SPECIAL COMMITTEE ON ARTIFICIAL INTELLIGENCE IN A DIGITAL AGE (AIDA)

Public Hearing on

"AI and the Future of Democracy" and

"Tech Developments and Regulatory Approaches regarding Disinformation"

Panel I: "AI and the Future of Democracy"
AIDA Special Committee

Lorena Jaume-Palasí, *Executive Director, Ethical Tech Society and co-founder, AlgorithmWatch*

Yannis Theocharis, *Chair of Digital Governance, Bavarian School of Public Policy, Technical University of Munich School of Governance*

Karen Kornbluh, *Senior Fellow and Director, Digital Innovation and Democracy Initiative, the German Marshall Fund of the United States*

Aza Raskin, *Co-founder, Center for Humane Technology and Earth Species Project*

*** * ***

Panel II: "Tech developments and regulatory approaches to disinformation"
INGE Special Committee

Rasmus Kleis Nielsen, *Professor of Political Communication and Director, Reuters Institute for the Study of Journalism, Oxford University*

Anna Bulakh, *Director at Disinfo.Tech and Co-Founder of Cappture.cc*

Alex Stamos, *Director of the Stanford Internet Observatory*

BRUSSELS

THURSDAY 15 APRIL 2021

1-002-0000

IN THE CHAIR: Dragoş Tudorache

Chair of the Special Committee on Artificial Intelligence in a Digital Age

(The hearing opened at 13.50)

Opening remarks

1-004-0000

Chair. – Good afternoon, dear colleagues, and welcome to this new hearing of AIDA. I will come very quickly to the topic and the order of business, but first we need to go through the usual housekeeping. We need to adopt the agenda and the minutes of the previous two meetings, the one on 1 March and 4 March and the one on 23 March. The minutes are available online and, unless there are any objections, I will consider both the minutes and the agenda adopted.

So, the subject of our hearing today is AI and the future of democracy. We are organising this hearing jointly with the Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE) and I would very much like to thank the Chair of this committee, Raphaël Glucksmann, and its members for agreeing to spend this afternoon with us and discuss topics which are clearly of interest to all of us.

The topic of how AI in new technologies impacts our democracies is perhaps the most important topic we have tackled so far. Technology is a tool. Artificial intelligence, beyond the hype, is a tool: a very sophisticated tool which can be used both for good and for evil. It can be used to consolidate a world in which individual freedoms and human rights are protected. A world in which the rule of law is respected and in which governance is a means for progress, economic prosperity and for furthering the common good. But it can also be used to prop up authoritarian regimes, to support dictators and their grip on power, to control, monitor, spy, rank, score and categorise citizens. Last but not least, it can be used against us and against our way of life. It can be used to destabilise our societies, democracies and electoral processes. It can be used to undermine and to manipulate, to misinform and to endanger our citizens, and this we must not allow.

At the dawn of the digital age, we must set in place rules worldwide which will ensure AI will not be used to undermine democracy. First, we need to look inward and ensure that we do not allow the use of AI for undemocratic practices, such as mass surveillance, mass social scoring by the State or discrimination in Europe. And second, we must reach out to the world's democracies and work together to build an alliance of digital democracies strong enough to set the rules, the standards, the red lines of our democratic digital future, and that we must do worldwide. And third, we need to ensure that we are protected by strengthening our cyber security, increasing our own citizens' resilience to fake news and disinformation through education and developing cutting-edge tools to counter cutting-edge attacks. And, last but not least, we need to understand that AI-powered attacks on democracy can be even more devastating than conventional attacks and we must treat them as such, which needs to be reflected in our defence policy, in our cooperation with and participation in NATO, in our transatlantic alliance and in our global strategy. AI is a means; democracy, progress and prosperity are our goals.

We will welcome today two separate panels, each of which will be followed by Q&A sessions between members and panellists, as always. I want to thank our guest speakers for their presence and participation and I would like to remind the speakers in all sessions that their initial presentation is limited to a maximum of ten minutes. As always, I will strictly enforce the rules so that we can all benefit from the speaking time we have. Also, as we have, by now, set our rules in practice, each Member will get a slot of two minutes to put their questions or make their remarks, and I would again kindly ask the Members to address their question to a specific member or members of the panel so that we can then do the follow-up. Then, for the panellists, I would kindly ask them to limit their responses to two minutes as well.

Panel I: "AI and the Future of Democracy" (AIDA Special Committee)

1-006-0000

President. – In the first panel, the one which I will host and moderate, we will hear from four distinguished speakers: Ms Lorena Jaume Palasí, Executive Director of the Ethical Tech Society and founder of AlgorithmWatch; Professor Dr Yannis Theocharis, Chair of Digital Governance at the Bavarian School of Public Policy, Technical University of Munich; Ambassador Karen Kornbluh, Director of the Digital Innovation and Democracy Initiative and Senior Fellow of the German Marshall Fund of the United States; and Aza Raskin, Co founder of the Center for Humane Technology and Earth Species Project.

Without further ado, I will now give the floor to the first panellist and I will also say that when the Members have finished asking their questions, I will give the floor to Ms Sandra Kalniete, INGE rapporteur, to address her questions to our experts. So, with that, I welcome again the panellists and thank them very much for their presence. Ms Palasí, you have the floor for ten minutes.

1-007-0000

Lorena Jaume-Palasí, *Executive Director, Ethical Tech Society and co-founder, AlgorithmWatch***.** – Chair, thank you very much for the invitation to speak. I feel very honoured. We are in times of a pandemic and in times of disruptions through new technologies. What this pandemic is showing us is that it is crucial to listen to science because science is bringing nuance and the necessary information to make informed politics. And it's showing that things are more complicated than it might look at first sight.

Let's take for instance the concept of colours. The science of physics will tell us that it has to do with how things reflect light. The science of biology will tell us that it has also to do with our biology so that insects are able to see more colours than human beings, whereas dogs are only able to see between the range of black and white and grey and nothing more than that. But also social sciences can tell us about the cultural dimension of something like colours. So that for instance cultures like the Japanese, that only have one word to both name the colour blue and green, are unable to make a differentiation between those two colours. For them, for instance, traffic lights are red and blue/green.

Now what science proves with that example that I'm bringing is that things are more contra-intuitive than they look at first sight. What seems logical is not always scientifically validated. So when it comes to the future of democracy and new technologies, what science is telling us is that technologies, as was stated before, are under-determined. They need first values that guide their implementation and conceptualisation and those values are not technology-related. Technology follows societal values either explicitly or implicitly.

So regarding the future of democracies, and particularly public opinion and the democratic processes, science says that public opinion is the counterpart of public power. This means that public power cannot interfere, it can only provide the framework to make sure that there is a plurality of opinions, that this is possible. So it is crucial, as the European democracy action plan states, to both make sure that political advertisement campaigns online or in the digital space are equally regulated, and here implementation will be key, because it is not a dichotomical relationship between the online and the offline. We see that there is a very organic relationship between both what we do online and what we do offline. And for this, regulation will need to make sure that it is coherent and consistent with what is already out there in regulation that is taking place in the, so to say, offline world.

The same goes for media plurality. I applaud the fact that there is a new specific focus on making sure that media plurality is also diverse and that special protections for marginalised journalistic groups are being taken into the focus of attention; for women, for journalists from different ethnicities, this is going to be crucial. However there I would speak a word of caution when it comes to the concept of disinformation because democracies, the drivers of democracies, like science, is dissent. It's not truth, it's not facts, it's not rationality.

Let's remember Holocaust survivor and Jewish philosopher Hannah Arendt, how she argued about the cruelty of purely rational societies. Public opinion needs to have a space for emotions and for other things than rationality. It needs a space for empathy and precisely in the point of disinformation we see that it is not about not knowing the facts, but we see that the narratives of disinformation are narratives that appeal to emotionality, that appeal to affiliation to specific political positions.

So quite contra-intuitively what science is showing us precisely in this field is that confronting *(inaudible)* with the facts might even radicalise them more because they feel that they are being put in a position where they have to express their loyal *(inaudible)* narrative. So when it comes to the future of democracies, one of the crucial points that we will need as a value to make sure that the technologies that are being developed are guided by that value, is both the possibility of having dissent through those technologies, but in such a way that – and that's one of the crucial elements of democracies, the legitimacy of a democracy depends on its degree of inclusion, its capability for balancing societal asymmetries, which is the basics of inclusion and making societies less discriminatory and unfair.

So the future of those technologies will need both to make this dissent possible but make sure that this dissent is performed in such a way that inclusion is key, and that marginalised voices are put at the centre and not on the periphery of the conversations.

We will also need once again, as I stated at the start, to listen to science and here I think that many of the tools that we have already been applying not only in the private sector, but also even within the boundaries of the European Union, need to have a revision regarding their scientific soundness. And we see that there are new technologies, such as biometrics, that are founded in non-scientific and non-ethical theories that, as a political entity that wants a high degree of legitimacy, must be questioned.

1-008-0000

Yannis Theocharis, *Chair of Digital Governance, Bavarian School of Public Policy, Technical University of Munich School of Governance***.** – Hello and good afternoon. I hope you can hear me well. I would like to thank the Committee for inviting me to this public hearing. I'm very honoured to be here.

My intervention is based on my and my colleague's research and is centred on social media environment's potential for democratic participation, but also the challenges emerging from it and the role of AI, especially machine learning, as both a problem and a solution to those challenges.

Digital technologies have opened up a new and important pathway to political participation via the use of social media. I'm talking about participation such as posting political content online for hundreds of others to see, or finding like-minded others online to organise a civic initiative. In the last few years, this participation has given rise to movements that brought sexual harassment and police brutality, among many other issues, to the top of the agenda through a new type of hashtag activism.

This is not a marginal activity I'm talking about; that's just for those politically interested. As you can see in this graph, in 24 European countries, social media participation is more popular that many traditional political activities, such as working for parties or demonstrating.

Why is this important? It is important because social media have brought many new voices to the political arena. Political participation has been traditionally stratified across socio-demographic characteristics, with those older, male, more highly educated and with higher-than-average income being most likely to take part in politics. Social media participation is actually changing this.

Social media allows regular citizens to gain direct access to their representatives, be listened to, and sometimes even shape the agenda. In the tweet you see British Labour politician Jess Phillips and German CSU politician Dorothee Bär give voice to random followers by quoting them in their tweets and directly engaging with them. This is a remarkable opportunity to bring citizens and representatives closer to each other and repair a long-strained relationship. But this interaction comes with a big challenge.

The challenge I'm talking about here is harmful speech, which is now rampant on platforms and where politicians are often at the receiving end. Here's what we know.

About 35% of MPs in many countries want to initiate discussion with citizens, and actually many more do so every day. But what our analysis of 10 million tweets sent to MEPs from Spain, Greece, Germany, the UK, and to Congress members of the United States, shows is that the more politicians engage (the X-axis in the left panel), the more abuse they receive (the Y-axis in the left panel). Reaching out to voters directly via social media generates higher levels of incivility than simply broadcasting.

Who is targeted? Politicians at the edges of the ideological spectrum, popular politicians, male politicians. Female politicians are more likely to be harassed if they are popular, but when they are harassed, female politicians are subjected to a different and more harmful type of abuse than men. Abuse in the case of so many politicians tries to demobilise them as a social group, and it is not focused on policy-related features but rather on references to their personal qualities, such as the looks, sexual identity, and morality.

What are the consequences? Well, first of all, everybody gets abuse – no matter whether it is a man or a woman, a conservative, a social democrat. I would like to argue that this is not part of the game of being a politician but a democratic problem, because it wastes the platforms' interactive potential that can genuinely enhance democracy; it impoverishes public discourse; it marginalises politicians with certain characteristics; and it even forces them out of politics.

This problem stresses both the challenges and opportunities of AI use in digital platforms today. It is actually in many ways both the problem and the solution. On the one hand, platforms do not do enough to solve these problems. On the other hand, dealing with these problems from an AI perspective is difficult, and it is not always clear what should be done. Why is that? Well, let me focus on two problems.

The first problem is that, even though incivility and hate speech – the term that governments define in their criminal codes, and platforms in the community guidelines – have been hotly debated by academics, legal experts, and policymakers, there is no single agreed-upon definition online or offline.

This lack of consensus has consequences for AI, because it translates to lack of consensus on what is the most effective way to deploy AI to detect hate speech across diverse platforms. The majority of AI-based approaches to identifying hate speech begin with a binary classification which identifies content as hate speech or not. Such methods have varying degrees of success and many problems.

Facebook's AI team, which develops machine-learning methods for harmful speech, shows very nicely how hate speech can be multi-modal. At the image on the left, not only the text is unlikely to be classified as uncivil by an AI algorithm, but things become even more complicated when it is combined with the image, where the statement takes another meaning. This subtlety is extremely difficult for a non-human to get right, as it is saying that a woman should stay at home and wash dishes rather than do politics.

It gets even more difficult when it comes to disguised hate speech. As you can see in the example at the right panel, hate groups have several ways to refer in a demeaning or racist way to ethnic groups.

Establishing clear and consistent definitions of hate speech among everyone concerned with the governance of online spaces is tightly connected to how AI can help us surpass this problem.

The second problem has to do with the fact that developing AI methods to tackle incivility comes against the platforms' business models. Social media companies have been studying hate speech and extremism-related issues since at least 2016, and Facebook, for example, found back then that their algorithms were actually promoting hate and extremist groups to its users through various features. Is it surprising that their automated features were promoting this content? Actually, it's not at all. Why? Let me explain.

Back in 2017 in a New York Times article, legal scholar Tim Wu propose what I would like to call the 'Trump circus theory'. He wrote that, while traditionally, politicians have measured success or failure by public approval and achievement of political goals, Trump was interested in a different metric: attention. And while Trump may have preferred winning to losing, he still kept winning by losing, because what mattered was a contest: the creation of a spectacle that creates controversy, dominates headlines, and grabs audiences.

We tested the Trump circus theory with an experiment in which we expose people to tweets by politicians. Some participants saw the tweets without comments, others with civil comments, and others with uncivil comments. When asked to tell us what emotions they felt after seeing each, we found that incivility did not cause anger, sadness or disgust, but rather enthusiasm. Following up, we found that people were significantly more likely to follow those spreading divisiveness and incivility than those whose tweets were normal.

This goes to the heart of the problem. Content that is enraging and titillating is great for engagement, and as it happens, social media firms' AI models that maximise engagement – and therefore profit and growth – not only do not filter out extremism, controversy, divisiveness, and incivility but actually favour them: a very problematic aspect from a democratic point of view.

But AI can play an important part in the solution here. AI-powered content moderation methods are used to automatically detect harmful content and ban users, and research has shown that in certain platforms this reduces incivility up to 80%.

But we know less about how these bans are actually implemented in practice. We cross over to difficult aspects pertaining to freedom of speech and censorship and, of course, there are the challenges with classification I mentioned earlier.

So here are two other strategies of using smartly AI to combat incivility on social media and which platforms can be encouraged to implement at a greater scale to create a safer and more open digital space: automated counterspeech and nudging – both methods that avoid some of the thorny aspects related to censorship.

Here’s an example of counterspeech. In an experiment, Kevin Munger programmed bots to automatically sanction individuals who racially harassed uses of colour on Twitter. He found that if users were sanctioned by a high-follower white male, it significantly reduced their use of racist slurs for at least two months.

Such AI methods, which had been used by others and have been proven to work really well, could be deployed at a greater scale. With more advanced AI methods, social media firms can also simulate how much counterspeech is necessary to drown out hate speech – which should be feasible, given that this is still a behaviour practised by a minority of users.

Automated nudging approaches rely on AI to detect harmful content and warn users prior to posting. Think of it as being warned as to whether you really want to post that angry message you’re about to post with a reminder that the language you’re about to use might result in harming others. Twitter is experimenting with this type of methods, but they have not rolled them out yet.

To conclude, social media have an incredible potential to enrich democracy through new forms of political participation, but that potential comes with serious democratic challenges too. AI is often part of those challenges, but most importantly, it can also be the solution, and in fact, novel, realistic solutions exist and can be deployed at large scale with much effectiveness.

1-009-0000

Karen Kornbluh, *Senior Fellow and Director, Digital Innovation and Democracy Initiative, the German Marshall Fund of the United States*. – Hello, thank you for including me in this important discussion. I’ve worked on the internet policy since the original policy framework that governs the internet today was developed in the mid-1990s. That was a time when digital technology appeared to be designed to advance democracy: it would bring decentralisation and disintermediation and provide voice to the voiceless and power to the powerless. And while it is true that the internet has unleashed great innovation, social movements and expression, at the same time we have seen the re-centralisation of power over information distribution and the loss that is entailed in the disintermediation of important institutions, notably the press and political parties.

Our offline worlds moved online, but our offline norms and laws, developed over years to protect democracy, were not updated. The January 6 insurrection at the US Capitol was the culmination of a longer siege of the information ecosystem. Recently, US FBI Director Christopher Wray confirmed that social media plays a role in disseminating the messaging of domestic violent extremists in the United States. Without guard rails, platforms lack the incentives to correct what amount to design defects that allow bad actors to hide their identities, deploy manipulative techniques such as deep fakes, or target misinformation-susceptible users using sentiment analysis, based on the platforms that store the data.

In our programme, we have found that a blatantly false story, such as the one in March that frozen windmills were responsible for crashing the Texas energy grid in March (in other words it was renewable energy, not the consequences of deregulation) – that this story, this conspiracy theory, travelled through an existing pipeline of deceptive outlets that had built-in audiences, networks of pages to promote them, fake accounts, willing volunteers and high-profile influencers that then transmitted to groups and users’ news feeds.

Social media artificial intelligence tuned to keep users on line then amplifies salacious content like this until it goes viral. After only a few days in the Texas case, these lies had swamped the news cycle nationally, distorting the evidence and forcing others to respond. The outlets involved are repeat offenders. We see them used again and again, responsible for a great deal of promotion of conspiracy theories but similarly with the networks of pages.

Information critical to democracy doesn't stand a chance against the motivated disinformation propelled by the power of these platforms and algorithms. It's no wonder we found, for example, that one single online network of coordinated pages that was promoting stories from health misinformation outlets had more interactions than the World Health Organization and the United States Centers for Disease Control combined. The platforms attempt to mitigate with after-the-fact content matter of moderation, referred to as whack-a-mole. It's no match for the machine. Flagrant misinformation is taken down only after it has gone viral, sometimes shared by millions of users, and the damage is done.

We have proposed a number of steps that one could take to build information resilience in support of democracy, and these steps would protect free expression. I'll quickly go over them.

These include enforcing seriously the basic rights and protections that operate in the offline world for the online world. In the US these include consumer protections against deep fakes and dark patterns, campaign rules for transparency, targeted harassment rules and civil fundamental rights protections. To address legal speech – and remember, in the US there are no laws against hate speech – a code of conduct would slow the spread of disinformation while it is checked against terms of service.

We propose, for example, that platforms use a circuit breaker, like the New York Stock Exchange uses, to prevent panics associated with market volatility. The code would also provide for transparency, but it must be done in a way that users can understand and take advantage of. GMF Senior Fellow Ellen Goodman, working with researchers at the University of Amsterdam, found that many labels currently used or even nudges are ineffective. More research is needed to determine the kinds of labelling and transparency that are effective.

We also agree that civic infrastructure must be boosted – trustworthy sources on important topics such as public health, climate science, election information – through funding and through preferences online. And then, of course, there is enforcement. In addition to domestic accountability measures of the sort proposed by the DSA, democracies should create a mechanism at the international level to monitor and provide transparency about compliance with terms of service and eventually domestic codes, as those are adopted and evolved for even greater impact.

And I'll just quickly move on to talk about other AI applications that similarly take advantage of a sort of a regulatory arbitrage – the same kind that we see in disinformation – and they create environments where algorithms promote anti-democratic actions. Similarly, laws and norms developed over time to protect social goals and protect individual rights must be updated to avoid undermining other protections. For example, AI poses broader challenges beyond disinformation to civil and human rights when it is used in cases such as identifying individuals moving in public places, remote biometric identification systems and, as was discussed, social credit scores.

The EU AI proposal apparently suggests banning these uses, although identification, for example, may be appropriate with sufficient safeguards for compelling social goals. The use of AI predictive analytics in areas the EU calls high risk, like those used for policing and criminal justice, employment, credit, housing and education, also pose threats to democracy. The EU apparently will propose assessing these *a priority* for explainability and bias. In the US, our assessment of civil rights violations includes disparate impact analysis, which is after the fact, to be able to measure invidious discrimination based upon practical effects after the fact for these sectors.

But in either case there are profound operational challenges in enforcing guard rails when AI is present. These include, first and foremost, capacity, training and explainability, to ensure that developers and workers at the point of use, and at the government level, can provide oversight. Because these processes are so complex, it will be essential to develop standards that are practical to clarify how to assign liability, and it will be essential to determine metrics to measure impact. Again, international monitoring can be very helpful in terms of providing transparency and learning about best practices.

Taking advantage of the enormous opportunities of the AI revolution while mitigating its risks requires new governance, institutions and mechanisms. This is not easy at a time when democracy is under assault, in part due to the failure I described above to respond to the last technological revolution. These mechanisms should be domestic but, importantly, also transnational, if we're to meet the rise of authoritarian uses of technology with a values-based alternative model.

By working together as democracies, we can take advantage of the efficiencies that these technologies can provide while affirming the importance of civil and fundamental rights. This is with regard not only to ensuring appropriate use of technologies but also to reinvigorate our democracies for the 21st century.

1-010-0000

Aza Raskin, *Co-founder, Center for Humane Technology and Earth Species Project*. – I wanted to thank the committee for having me here and for this important conversation. So I wanted to start by saying we have yet to invent a technology that is democracy built to survive in perpetuity. There is nothing that is set in stone or inevitable about forms of governments' *(inaudible)* and keeping them requires incredible vigilance.

The way that a society is wired up as new technologies emerge drastically changes the kind of governance that they can have. It used to be, for instance, that monarchies and centralised forms of authority were the most efficient for running a nation state, up until we get Gutenberg, the printing press, and as that distributes throughout the world, pushing information to the edges becomes a more efficient form of governance and democracies at the level of nations becomes possible. So, new information technologies fundamentally rewire societies and that changes the kinds of governance which are possible. So, as we get new forms of information technologies we should expect to see similar kinds of phase shifts.

I think now it's important to zoom out and say social media, but more generally information disintermediation technologies, so that includes Google and YouTube, the way we see information and the way we as societies place our attention, is acting like a brain implant in our societies, and – at least here in the US, it's Twitter – what does it do? It wires up its imaginary brain.

Imagine a brain implant that we are testing in real time and it's rewiring up every neuron to every other neuron. It's sort of the Twitter or Facebook broadcast model, the YouTube broadcast model, and what do we expect to get except epileptic seizure when every part of the brain is broadcasting at maximum yell to every other part of the brain. When you compare that to, say, totalitarian dictatorships or authoritarian regimes, as the world looks to see which model of governance is most effective.

In the US, we are writhing in a sort of epileptic seizure, especially after 6 January, unable to make decisions and come together because we cannot agree on that which is true. We are constantly mis-seeing the other side, versus, say, a China form of governance, which feels from the outside like it is a unifying way of moving a large group of people, together, of course, without upholding the values that we care so much about in democracy.

So, if the rate at which one brain implant is causing the brain to be able to observe, orient, decide and act in relation to reality, and the other is causing it to be unable to observe, orient, decide and act at the clock rate which the new problems of the 21st century demand, the group of people that cooperates better together wins. That is one of the core problems of democracy and AI in the 21st century. How do we wire up a society so that we can uphold the values of expression, generativity, of human dignity and, at the same time, have our systems outcompete totalitarian digital authoritarianism in the 21st century?

As we've moved from the digital to the physical we've lost a lot of the protections of the physical realm, and actually I want to zoom out once again to an E. O. Wilson quote, the father of socio-biology, who said the problem we face as humanity is that we have Palaeolithic emotions that are not changing, medieval institutions that cannot think at the clock rate of modern technology and accelerating godlike technology, and that unless we have the equivalent form of godlike wisdom, these technologies will tear us apart.

It's as if we are, as an intelligent species, pointing the telescope of our own intelligence back at ourselves, opening up our metaphorical skulls and figuring out how to poke and prod us to get us to do things. We are reverse engineering how we work and, of course, that started with sociology and anthropology, psychology, magicians, conmen, but now it's happening on an exponentiated scale.

In 2019, there was a fascinating study where researchers at Harvard put a monkey into a chair, implanted electrodes in its brain, into its visual cortex, pointed the monkey at an AI system generating images and then had the AI generate image after image after image until they could get those neurons to fire at a rate that no normal image could. And what images emerged that could make these neurons fire? Well, researchers saw images that included their own faces in the mass emerging from this sort of miasma, they saw cages, they saw the faces of other monkeys. It was the first time that we as humans had learned how to extract memory directly from matter. And note it could happen without the consent of the monkey.

I think this is a very powerful example because it shows the kind of asymmetric power that our technology is beginning to wield over us, that we can generate images or text or stimuli that are hyper-normal stimuli to human beings, that get us angry, that get us emotional, that find the soft animal underbelly of our minds and then exploits it for profit.

Modern democracy is based on the principle of the voter is always right, the customer knows best, trust your gut, trust your heart, trust your feelings. But these AI technologies are fundamentally undermining our ability to trust our gut, trust our feelings, trust our minds.
Let me give an example of the kind of persuasive power that AI has. Right now, there's a technology called style transfer. It lets you point AI at any image, say a picture of Picasso and it learns the style which is Picasso and then applies it immediately to other images. It's sort of fun, you apply it to a portrait of yourself and all of a sudden you have your face painted by Chagall, what's the harm in that?

Well, the same technology is now being applied to text. So it's no longer style transfer for images, it's style transfer for text, where you could point an AI at, say, things that you've written. Google could do this, for instance, point AI at all the things that you've ever written and learn to write in the style which is uniquely you, and in fact they already do this. When you hit tab inside of Gmail, it autocompletes in a voice which is starting to approach yours. But they could also train it on all the emails you’ve ever responded quickly to or positively to, to learn the style which is uniquely persuasive to you, then turn around and sell that to anyone who wants to target ads to you.

And the interesting thing here is, where have they broken privacy? There are no laws to protect us. They haven’t sold your data, all they’ve done is use your data to make a model of you which can begin to out-predict the things you’re going to do before you do them. Instead of calling it data, I think we should call it ‘history of decisions’ because then it’s clear that, as Google and Facebook and Twitter and all these social platforms collect your entire history of decisions, correlate it with your history of decisions of where you move as an individual, correlated with your history of decisions of purchases, correlated with your history of decisions of usage and what content you engage in, it makes it very clear that it’s easy to predict what your decisions are going to be in the future and where to intervene to change those decisions.

And in fact, Google, Facebook, Twitter know more about you than, say, your doctors, lawyers and therapists combined. A list of the kinds of things that can be predicted are: with whom you sleep, whether you’re having an affair, what drugs you do, if you’re depressed, your sexual orientation, often known before you know it, your disease states, whether you’ve lost your job, whether you’re thinking about leaving your job. These are just a couple of the kinds of pieces of information that can be computed about you.

This gives a kind of asymmetric power and this asymmetric power, we have it in typical relationships, that of a therapist... In the US, it is not lawful for a therapist to date their client, why? Because, in order for them to give their services to the client, the client has to give up information about themselves that could be used to exploit them and hence the therapist must act in the user’s best interest with a fiduciary or duty of care.

For the first intervention, I feel like I’ve talked too long now. I think one of the most hopeful things is... *(inaudible)* and More in Common did a set of research on perception gaps; the inability for us to perceive the other side, whatever that other side is, accurately. And there are two crises happening at once: there is the truth crisis and there is the perception crisis – we cannot see what the other side believes. So, if instead of optimising to try to get rid of disinformation polarising content we instead tried to optimise for content which lets us perceive the other side accurately, I think there is an incredible power for that to ameliorate disinformation, polarisation and hyper polarisation content.

1-011-0000

Chair. – Thank you very much. Four very interesting and thought-provoking presentations. I’m sure it gives enough for our colleagues to direct their questions and to shape their thoughts and remarks. We have a little bit less than 45 minutes, which means that we’ll have to stick thoroughly to the slots allocated. So I will now open the floor for the first Member speaking on behalf of EPP, Anna-Michelle Asimakopoulou, you have the floor for two minutes.

1-012-0000

Anna-Michelle Asimakopoulou (PPE). – Thank you Chair, my question is for the Ambassador. As artificial intelligence and machine learning has become a more and more important component of the digital landscape, different issues have come into focus, whether it’s perpetuation and amplification of bias, the need for transparency, the need for interpretability and auditability of algorithms, and more broadly the need for norms and regulations for these intelligent technologies.

Especially after Cambridge Analytica and after the elections in the US and the UK, I think we realised how much social media platforms could be used to weaponise information at a scale that is so large that it may undermine the foundations of our democracy. So we’re now starting to see all this synthetic data, as you said – photos, videos, audio files – manipulated by AI in ways that are very hard to detect and this is becoming more and more commonplace, along with deep-fake technology that can essentially create any kind of reality that the creator desires.

I note that a number of initiatives have been implemented in Europe against fake news, as you know, and disinformation, like the code of practice on disinformation in the European Digital Media Observatory, and for those of us who have seen the advanced copy that has come to light of the DSI proposal, it actually bans AI systems designed or used in a manner that manipulates human behaviour, opinions or decisions through choice, architectures or other elements of user interfaces, causing a person to behave, form an opinion or take a decision to their detriment, and also it provides that users of AI systems who use the same to generate or manipulate image, be it audio or video content, that appreciably resembles existing persons, shall disclose that the content has been artificially created and manipulated.

So, in light of the fact that as AI develops very fast and the new possibilities arising from AI-related matters are not at all predictable, I think that we'll all agree that whatever we regulate is just not going to be enough. So, and based on your extensive experience, I would ask if you would propose concrete complementary actions that can be put in place to prevent using AI technology to manipulate users and citizens, to distort democratic debate, notably in relation to disinformation, and to ensure that there is democratic oversight?

1-013-0000

Karen Kornbluh, *Senior Fellow and Director, Digital Innovation and Democracy Initiative, the German Marshall Fund of the United States***.** – Thank you for that very insightful question, which has raised so many great issues. This idea of manipulation of users through the use of their data for them to act against their own self-interest – we've already seen with dark patterns where subverting even the GDPR by making it complicated for you to exercise the options that the regulation gives you, as it seems very easy to surrender your data and very difficult to say no and yet gain access to the service.

So I agree with you that these are very, very important. What we think of as design problems, that the platforms have embedded design features, whether it's in terms of user interface or broader design factors that manipulate users or allow the manipulation of users by bad actors that amplify the negative. So what really needs to happen – instead of, as you say, it's very difficult to correct after the fact – is to change the incentives, to ensure that there is clarity and that the kind of behaviour that we're talking about will be punished in the end and that repeat offenders are not allowed to continue to act in this way.

And so we agree that we need to update our laws. Some of the things that you've talked about should fall under the consumer protection rubric in the United States, and so it's really important that we do that. But I think that some of these other co-regulatory schemes that have been discussed in the context of the DSA certainly are really important to evaluate. So we've talked about a code of conduct in the US as well and I know that there's going to be an update of the code of conduct around disinformation in Europe. Those kinds of codes can elevate increasing best practices. They can require that the platforms take risk mitigation steps.

But that's going to be an ongoing process. It's going to require a great deal of transparency: researchers will need to study it, but they'll have to get access to the data and agencies that provide oversight will need to have capacity and training to provide oversight as well. It's very complicated, as you said: very difficult to get governance of these incredibly complicated technologies right and I think we must address it on an international basis as well. These companies are international; the technologies do not know borders and we should be working together to elevate best practices and to provide real transparency that's usable by watchdogs but also by users.

1-014-0000

Miapetra Kumpula-Natri (S&D). – Thank you Chair, and thank you for the very good insights from all the panellists we had here. I'm very happy to have that.

I want to try to find your answers to go deeper on what can we do if we do have a good legislation on the puzzles. But the main driver for the platforms is making business, and making business is based on the structure that more hours we stay there, the more we click. And we know, as also Ruskin Azar said, that emotions are guiding us. So if it's inbuilt in the system that the more you click, the more you watch, and the more anger you get – or love – but it might be often the negative feelings that really create the diversities, and it doesn't bring us together but increases the polarisation. It's not that we come together and sit here with different ideologies or different opinions, and then we have the democracy to sort things out, but these are emphasising the polarisation in the end. And is there something we can do on that one?

My second part of the question was about the 'deep fake' and how much we can do. It's quite nice to see Putin riding a bear, and then you can think about whether it was a manipulation of the picture or the bear, but then having him saying something now with his voice, his picture about Ukraine, and we don't know if it's true or not. If that will be the very short future, then we are not safe either.

So I pose this question to Theocharis from the Munich School of Governance. He touched a little bit on this governance or the social media. I do see also that it gave the power for the silent and small, and not only the centralised. Maybe if there is time, also Lorena from the AlgorithmWatch can answer.

1-015-0000

Yannis Theocharis, *Chair of Digital Governance, Bavarian School of Public Policy, Technical University of Munich School of Governance***.** – I have to say that I'm not entirely clear what the question was in what you said. Shall I stick to the idea of how do we deal with the fact that these outcomes are actually part of how these companies work, so part of their business models?

I would say that, if that is the question, this is a very difficult question. It has to do with regulation, both at the international level and at the level of the companies, of course. But I do not see any other way, other than long negotiations, research-driven negotiations with those companies with regards to what works and what does not; what is harmful and what is not harmful.

I know that many of the social media companies that I actually referred to have policy strategists who speak with the research teams and try to figure out what is harmful and not harmful, and how to regulate it, how to kick it out.

Actually, the process of training a machine to recognise harmful content involves testing and retesting, and considering conflicting normative ideas, if you like. On the one hand, we have a model which is *[inaudible]* good for the company, if you like, and on the other hand, we have harmful content. So how do we deal with this? I think this can only be resolved with long, rather tough negotiations with social media companies.

1-016-0000

Lorena Jaume-Palasí, *Executive Director, Ethical Tech Society and co-founder, AlgorithmWatch***.** – It's indeed a complicated question because of course polarisation is a very complex social phenomenon – so it's multifactorial. So of course this digital factor, of social media, plays a role. However, we must understand that the degree of permeation of social media in our European Union societies is not that deep: it's only 8% of people in France on Twitter; it's only 5% of people in Germany on Twitter; 7.5% in Spain. So we're talking about a minority here and we should not make the mistake of thinking that this is all of society. But of course this plays a factor.

However, there are other factors that have to do with the socio-economic situation in our different countries and we are right now, of course, in the middle of a pandemic so that sort of crystallises many other immanent, already existing asymmetries in society that can be channelised through social media on the one side, but also offset, and we see there is a clear correlation between a massive amount of physical protests on the one side, but also on social media. But again, it’s 5% in some countries represented in social media.

So, on the other side, I think it’s important, just two points: to make a difference between polarisation and radicalisation. Polarisation in a society, in democratic societies, happens often, and it’s not problematic so long as there are balancing measures, and there is more than only public opinion control. I think we need to be careful when it comes to public opinion control. I think it’s important to reinforce press and plurality of press. This is what really has worked well, history tells us, in democratic societies. So that would be my pledge, *(inaudible)* deep fakes.

1-017-0000

Karen Melchior (Renew). – Thank you very much to the panellists for your interventions, it’s been a pleasure to listen to you. However, your interventions have further convinced me that AI is not what will save our democracy, because AI with bad intentions cannot be dealt with by more AI.

I had the pleasure to be on a panel with Lorena Jaume-Palasí on emerging technologies beyond AI a few weeks ago, and what she said stayed with me: you cannot regulate a forest by regulating each tree. We need to make sure that ethics is more than just a popular buzzword but an actual competence for AI developers and that it’s taken into account by the platforms.

So how do we policy workers, politicians, prepare for creating political solutions that are different than just an illusion of technology as a silver bullet? As Professor Yannis Theocharis’ research shows, tech platforms are the ones moderating the debate online. But the AI is not encouraging listening and learning, but placing us in a cloud of shock and rage and disbelief. This is not beneficial for democratic dialogue, where we need to listen, reflect and even admit mistakes, not something that gives us a boost of endorphins.

The lack of understanding of the Trump circus effect by traditional media further aggravates this. So how do we as regulators make sure that ethics and democracy is taken into consideration? I truly believe that dealing with the structures and mechanisms with the platforms is the way forward, because we need to make sure that the risks to society and democracy are mitigated before new features go live, because platforms need to stop to just move back and break things.

So my question is for the Ambassador: how do we make sure that we have regulation, not just in Europe but also in the US, in the regions that want democracy to be built into the technology, that we fight such things as dark patterns and illicit nudging made by the platforms?

1-018-0000

Karen Kornbluh, *Senior Fellow and Director, Digital Innovation and Democracy Initiative, the German Marshall Fund of the United States***.** –I think the issue of ethics is very nuanced and complicated. We can have better training of the engineers, but until there are real guard rails it’ll be very difficult to tell them what they should and shouldn’t do in a given situation. And when we look at other kinds of risks, there usually are such guard rails, either in terms of norms – let’s say in accounting – or laws about how they should operate and whether they will be punished. And these kinds of guard rails can also change the incentives for the employers of these employees who are learning about ethics.

So I think ethics is very important, but it must be informed with some public acknowledgment in terms of norms and laws about what the guard rails are and what the risks of misbehaving are. And when I say norms in addition to laws, I think of the United States, where we have very little law about news media – we have very weak libel laws in the US, but the news media in the middle of the 20th century decided to implement norms in industry codes about how they would behave. So we have a masthead, we have codes and standards, we serve the public interest. Even though it was famously said ‘if it bleeds it leads’ – in other words, if it’s a very salacious story, it will bring readers, and so we like to have it on the front page – but they don’t have the whole newspaper full of the crime and the murder, because they felt some obligation to serve the community.

So we need those kinds of norms in this new system, as well as laws. I think you’re absolutely right for everyone to be emphasising the dark patterns and the deep fakes. These are really pernicious threats, and also I think the sentiment analysis that has been brought up here and the asymmetry of power that folks who have so much data and the AI technology have. And we must update our whole notion of consumer protection and empowering consumers. And that requires one thing we haven’t talked about enough: much more research and development of tools about what is effective in terms of empowering users with not just transparency, but the time to understand and the options for what to do.

So if you have to make a very quick decision about whether or not to allow cookies or not, and one thing is easy and one thing is difficult, how do we counter that? What can be done to really allow the human lizard brain to stop and think and make a decision in his or her own interest and in democracy’s interest?

These are really, really complicated, so I think we should think of them in terms of consumer protection, in terms of democracy protection. We must do the research as well as developing the laws and the norms.

1-019-0000

Alessandra Basso (ID). – Thank you, Chair, and thanks to all the speakers. I have a question for the Ambassador.

Ambassador, I read an interesting article you wrote for the *Washington Post*, in which you set out three steps to tackle disinformation. One of these is, quite rightly, the need for large online platforms to abide by codes of conduct that set communication standards in line with democratic principles. Under such a code, platforms would need, for example, to assess the credibility of the sources themselves.

But let’s say we had a whistle-blower who had disclosed a true and verifiable fact on a platform but felt unable to reveal their identity. Such a source would be deemed to lack credibility and would, therefore, probably be censored. Do you not foresee a problem with equating the veracity of content with source credibility?

1-020-0000

Karen Kornbluh, *Senior Fellow and Director, Digital Innovation and Democracy Initiative, the German Marshall Fund of the United States***.** – I’m really sorry, I don’t have the translation. Perhaps you can go to another panellist.

1-021-0000

Chair. – I would ask kindly the colleagues from the technical team to maybe send a message on how to switch on the translation, and maybe we can come back to this, or any of the other panellists who would like to pick up on the question.

1-022-0000

Lorena Jaume-Palasí, *Executive Director, Ethical Tech Society and co-founder, AlgorithmWatch***.** – *(inaudible)* correct: credibility does not stand for veracity; quite on the contrary, it might lead to *(inaudible)* of truthful information and relevant information coming from marginalised communities that are usually the subject of discrimination and for that reason do not have enough credibility – which doesn’t mean that what they are sharing through the media is not relevant and not important. So this is the reason why in democracies we try to push for plurality. And this is what I would plead to do, because of course what we see is that society is polarised. But we see that radicalisation has not increased. Radicalisation and polarisation are two different things, and overall, from a historical point of view, conspiracy theories: we had more in other centuries. We are in a century with mass media that are democratising access to good-quality news more than ever before. So putting an emphasis and protecting marginalised journalistic offers is here, from my opinion, key, and making sure that marginalised communities have the possibility of having their say is also important. Again, public opinion is the counterpart of public power. This means that public power must be very careful, and the concept of harmonising society is a very conflicted concept. *(inaudible)* society to make sure that there is no polarisation and with that *(inaudible)* with you.

1-023-0000

Alexandra Geese (Verts/ALE). – Good afternoon to everybody, I have a question for Professor Theocharis. You explained very well the polarising content in the internet and hate speech, and I would like to mention that hate speech is the reason that 60% of women in Europe do not express their opinion in the internet freely. So clearly we have a democracy problem here.

It’s not a bug of the system. It’s a feature, because it creates profit for those companies, and this is a business model. It’s a business model called surveillance capitalism, and specifically targeted advertising, which is something that, according to a survey published this morning, 80% of respondents in Germany and France don’t want. They don’t want to be targeted for ads according to their income, or their gender, or their sexual orientation.

I was quite intrigued by hearing your say that the solution to this polarising content or to hate speech would be automatic counterspeech or automatic detection of certain accounts, of certain kinds of speech, which sounds rather dystopian, I think. Thinking of public discourse in a democracy that is just done by artificial intelligence – that is dystopian to me, and I don’t think this is a very good solution.

It also means to give even more power to the same companies who optimise algorithms of content moderation for polarising content in the first place, because the problem here is not the Artificial Intelligence, it’s what it is optimised for – to generate profits through engagement, through hate and anger.

So I was just wondering: why are you so reluctant to tackle the business model rather, which is something we could do with in the Digital Services Act (DSA) – putting a ban on targeted advertisement that people in Europe don’t want, rather than suggesting solutions that put even more power in the hands of the same companies that have been causing the problem. And I’m very happy to engage in this debate with you here.

I would also like to note that the very prestigious university you are representing here has an Institute for Ethics in AI that received EUR 6.5 million from Facebook in 2019, if I’m not wrong. This doesn’t concern your Chair – I’m saying this very explicitly – it concerns a colleague of yours, but I just wanted to make that point. So maybe if you want to comment a little bit on freedom of academia and how we can trust, and what your colleagues are saying, that would be helpful.

1-024-0000

Yannis Theocharis, *Chair of Digital Governance, Bavarian School of Public Policy, Technical University of Munich School of Governance***.** –Thank you, this is a very good and interesting question.

The reason I'm proposing these different models, if you like, is because I've had the opportunity to actually meet with people from social media companies and be asked about my opinion because of my research on incivility: how do you deal with this problem? How do you deal with that problem? How do you deal with that other problem?

And the problem is that, when it comes to resolving issues that have to do with incivility, you always have to deal with two clashing normative sort of standards, if you like. On the one hand, there is a freedom of speech advocate, and on the other hand, there is obviously harmful language, which basically marginalises people, kicks him out of the platform.

But internal research in those platforms also shows what happens when you provide these people or those people with more advantages in stifling other people's speech. So the dynamics are extremely complex, and I think that's one of the reasons why they have been able to get away with, let's say, not regulating these spaces, not making these spaces safer faster, not turning their attention to these problems earlier than now (now they are, of course, forced to because all the attention is turned on them).

Counterspeech experiments based on a scientific research are very well published in very prestigious journals, and they seem to work. In my view, this is a middle of the road, faster solution, if you like.

In the long run, you can discuss about negotiations with companies, how to do this, how to do that, whether we should ban them right away when they're targeting people in this or that way, but that takes time. Encouraging them to develop counterspeech methods is something that can work now, it can work fast – that's very simple artificial intelligence programming for them. So that would be my view on that topic.

1-025-0000

Adam Bielan (ECR). – Thank you, Chair, and I promise to be as quick as possible. Good afternoon. First of all, I would like to thank all the experts for their interventions. My questions will be mainly directed to Ambassador Karen Kornbluh.

Concerns about democratic interference and misinformation campaigns, fair taxation, privacy, fake news and other issues have brought critical perspectives on digital technology to the public opinion. In your opinion, what could be done to prevent the growing concerns of citizens and to prevent the misuse of AI in these crucial domains? Indeed, filtering may raise some issues concerning confirmed discrimination to the extent that the content delivered by or concerning certain groups may be excluded or deprioritised. How can we make sure that the opinions of people who are not in the mainstream are also represented? And, finally, how can we make sure that the future boundaries for AI are inclusive enough not to follow only a mainstream trend? Thank you.

1-026-0000

Karen Kornbluh, *Senior Fellow and Director, Digital Innovation and Democracy Initiative, the German Marshall Fund of the United States***.** – Okay, I'll try to be even faster than that. Yes, I think the problem in the disinformation space of doing the content moderation after the fact gets us into this tension that you described of over-moderating or under-moderating. Far better than approaching after the problem is to have some standards and some clear guard rails providing incentives for the companies so that they correct the design defects, I would say, that allow bad actors to operate. So that means slowing the spread of disinformation; that would mean taking down repeat offenders in their part in the case of disinformation, whether it's outlets or networks of pages. We see the same groups again and again. Maybe they just don't take them down but don't amplify. That's much safer from a free expression point of view: don't provide that great amplification.

And I think similarly, we can see a design approach is a good one for other uses of AI but it requires that we not just have the overall framework, as I believe Europe is leading on thinking through, but that we also eventually can distil it into some standards and some norms so that companies know what they should and shouldn't do and it can be very clearly articulated to employees, it can be measured and there can be appropriate oversight.

1-027-0000

Sabrina Pignedoli (NI). – Technology's dizzying advancements are opening up many new ways in which we can exercise our rights: whether it's through direct participation or access to information, they are making for more informed voters and more inclusive voting processes.

There is one caveat, however: more information does not mean more informed decision-making. Too much information can leave people feeling overwhelmed, and so make it harder for them to decide who should get their vote.

This is where artificial intelligence comes in. Like it or not, AI is already playing – and will continue to play – a key role in determining what information gets through and in influencing voting behaviour.

In the light of this, I have a few questions for Theocharis.

What common rules need to be introduced at European level to stop the use of data by AI and democratic choices?

Do you believe we can realistically rule out this kind of influence?

Is there not a danger that AI systems run by non-governmental actors, such as multinationals, could interfere with democratic processes in Europe?

How can we counter such interference effectively?

1-028-0000

Yannis Theocharis, *Chair of Digital Governance, Bavarian School of Public Policy, Technical University of Munich School of Governance***.** – I didn't hear the question. If another colleague, if another one of the presenters can address this question.

1-029-0000

Chair. – Well, I'm not sure who had the translation. Ms Pignedoli: any way of doing it very, very fast again? But Mr Theocharis, did you get the translation? Ms Pignedoli, could you summarise the question into 20 seconds please?

1-030-0000

Sabrina Pignedoli (NI). – The thrust of my question was this: given that too much information does not necessarily lead to more informed decision-making and that when there is too much information and more knowledge, this can make it difficult for the algorithms to select information, what common rules need to be introduced at European level to stop data being used to influence democratic choices?

Do you believe we can realistically rule out this kind of influence?

Is there not a danger that AI systems run by non-governmental actors, such as multinationals, could interfere with democratic processes in Europe?

How can we counter such interference effectively?

1-031-0000

Yannis Theocharis, *Chair of Digital Governance, Bavarian School of Public Policy, Technical University of Munich School of Governance***.** – Very briefly, I would like to say that, first of all, more information generally does make people make better choices. We know that from plenty of behavioural research. And one of the major benefits of social media and many of those platforms that actually provide political information is that people can and are able to receive political information and make better choices, purely by being accidentally exposed to political information often times.

I'm not certain with regard to what common European rules can be put into place with regard to how data are being used to influence democratic choices, but I would like to add here – and this kind of echoes some of the comments and the questions, the topic that many of the previous speakers actually addressed – from a purely scientific point of view, scientific research is showing for a very long time now that many of the risks that you are referring to actually are very, very minimal. There is very, very contradictory evidence at the very best that misinformation is actually influencing people to make the wrong choices. People usually influenced by misinformation belong to very small and very particular strongly partisan groups.

Behavioural research – scientific research – doesn't show us in any way clearly that there are behavioural outcomes that are dangerous for democracy when it comes to the spread of misinformation. I do realise that this goes against some of the things that some of the previous speakers already discussed, but I do think that it is extremely important for this to be taken into consideration, and I will repeat it: we do not have clear evidence either about the extent of information, of misinformation if you like, and certainly no clear information about these types of content leading to people making undemocratic choices or problematic-for-democracy choices, certainly not at any grand scale.

1-032-0000

Chair. – Now I have two more speakers, two more members from AIDA and the INGE rapporteur, Ms Sandra Kalniete. I will take all three speakers in one go. I would kindly ask the panellists to pay attention to the interventions, because afterwards I will then give you the floor for the answers, and I will have to concede my closing remarks time as always. So let's try to do all this very quickly. For EPP, Karlo Ressler, you have the floor.

1-033-0000

Karlo Ressler (PPE). – Thank you very much for the really thought-provoking discussion. I will try to be really brief, but I think it's quite clear that artificial intelligence systems have real potential to create a special asymmetric advantage, and because of this, create really powerful forces that are capable to undermine democracy, and this is not always necessarily intentional.

But my questions would basically go in the other direction and they would try to remain on a more positive note. Taking into account the whole discussion of these challenges and of the negative consequences, I would like to be a bit more positive and try to hear from our speakers, from Mr Theocharis, especially. How can the public sector and the whole society, basically, contribute to addressing these challenges better and to really achieve that balance between democratic practices but also without violating the freedom of speech?

And secondly, but even more important, how can and what are some positive examples of how the artificial intelligence can, on the contrary, not undermine but strengthen democracy and democratic processes?

1-034-0000

Maria-Manuel Leitão-Marques (S&D). – I have two questions to our speakers, and I also thank them for this interesting and important debate. The first one is about the access of platforms to our data, our likes and our dislikes, because this allows for the private groups and platforms to use AI to micro-target individuals, for example political apps. And the disease of data has been linked to the spread of misinformation and radicalisation, because it is different. Radicalisation means when we confront different positions and in social media to live in bubbles, and these attitudes are a threat to democracy. What are your views on restricting companies' and platforms' ability to collect these very granular data or even banning target advertising altogether?

And my second question is to Professor Yannis Theocharis, that mentioned that there are AI-based solutions to deal with some of these problems – good news – such as automated counterspeech and automated nudging. Is there enough evidence to support the claim that these tools can have a real impact in addressing issues such as misinformation and hate speech online?

I ask this because we need to have a strong evidence base before we support these deals, because otherwise the problems – I'm going to finish – will remain, and tech companies might use these tools to argue that they can address these issues by themselves and that the EU...

(The Chair cut off the speaker)

1-035-0000

Chair. – The first question: who was it addressed to? Sorry, just one last speaker and then I will give you the floor.

The INGE rapporteur, Sandra Kalniete, you have two minutes, please.

1-036-0000

Sandra Kalniete (PPE). – Thank you Chair. There is a multitude of questions to ask and I thank all the experts for their very interesting presentations. It shows how close both of our committees, the INGE Committee and artificial intelligence, are. As we are covering the same areas, I would ask just two questions.

The first is to Ambassador Kornbluh. This is on how to strike a balance in building an ambitious transatlantic artificial intelligence partnership. It is clear that Europe and the United States must work closely together to offer a regulatory framework based on our shared values and counter-authoritarianist exploitation of artificial intelligence. On the other hand, as the recent Clearview scandal shows, the EU and the US do have a different understanding in their approaches to protecting privacy rights. How do we balance these considerations?

And another question – I'm not sure, but probably also to Ambassador Kornbluh. I was elected in Latvia, which is a small country with a language that is not widely spoken, and I know that on platforms, this language – like many other smaller languages – is systematically discriminated against. That's why I would like to insist that it is crucial to ensure respect for multilingualism in the context of artificial intelligence development, because diversity is a core value of the European Union.

Just a few examples showing the incapability of artificial intelligence tools used by Facebook and other digital platforms to recognise harmful information in small languages: Facebook recently blocked a French town whose name had been misunderstood – Bitche; and the name of the Prime Minister of Latvia – Kariņš – which means war, was also blocked on many occasions. And then there is also information on the Cyrillic alphabet in Bulgaria. What I plead is that we pay more attention to this aspect.

1-037-0000

Chair. – So now: the impossible task for the two panellists to respond in one minute each. I'm sorry, but we are already out of time for this first panel. I will start with Mr Theocharis. Do your best and be quick.

1-038-0000

Yannis Theocharis, *Chair of Digital Governance, Bavarian School of Public Policy, Technical University of Munich School of Governance***.** – How can the public sector contribute to addressing these challenges? One direction is the direction that the EU is already taking. We still don't have a clear understanding of how these behaviours diffuse on social media, and what their online effects are, so more funding for research into better understanding what kind of additional methods can be deployed to counter these behaviours is a great way forward.

In your second question you ask whether there is enough evidence that these tools can have a real impact on the solutions I propose. Yes, there is evidence, and one encouraging aspect is that one can imagine that they can have a real impact, because as I mentioned earlier, there are very few spreaders of misinformation. Research in the US during the 2016 election found that the vast majority of misinformation came from less than 1% of Twitter users. So one solution is figuring out ways to crowd out this information. That's definitely feasible.

1-039-0000

Karen Kornbluh, *Senior Fellow and Director, Digital Innovation and Democracy Initiative, the German Marshall Fund of the United States***.** – I just want to endorse very much this idea of a transatlantic partnership. We really should work together to determine a values-based way to approach this new technology in a way that can provide a counterweight to authoritarian uses of the technology, and I agree with the idea that we should be positive.

Our democracies have always embraced new technologies and found ways to make them more supportive of human needs. The US and Europe together, I think, can lead on that and bring other democracies along. It's very important, but government must update itself: good government must have better training and capacity to meet the challenges of these digital technologies. Thank you so much for having this very important hearing.

Closing remarks

1-041-0000

Chair. – Thank you very much, Ambassador, and I would really like to give a very warm thanks to all four panellists. It's been very, very interesting: apart from having to rush it at the very end, it's been one of the most interesting debates we've had so far. With that, I close the AIDA part of this session, the first panel, and I will give the floor, with my excuses for running a bit out of the initial time, to Mr Glucksmann for the second panel chaired and organised by INGE.

Panel II: "Tech developments and regulatory approaches to disinformation" (INGE Special Committee)

1-043-0000

IN THE CHAIR: RAPHAËL GLUCKSMANN

Chair of the Special Committee on Foreign Interference in all Democratic Processes of the Union, including Disinformation

Opening remarks

1-045-0000

Chair. – Thank you very much Dragoş. Don't worry about the delay – we're used to that as well. And thank you to our guests on the first panel for the quality of their presentations. Let's move on to the second part of this meeting, which concerns tech developments and regulatory approaches to disinformation.

As we have seen, tech developments can be put to both good and bad uses. Machines and social networks can be used to subvert our democratic frameworks and equally for their regeneration. Legislation on digital services could be a useful regulatory tool in combating disinformation campaigns orchestrated from abroad.

Our task is to ensure a balance between defending freedom of speech and protecting the democratic framework. I hope our guests in this second session will help us to establish or improve our grasp of this balance.

Our first guest is Mr Rasmus Nielsen. You are Professor of Political Communication at the University of Oxford and the Director of the Reuters Institute for the Study of Journalism. You carried out a major research project on recent changes in the media and political communication in connection with digital technologies. We are very pleased to have you here, and you have the floor for ten minutes.

1-046-0000
A technical problem – I'm very sorry about this – means that we will move on to our second guest, Ms Anna Bulakh. We will return to our first guest a little later.

Ms Anna Bulakh, you are the Programme Director at Disinfo.Tech, a company which uses technology to build solutions against disinformation, false information and online propaganda. You are also a co-founder of Cappture.cc, where you help investigative journalists – fact checkers – and researchers to store online content securely.

Ms Bulakh, you have the floor for ten minutes. I hope the technology won't let us down this time.

1-047-0000
Anna Bulakh, *Director at Disinfo.Tech and Co-Founder of Cappture.cc*. – Just to add to what you told about me, my biography: I also just recently became a policy adviser to Reface.ai. It's an application that creates a deep fake and is based on synthetic media. Actually in today's presentation I wanted to focus exactly on this aspect, on deep fakes, that is also linked somehow to fact-checking and other issues that I am working on as well.

So thank you for having me on this panel, and thank you for giving me the floor to share my observations and ideas from both the security policy and tech side.

In this presentation I want to talk about new technologies that can shape the media ecosystem. In this ecosystem we are all consumers. The question for all of us is how to make it a safer space for users and creators and then how to develop effective initiatives to fight online disinformation.

New technologies available for user generation of content, called UGC, are appearing at a rapid rate. Consider the development of synthetic media such as in the case of deep fakes. The term 'deep fake' describes a face-swapping technique. The image of an individual is used by artificial intelligence to generate a digital look-alike copy of a person. Commercial applications allow the production of a realistic face swap with one selfie. The amount of deep fakes is *(inaudible)*.

Just imagine: in 2019 there were only 14 000 deep fake videos online. After Reface.ai, the face-swapping application that went viral in 2020, the number of user-generated synthetic media surpassed 3 billion videos online in just 14 months. Reface.ai is company that I advise on security policy.

Technology is getting better and sophisticated. The definition *(inaudible)* media is changing. What we observe is the *(inaudible)* of AI and deep learning tools. 100 million users worldwide installed Reface.ai in just 14 months. It’s one example of an application using such technology. This is a trend led by the development of the creative economy, where the content creators are becoming the driving force – also information markets, not broadcasters as we have been used to. This means we must access to the tools which allow content modification such as deep fakes.

Yes, the creativity tools are developing with unimaginable speed. We also find more vulnerabilities to misinformation, disinformation and criminal operations. Some of the initial concerns focused around political applications: the widely-circulated deep fake of former US President Barack Obama you might see. However, probably the most widely-deployed bad use of deep fakes are not political, but ethical and criminal in respect to *(inaudible)*. And deep fakes also have been deployed to defame individuals and to assist criminal plundering activities as well as to provide opportunities for disinformation operations. We have an alarming problem also with the growing amount of inauthentic content that fills the web space and platforms.

Such content is attributed to fake accounts and anonymous users. It is difficult to trace such content to establish authenticity and ownership. Deliberately-deceptive media and bad actors use this gap in how we allow users to operate on the platforms. And with the changing nature of what we call media today, we need to agree on clear approaches that leverage the massive amount of data, both structured and unstructured. And that’s exactly the *(inaudible)* from experience of working in the fact-checking industry.

The nature of how we mark online content – its texts, its photo, its video and audio – is a question of the global standard on content metadata authenticity and transparency. And in future this could lead to an intelligent analysis of user-generated content if we mark it well and *(inaudible)* creative advantages of the technology all creators are craving for.
So the question: how to design a digital ecosystem of accountability, as I call it? And the solution to the problem of inauthentic content and the erosion of trust rely on efforts in three areas, as I define them.

First, creating a common standard ensuring content authenticity. Second, the need for harmonisation of standards and codes of practice, such as labelling of the content. And third, we need to integrate security thinking into product design among tech developers and especially those fast-growing tech applications.

To ensure content authenticity, we need a commonly adopted approach to marking content. It is often referred to as provenance. It empowers content creators and editors to disclose information on who created the content, how it was changed, which technology was used to modify it. For instance, if a lip sync was used or if a visual modification was applied, then which technology was used. In fact checking, in text content, this would be marking in *(inaudible)* standard *(inaudible)* will be structured.

Such metadata helps to safeguard content authenticity and making data accessible on platforms, so you would ask: what advantages would it provide? First, it would empower fact-checking and detection initiatives. It is easier to deploy bigger technologies and algorithms, because we would have a mass of data. Second, this would engender trust between creators, publishers and consumers. And finally and more broadly, it would enable us to create an ecosystem of accountability.

Second, platforms and companies are developing a number of labelling and watermarks, and here I speak about a second point of harmonisation of standards. There should be harmonisation accompanied with awareness and user education on how to spot the modified content with clear labelling, and platforms could concentrate on moderation. So the moment the content leaves the applications on the search platforms, the users – the consumers of content – should be notified whether they are seeing synthetically-modified content.

The EU has taken a leading role here. I found today’s panel here and actually initiated and hosted by the European Parliament as one step closer to develop new policies in cooperation with the tech sector. The EC White Paper on AI published in 2020 provides a step forward on addressing the labelling standards for synthetic media in creative industries. It is different from big tech giants, because applications that are growing and growing very fast on synthetic media are filling in the information space with such content. What is important is to ensure the communication on the standards between the regulators and companies.

And the third, and it is a really interesting insight that I found myself just with my background from policy – security policy – *(inaudible).* There is a need to integrate security thinking into product design among tech developers. We have to rethink how we build a product. We need to integrate security thinking into product design. The answer is to align policy and technology from the moment of product development and with clear communication to users and creators. This includes integration of moderation and detection from the starting moment of creation of commercial tools on synthetic media. Whatever steps the industry and government take, we have to understand that deep fakes and this new alarming media lie in a space where tech and ethics meet. The synthetic media industry shouldn’t be at first place a consumer secure oriented industry.

Platforms have to educate creators. Well-intentioned creators and consumers will need to understand the danger of disinformation and the use of techniques to prevent it. They must also understand the ways to use sophisticated creative tools responsibly. That is why you see me taking *(inaudible)* growing fast tech and advising on the security policy. It’s a forward-looking step that the other companies should adopt and to look from the beginning for security applications of *(inaudible)* they are creating.

Such skills, as I indicated in the third point, must be learned and passed on through direct communication between platforms and users, regulators and platforms, governments and users. So there is an ecosystem of accountability. Expect all actors to understand the levels of responsibility, everyone in each.

1-048-0000

Chair. – Mr Alex Stamos, you are the Director of the Stanford Internet Observatory at Stanford’s Freeman-Spogli Institute, and you are also a partner at the Krebs Stamos Group. You are a recognised expert in cybersecurity; you are currently a member of the advisory board to NATO’s Collective Cybersecurity Center of Excellence, and you are a member of the Aspen Institute’s Cyber Security Task Force.

In the more distant past you were the Chief Security Officer of Facebook, and you led the company’s internal investigation into manipulation of the 2016 US election.

I know that your team at the Stanford Internet Observatory recently carried out a very detailed analysis of disinformation activities during the 2020 US presidential election. Could you please describe the main conclusions and explain how the European Union might also learn from your observations? Thank you very much.

You have the floor for ten minutes. I hope it will work.

1-049-0000

Alex Stamos, *Director of the Stanford Internet Observatory***.** – Thank you Chair, ladies and gentlemen, thank you for the opportunity to speak to you today. This is an area that I have spent the last several years very much involved in and I’m looking forward to discussing how the things that we have learned in our study of disinformation activity around the world and in the 2020 US election to European democracy.

I have a short period of time, so I'm going to try to hit nine points very quickly during this time, and I look forward to your questions. First, a really important thing to keep in mind here is that the vast majority of online political disinformation and influence operations are domestic. They are not foreign. In the vast majority of situations that we study in our group at Stanford and in the majority of these situations in which the large tech companies have acted to take down disinformation actors, the biggest group of those are acting domestically and are often involved with domestic political parties or are from the ruling party of a current government. And so that's something we need to keep in mind. I know the hearing is about foreign influence, but as we talked about this week, I remember that everything we talk about here is actually much worse in most countries targeted internally than it is from foreign actors operating in that country.

Both those foreign and domestic influence operators are active intelligent adversaries. We're not talking about a static situation here where there is a problem that we can solve. These are intelligent adversaries who will adjust to anything anybody does. As a result, there has been a huge change in the way influence operations have evolved from 2016 to now, and one of our problems in this overall discussion is we're still stuck in a 2016 mindset, and a lot of that, I think, is due to the election of Donald Trump in the United States. I don't have to tell European parliamentarians that Americans love to talk about ourselves and to talk about our own political situation and that that influences the overall global discussion of these situations. But because the 2016 election of Trump and the Russian interference during that period of time is so widely studied and so widely discussed, it is also somewhat frozen in time. The discussion of this issue in civil society and in political spheres, and the attackers – the adversaries themselves – have now completely changed how they operate since 2016. So we have to keep in mind what is going on today. If we want to come up with solutions that actually address the problem, we can't come up with a solution today that would have helped in 2016.

As of 2021, one of the big changes in the way foreign influence operators operate is that they are no longer mostly focused on the creation of many fake accounts by which they inject information into a political sphere. The two most effective mechanisms for foreign influence these days is either (A) the injection of an idea that is then amplified by the real political elites by a country. This is often combined with offensive cyber capabilities, and good examples of this would include, back in 2016, the GRU insertion of hacked emails into the American political sphere, the attempt to do the same thing by the GRU for President Macron of France, and a variety of other situations that have existed since then where hacked or leaked information is injected into a political sphere but then the actual amplification happens by domestic actors and therefore does not have the fingerprints of the actors on it.

The other technique that we see used a lot is that foreign influence operators will use local proxies within countries to create and spread disinformation on their behalf. I will send links to two papers that are relevant to this when I'm done speaking so parliamentarians are able to read that later. But a good example of that is the actions of the Russian Internet Research Agency in Africa. We've written extensively on this, where, instead of having people in St Petersburg, Russia who speak the local languages and have understanding of local politics in Africa, what the Russians have done now is hire local proxies to create entire fake media outlets in these countries that then push disinformation that is in the benefit of the benefactor of the Russian Internet Agency: a Russian oligarch named Prigozhin. And so by using those locals, they end up (1) having a cheaper cost structure; (2) having people who are much more aware of how people speak and interact in that country – and it's much harder for platforms to figure out, because at a first glance, this kind of activity looks like it is legitimately people operating within these countries.

Another example from that same Russian group in the United States was a website called Peace Data, which is a an entire fake antiwar website where the content was actually created by real American freelancer journalists who had been contacted and paid by the Internet Research Agency to create content along the lines that they were looking for. And so, due to cooperation between the US FBI, Facebook, Twitter and some other tech companies, Peace Data was banned from all the major platforms. It was taken down, and what we found out is that you could talk to these Americans, who had no idea that they had become tools of Russian propaganda – that was something that did not occur to them at all when this was happening, when they were contacted and paid to create this content.

Because of these changes, there's a huge benefit to disinformation actors that have offensive cyber capability, and something we need to keep in mind here is that there are disinformation actors that are stand-alone; there are cyberactors that are stand-alone. But when you talk about organised interference by governments, almost always those actors are now met up and have capabilities both in the offensive cyber side and the disinformation side. So, often we are talking about what are effectively hybrid attacks against democracies where there's a hacking component as well as a disinformation component, and those two things reinforce each other and have to be dealt with together if you want to mitigate the damage.

The political disinformation is now often found in many platforms and formats. It has become multimedia. So one of the conclusions from our work in 2020 – and again, I will post a link of our massive report out of the election integrity partnership, which is the group of four institutions we led to look at the US election – the most prominent and effective disinformation actors were multimedia stars with large intentional followings. So this is: hosts on right-wing TV and radio in the United States, for example, Fox News, OANN: the people who are paid employees of those companies, have television shows but they also have massive online followings; the candidate Donald Trump and his children, all of whom are large influencers in the right-wing sphere; actors; other kinds of people that are political elites who are not anonymous – we know exactly who they are, they have verified accounts, but they have half a million to millions of people who have said: 'We want to see their output': they were the most effective spreaders of disinformation, and it was often multimedia. You would see a jump of a rumour that would start on line that would then be retweeted by a child of the candidate, which would make it on to Fox News, which would then be massively amplified and reposted over and over again. And so this jump between social media and traditional media creates a lot of challenges, both for regulators as well as for the platforms themselves, because you end up creating rules that directly have to affect traditional political speech from traditional media outlets.

I'm just going to be frank about a lot of the discussion that I've heard all over the world, which is: the most overused word in all of these discussions is the word algorithm. There is no magical algorithmic problem here and there is no magic algorithmic solution. There are situations in which algorithmic applications make things worse. The vast majority of situations we look at, that is not true. This is not algorithmic application by some algorithm that you can just regulate and change. You're talking about the emergent properties of millions of people's individual choices of what information they consume and what information they amplify. And so, while there are algorithmic changes that can make things better, it will not solve the problem. And the huge amount of focus on algorithmic application, I think, gives people a little bit of an out – that they think there's some kind of solution where they don't have to deal with the underlying behaviour of human beings, many of whom are actually political actors within democracies, if they could just fix the algorithm. And I'm just going to tell you that's not going to work. We have to look at the kind of behaviours of individuals and the powers individuals, especially political elites, have on these platforms.

Two quick things looking forward: (1) disinformation in Western democracies is trending towards the model we see more often in places like India – developing democracies – where disinformation is peer to peer. It comes from your aunt, it comes from your college roommate, it comes from somebody you know and it goes over a peer-to-peer network that is often encrypted. This is how political disinformation has operated in India for years now, and we're starting to see more and more of that behaviour in Western democracies. This creates lots of complications, because these peer-to-peer networks are often encrypted and don't have single choke points, so any platform or government response that requires a centralised capability to see what people are saying are no longer relevant. And because of that and other issues in Europe, fighting political disinformation on line is going to bring up two really important questions around sovereignty and privacy. And they're just irreducible trade-offs here. If you tell political platforms that you want disinformation to be taken down in your democracies, you will be giving them the power to decide what is legitimate political speech within your democracy. If you tell them: 'We want this content to be taken down or down-ranked', then you're telling them that they have to be able to see the speech, which necessarily violates the privacy of those users. It makes certain kinds of privacy-protecting technologies such as end-to-end encryption something that they will not deploy on these products. And so that trade-off between fighting disinformation, sovereignty and privacy is going to be a very difficult issue that has to be weighed in all these discussions.
Anyway, thank you for the time, sir, and I'm very much looking forward to the questions.

1-050-0000
Chair. – Okay, so it seems we cannot do anything from here, so we are really sorry. If ever you have a written presentation, we would be very happy to circulate it in both committees. And once again, sorry, it's the first time it happens and it had to be on the technological revolution session. So now, let's go for the questions.

1-051-0000
We will now move on to the Members' questions. For the European People's Party, Ms Juknevičienė, you have the floor. I hope it will work.

1-052-0000
Rasa Juknevičienė (PPE). – Today we cannot imagine our lives without social media. It has changed the way we receive information and made it possible to communicate our ideas to much wider audiences. But social media platforms are also seen as the most crucial tools of spreading disinformation, and yet there are no global or even EU-wide regulatory standards. We have discussed many different aspects of disinformation online in this committee. One of them has been the important role of bots, troll factories and other types of inauthentic behaviour in spreading disinformation on political matters, especially from third countries. Recently we got interesting information from Deutsche Welle; they made interesting research on that.

So, my first question is: how do you think we should tackle inauthentic behaviour online? Would you agree with the suggestion to make it illegal to use bots and sell inauthentic engagement on social media across the EU as a first step, especially in the political area? And more broadly, what do you think should be core elements of EU regulatory standards?

Secondly, supervision and enforcement. Having well-designed regulation is just the first step. To truly combat disinformation, the regulation has to be well enforced. It has to work across the EU in all of the languages that are used in our Member States, including the smaller ones. So my questions are: what do you think would be more effective: relying on a network of national regulators or creating a fully supranational structure? And finally, how do you think it will be possible to apply the standards for monitoring and removing illegal, condemned or accounts equally across all languages?

1-053-0000
Pierfrancesco Majorino (S&D). – Thank you, Chair. I hope it's not interference that's causing our technical problems. That would be a shame. Joking aside, I am very concerned about all the

things we’re told, all the information we receive on the dangers of innovation. Innovation will open up great opportunities – but there are many pitfalls along the way.

So, I thank our speakers and wish to ask them a very simple question, one that we have been asking ourselves repeatedly in the INGE Committee: in their opinion, what choices should the platforms be making? Or rather, what choices should the platforms be forced to make in order to contain the risks of disinformation, interference through disinformation and the spread of fake news, in all their possible manifestations, which promote harmful values or could even be dangerous for the people they target?

1-054-0000

Sandro Gozi (Renew). – Thank you to our guests for your excellent interventions. I would like to know, in the light of what they say, if they think that four solutions, identified and proposed in the digital services sector, are a step in the right direction. In particular, what do they think this obligation of the systemic platform concerning the systemic risk to security and fundamental rights should be? There is just a *(inaudible)* make a specific reference to this obligation to report this systemic risk for the platform in terms of security and fundamental rights. I do believe that this could be a basis to develop our action against disinformation. What do they think about that?

And then I have a specific question for Alex Stamos. I’m not sure I have understood what he said about algorithms. In my view, what I call the ‘black box’ – the lack of transparency of the algorithm – take, for example, Facebook, is one of the problems they are talking about here.

It is true that there is no silver bullet, that there is no magical solution for algorithms, as you say, but it is clear that the viral effect the amplification of the algorithm is one of the best weapons to spread disinformation. After all, they go and look in the platform for a specific, marginal segment of the users and they put them together. And this is at the origin of the viral effect. So on the one hand I agree that we don’t have an algorithm silver bullet. On the other hand, I got the impression that you, Mr Stamos, underestimate the impact of algorithms somewhat. I may have misunderstood, though, and I would kindly ask you to better develop this point, which I think is very important.

1-055-0000

Alessandro Panza (ID). – Good afternoon and thank you to the speakers for their fascinating insights.

I have two concerns and two questions. The first relates to the first speech we heard. I am a little concerned by what was said about the need to have a regulatory authority that would dictate the rules of engagement when it came to determining whether news were true or fake. Naturally, this authority could not be run by private companies.

If it were – and here I come to my second point – we would run the risk yet again of finding ourselves in a situation in which, as happened during the recent US presidential election, platforms, like Twitter, become de facto editors-in-chief, deciding who can and can’t post, and so become more than just platforms, or what we commonly understand platforms to be.

We need to think carefully about, first, what form the regulatory authorities will take and who will be the content regulators, so that we don’t find ourselves in some Orwellian dystopia.

Second, we need to understand precisely what it is that the large platforms do. I don’t just mean in the active sense of sharing information, but I’m also referring – and here we often talk about the Russians but never the Chinese – to the role they play in hacking. Because this is another highly sensitive topic – think of platforms like TikTok. I think we need to think carefully about this too.

1-056-0000

Markéta Gregorová (Verts/ALE). – Thank you, Chair, and welcome to our guests. I'm sorry, Mr Nielsen, if it has been impossible to connect with you today because I was looking forward to your remarks. I do hope it will be possible to reach you via e-mail or some other way because I have a question that is keeping me awake!

But now to an oral question, Mr Stamos. It's nice to see you again, and your remarks have been great and timely, as always. I would like to react to your issue with the overuse of the word algorithms. While I agree that there is no magical solution, it is true that algorithms stand considerably behind our information bubbles in which a lot of people are encapsulated. And this needs to be addressed somehow. So I would like to ask you if we could brainstorm on how to make users more emancipated, if not by some regulation or transparency of algorithms, so that corporations and governments don't have to hold their hand as if they are children on the internet all the time. Thank you.

1-057-0000

Dace Melbārde (ECR). – I'm also sorry that Mr Nielsen couldn't join us, because I had prepared some questions, particularly for him. So it means I will be brief.

1-058-0000

Chair. – Still, ask your question, because we will try once again after, so if by any chance it's working, ask your question.

1-059-0000

Dace Melbārde (ECR). – Okay, now I go ahead with a question to Ms Bulakh. Ms Bulakh, you touched upon a very topical issue: the usage of deep fake. I personally find it a very scary and dangerous tool that opens diverse opportunities for constructing realities in favour of malicious political and economic interests. I believe we have to ensure close monitoring of developing such technologies. My question is: what is your prognosis for the future? How accessible and sophisticated these technologies could become and what regulation is needed at EU level, or maybe not only regulation; maybe some other coordinated activities, to prevent foreign adversaries and disinformation actors from using these fake technologies for disruptive actions in our societies?

And Mr Nielsen has joined us finally, and I would be also happy to hear from him what regulation is needed to stop the amplification of disinformation on online platforms and what is his view on putting 'must show' obligations on social media and search engines, meaning requiring block funds to provide fundability and prominence to public value of media content?

1-060-0000

Eva Kaili (S&D). – Thank you so much and thank you for organising such an interesting discussion. So my question would be: we talk about disinformation and also we understand that it's very important to have a resilient democracy under these exponential technologies. So at the same time as we are trying to tackle disinformation, which means to remove in an automatic way harmful content, at the same time we create another problem: a concern of over-removal of content, that this could actually become itself a risk for our democratic societies.

This is big power. It's really powerful to have the obligation to remove content. The free expression of opinions is the cornerstone of our democracies and when it comes to disinformation and deep fakes the line between free speech and illegal content is not always clear – it's clear for the illegal content once you have a decision from the Justice, from a court – especially when deep fakes can be used for humorous creative purposes or when you have something go hugely viral and suddenly you don't have enough time to remove the content, so immediately content is being removed. It's not very easy to say that this should have happened.

So how can we, as policymakers, ensure that the identification of offensive fake material does not violate free speech requirements, given the likelihood of a false positive? And how can you prove the intent also of a deep fake creator? So I would like to hear your opinion because we are dealing with all these findings this year.

And if I have time, I would like to ask a second question. Online platforms are repurposing data collected in one context and they use it in another; it's another related context but they are big platforms, they own different services. So these practices are *(inaudible)* invasive interferences and they are utilising individuals in clusters to make decisions that are significantly affecting their lives, for example, information to serve them, which means they can actually manipulate perceptions. We saw it with Cambridge Analytica. We saw how they can use data, so we have online platforms to repurposing data. So do you believe *(no sound)* throughout the whole lifecycle of AI? So, these would be my two questions and thank you so much for giving me time.

1-061-0000

Gilles Lebreton (ID). – Chair, I would like to thank the speakers. The internet is a marvellous thing, but unfortunately it is also where disinformation happens, and that is distressing. We must try to fight disinformation while at the same time respecting freedom of speech. There is sometimes a thin line between interference orchestrated from, in particular, abroad, which might be difficult to identify, and the simple right to express *(no sound)* by a private enterprise.

Apart from these considerations, I would like to ask our experts two questions, as I am by no means an IT specialist.

My first question is for Ms Bulakh: you suggested setting up a common standard to guarantee the authenticity of content and, taking the idea further, you mentioned 'labelling', which is a rather abstract notion for me. What is this 'labelling' you're suggesting? Do you think it will be effective? I imagine this kind of precaution can always be bypassed.

My second question is for Mr Stamos: several times you mentioned President Trump and the Russians, who are accused of engaging in some interference. But is this not rather a case of not seeing the wood for the trees, with them as the trees? As you yourself said, in the vast majority of cases (I am quoting your words), the interference is in fact internal – within a state – and not from abroad. In particular you said that it might emanate from *(no sound)* factions orchestrated by factions within the European Union.

1-062-0000

Chair. – As we are stubborn and we really want to hear you, Mr Nielsen, we really hope it will work this time. We will try one last time. If it should work, please take the floor for ten minutes and try, if you can, to adapt your presentation to the questions which have been asked.

1-063-0000

Rasmus Kleis Nielsen, *Professor of Political Communication and Director, Reuters Institute for the Study of Journalism, Oxford University***.** – Thank you very much, Mr Glucksmann and all your colleagues for your patience, and to the technical team for their assistance.

I've been asked to speak about foreign interference and disinformation, and what research tells us about the challenges they represent in the context they are appearing, and how we might respond. So, I'll take foreign interference here to include information operation specifically, but also just note, it's important to remember that this is a subset of a much wider range of soft power public diplomacy, but this is in communications operations often.

In line with the EU Commission Action Plan, I'll take disinformation to mean verifiably false or misleading information that is created, presented, and disseminated for economic gain, or to intentionally deceive the public, and may cause public harm, and that is almost always, as several of the Members of Parliament have noted, legal speech.

So where are we with foreign interference and disinformation? I think we need to understand the challenges we face, and the context they exist in if we are to address them in credible and effective ways.

So let’s take the challenges first. Foreign interference often aims to increase division in our societies, undermine trust in institutions, and on that basis influence individual and collective decision-making. Disinformation is only one way in which foreign governments try to achieve these aims; as said there are other means as well, often deployed for the same purposes. And some of these means in part work via domestic actors wittingly or unwittingly, as Alex Stamos noted.

And crucially, of course, many other factors are far, far more important in shaping divisions in our societies, trust in institutions and individual and collective decision-making than disinformation is, let alone disinformation from foreign interference narrowly. We face real and serious problems with disinformation, but as with many societal problems we need to understand the scale and scope, and the way in which the public thinks about them, if you want to respond in effective and credible ways.

We don’t always have evidence and research on these issues that is up-to-date or that captures differences from country to country across the European Union, for example. But I do think some of the research we’ve seen from the United States, which has had very severe problems with disinformation in recent years, both domestic and foreign, can give a sense of the scale and scope, and our own research from the Reuters Institute can help us understand how the public see these problems.

But first, on scale and scope. In the United States, for example, one team of researchers found that across offline and online media news, news consumption is about 15% of Americans’ daily media diets, whereas fake news, narrowly defined, compromises only 0.15% of Americans’ daily media diet. So the time spent with news is outweighing fake news, highly biased and hard partisanised by a factor of almost 100.

If we look specifically at Twitter, which may give at least an indication of dynamics on far larger platforms such as Facebook and YouTube, where it’s harder for researchers to access data, another research team in the US found that fake news there accounted for nearly 6% of all news consumption on Twitter, but was heavily concentrated, with only 1% of users exposed to 80% of the fake news and just 0.1% of users responsible for sharing 8% of fake news. So highly motivated small minorities, both in terms of consumption and dissemination of fake news, at least on Twitter.

There are, of course, wider issues than fake news as narrowly defined in these studies, including dangerous narratives that aren’t necessarily tied to discrete checkable claims for specific sites, various forms of network propaganda, whether from domestic political actors and parties on the media or other sources, and problematic information, including various kinds of hyper-partisan material, harassment and trolling, often targeted at women ethnic minorities and marginalised communities.

But nonetheless, I think this research suggests to us that while very real and serious, the scale and scope of identified mis- and disinformation, narrowly conceived and nurtured, is more limited and more concentrated in highly partisan sub-communities than is sometimes imagined.

So, secondly then, how does the public see these problems? *(inaudible)* what source of potentially false and misleading information they are most concerned about online. If we look at the 20 EU Member States that we cover in the report, 11% respond foreign governments as the source of false and misleading information they are most concerned about. By comparison, 12% identified journalists and news organisations. And, I'm sorry if this is awkward to mention in this setting, but 38% say the government, politicians or political parties in my own country.

This finding is important for two reasons. First, because as with any social problem public perception will influence the effectiveness and credibility, especially of any response. And when it comes to disinformation, a large plurality of the public is more concerned about false or misleading information from domestic politicians or domestic news media than from foreign governments. And second, again apologies if this is inconvenient or even rude in this setting, I'd say that social science research largely suggests that the public is often right to be more concerned about domestic sources of false or misleading information.

I think that this research leaves us in a place where we must recognise two things. First, if the goal of foreign interference is, amongst other things, to undermine trust in institutions, there sometimes is a risk that our very own public conversation about disinformation help *(inaudible)* the Kremlin's information operations.

Second, if the goal of foreign interference is, amongst other things, to undermine trust in institutions, but much of the public see problems with disinformation as being about domestic politicians and media spin, false and misleading information about them, I think there is a risk that attempts to counter disinformation that are narrowly aimed at specifically foreign interference, that does nothing to address what much of the public see as the main problems, may come across to some of the public as self-serving attempts by governments and established domestic political elites to protect themselves by censoring out sources of information and stifling criticism.

So what can we do other than take problems seriously without exaggerating them and other than not pursuing options and responses that may seem so selectively partial as to be self-serving. I won't talk about technology in tech companies because Anna and Alex have focused on that, other than just to say that there clearly are a range of tactical technical interventions that can help: labelling context, introduction of friction, provision of authoritative information, in some cases reduction or even removal of content, provision of data and tools to independent third parties and the like.

And also just to note that of course our research documents that the public clearly, and in my view rightly, see technology companies, especially Facebook and the Facebook-owned WhatsApp, but also to a lesser extent, Search, Twitter and Google's YouTube as part of these problems and will expect these companies to be part of the solutions.

But while all these tactical and technical interventions can help make a difference, at a more fundamental level, if what we want to prevent is that disinformation from foreign interference increases divisions and undermines trust in institutions, if we remember that much disinformation is legal speech protected by the fundamental right to receive and impart information, and that narrow direct interventions targeted exclusively at foreign actors may exacerbate these problems because they will look like self-serving to a public that sees domestic actors as central to disinformation problems, – a view that is well supported by academic research – then I think indirect interventions focused on building resilience might be the best response to surveil upon.

Open societies with robust institutions will not be free of disinformation and not be free of pernicious forms of speech, but they will be better able to withstand the problems that disinformation and pernicious forms of speech create. Building resilience will involve investing in strengthening the independent institutions – not government, not the executive, but independent institutions – to help people be informed, connect with one another and work together, including independent news media, both private sector, public services, non-profit, independent fact-checkers, independent research, ideally with better access to data from both platforms and public authorities, and independent media literacy programmes for citizens of all ages.

And indeed of course the 2018 report of the European Commission High Level Group on online disinformation on which I served, recommended, amongst other things, exactly such investments, calling for the European Union with its annual budget of well over EUR 160 billion to commit at least EUR 100 million in funding for independent initiatives in a context where we know that several foreign governments are estimated to be spending a billion euros or more a year on their own state media and influence operations abroad.

This has not happened in the three years since the report came out, but the recommendations, I think, still stand. It's tempting to imagine that there are simple, cheap and uncontroversial solutions, whether technical or otherwise, to the very real and serious disinformation problems that we face across Europe, but there aren't. There are only complicated, often expensive and sometimes controversial options. Research can help provide an understanding of the challenges we face and inform the decisions we make, but fundamentally, how we respond to this is about choices and priorities, and you, in the European Parliament and your counterparts at the Member State level, are the ones who have a democratic mandate to make these hard choices.

1-064-0000

Chair. – Thank you so much, and we are very happy that finally you were able to deliver this speech and give us this information and analysis.

1-065-0000

Anna Bulakh, *Director at Disinfo.Tech and Co-Founder of Cappture.cc***.** – So, the questions *(inaudible)* will cover. So prognosis and accessibility of technology as an applicant is growing and we will see a moment of commonisation of technology; it means that masses will have an access to such tools and commercial applications will be growing. On labelling I would recommend *(inaudible)* what I'm suggesting it's exactly *(inaudible)* labelling on artificial intelligence modification of the content will be *(inaudible)* on search platform. So let's say this fast-growing tech companies *(inaudible)* start times *(inaudible)* that are taking off and having 100 billion subscribers in 10 months, the consumers and users *(inaudible)* a generated content is cross shared on other platforms, so here as a labelling *(inaudible)* and user education is necessary because we will see ever bigger generation of augmented reality and in the context of personalisation of a content.

Second, I would add that to all questions how to regulate tech *(inaudible)* firms, how to deal with disinformation and information operations and foreign influence and my experience being in research, *(inaudible)* Russian information operations from the past and working a lot *(inaudible)* stop *(inaudible)* checking organisations and civil society in Ukraine a lot and we exactly applied the concept of resilience because the time *(inaudible)* couple of years *(inaudible)* I was working in Estonia in the Centre for Defence *(inaudible)* and Security and Estonia is one example of application and whole society approach to security. And here I would stress that we have to understand that the ecosystem of accountability what I was talking about in digital terms it is applicable to any sectors that we want to make more secure *(inaudible)*. This means in terms of new technologies that are appearing *(inaudible)* its ever greater cooperation with new rising tech start-ups that are using new technologies, it's not just about big platforms anymore and bringing in to such hearings and discuss what kind of labellings *(inaudible)* or what kind of technologies, how it's progressing because the market is moving very fast.

Then on authentification *(inaudible)* of a content. Having worked with fact-checking community, what I've seen, it's under financed, it has been under financed *(inaudible)*, of course, such initiatives to take off and *(inaudible)* need tools and software *(inaudible)* tools a lot. And, of course, as a compression *(inaudible)* of this *(inaudible)* giant algorithms to push up the fact-checking *(inaudible)* information that is sent *(inaudible)* in because outreach has been quite low. So it's a time *(inaudible)* and it should be well financed. I would say resilience is never a cheap approach because we have to distribute responsibility. You have to include and always communicate between three *(inaudible)* sectors and this means a kind of trust-building issue. Thank you.

1-066-0000

Alex Stamos, *Director of the Stanford Internet Observatory*. – I'm glad Professor Nielsen was able to join us, because I was thinking that I totally agree with the vast majority of his statements. There are a lot of questions I wrote down here.

I'll start with the algorithm one. My point being that we need to separate out when we talk about amplification. When algorithms are being used by the platforms to choose what people see versus people deciding that they want to see and amplify certain content. And so different platforms have different amounts of algorithmic-driven consumption of content.

The platforms that actually have the least are the ones where the content you see is mostly determined by who your friends are, or who you follow, in the parlance of the platform. So in the case of Twitter or Facebook, for example, the number one reason why you see content from them is that you have decided 'I want to see content from this person'. You have made an affirmative decision that you have communicated clearly to the platform that there is something that you want to see.

Now, there is algorithmic ranking in both of those companies within that thread, but there have been a number of studies that have shown that even with reverse chronological order, which is where you just show all of the content in order without any kind of ranking, you still have the same kind of issues that we deal with, because people are choosing to see this content. On the algorithm point, as you can see on my shared screen, is a great example of what we saw in the US election. This is a graph of discussions of what was called 'Sharpiegate' in the United States, which is basically a conspiracy theory whereby Trump voters were being given a pen and, if they used that pen on the ballot paper, their votes would not count. We call them sharpies here. I'm not sure what the European brand is, but this is totally not true. These were the pens that were recommended by the manufacturer of the voting machines to be used.

This started from people talking about the fact that when they voted, they could see the ink bleed through the ballot. Again, this is something that is known by ballot manufacturers, which is why on ballots in the US, and I'm sure in the EU, you don't put something on the back you don't have the areas line up for voting. And so if the ink bleeds through, it does not cause a misvote.

And so several people noticed this and talked about it, but there was no kind of algorithm amplification of this conspiracy theory. Several people pointed it out and a number of people retweeted it, but you can see this line here that in those initial discussions this did not go viral on its own. What happened was a specific influencer, who has a very large following, decided to amplify it and retweeted it – a guy named Charlie Kirk – which started this curve.

And then, when Donald Trump Junior and Eric Trump, the children of one of the candidates, ended up deciding that they wanted to amplify this message, our graph goes vertical. And this should not become a large discussion until those people made a decision. The people who saw that content decided that they wanted to see tweets from Donald Trump Junior and Eric Trump. They made that decision – that is not algorithmic amplification. And if you look at the most effective disinformation during the US election, it was very strongly driven by a small number of influencers.

And so this is my point about the algorithm. You have to separate out the people deciding that they are going to follow somebody and those people now having a lot of power to do amplification versus decisions that are made by the platforms.

Because there is another question about fundamental rights. And one of the fundamental rights that we have as information consumers is to decide what information we want to see. And I think that the challenge here is to balance that fundamental right versus the fundamental freedom from disinformation.

I'm going to hit the other questions as quickly as possible. There's a question about regulating bots. Again bots are a very 2016 kind of issue. There are still bots issues, mostly around fake 'likes' and such. If you're going to regulate bots, I would regulate bots around ad fraud. I think, actually, the most effective use of bots these days is around trying to steal money from advertisers using fraudulent ad clicks, and so I would start there. That's actually a really important issue. The use of a bots in political disinformation is much more mixed.

Should we have a supranational structure for regulation? One of the problems here, like I talked about, is that there's a huge amount of disinformation that is domestic, and so a number of governments are themselves the problem. When we look at the world, we want to try to think about regulation between liberal democracies versus emerging democracies and non-democracies, where governments might try to use that regulation to benefit the ruling party.

And so that's one of the huge challenges I think we have when we look at these problems: what rules do we set that make sense perhaps in France or Germany, but make less sense in Turkey, and no sense in the People's Republic of China?

Do you mind if I go over a little bit, because I had about twelve questions, I think, directed towards me. Okay, I'm going to keep on going until you tell me to be quiet.

A question on enforcing language equally. This is an area where we need a lot more AI research. This is actually a positive use of AI, it's an automatic machine translation in the use of AI to be able to do content moderation in languages that are not spoken as widely by the moderators themselves.

There's a question about the Digital Services Act (DSA). So I don't consider myself an expert in the DSA. When you talk about the risk of fundamental rights, I see this less as a risk to individual fundamental rights and more about the balancing of fundamental rights. And so if you're going to talk about transparency in this area, I think transparency in how companies make decisions to balance between fundamental rights is actually the question you want to ask.

And there's a question about information bubbles. So actually Professor Nielsen is more of an expert in this. In fact, his team has published some great research in this. But the actual quantitative research in information bubbles is much more mixed than the public discussion in that it turns out that the internet does bring people a much broader set of information sources than what they consumed before. The kind of fantasy world of 30-40 years ago where people were able to get information from all over the political spectrum never really existed, and so the information bubble question is actually much more complicated. I'll put a link for one of the things that Professor Nielsen's team published.

There's a question about the line between free speech and illegal content. I think that a really important issue is that all of the big tech platforms will enforce local laws on what is illegal content, but a huge amount of the content that is actually problematic here is not illegal in the local jurisdiction. In the United States, that's a huge amount of it. Even in Europe, though, with your tighter speech laws a huge amount of political disinformation is not illegal in the countries where it's happening. So there is a significant problem here that if you create requirements to take down speech that is not illegal or that is not determined to be legal through a lawful process in a democratic process, you are saying that these companies are the ones that need to make that decision. And so the fundamental difficult trade-off here is that giving them responsibility also gives them the power to make these decisions.

There's a last question about *(inaudible)* manipulation of political parties in the EU. I'll post a link of something that we saw in Poland, for example, that there have been situations in EU elections where you have political groups that try to massively amplify their speech online through fake accounts.

1-067-0000

Chair. – Mr Nielsen, would you like to make any comments by way of a conclusion, after your speech? You will be able to round things off.

1-068-0000

Rasmus Kleis Nielsen, *Professor of Political Communication and Director, Reuters Institute for the Study of Journalism, Oxford University***.** – I will be brief since sadly the technical issue is somewhat distracting me from following the full discussion. There are two specific questions I noted that were directed in my general direction. One was the question of the desirability of creating some form of a must-carry obligation for information intermediaries for public service content in the European Union. This, of course, is something that's been proposed by the European Broadcasting Union (EBU) amongst other actors. I think it's a political question whether that's desirable.

I will offer two research-based qualifications on that decision. One is just to say that the EBU membership includes a wide variety of different broadcasters, some of whom I think we can safely consider to be independent public service media, others that I think researchers would described as state broadcasters controlled by the reigning government of the country in which they reside, and whether one wants to structurally privilege them at the European level, I think it's a complicated decision to take.

The other research-based qualification I would offer on that proposal from the EBU and others is that news is an important but ultimately small part of what people consume on information intermediaries and technology platforms. The companies behind these services have few incentives to prioritise news in general because it's of relatively limited commercial value to them and any obligation to privilege certain information providers will thus necessarily come at the expense of others.

So if one requires these companies to privilege public service media, that will have negative consequences for the reach and traffic that goes to other media, private sector or non-profit, and it's an open question, I think, whether that is good for diversity and I think it's an open question of what the consequences would be for the sustainability of independent, private media. So, the decision is, I can see the rationale for it, but I think there are a couple of complications to consider.

The other question that was directed at me, I think, was around transparency and the challenges for citizens of understanding the economic motives behind the kinds of disinformation that are not politically motivated but simply purely mercenary, driven by the desire to make a quick buck.

Part of this general problem of opacity in the digital environment, and I'm very glad that the Digital Services Act is looking at ensuring greater access for validated researchers in privacy compliant fashions, but some of these problems are much older problems, which is that for a long time, and as was pointed out in 2013 by the EU High-Level Group on Media Freedom and Pluralism, we have had very low levels of transparency on something as basic as ownership of media in many countries in the European Union.

And in fact often it's impossible or very hard for a citizen to determine who actually controls a source of news, not just a random website but even a newspaper or a broadcaster, and if we have that level of opacity and have had it for more than a decade, well over a decade in many countries across the European Union and indeed for many decades in most cases, clearly in that sense the transparency problems we have today are perhaps accentuated in the digital environment but they are hardly unique and hardly new and frankly there's been no real political or regulatory appetite, it seems, in the European Union to, in fact, ensure a more intelligible environment where citizens can understand what the ultimate controlling interests are behind the information that they are presented with.

This, of course, also parenthetically goes for the conspicuous absence of reform or regulation of online political campaigning, where I have to say that the lack of political interest in regulating political speech online is sometimes, I think, striking from the point of view of individual citizens.

The final thing I'll say in my concluding remarks is that, while I think it's clear that there is room for improvement in terms of what research suggests could help create a more robust environment and a more resilient public against various forms of disinformation and problematic speech online – I've outlined some of the options in my remarks today, I'll share the full text with your team members and post it probably as well – and thus, we have some real opportunities ahead of us if we decide, as societies, that we believe it's important to commit publicly and public resource to strengthening our democracies against the challenges that we face.

We have some very real opportunities to do so; there are clear options available. It's a political choice whether we believe that this is the right thing to do, or not, and research can inform those choices, but the choices should be made by elected officials such as yourselves. So, there are opportunities ahead of us and real options on the table. None of them are easy, none of them are simple and none of them are cheap, and I realise that if I was an elected official, I would probably prefer things that were cheap, simple and easy to ones that are complex, expensive and often slow and sometimes controversial. Nonetheless the options are there nonetheless, and it's a choice what we decide to do as societies.

I will also end on a sort of a happier note, just to say that I think when we look across the world, it's worth noting that while there is a lot of room for growth in the years to come, I think it's important to recognise that the European Union has taken some important steps in using its soft power to convene collaborations with different private sector players and across different industries and with civil society around addressing problems of disinformation. And when we look at equally complex policies, whether in the United States or in Brazil or in India, the absence of such initiatives is conspicuous. And in that sense, the European Union has achieved more than its peers around the world.

I would also note, coming from a small country myself, that while I expect the private companies that are most in the limelight in this discussion, Facebook, Google, a much smaller company like Twitter, to have done many of the things that they have done in the European Union in large and lucrative markets such as Germany or France, I think we have few if any reasons to believe that they would have taken similar steps and made similar investments in small and less lucrative markets and when they have, I don't think we can understand why without recognising that the European Union has played an important role in that.

I think we can hope for more and expect more and demand more, also of these companies, just as we can of elected officials and policymakers, and in that sense, I think the striking difference between the level of access and collaboration that’s been offered around research around the US election in 2020 versus what we have seen in Europe suggests that also policymakers like yourselves who may want better evidence to base your decisions on can hope that, in the future, these companies will collaborate, not just with researchers at prestigious universities in the United States, but also with researchers elsewhere. And ideally, researchers in smaller countries in Europe and countries in Europe where the language is not English or French or German so that we can understand the differences in the disinformation problems we face in different parts of the Union and address them on the basis of up-to-date evidence, and I very much hope that your work in these committees can help drive that development, so we can move towards a better environment in the future.

Closing remarks

1-070-0000

Chair. – Thanks to all three of you for your presentations and your replies. I would also like to thank the members of the Special Committee on Artificial Intelligence in a Digital Age (AIDA) and the Special Committee for foreign interference in all democratic processes in the EU, including disinformation (INGE); the interpreters; the technicians; the AIDA Committee Secretariat and the INGE Committee Secretariat.

I would like to inform you that the next meeting of the INGE Committee will take place on 10 May. I wish you an excellent evening, and thank you.