapid progress and putting something in place rather than letting more elections take place in the absence of action. Perhaps the Minister will respond before I put a question to the panel.

Deputy Richard Bruton: In developing Government legislation on an online safety com-

missioner, we will adopt the principles set out in some of the Private Members' Bills, particularly provisions defining harmful content which listed issues such as cyberbullying, creating suicidal intent and so on. We will look at how we accommodate those. Nonetheless, getting legislation through the Office of the Parliamentary Counsel requires the Attorney General's sanction for the different elements. A number of elements of these Private Members' Bills run into significant problems. While we can transpose significant blocks of these Bills in our legislation, we also have to change significant blocks of it. The difficulty is that I have to get someone to stamp the legislation. I am exerting maximum pressure to have exactly what the Deputy says done. He is correct that the best is the enemy of the good and there will always be a reason to have another legal assessment done of this or that aspect of legislation. I am trying to avoid that scenario and trying to hit the end of the year deadline I have set.

Deputy James Lawless: The Minister mentioned the Digital Safety Commissioner Bill 2017. Does the same logic apply to the Online Advertising and Social Media (Transparency) Bill 2017? Is the Minister referring to both Bills?

Deputy Richard Bruton: The Online Advertising and Social Media (Transparency) Bill 2017 will be handled by the Minister for Housing, Planning and Local Government. It is part of the electoral legislation. I am sure the Minister will seek to adopt the principles set out in the Bill. The Department has articulated clearly what its definition of political purpose is and it has started to list what the informational requirements will be. Those requirements will have to be set out in legislative form so I expect there is a bit of work left in that.

Deputy James Lawless: I thank the Minister. I have a brief question for the panel. We are attempting to formulate regulation and legislation and while some countries have had more success than others in that regard, we are all moving in that direction. However, enforcement is the key to legislation and regulatory activity in any sphere. The Data Protection Commissioner has had some success in enforcement and has acquired some additional powers. One of the difficulties, however, and one to which the Minister alluded to in his opening remarks, is that this area tends to fall across a number of different Departments and agencies. What is the most appropriate model? Is it a multi-agency response? Is it a dedicated agency being tasked with online regulation? Is it a first on the scene type scenario? What is the best practice or what have the witnesses seen work best?

Mr. Marc Rotenberg: In addition to my work at the Electronic Privacy Information Center, I have also been a professor of law at Georgetown University for 30 years. I have taught privacy law and have two different case books. All roads lead to the GDPR. I say this for three reasons. First, the GDPR is not a set of principles but a set of rights and responsibilities associated with the collection and use of personal data. When companies choose to collect personal data, they should be held to account. Second, the decision in the Schrems case of 2015 makes clear that while co-ordinated enforcement anticipated under the GDPR is important, individual data protection authorities, DPAs, have their own authority to enforce the provisions of the charter, which means individual DPAs do not need to wait for a co-ordinated response to bring an enforcement action. My final point is a matter of law. The GDPR contains the authority within its text to enforce the other laws of the European Union. This is largely about the misuse in the collection and use of personal data for micro targeting. That problem can be addressed with the GDPR but it will take an urgent response and not a long-term game plan.

Dr. Janil Puthucheary: I will address a few questions to the Minister, Deputy Bruton, if I may. Ireland is no stranger to attempts of foreign interference, as was seen in the May 2018 referendum when some civil society organisations tracked various inauthentic accounts and

suggested that up to 70% of them came from across the Atlantic on the basis of time zones. How has the experience with foreign interference altered or informed the approach to designing the online safety legislation? Are there concerns that once the legislation is passed, the online safety commissioner is in place and the various processes are working, those processes might be used by foreign actors to interfere with domestic matters?

In the previous session I was quite struck by the assertion from Dr. Bickert from Facebook that even if this proposed Act, the safety commission and the processes provide directives and measures for content to be removed or adjusted, Facebook would test these directions against its internal policies. Does the Minister have a view on what this means for the operation of that legislation? We have had some arguments as to whether the fundamental problem is the underlying business model of the social platforms. Does the Minister have a view on the matter?

Deputy Richard Bruton: There is no doubt there was an attempt to interfere in some of the referenda and in those instances it was a voluntary take-down policy that was adopted by platforms rather than a legal provision. I spelled out earlier that aside from the requirement to have transparency around political advertising, the reporting of targeting and so on, much broader legislation will cover the funding of referenda in particular. We have ceilings on funding for individual candidates and parties but funding from overseas is not regulated. Foreign donations to Irish political organisations are banned and a lacuna will need to be addressed.

The legislation I am introducing is limited to harmful content such as cyberbullying of individuals rather than the addressing of political fake news or distortion of views. We are not designing it in that way and we are defining harmful content in quite a narrow way. We are working on how such definitions can evolve over time in a way that is legally robust. That will have to come back in some form to the Legislature and an online safety commissioner cannot create that legislation. We must devise a vehicle for that.

It is a fact that any online platform operating in Ireland must respect Irish law and would find itself with enforcement action against it in an Irish court if it failed to do so. There is no doubt that these Acts can be enforced.

Dr. Janil Puthucheary: To follow up, one of our concerns in Singapore and in several other neighbouring countries in Asia is that many of the issues not overtly labelled as political can be easily exploited for political gain. That is why I asked the second question as to whether the Minister had concerns around issues covered in the proposals for this online safety effort. From our perspective, such issues may well be exploited for political gain through foreign interference. Does the Minister have any comment to make?

Deputy Richard Bruton: We have not encountered that but I am interested to hear about those. We have been working on a narrower definition of creating legislation that would require companies to have codes and an online commissioner to vet those codes. There would be a power to serve notice on platforms where a code is deficient in some respects. The crime would be created if there was a failure to comply with notices. That is the structure we are seeking to put in place. We have not identified in that work foreign interference as being a feature of this legislation, although it would be with some of the more politically orientated legislation.

Lord Puttnam: My question falls into the category of political priorities and is addressed to Ms Dixon and the Minister. I am looking at this from the perspective of somebody who is worried that the big tech companies are beginning to see themselves as nation states, in effect. That is not an overstatement. One of the very few successes we have had in the United Kingdom is

getting adequate resources, staffing and money to the authorities to take on their responsibilities. If the UK Information Commissioner, Ms Elizabeth Denham, were here today I am sure she would confirm that. It was quite a struggle within the British Parliament but I believe she feels she is adequately looked after.

I am concerned that a number of nations are engaging in a dangerous tension between going out of their way to get investment income from big tech companies while not looking at the investment required to regulate those companies they have actively encouraged to come to this or that country. It is a real worry. Does Ms Dixon absolutely believe her office has the resources to take on the responsibilities that in effect it is taking on for the European Union to regulate the companies already in Dublin?

Ms Helen Dixon: Going back five years we started from a very low base in building towards the GDPR and exploiting all the strong enforcement powers we have been given. We started with approximately 27 staff when I came on board at the end of 2014 and we now have over 140. The composition of the staff has changed significantly in that we have hired top class lawyers, litigators, technology experts and investigators. We are in a radically different position. We have just had the budget for 2020 announced last month. I made a submission on the resources I anticipated I would need in 2020 as part of that budgetary process. Ultimately, we secured significantly less than what we sought for 2020. However, we secured increased resources for next year that will allow me to recruit an additional 30 to 35 experts to the staff. I should say that in that context, even if 140 sounds like a relatively modest number, we are among the top tier of highly resourced data protection authorities both in the EU and globally.

I agree with the statement. We do not have enough and that is why we sought more. We see the scale of the challenge more clearly than anybody else can see it in terms of what we face. All of these hard enforcement cases we are trying to drive in the investigations we have open are extremely labour-intensive in terms of the process we must follow. I mentioned that we are being challenged and questioned at every turn. We need more resources and this must see continued investment as an area of regulation.

Lord Puttnam: I can typify this as a tension between jobs and democracy and my concern is that democracy is in danger all the time of losing out to the jobs argument. I cannot think of a better invitation to populism than that. The Minister referred to draft legislation or the development of such legislation. An election will certainly come next year so is there a chance the legislation will be put in place? Our experience in the United Kingdom is that we badly dropped the ball. We are having an election right now with nothing like the recommendations the British Electoral Commission suggested are needed to have a fair and free election. My concern is this. If the results of the UK election are contested, that would set up a time bomb in democracies throughout Europe, which would be very difficult to control.

Deputy Richard Bruton: By its nature, regulation always tends to be catching up with developments that have moved ahead of it. As for, artificial intelligence, I read a book by Mr. Jamie Susskind, a US writer who has written about the processes embedded in artificial intelligence that will determine things like our right to get insurance and jobs. The political and governance system, in Ireland and internationally, has not yet caught up with this and struck a balance between freedom of expression and regulation. These are complex issues. The problem is not a lack of willingness to find solutions. I have found that even the narrow aspect I am trying to deal with, the definition of harmful content, is quite tricky to regulate in a way that balances freedom of expression with the need to protect citizens, particularly vulnerable citizens, from its abuse. It is not as simple as governments not bringing resources to bear. These are

genuinely tricky issues. We need international co-operation in the design of a robust and enforceable response. While it is important to ask whether sufficient resources are being devoted to the enforcement of existing legislation, many of these challenges are far more profound than that. The regulators have not quite caught up and learned how to design these systems.

Lord Puttnam: I understand everything the Minister says and I appreciate it. Does he think there is an understanding within the Government that these are existential issues for democracy? These are not trade issues or even harm issues. They are existential-----

Deputy Richard Bruton: The Government is absolutely aware of that. That is why a lot of work has gone into this and it is being led from the Taoiseach's office. There is no doubt that the importance of this is recognised. Equally, we recognise that what we do is interdependent with what colleague nations are doing. We need to work together in designing systems that will be enforceable, robust and consistent across geographies. As Lord Puttnam rightly said, these are not nation state companies. These are companies for whom we, to are large extent, are the product and they transcend boundaries. That is the greater challenge, not the issue of finding resources to enforce well designed policy instruments.

Mr. David Cicilline: I thank our panellists for this very useful discussion. Mr. Rotenberg has argued that the $5 billion settlement concluded by the Federal Trade Commission, FTC, with Facebook was insufficient, saying it was too little, too late. I have raised similar concerns, saying that this fine was essentially a speeding ticket that will not help consumers and that the remedy in this case will not serve as an effective form of deterrence. Can Mr. Rotenberg describe for us what an effective remedy in that case might have looked like?

Mr. Marc Rotenberg: I thank the Representative. In our statement to the FTC prior to the judgment, we set out several proposals. We said that effective data protection standards should be imposed on the company. The FTC has failed to do that. Second, we said that WhatsApp and Instagram should be divested from the company, not because of any grand political philosophy but because Facebook violated its commitments to protect those user data. We had additional recommendations with regards to civil rights issues, which are widely discussed in the United States. These proposals were not taken on board and as the Representative says, the settlement is a speeding ticket.

Mr. David Cicilline: I thank the witness. Some scholars argue that Facebook's ability to collect such large swathes of data is largely due to its market power. To what extent has Facebook's market dominance permitted the development of a comprehensive surveillance infrastructure?

Mr. Marc Rotenberg: I would say that Facebook and Google together are probably unparalleled in the amount of information they collect on individuals. A key point, which I believe was made on an earlier panel, is that the vast majority of this information is not collected directly from the user. This is particularly true with Facebook. Users are tracked across the Internet, which makes notice, consent and transparency mechanisms effectively useless.

Mr. David Cicilline: Of great concern to many, including me, is that Facebook has become a dominant communications network while running a behavioural advertisement-based business model. It seems increasingly clear that this combination is lethal for our democracy. There was a reason AT&T was never allowed to surveil the conversations of telephone users to sell them advertisements. What problems does Mr. Rotenberg see with the behavioural advertisement business model? What does he think should be done about these problems? Rather than

improving transparency in the online ecosystem or policing the use of data collection, should there be an outright ban on behavioural advertising?

Mr. Marc Rotenberg: Yes, there should be an outright ban on behavioural advertising. People fail to understand that the behavioural advertising model of Facebook has taken advertising revenue away from contextual advertising, the advertising that supports the editorial content of genuine news organisations. This is a zero-sum game and journalists are losing it.

Mr. David Cicilline: Turning to Ms Dixon, as I have mentioned previously I have deep concerns that the enforcement policies for both consumer protection and antitrust regulations in the United States have not kept pace with the digital economy. The fact that the press has to rely for survival on the Facebook News tab and Mark Zuckerberg's views on the First Amendment shows how dire the situation really is. What is the European Commission doing to ensure that enforcement is effective and timely and that it stays ahead of the curve? What is Ms Dixon's response to concerns that delays in enforcement have entrenched the market power of firms that are dominant online? Does she have any recommendations for us in improving enforcement in the United States?

Ms Helen Dixon: Is the Representative asking me about the Irish Data Protection Commission, rather than the European Commission?

Mr. David Cicilline: Yes.

Ms Helen Dixon: There have not been delays in enforcement under the general data protection regulation, GDPR. This regime is 18 months old. As an individual data protection authority, we have handled 11,000 user complaints, many of which have been in respect of the platforms where individuals have tried to exercise rights. We have intervened and ensured this has happened. We have also prosecuted several companies in the last 12 months for e-privacy regulation infringements. We have 29 litigation cases in the Irish courts at the moment. Mr. Rotenberg referred to the Schrems I case earlier. We have brought forward what is referred to as the Schrems II case in the meantime. There has been a hearing on the critical issue of transfers of EU personal data to the US this summer. It is pending the judgment of the Court of Justice of the European Union. It is a mistake to say there has been no enforcement but I think the Representative is referring to the fact that there has not yet been an outcome to the large-scale investigations into the big tech platforms which are currently under way on lawfulness, transparency, privacy by design, default and so on. Eighteen months is not a long time and not all of the investigations have been open for 18 months. We must follow due process or we will not secure the outcome in the end. As these companies have market power and have the resources to litigate forever, we have to make sure we follow due process and allow them a right to be heard. We conclude the legal analysis carefully by applying the principles of the GDPR to the scenarios at issue, and then we can hope to deliver the outcomes that the GDPR promises. That work is under way. We could not be working on it more diligently. The first set of decisions will start rolling out in the very near future.

Mr. David Cicilline: I thank Ms Dixon.

Chairman: Does Senator Higgins have a question? I must confine her to 30 seconds.

Senator Alice-Mary Higgins: My question is to the Data Protection Commissioner. Are the special categories of personal data under Article 9 a tool her office could be using? How do they relate to observed data, that is, behavioural activity? How does one make sure that

observed data, which relate to the Article 9 categories, are included? Is that a key tool which could be used in the regulation of micro targeting?

My second question is directed to the whole panel. The business model has been talked about again and again. One of the key things we can do to disrupt a business model is to apply financial penalties. How important are financial penalties under the GDPR to disrupting the business model? Should a portion of fines collected under GDPR be ring-fenced for digital empowerment or education?

Chairman: I apologise, as we do not have time for the whole panel to respond. Only 30 seconds are available.

Ms Helen Dixon: Article 9 is most certainly in scope in terms of the investigations I referenced earlier. There is no doubt that sensitive categories of personal data come into the online behavioural advertising model. On the question of fines, there have been studies done and David Wright and Paul De Hert published a book on enforcing privacy in 2016, which looked at the effects of what was a new fining regime in the UK from 2010 that applied to the information commissioner's office. It concluded that the fines made no difference. We will be obliged to impose fines where we find infringements so that is what will happen but we expect the corrective powers we apply, such as bans on processing and requirements to bring processing operations into compliance, will have the more significant effects.

Chairman: I thank all the witnesses for appearing before us this afternoon.

Sitting suspended at 2 p.m. and resumed at 2.46 p.m.

Session 4: International Collaboration

Chairman: This is the fourth session of the International Grand Committee on Disinformation and 'Fake News'. I welcome Mr. Rogier Huizenga, human rights programme manager, Inter-Parliamentary Union; Mr. Adrian Lovett, chief executive officer, Web Foundation, and director of policy, Ms Áine Kerr, co-founder and chief operations office, Kinzen Limited; Mr. Frane Maroevic, director of the content and jurisdiction programme, Internet and Jurisdiction Policy Network and Lorna Woods, professor of Internet law, University of Essex.

I advise witnesses that by virtue of section 17(2)(*l*) of the Defamation Act 2009, they are protected by absolute privilege in respect of their evidence to the committee. If they are directed by the committee to cease giving evidence on a particular matter and they continue to do so, they are entitled thereafter only to a qualified privilege in respect of that evidence. They are directed that only evidence connected with the subject matter of these proceedings is to be given and they are asked to respect the parliamentary practice to the effect that, where possible, they should not criticise nor make charges against any person, persons, or entity by name or in such a way as to make him, her or it identifiable. Any submissions or opening statements made to the committee will be published on the committee website after the meeting.

Members are reminded of the long-standing parliamentary practice to the effect that they should not comment on, criticise or make charges against a person outside the House or an official by name or in such a way as to make him or her identifiable.

I now invite Mr. Huizenga to make his opening statement.

Mr. Rogier Huizenga: I thank the committee for inviting the Inter-Parliamentary Union, IPU, to this meeting and for giving us an opportunity to follow the debate as it is happening. I would like to use my time to share with the committee some of the challenges that we see from the perspective of our organisation for parliaments being mobilised around the topic that is under discussion today and some of the opportunities.

For those who are unfamiliar with the Inter-Parliamentary Union, it is the world organisation of national parliaments. There are 179 parliaments in the world that are members of the organisation. With the exception of one, all of the parliaments that are represented here are members of the organisation. As an international organisation we are grappling with this question. In terms of challenges, we see that parliamentarians are not well equipped to deal with it effectively. I am speaking from purely from a global perspective. They have a lack of understanding of the technical issues that are at stake. They are also finding it very difficult to situate the debate between what needs to be done at the national level and what is happening at the international level. In addition, as was said earlier, there is a lack of clarity for them as to the governance structure which is dealing with this question at international level. There is also a challenge for them in getting access to the right information. What I really appreciate is seeing a variety of Members of Parliament represented here in the room. That said, they are obviously from advanced countries so they have some similarities when it comes to their own national context. Maybe also, because they are from advanced countries, they can more easily access representatives of tech companies because I would doubt if high-level representatives of the major tech companies would come before national parliaments far away from the West.

There is also the reality that we see in our discussions at the IPU about differences - legal differences and philosophical differences - around some of these major questions between countries but also between continents. Even today, obviously we have two sides of the pond being represented. Also, I guess there are fundamental differences between how freedom of expression is seen and what the limits are. We all know that hate speech is not necessarily criminalised in the United States. In addition, there are issues with regard to the financing of political campaigns. In the United States, spending is pitched whereas, in Europe, the tradition is more one of using public funds to finance public campaigns.

We come from different realities and this is just the western world. So what we are also facing in our discussions within the organisation is that there is a real variety of organisations and bringing everyone together is very difficult. Where do we find common ground? In trying to adopt a shared vision both of the problems but also the solutions.

We have seen that there is a growing sense, which was stated in the course of this morning, is that the business model is the real heart of the problem and that is something that needs to be tackled. Now, also within the IPU, there is discussion around that. I really like the statement that was made this morning around human rights and personal data. Of course, if we could reset the clock and start again things could possibly look differently now. Is that realistic? Short of a radical reform, there is discussion within the organisation to push for increased transparency of the work of the tech companies, particularly when it comes to the algorithm amplification and political ads. There is also a lot of debate on making a distinction between illegal versus harmful content. Also, to see the issue as something slightly larger than misinformation and see it really as something that concerns society, as a whole, in the sense that we are faced by what has been termed "junk news" rather than fake news, which requires us all to move and come together to promote better civic education, to help promote civil discourse and help the people, at large, to be better able to recognise fake news.

Mr. Adrian Lovett: I thank the Chairman and her committee for the opportunity to present the Worldwide Web Foundation's views on this topic. The foundation is a non-profit organisation founded by the inventor of the world wide web, Sir Tim Berners-Lee, to promote and defend the web as a basic right and public good for everyone. We work to achieve this mission by securing policy change based on evidence and robust research. Crucially, to a point that the previous speaker, Mr. Huizenga, has just made, we work equally and are equally active in developing countries as we are in the countries represented by the Parliaments here.

I guess the committee has heard a lot of important things today, many of which I would agree with, but I would like to make one further, very specific, proposal for the members of the committee and that is as follows. We believe that a crucial step for lawmakers like yourselves is to require companies to publish regular human rights impact assessments and transparency reports. That means companies will be expected to tell us how they have weighed the impact of their policies and products on individual human rights, and on our societies. These reports should be grounded in international human rights frameworks and focus on disinformation and misinformation, hate speech, electoral interference and political ads. These kinds of assessments have been more and more prevalent in other sectors such as extractives, manufacturing and agriculture but less so in technology. Although some tech companies have started to publish transparency reports but we think they can go further. The more we learn about how companies make these decisions then the more informed and empowered governments will be to regulate effectively in this area.

Before I go back to a little more detail on that, I will step back for a moment. When Sir Tim Berners-Lee invented the world wide web in 1989 - 30 years ago - he changed the world. He expanded our access to knowledge and freedom of expression more than arguably any other development in modern times. In recent years, and as today's conversation has shown, we have seen the web misused to spread lies and hatred, and sow division within our communities. It is a complex dynamic and tackling it, we think, will require an equally complex set of policies and, crucially, long-term thinking.

As public representatives, you are faced with a difficult balancing act: the need to respond swiftly to the harms caused to your constituents by disinformation, with the responsibility to uphold people's human rights and freedom of expression and avoid triggering unintended harms. There are numerous challenges in the context of international co-operation on disinformation, and a number of them have been mentioned already. Like the web itself, the platforms where much of the disinformation is spread operate globally but national laws vary and sometimes diverge. Platforms struggle to fact-check content consistently at a global scale. While platforms are making decisions that impact billions of lives globally, we have not had real insight into how those decisions are made.

Despite all of this, our sense - and certainly Sir Tim Berners-Lee's sense - is that there is hope. Sir Tim Berners-Lee would maintain, in spite of it all, a determined optimism that there are ways we can come together now and in the future to address these challenges. Last year, Sir Tim announced the creation of the contract for the web. It is a social contract that would bring together governments, companies and civil society to agree on a set of ground rules to guide digital policy agendas. More than 350 organisations have been part of the process so far. The initiative began with a set of nine principles small enough to fit on a postcard. In the next few weeks we will announce the full contract for the web with 76 clauses that emanate from the nine principles. It is intended that this contract, which we will launch at the Internet Governance Forum in Berlin, can play its part as a broad plan to protect and secure the web as a public good.

In that context I shall return to that one specific proposal, which, in our view, sits very much at the heart of the contract for the web. I refer to the increased commitment to transparency around risk assessments by companies. While transparency is not, and should not be, the end of the road, it is an essential first step that supports evidence-based regulation and enforcement but it is that necessary first step. So we call on companies to publish regular transparency reports that tell us how they have weighed the impact of their policies and products on human rights when it comes to misinformation and disinformation. We also call on national parliaments around the world to take this first step by requiring platforms to take that step of their own. I am happy to discuss this matter more as we get into questions.

Ms Áine Kerr: I thank the Chairman and members for the opportunity to speak here today.

We are in the midst of a wicked problem and are running out of time. A wicked problem is, by its very definition, something that is difficult or almost impossible to solve because of incomplete, contradictory and ever-changing requirements. It cannot be solved through one solution alone. Our wicked problem is an information disorder and that disorder is a symptom of a much wider societal problem - a collapse of trust in institutions, including media.

I have worked as a traditional journalist with Ireland's main newspapers, with Storyful, the world's first social media news agency, and with Facebook, the world's largest social media platform. I launched a new start-up called Kinzen, the purpose of which is to reconnect people with quality news and information. Throughout 16 years in the industry, I have remained very resolute about the importance of journalism to better help people to understand the world around them but also ever concerned about the phenomenon of more and faster content everywhere. I have seen a new information ecosystem emerge in which everyone became a publisher, the means of consumption changed and the modes of distributing news became fragmented. There were positives, of course. We have largely become more connected, engaged and educated because of the Internet. However, amid that period of massive disruption and digital transformation wherein online experiences were built for speed, clicks and scale, the connection between people and journalism was lost.

We are at another crossroads now and there is an opportunity for correction. While the task list is long and complicated, there are three core areas in which to make a start: to ensure that we connect people with quality news and information; to build collaborative projects across multiple sectors so there are shared learnings; and to find thoughtful and pragmatic ways to hold technology companies accountable.

What does that mean in reality? I believe that today's recommendation systems are a root cause of information disorder. We need radical transparency on the programming of algorithms. A new generation is seeking alternatives to the toxic noise, hidden surveillance and the endless distraction of their social feeds. They demand an experience of information that rewards their best intentions, fits their daily routine and protects their privacy. That means, we as an industry, need to build radically different news experiences. In Kinzen, for example, we are building a citizen algorithm, in which data science and machine learning is guided by human curation and explicit user feedback of every single individual person.

We also require collaboration at an unprecedented scale across multiple industries. In journalism, we need to find more opportunities for newsrooms to collaborate and not compete. That means funding projects like the CrossCheck initiatives undertaken by the news organisation, First Draft, in places like Brazil and France where journalists from competitive organisations worked to find, debunk and report on different rumours during election cycles. In digital lit-

eracy, we need long-term joined-up education initiatives, rather than one-off campaigns, when it comes to giving people - young and old - the skills and tools for consuming information online. That means taking successful models like the Finnish Newspapers Association's work in schools for the past 50 years or the news literacy project curriculum in the United States, and using schools and libraries as the key gateways to build global media and information literacy, MIL, playbooks.

In research, we need to find more opportunities for academia to study anonymised data from technology companies so they can better understand what is working and not working. That means scaling efforts like Social Science One - the non-profit commission launched in 2018 - to establish concrete partnerships between academics and data-rich institutions. It now has 32 million individual links extracted from Facebook upon which to conduct research.

To be truly collaborative, we need to bring together civil society, technology companies, publishers, academics and governments so we can answer the question: what can we do together to tackle this wicked problem, while protecting freedom of speech?

Regulating the Internet is complex. The risks are immense and committees such as this one must ensure there is careful deliberation of well-researched evidence so that practical enforceable standards and laws can emerge.

A new report emanating from France outlining a detailed strategy for increasing oversight of social platforms while allowing for an independent regulator to ensure compliance with standards, deserves consideration. Ideas are emerging from the Transatlantic High-Level Working Group on Content Moderation and Freedom of Expression, which propose to enable platforms to set standards while enabling governments to hold those platforms accountable to those standards via Internet courts.

Wicked problems are difficult but not impossible to diminish. It will now take collaboration, transparency and innovation on an unprecedented global scale for us to realise if the moment for correction is upon us.

Mr. Frane Maroevic: It is my honour to contribute to the committee's deliberations on advancing international collaboration on online regulation. Clearly there is no need to stress that this is a transnational issue: that the committee has come together to discuss this issue speaks for itself. The initiation of the Grand International Committee is also a sign that the existing institutions and processes are not adequate to deal with these issues.

Most online interactions and data flows today involve multiple jurisdictions based on the locations of users, servers, Internet platforms or technical operators. Current frameworks for interstate legal co-operation struggle to handle this new digital reality. In many cases they hinder or even prevent co-operation. In some cases, they empower those who want to do harm or commit crimes.

How do we address issues such as the interoperability between the different norms; the interplay and the hierarchy between companies' terms of service, national legislation, international treaties and commitments? Who sets the standards? What are geographically proportionate and relevant responses to these issues? How do we ensure the rule of law and transparency of all these processes?

How do we effectively co-operate to ensure that those who commit crimes and inflame hatred or violence are prosecuted? What is an appropriate punishment and what is the recourse

for the victims? We need institutions for all these things because the most common forms of punishment and redress seem to be take-down of problematic social media posts or accounts.

In order to come up with workable answers, we need new international tools and institutions for Internet governance. This is one of the greatest challenges of the 21st century that no one can solve unilaterally. In the absence of policy standards and appropriate frameworks, we face increasing tensions that trigger unco-ordinated short-term solutions. National laws are enacted to try to deal with transnational problems, resulting in a legal arms race that risks unintended and harmful consequences, including jurisdictional conflicts and unwanted fragmentation of the Internet.

The organisation I work for, the Internet & Jurisdiction Policy Network, is about to publish the first ever report on the status of global Internet governance which shows that globally there are more than 300 such laws or Acts. As the majority of them are not co-ordinated we risk fragmenting the Internet.

We need solutions that will bring values and rules-based international order to the Internet, while at the same time ensuring that our democratic institutions and all our fundamental human rights are fully respected. This is a colossal task and shows why Internet governance must be a multi-stakeholder process. In reality it is not because in most cases when we discuss inter-governance it ends up being an intergovernmental process. In a true multi-stakeholder process all three branches of the state need to work with the fourth estate, the media, along with civil society groups, academia and the companies. This is what the Internet & Jurisdiction Policy Network does as a multi-stakeholder Internet governance process. We bring together approximately 300 key stakeholders from governments, Internet companies, technical operators, civil society groups, academia and international organisations from more than 50 countries to work together to develop policy standards and operational solutions.

In recent months our contact groups, working in three separate jurisdiction programs on data, content and domains, produced a series of proposals norms, procedures and mechanisms that we call operational approaches and I would be happy to share them with the committee. The next focus for us will be on standards for recourse mechanisms, looking at issues of normative interoperability and transparency.

Regarding the committee's work I would like to highlight transparency, a matter mentioned by a number of people today, as one of the most useful tools in tackling disinformation. I am referring to establishing standards and mechanisms to deal with the abuse of platforms and technical infrastructure for political, financial or other gains.

Members of the committee know the challenges of regulating speech. The most problematic content does not fall neatly into what could be restricted under international human rights standards on freedom of expression. These issues are constantly evolving and changing, and artificial intelligence only contributes to the speed and complexity of the problems to be solved.

I call on the members of committee, as representatives of the people, to support a multi-stakeholder, transnational Internet governance process.

Professor Lorna Woods: I am grateful for the invitation to give evidence to the committee. A way forward is to try to identify a model which is common - perhaps not a model law, but an underlying model that can then be deployed around the world in different jurisdictions.

The difficulty that is often raised with regard to content regulation is the subjectivity of

content and the fact that standards differ from state to state. To address this problem, I would suggest a regulatory system that looks at the underlying systems, one that moves the focus from the content to the mechanisms that encourage content, facilitate its sharing and distribution, and select the content that comes to people's attention. It is my contention that the platforms have developed with a disregard for the impact on the sorts of content and the sort of content that is prioritised and widely shared. This goes back to the discussion about the business model, which is about encouraging user engagement with the aim of getting more data, which is then used as a commodity. The principle put forward by Carnegie United Kingdom Trust is that there should be a statutory duty of care as regards the systems. It is starting with an assessment of risk; identifying the consequences, be they intended or unintended; and, crucially, taking steps to mitigate. Rather than leaving it at transparency, it involves asking why something has been deployed and how it can be made better.

When Google first started, it said that it viewed data as an exhaust product of the search engine business. I now wonder whether we have reached the point where people's content is the exhaust product of the data collection business and that we should be moving to try to get a cleaner engine rather than a dirty diesel one. That is what the Carnegie project is about. I am happy to share further detail. We have done quite a bit of work on this but I do not want to weigh discussions down. I would suggest that using a model that focuses on systems is beneficial in an international context because one does not have the difficulty of agreeing about difficult content. What one is looking at isn on the whole, further up the process and it is possibly easier to find common ground there so one can then be in a position of deploying a common model that can be responded to within an individual state context. I would emphasise that this can never be a silver bullet. There will probably always be a role for moderation for take-down and in some instances, possible law enforcement engagement but this sits on top of this common model. It is when one starts looking at particular items of content that the difficulty and differences arise. That is the proposal. It involves a statutory duty of care aimed at the systems - the infrastructure itself.

Chairman: I thank Professor Woods. We will start again with Australia.

Mr. Milton Dick: I will return to where Professor Woods finished about the model. My next question is directed to Mr. Lovett and possibly the IPU. In terms of best practice, which countries either through the IPU or otherwise are leading by example? This is where the rubber hits the road in terms of where we move forward. I have not heard a lot of examples today of any nation states or countries leading by example with new laws, technology or common models to deal with the "wicked problem". Are we the people who are setting the scene or are there other people, who I would hope are outside this room, who are dealing with this?

Mr. Rogier Huizenga: The reality of which we are aware is that there are quite a number of initiatives at national level, particularly in Europe, that are also shared within the IPU. There is no full analysis of how these different national initiatives regarding hate speech compare to each other. There are a number of what seem to be good examples but with some potentially difficult implications.

Mr. Milton Dick: What are the good examples?

Mr. Rogier Huizenga: France has recently developed a law to tackle hate speech and harmful content. The law adopted in Germany is another example so there are a number of examples. The challenge is that these examples differ from each other so how do we compare them? This is also where we see real merit in having these kind of discussions among parliamentarians

possibly first as a start, as is happening here, for more like-minded situations but also extending it to a slightly wider audience. I certainly think that the countries from which the participants today come are already tackling this. I am not saying they are producing the best of results but they are already to the forefront of dealing with this.

Mr. Milton Dick: I am glad Mr. Huizenga said that. Australia has been leading the way in some respects in terms of our eSafety Commissioner and the laws our nation has passed. I will use Australia as an example; to our north, there are countries like Indonesia and further north, there are anti-democratic countries like China and Vietnam. Regarding a common regulatory system, the involvement of law enforcement was mentioned. What would suit our nation in the Indo-Pacific region - the freedom of speech argument - would not apply inside China and Vietnam. I would not want a system that is one-size-fits-all so I disagree slightly with the witness statement about a common ground versus what is already happening around the world. I would be interested what the panel thinks about that - either a two-series or a two-step process in terms of democratic reforms versus the opposite.

Chairman: Does Professor Woods wish to come in?

Professor Lorna Woods: I would like to clarify what I said. The model that I said might provide a common ground is based on process. It is not based on specific items of content. In a way, it is a two-step process. There is common ground about standards for recommender algorithms or whether metrics such as "likes" and those sort of devices have unforeseen consequences. I think agreement can be reached there. It is when one goes into the question of whether a particular item of content is problematic that one finds a lot of difference. We must accept that there is a limit to how far we can go with that.

Mr. Adrian Lovett: I will take both those questions. Regarding the first question, I wish we could put an excellent national model before the committee. I think what has happened in Australia, and Ireland is looking at something similar in terms of the role of the Data Protection Commissioner, is important. Our view is that what has been taken forward in Germany is not a model to follow so there is a lot of work to be done there. The committee is at the front line of trying to figure this out - what it looks like at a national level. I agree with Professor Woods that for us, a focus on the process is as, or possibly more, important as a focus on the end content. Our hope is that the idea about transparency reports and human rights assessments will expose not just the numbers of take-downs and so on, which we are starting to see more of, but the basis for decisions. One could look at it and say "well, we wouldn't have done it that way" or "we can see why they came to that conclusion". It involves having that qualitative understanding of how decisions are being made.

Mr. Dick mentioned Indonesia. I was there earlier this year and spoke to Ministers and so on. To underline the challenge mentioned by Mr. Dick, it was clear that when we and some government officials were talking about a healthy Internet, we meant very different things.

Ms Áine Kerr: Parts of this are done country by country, i.e., speech, while parts can be done at an international level around political advertising. Regarding the point that this is about process and framework, I mentioned that high-level working group earlier. There is a formula - a framework - there to which it has given a lot of thought. It involves whether one can work with the public, civil society and a coalition of organisations to build standards that are about behaviour and, in parallel with that, the technology platforms would build covenants - that these are their warranties - so that they are held responsible as well to ensure there is platform responsibility matched to those standards. Layered on top of that could be independent regula-

tors tracking and monitoring the implementation of the standards and covenants and, ultimately, imposing huge fines where there has been a stepping out of line. In parallel, there may be a need for Internet courts on very specific issues to deal matters on a case-by-case basis. Obviously, Facebook would be considered. There is a role for the oversight boards. We are starting to see, in some of the high-level working groups and in the conversation today, that there is a framework and process that could be built in country by country and company by company.

Mr. Frane Maroevic: I will be brief because many of the points of been covered. I agree very much with what was said. I do not believe we have come across perfect legislation that we could just forward or copy. Most legislation that deals with content and its regulation has potentially serious implications for freedom of expression and freedom of speech.. That is why we are all talking about trying to find processes to deal with these issues, examining issues of impact, virality, reach and proportionality. Regulating speech in the analogue world was also about the impact and the possibility speech having an effect. That is important. It is not just about the speech but also about the context. That is why the call is to try to find models and mechanisms that would be agreeable to a larger group of nations in terms of systems. One will never find an agreement on specific regulation of content between each country. We need a certain level of flexibility.

Mr. Tom Packalén: What is Mr. Lovett's view on the approach to fake news and fact-checking? There are great dangers. What really is fake news? There is nothing there but there are also different kinds of realities, and people see the same issues in different ways. In the same country, different counties might have different views and see certain problems in different ways. What should the approach be so that we will not be in some kind of Orwellian world when it comes to free speech?

Mr. Adrian Lovett: If one starts from a perspective of human rights, it does not answer the problem, at least not easily, but it does frame the challenge and the question. If we are clear that we are equally concerned about a range of human rights, including the right to freedom of expression but also the right not to be harmed in various ways, that has to be the starting point. The way we look at it, the disinformation and misinformation have three parts. First, there is deliberate, malicious intent, whether it is state-sponsored or otherwise. That was talked about today. I refer to intent to bring about an income systematically and in a very determined way. There is system design that creates perverse incentives and rewards. The teenagers in Macedonia churning out factually incorrect stories about Hillary Clinton's health, for example, did not in most cases have a political axe to grind. They figured out how to make a few euro. That was a result of the incentives created by the system. Then there are the unintended negative consequences of design, which also come with what we might argue are positives associated with the more open discourse we are now able to have online. It breaks down into those three areas, at least, and a different approach is required for each.

Mr. Tom Packalén: Does Mr. Lovett have some kind of solution for establishing reliability or for regulating?

Mr. Adrian Lovett: The challenge to address that lies with the companies. There is no easy answer. It requires a really determined effort and dedicated resources tailored to different contexts, countries and languages to deeply understand the nature of the content being looked at.

Professor Lorna Woods: Let me follow up on that. Maybe solutions are not about looking at content but about companies looking at the factors they put into their recommender algorithms in terms of whether they value reliable content rather than content about particular

stories. There was some research done on the recent Indian election and the role of WhatsApp. Some of it was suggesting that the intimacy of a WhatsApp group has an impact on people's tendency to believe. A question arises, therefore, about the design of groups. Are they really small groups of friends or are they just conglomerations of relative strangers? One might want to consider how easy it is to embed content from sources because one then gets contextualisation, which makes it more difficult for people to assess. There are issues with unintended consequences and design in respect of how we share information.

Ms Áine Kerr: There are a couple of levels. On the technology level, we require fundamental rewiring of the recommendation or algorithm I talked about in terms of transparency. This is so people will understand why they are seeing certain recommendations. They should have the ability to reset their preferences. We need to accelerate our AI machine-learning efforts ultimately to be preventive and remove bad actors who are trying to spew confusion. There is a human layer on top, whether it is through the fact-checkers and efforts like First Draft, which I mentioned, whereby one is ultimately accelerating the efforts of the fact-checkers but ensuring the fact check travels back to those who might have viewed something false. A problem with many of the fact-checking efforts mentioned earlier is that they often occur long after the viral peak window. We are not capturing the people in the first 12 hours when there is peak virality. Therefore, we need to build systems and technology that identifies and goes back to the people and asks them whether they have seen a certain other perspective, which is from a trustworthy source. On that, there is a considerable amount of work happening across the industry on trust metrics and nutrition labels. We keep talking about transparency today. What does it look like if one can click on a little icon across multiple platforms or websites that indicates who owns information and how long the owner has been up and running. Thus, people can engage in critical thinking to determine whether they want to trust the information.

Ms Nino Goguadze: My question is for all who wish to answer. The issue has already been covered in one of the statements but I would like to go a little more deep in discussing it. We know that there is no unified definition of hate speech or harmful content. There is no common understanding as to what constitutes information or fake news. There is no one certain definition for these terms. The legal frameworks of the countries show there is no common approach among countries towards regulations. Today, when we are discussing the possibility of parliamentary co-operation and how we can work together and address the challenges together, do we need to agree on basic definitions of terms or basic issues of regulation? Would this have a role in addressing the issue?

Mr. Frane Maroevic: To build on what I already said, I fully agree that we might not find agreement on a panel, never mind in this room, as to what constitutes hate speech or harmful speech. It would be a very difficult and useful discussion but, as we are all saying, we should start off trying to examine regulatory aspects and what we can agree on. Sometimes the problem with speech is not just what is said but the context, virality, reach and impact. These can be examined in much greater detail and measured. I call for us to try to find a way to get together and reach agreement on the terms of the regulation on as broad a scale as possible. That would allow us to compare different countries and it would be much easier to implement. It would give the experience of the Internet a much more uniform approach; therefore, it would be much more positive and useful in this context. Nevertheless, the discussion on what constitutes difficult, harmful speech needs to continue, but it would be difficult to implement.

Professor Lorna Woods: We are probably saying something similar. I emphasise the point that if one is putting the obligation on companies to look at how their systems are facilitating

the spread, one does not rely so much on definitions of how one categorises certain kinds of speech. The techniques for allowing the content to spread cut across a range of harmful content. It softens the need to understand it. Finding an agreement on hate speech would be difficult, but perhaps one could start with asking whether there were repeat instances and other such technical questions, on which there might be agreement.

Mr. Rogier Huizenga: On the question of hate speech, we should not forget that there is a series of international standards and instruments that apply to pretty much everyone in the world, including the International Covenant on Civil and Political Rights in Articles 19 and 20. Most countries have ratified that treaty. The UN human rights committee has jurisprudence. There is a UN special rapporteur on freedom of expression who has just produced an interesting report on precisely this topic and human rights. A lot material is available. There is the Rabat plan of action on hate speech which was developed eight years ago. It is supposed to serve a global audience. The international standards are in place for some specific forms of expression. They need to be adapted to the national context.

Deputy Eamon Ryan: We need to distinguish between the worldwide web which, in my mind, has a basic structure that is holding up and the platforms which are using it, in respect of which there is a governance gap. Tim Berners-Lee and the Web Foundation have a very good insight into how that is happening. Our key question is where is the governance and how do we secure collaboration on it. Mr. Lovett has said he is travelling to Berlin at the end of November with the Internet Governance Forum. To use an expression he might know, he and whose army? How can national jurisdictions and the European Union, as several others have said, make sure it is collaborative across jurisdictions? Where are the teeth? How will that collaboration be brought about?

Mr. Adrian Lovett: About 0.5% of the world might say the Internet Governance Forum is a good place, while the rest of us wonder what it is. Tim Berners-Lee's idea on which we have been working for the last year or so has three phases. The first was to land the set of top line principles that I mentioned. They consist of nine principles, with three for governments, three for companies and three for citizens. On the question of us and whose army, approximately 350 organisations signed up in support of the principles and committed to engaging with the process of turning them into concrete actions. The 350 organisations include most or all of the major platforms, a number of governments, including the German Government and the French Government, and some terrific civil society organisations in the global south and elsewhere. That was only the first step and if we had stopped there, it would have been useless.

The second step is the one at which we will land in two or three weeks' time in Berlin. Approximately 80 experts from different sectors and backgrounds have deliberated over the last three months or so to announce 76 clauses related to the nine principles, covering the whole range of what we saw as challenges in ensuring the web worked for everyone.

The third stage is to ensure all those who have signed up to these commitments - we hope as many as possible of the 350 organisations involved in the first stage will do so - will be held accountable. The Web Foundation will take it on itself to ensure there will be a robust monitoring mechanism that will track progress against the commitments made. Part of the conditions in endorsing the contract for the web in Berlin by companies, governments and civil society groups will be publishing an annual accountability report of their own addressing the elements of the contract.

The Deputy made a good point about the web versus the wider Internet, including the big

platforms. We absolutely recognise this. Tim Berners-Lee has always had a strong sense that while Facebook and Google are not the web, there is an opportunity which perhaps is unrealised for those players and others to help to strengthen and build the web and, within the wider Internet, to reinforce the values of the web, including transparency and openness, to have a permissionless space and enable people to have the opportunity to be creators, as well as consumers. While we are, first and foremost, concerned about the worldwide web that Tim Berners-Lee invented, we are also determined to see how much of the spirit, value and ethics behind it can be experienced.

Deputy Eamon Ryan: I have a question for Ms Kerr. It is a sad day for Irish media, with job losses having been announced at the national public broadcaster. I thought her contribution was very important as we have been thinking about the business model. Is it data harvesting to fund advertising or is it a paid subscription model? That is not, however, the whole picture because, as Ms Kerr says, everyone has to be able to connect to quality journalism. As some people will not be able to pay subscriptions, we need public service, high quality journalism that everyone can access. What is ironic is that the current business model for social media makes it impossible to fund public service broadcasting in this country. Does Ms Kerr have any specific proposal for the funding of public service broadcasting?

Ms Áine Kerr: The advertising model is broken for the journalism industry. We need to think about devising radically diverse models for the funding of journalism. The Deputy is right that, when it comes to public service journalism, we need to help to fund it. In this country that includes rethinking the television licence fee. As we all know, the mode by which we consume media has changed. We are the Netflix and Spotify generation. We need to think about taxes and subsidies that address this device by device mode of consumption.

On the model itself, we have to think about a system wherein people will understand why journalism is important and make a donation or contribution or become a member. That means that we will have to do a better job as an industry in amplifying the reasons. With that comes a new form of journalism that will be people-powered. It states less is more and that we are going to stop annoying people with irritating advertisements. Instead of having a lot of content that keeps people scrolling endlessly on platforms, applications and websites, the new form of journalism should give people a productive experience. That means giving them the right content and right format in the right amount of time that feels purposeful and productive. Right now all of the evidence shows that people feel incredibly overwhelmed by the amount of content online. They hide their digital footprints and turn off. There is, however, an opportunity. There are means for governments to ensure taxes incentivise and subsidise media. Perhaps there could be a tax incentive to pay a subscription or become a member of a media organisation whereby they could claim back the fee when making their tax return each year. It also comes to funding it from the ground up to ensure that local journalism can survive. If we look across at the US desert, that is a phenomenon that increasingly, we will see across Europe. We must ask how can we fund local and public service journalism and ensure that there are institutions that can take the funding and distribute it to the media at large.

Deputy Eamon Ryan: Yesterday, we heard a great deal about the duty of care process approach. I understand that informed the UK Government's White Paper on harmful content. I expect Professor Woods worked with the UK Government on that. Was there any indication from the outgoing UK Government that were it to return to office, it would continue with the approach set out in the White Paper? Is it agreed? Would it be implemented if the outgoing Government is returned?

Professor Lorna Woods: While I do not know the thinking of the current occupants of No. 10 Downing Street, the Queen's Speech certainly contained a commitment to publish a draft Bill in 2020, which indicates a determination to take it further. While I do not know whether the committee is aware of it, the Digital Economy Act contained a provision to have age verification for online pornography. That took a while to be sorted out and was at the brink of coming in when the Government said it would not do so. The Minister with responsibility for digital was questioned on it and said the issues around online pornography would be swept up through the progression of the online harms White Paper. I do not know what will happen but this is an indication that there is an intention to continue.

Chairman: Now we move to questions from the Singapore delegation.

Mr. Amrin Amin: I thank Professor Woods for her very interesting proposal. Does the model envisage sanctions?

Professor Lorna Woods: Yes.

Mr. Amrin Amin: I seek thoughts in this regard because an earlier panel discussed a voluntary code of practice. Why are sanctions necessary? Does Professor Woods think that voluntary codes work? Will she clarify whether this would be a regulation that is enforced and monitored locally and that the policies and oversight boards or internal checks would be subject to this process or regulation?

Professor Lorna Woods: Yes, we envisaged a formal legal obligation on companies falling within the remit and that it would be enforced by an independent regulator. We suggested Ofcom, the communications regulator in the UK, which has a track record for evidence-based and proportionate regulation. We envisaged that there should be sanctions for a company that did not comply but that there would be a sliding scale in order that the starting point for the regulator would be to try to engage and inform before going to enforcement. We thought that given the size of some of the companies at issue, we should look at GDPR-sized fines and we discussed whether, in the financial model, there might be personal liability for directors to get them to pay attention. The underlying model was the Health and Safety at Work etc Act. The Health and Safety Executive, which is the enforcer for that legislation, has the power to prosecute. Then the question was whether one goes further with recalcitrant operators. The problem with that is that we are still in a free speech context and that would be a very heavy sanction and would be difficult to make proportionate.

Mr. Amrin Amin: I understand. I wish to touch on a point on free speech. Earlier, Facebook stated that one of its core values is to protect freedom of expression. As a professor of law, does Professor Woods believe that deliberately deceptive political advertisements paid for by politicians and the use of bots by foreign entities to influence an outcome, as we saw in the Irish abortion referendum, as well as in the US with alleged Russian interference, covered under the concept of freedom of expression? Is it not the case that these things harm our democracy?

Professor Lorna Woods: My response is based on the European context, which is what I know about. The speech probably does come under the scope of the guarantee to start with but that freedom of expression in a European context is not unlimited. It can be limited in the public interest-----

Mr. Amrin Amin: As with all rights, yes.

Professor Lorna Woods: ----- in a proportionate way. Speech that is deliberately lying or

false would have a very low value and so while political speech is normally highly protected, rules to minimise the impact of free speech-----

Mr. Amrin Amin: Is it the case that calling out a fire where there is none, outright lies such as the wrong election dates to mislead voters or Hilary Clinton's health, would not be protected?

Professor Lorna Woods: In principle, they would be protected but a state acting to limit that sort of speech in the public interest would like to be proportionate.

Chairman: We will move on to the United Kingdom.

Lord Puttnam: I may be able to help with Deputy Eamon Ryan's question earlier. Our analysis of the Queen's Speech and the notes to it, indicate the online harms Bill will reach Parliament but that it has been watered down quite significantly. It is not the same Bill to which most of us made submissions.

Mr. Huizenga referred to digital understanding, we could also call it digital literacy or many other names. In the UK's every attempt, we have been unable to find best practice. Many countries say they are doing various things but there does not seem to be a European agreement about best practice. Finland is at the top of the list, UK is in eighth place and Estonia is fourth. It has become quite clear to me that the Department for Education, and this is probably true in other countries, is not equipped to deliver what we are talking about. In the UK, the Department for Education sees this as part of computing lessons and rolls it under such lessons, when it clearly is not. What advice does Mr. Huizenga suggest and where would we go to to look for best practice?

Mr. Rogier Huizenga: I have no concrete advice on that. It is a very valid question and is something we see in other countries where because of the new ways of communicating, it fall between the cracks. We have heard this before. However, I cannot give precise advice on how some countries have been able to deal with it effectively. Maybe it is with the Finnish experience, as Lord Puttnam observed. We are aware that the digital literacy initiatives which have been developed in Finland had been appreciated everywhere. Maybe the committee's Finnish colleagues can elaborate.

Ms Áine Kerr: I am a member of the Council of Europe's committee of experts on quality journalism in the digital age and as part of its work, there has been a massive audit of news literacy projects globally. Its report should be published in coming weeks. It will include everything from NewsWise in London, which is part of *The Guardian*, to the Finland newspaper model and what is working and not working. Out of that we should see some best practices emerge.

Lord Puttnam: That is very helpful. We looked at NewsWise but scaling it up is quite tough.

Chairman: Professor Woods wanted to come back in.

Professor Lorna Woods: When people speak of education, there is a focus on the users but we might want to include our computer scientists and software engineers to actually think about not only the law and tick-boxing the GDPR but actually thinking of the ethics of what they are doing.

Lord Puttnam: Something that might be helpful to the committee is the evidence given to

our select committee by Baroness Onora O'Neill, who is a philosopher. Her laying out of the ethics of this issue and the ethics of free speech applies directly to Professor Woods's point. In Europe, we do not have first amendment rights. Ours is not binary. It is quite subtle. I sometimes feel that in Europe we get dragged into the same basket as first amendment issues and in a sense we have more space. That is an observation.

My last question is to Ms Kerr. Deputy Ryan, to an extent, asked it already about public service broadcasting, which is under pressure everywhere. What I find extraordinary, and we got this more of less right in the UK when I was growing up in the 1950s, is that an understanding of the subtleties and importance of public service broadcasting was entirely understood. It got badly beaten during the Thatcher years, and reconstructing the understanding that existed generally - it was not an imposed but a societal understanding - is extremely difficult. It possibly means levies and it definitely means a transfer of revenues from the major players to public service broadcasting of some sort, be it online or offline. Has Ms Kerr an observation on that?

Ms Áine Kerr: There is definitely an argument for a fairer playing space, particularly when it comes to advertising. As we know, the monopoly platforms are acquiring much of the new digital revenue. Is there an effort that can be made where we can create a fairer competitive space? It comes back to the point I tried to make earlier, that for public broadcasters or journalism in general, we have to get away from the attention economy to the intention economy. What I mean by that is that we are being tracked across the Internet. What does it look like for a public service broadcaster and others to give power back to people, to give them control of their experiences and, by doing that, for them to feel that experience with journalism? That is where the imperative is at in general for us, but it will take a level playing field and taxes and subsidies to ensure that from the ground up people understand that role.

That is why Lord Puttnam's media literacy question is important. We have to ingrain this from the get-go for people to understand why the institution of media is important. Critical thinking skills are important because, unfortunately, misinformation and disinformation are a part of our lives. They are part of the human condition. There will always be bad actors. They will get more sophisticated about how they go about their business. Much of the analysis from the United States suggests we will want to inoculate children from the age of 12 against misinformation so that they will seek out the public broadcaster and engage with it as a source of truth, fairness and accuracy.

Lord Puttnam: That is a good answer.

Chairman: I call Congressman Cicilline.

Mr. David Cicilline: I also concur with Lord Puttnam's comments about media literacy and best practice both in terms of our ability to make that available and real investment, at least in the United States, in civics education in order that people understand the implications of some of this. That is a critical step. We look forward to that report for some guidance.

Mr. Lovett, in his written testimony, referred to prohibiting the use of micro targeting for political ads. Will he explain why he believes that is a good recommendation?

Mr. Adrian Lovett: This has been covered already to some extent. We as the Web Foundation joined with the Mozilla Foundation and others in recent days to call for a temporary ban or moratorium on political advertising in the UK around the current general election. We did that not mainly because of the threat of clearly false information being put into the public domain.

A very bad example of that in recent days was a doctored television interview with one of the major UK party spokespeople, but everyone could see that and it was quickly exposed. We think it is right in the UK context to pause because of what is not seen and because of the degree of micro targeting. There has always been targeting in advertising and we have had that for centuries, but what is different now is the scale and speed at which that works and the opacity of it and the great difficulty we have in seeing the effect of it. We should recognise it is not a simple question, because while there may well be a place in some form for political advertising, properly regulated and fully transparent, there is not enough confidence at the moment that the unseen is not doing great harm. While that is the case we think it is important to step back from political advertising, but in the longer term what is required is a way to be found such that micro targeting is not applied in the case of political advertising because it is too important a context for that.

Mr. David Cicilline: During the community's last meeting, Peter Kent noted that dominant platforms may simply pull out of jurisdictions in the absence of harmonised regulations across our democracies. We are seeing this in real time with Google's threats to withdraw its Google news service in response to the European Union's copyright directive and its more recent decision to stop displaying news previews of articles in France to avoid complying with this law. What recommendations, if any, does Mr. Huizenga have for harmonising regulations internationally to avoid this kind of dynamic?

Mr. Rogier Huizenga: That is a very complex question because it cuts across many of the issues we are discussing. It is about seeing if there is a real willingness for countries to come together around a common norm. I could see that happening with regard to some issues. I mentioned hate speech, and there are quite a number of international standards in jurisprudence, but there are still many differences between countries, including at the European level, and different approaches are being followed. I do not see an immediate end of the tunnel with countries coming together with a unified approach and vision as to what harmful content, and even hate speech, should exactly look like. This is all the more reason for countries to make that extra effort to see if it is not possible after all to do just that. Ultimately, if tech companies can move their business around and simply disappear but continue with the same business model wherever they can, that is not a long-term solution.

Mr. David Cicilline: Mr. Lovett described a contract with the web which sounds exciting, consisting of nine principles and involving 87 directives, but I take it that essentially requires voluntary compliance with the large technology platforms. Has he thought about what would be the most effective way to operationalise that because, as we have seen, there is very little likelihood these technology platforms will regulate themselves or correct their own misbehaviour? They seem to be driven by a model that is about growth and revenue. Therefore, does it involve public shaming or is it intended jurisdictions would take these principles and directives and incorporate them in legislation, or what is his view on these issues?

Mr. Adrian Lovett: We try to recognise that, in such a broad challenge, different approaches are needed. For example, we think the GDPR standard will be pretty much reflected in the relevant parts of the contractual web clauses because it exists, is a good start and can be built on. The contract with the web does not try to offer an overall regulatory approach. It tries to acknowledge where there are relevant initiatives and mechanisms already in place. Beyond that, we believe in the power of transparency and the public spotlight not as an answer to everything but as an important element. The reason the human rights assessments I spoke about earlier would be important is that it would put information in the public domain. Companies would

be required to do that, we would then see that and those companies could be held to account. In some aspects of the contract for the web's scope, there would be regulatory and legislative means to do so. In other parts, it would be the within the power and ability of the public to scrutinise and see what companies are doing and to judge them accordingly, including where they take their business.

Mr. David Cicilline: I probably know the least about the duty of care Professor Woods described. What is the nature of the duty? Is it imposed on the platform? Can Professor Woods tell us a little bit about that?

Professor Lorna Woods: It is borrowed from our health and safety at work legislation and is an obligation on the platform to take steps to prevent against reasonably foreseeable harms. It is pushing it back to a company and essentially saying to do a proper risk assessment, identify what is happening with one's platform and the way one has designed one's services. Where there are downsides, companies should try to mitigate these. This is in the context of the service provided. One would look at how large the platform was and also at the sort of services offered. Live video streaming, I would say, is quite a high risk thing to do, as opposed to just text. If one is aiming a service at children, then one will want more safeguards than if one is aiming at adults. This allows a certain flexibility to the company to do things in the way they want to, but within a framework of having to do it, keeping an eye on this, not just doing a tick-box exercise but to keep monitoring. I am afraid that the time for self-regulation is over.

Mr. David Cicilline: I thank Professor Woods.

Chairman: I call Deputy Lawless to speak now.

Deputy James Lawless: Can I ask Mr. Lovett - although I am interested in all views on this - about another old chestnut which is the question of net neutrality, and how we enforce this? How do we aspire to it? This is dual-layered because even if we manage our service providers, and legislate that service providers cannot boost or block particular types or sources of content, social media platforms are themselves adopting a net bias, in that they are promoting sponsored contents and applying their own algorithms as to what bubbles to the top and what does not. Going back to Sir Tim Berners-Lee, Mr. Lovett eloquently described his original vision earlier on. The power of the web was that sort of randomness, where it was built on meritocracy and random discovery. That, in turn, drove content producers where indigenous content and citizen journalism could come about. Ms Kerr has talked about that as well today. That was the dream, the goal and the utopia of the web at the outset. That has been choked back in two ways. The net neutrality debate rages on. The platform is layered on top of that and is equally filtering material out. For some people Facebook, or Google to an extent, are the Internet. In this context, and with a view to the platforms and the kind of regulation we are discussing today, how do we best manage that? I do not know if we can turn back the clock, and maybe we do not want to completely turn the clock back, but there is a goal from the earlier days of the web that is worth preserving, which is the meritocracy model and that citizen journalism and openness to anyone to have their 15 minutes of fame on whatever channel it may be.

Mr. Adrian Lovett: We are still very focused on that fight for net neutrality, most particularly in the United States, where there was a great step forward, and now we are fighting to resecure that several years on; we have not given up on that fight.

On the broader question, it is true that we cannot turn back the clock. Tim Berners-Lee and others of those Internet pioneers would not want us to do that. Channelling some of the inspira-

tion and vision of those early days and applying it to the very different times we find ourselves in now, it may be time to think about a new connecting imperative. Perhaps this might help. I was talking a little while ago to one of the chief executive officers of one of the big airlines. I was asking him what his focus was. He was quite new in the job, six months in, and said obviously his was an airline company so the first priority is safety. He went on to talk about the things I thought he was going to talk about around the brand, staff relations, and so on. He got me thinking then about the aviation industry being a place where businesses make healthy profits and provide a service to customers but also where public safety is the first priority and where companies are required to co-operate with each other, as well as with regulators. There is zero-tolerance of mistakes and a significant degree of transparency. If we agree that the Internet can not only improve and enhance lives, upon which we all agree, but that it can also profoundly damage and - it is not too much of an overstatement - can cost lives, then surely the evidence is that we could agree that for companies on the web, the universally-accepted imperative must be public safety. That might be a new driver for how we organise all of this thinking for the next 30 years, quite different from the thinking that has prevailed for the past 30.

Chairman: I thank all of the witnesses.

We will suspend the meeting for our final session and we will resume at 4.30 p.m.

Sitting suspended at 4.06 p.m. and resumed at 4.30 p.m.

Session 5: Future Collaboration

Chairman: The fifth session of today's proceedings gives members an opportunity to discuss options for future collaboration. I asked members in advance to think about which organisations or mechanisms they would consider appropriate for working together to advance a cohesive multilateral agenda of regulation. This is our third international grand committee hearing. We have had social media companies before us. We often hear many of the same answers to our questions. Today's meeting has been very productive. We have heard expert views that have given us options for a path forward. It is clear that no international rule-making body is dealing with this issue in a coherent way. We need the rule of law to apply to social media when it comes to political interference, political advertising, online harm and fake news, but it is not there at the moment.

We will hold a press conference at 5.30 p.m. I want to open the meeting up to members before then. What is the overriding message that is coming forward? From my own point of view, I think the issue of targeted political advertising on social media has been recurring throughout all the hearings today. I will let those present think about our message for a moment. Maybe we could consider recommending a moratorium on micro-targeted political advertising until regulation is in place. I am not suggesting that there could not be political advertising online, but that the micro-targeted approach could be stalled temporarily. This is something the members might want to discuss. Perhaps we can all agree on this as an issue that could come out of today's deliberations.

There is another issue that I would like to open up to members. We might consider the taxation of social media companies to support public service broadcasting. There is real concern about journalism, factual information, factual news, combatting fake news and supporting public service media and public service broadcasting. We are looking at ways to support that.

Are members in agreement on coming together on these issues before the press conference later this afternoon?

Lord Puttnam: It might be helpful if one thing could be clarified. One of the real concerns in the UK, where an election campaign is just beginning, is that the micro targeting of individuals avoids the rules and regulations regarding constituency expenditure. I do not know whether that needs more explanation. National parties can spend X amount; constituencies are restricted to £15,000 each. If those individual voters are micro targeted, it does not count as part of the £15,000. In fact what has happened is that a coach and horses has been driven through a law that has existed for 100 years that did attempt to control electoral expenditure. It sounds like a small thing but actually it is a very big thing.

Chairman: Lord Puttnam feels that the micro targeting of political advertisements is a real issue in the UK.

Deputy Eamon Ryan: I agree. We have done very good work today and yesterday. It has been very informative. We set ourselves the ambitious target of answering where is the point for international collaboration. As the Chair says, there are myriad different possible points but none is immediately achievable.

To cite our experience in the referendum, which our Singaporean colleagues cited several times, this became an issue of concern and at the last minute the platforms withdrew from advertising because it was so contentious. It would be very useful if we, as a group representing several parliaments, came out with the sort of moratorium the Chair talks of because it would not just leave it to the platforms to make the decision. It would be one political voice in this space asking for that action to take place. As Lord Puttnam says, this is a fairly immediate issue in the UK. We have an election coming up in the spring and our Singaporean colleagues are on the same sort of timeline and the US presidential election is not very far away. If we could get broad agreement on such a moratorium, it would be very beneficial and it would prevent what happened in our case, when it happened by default without any political contribution. Our contribution would be useful and timely and may encourage the wider collaboration that is our overall aim. It is only one measure, it is interim and temporary, but it would not be insignificant.

Mr. Tom Packalén: It would be a problem if we ban micro-targeted advertising. There are many MPs and there is a huge difference between the US presidential election or elections in some small countries because the budgets are totally different. There is a big difference if somebody has a budget of €10,000 or €20,000 because with these kinds of resources they do not have enough resources to use TV or other media and need to be careful where they put their money. If we ban this, we could also do a lot of harm.

Mr. David Cicilline: There was a lot of testimony in this set of panels about the dangers of micro targeting but particularly in the dissemination of false information. It seems to me the harm is much less serious in micro targeting if it is accurate. The fact that it is one on one is not perfect because there is not that public discourse that is the business, but it is really egregious and harmful when it is false and is micro targeted because there is no public square. It would be strange for us to leave here and not say something about this publicly articulated policy of Facebook that says it will sell completely false advertisements for anyone who wants them and in whatever quantity they want. The really pernicious harm is the false declaration combined with the micro targeting. Maybe we can speak about the two together.

Chairman: Yes, in respect of falsehoods or where there is misinformation, that is very good

and very positive.

Mr. Milton Dick: We would support what the Congressman is saying. I do not have a problem if micro targeting happens and is about a factual issue or a local campaign or particularly in developing countries. It is when it deals with falsehoods or deliberately misleading information, and we have heard enough evidence today from the witnesses to say that is growing not only here in Europe but around the world. It would be important for us to act on the evidence we have been presented with today.

Lord Puttnam: If we are going to go down that route, and I am fine with that, what about anonymity and the fact that these advertisements are not tagged? We do not know who they have come from or what party they purport to be supporting, believe it or not. They can actually be not only malicious but also anonymous. Do we have a view on that?

Mr. David Cicilline: We have mentioned disclosure and transparency in the declaration. It states:

> All of our signatories leave here today having agreed to support or introduce legislation in their own parliaments to require disclosure and transparency of online political advertising while at the same time respecting free speech. There is an understanding that free speech also requires transparency of source and adherence to national laws.

We could refer to that.

Chairman: Does that cover the point for Lord Puttnam?

Lord Puttnam: Yes I just hope that people will understand what we mean by transparent.

Deputy James Lawless: I drafted that part of the principles. The thinking behind it is to include this ticker. How we do it is immaterial but it is to include a transparency or disclosure notice such that all of these political advertisements have a ticker tape running beside or under them where the user can click to see who brought it to them, who sponsored it, and who funded it. That gets around many of the issues we have been talking about. It promotes transparency in the political advertising but also in terms of micro targeting and when it is and is not permissible. It is always permissible if everybody else can see it. It is the dark hands that are hidden away behind micro targeting to see one particular micro sector of which nobody else has visibility. If there is transparency on it and disclosure behind that, and if we mandate that it must be available through a library or regular access, that takes away the dark web and dark advertising. I hope that paragraph summarises that.

Dr. Janil Puthucheary: I support the idea that we have this moratorium because in Singapore our statute against online falsehoods came into effect on 1 October and everything we have discussed in the past five minutes is entirely coherent with the position we have taken. We would be more than happy to support the suggestion. Under our legislative framework we have targeted the issue of falsity and as a result have also put into place codes of practice around advertising transparency and political advertising transparency. The legislation that came into force in Singapore on 1 October is entirely coherent and consistent with what has just been described around a moratorium on a false politically motivated micro-targeted advertising.

Mr. David Cicilline: That makes me think of one question that we might be asked in this context. If we start off by saying disclosure is an important value in terms of knowing where the advertisement came from, who paid for it, that is right. If we say micro targeting, when

coupled with false or erroneous misleading information, is particularly pernicious, the next question people will ask is whether, if it is not micro-targeted, we are okay with false political advertisements broadly being placed on these platforms on the Internet. That would be a fair question for a reporter to ask. My view of that would be no, we should not allow it. In fairness, however, people should be comfortable with that because it is the next obvious question. Micro targeting is very dangerous when it is false and everyone agrees that should not be permitted, but the next question is whether we support a ban on false political advertising, even if it is of a high standard but is demonstrably false and the platform is put on notice of it. That is the next obvious question, which I would support if I were asked that, but I would not just raise it with my colleagues here.

Dr. Janil Puthucheary: I would support that as well.

Deputy Eamon Ryan: I do not want to complicate things by throwing up questions but there is a very serious question, namely, what is political advertising. Whether it is a company such as Twitter, which takes a certain stance and has to answer that question, or whether someone takes a different view, I do not think we were able to answer that here. Some of the various collaborative measures we have seen and that have been presented to us have an urgent task in managing that. I do not think, however, we can definitively give an answer on that here this evening but it is right for us to call for the sort of moratorium, with the caveats we have presented, recognising that some of the details have to be worked out.

Chairman: Does anyone have anything to add on the themes or issues that have arisen?

Ms Nino Goguadze: I thank the committee for inviting me. It is the first committee meeting I have attended and it has been very interesting to look at the issues involved from the perspective of different countries. Georgia applies very high standards of freedom of expression and freedom of speech, although I would say we apply more American, rather than European, standards. Stakeholders in Georgia are very reluctant to regulate freedom of expression in this or that way, or the Internet and so on. This discussion has given me some ideas to take back home to discuss with my colleagues and political party representatives. It is a unique format. We have to work together to deal with the challenges all of our societies are facing.

Deputy James Lawless: On another output from the committee, it is important that when we leave here today we have some framework agreed among us for further follow-up actions. We had a discussion earlier with some of the panellists about this, but I am not sure if we reached any definitive conclusion. In the absence of an external framework, the grand committee retains the mantle and it falls on us as parliamentarians working collectively. I assume there will be another session, perhaps in a few months' time, wherever it takes place, but it would be useful if we could agree among ourselves to keep up the momentum and activity level. What is measured is managed and done. We have the principles, as part of which we are all making certain commitments. If we can begin to trace and track them in our own systems and our own way and then report back at the next session such that we are taking away some actions and can begin to translate words into doing, that will be a very positive outcome from this summit in the absence of an alternative international mechanism. I do not see anything else jumping out from our deliberations. We retain the mantle until such time as there is something preferable.

Deputy Eamon Ryan: We have been chatting to each other and the US Congressman has brought a huge bank of wisdom and work in this area. For our next meeting, it would be perfect if the Houses of Congress were able to host us. The meeting would have to build on the three we have held to date. Given the timeline of our meetings to date, it would be hugely positive if

the Houses of Congress were able to facilitate the holding of a further follow-up meeting.

Mr. David Cicilline: I appreciate the suggestion and would be very proud to host a meeting of the grand committee in Washington. Obviously, I will first have to check with a number of individuals as we have very specific rules for how House proceedings can be used in dealing with outside organisations. I am, however, flattered by the suggestion and, obviously, the Congress of the United States considers to be this very important work. I am happy to follow up on the suggestion made and explain that my colleagues at this meeting have urged that the United States be the location of the next meeting. I will do all I can to make it happen.

Chairman: We would be delighted if it could be held in the United States.

On the taxation of social media company profits to support public service broadcasting, again, this is an issue for members on which to agree, although how it would be worked out would be for others to decide. The aim is to support public service broadcasting to ensure we will have access to reputable, quality journalism and that we are working towards combating fake news.

Lord Puttnam: In the UK context, a word like "taxation" does not go down well, but if we were to use the word "levy", people would not be quite as neurotic.

Chairman: It would be a levy on social media companies, not citizens.

Lord Puttnam: It would be a levy on the social media companies' revenues.

Mr. Tom Packalén: If we are to have the taxation of social media companies, at the same time national broadcast companies should do fact checking in order that they could give something back.

Chairman: They would be giving back in the sense that we would be investing in quality journalism in public service broadcasting. We have heard at these hearings that they need to be supported. In their journalism and reporting they would be fact checking.

Mr. David Cicilline: One issue of concern in the United States is the Government funding what we would consider to be good journalism; there would there would be a lot of reaction. One of the most important responsibilities of good journalists is holding the government to account and exposing misconduct in government. Therefore, the notion of taxing a private entity for the purpose of generating revenue for the government to provide training or invest in good journalism would cause a lot of anxiety for historical reasons, but that is not to say public service announcements would not be fine. However, the question of whether we would actually want the government-----

Chairman: Could it be a regulator? Here, for example, we have the Broadcasting Authority of Ireland. It is OFCOM in the United Kingdom. Again, every country would have its own independent regulator.

Mr. Milton Dick: It would be very difficult. It is a great concept for a noble cause, but, in practical terms, I am not sure how it would work from country to country. I do not think I would be able to agree wholeheartedly with its implementation in the light of what the Congressman has said.

Chairman: That is okay. These are things at which we can look and explore in the future. It is about protecting journalism and dealing with fake news and how it happens. We do not

have to decide on the issue today.

Mr. David Cicilline: We can all agree that we have to figure out how to promote and incentivise good, reputable, trustworthy journalism without necessarily saying-----

Mr. Milton Dick: Without linking it with taxation.

Chairman: Or a levy.

Lord Puttnam: The Chairman's word "explore" covers it.

Chairman: Yes.

I thank Gina Long and all of the team who have worked so hard in the past few months on the co-ordination of this event. It was a big event for the Oireachtas. It is a really proud moment for us to host all of you here in Ireland. It has been wonderful. Your contributions have been very worthwhile and the meeting has been very informative. I believe we have some solutions and while there is an awful lot of work to get through and there is no one silver bullet, this has been a very worthwhile exercise.

I thank my two colleagues, Deputy James Lawless who is Vice Chairman of the committee and Deputy Eamon Ryan, who have worked closely with me, Ms Long and her team in co-ordinating this event in the past few months and bringing really good delegates here, as well as committee members. It has been incredible.

I thank the ushers and all of the team in Leinster House who have been working so hard behind the scenes, in particular Ms Cáit Hayes and her team. I am sorry; I should not name names because once I start to do so, I will leave somebody out. Nonetheless, there has been a huge team effort within Leinster House and we thank all those involved.

We will hold a press conference at 5.30 p.m. in committee room 2 and have dinner at 7.30 p.m. in the Members' dining room.

Dr. Janil Puthucheary: It behoves us to thank you, Chairman, for your able leadership of the committee. We thank you for taking us through what has been a very productive day.

Chairman: It was my pleasure. Thank you very much.

The joint committee adjourned at 5 p.m. until 3 p.m. on Tuesday, 12 November 2019.