High-Level Hearing

Preserving Democracy in the Digital Age

22 February 2018
15h00 – 17h00

Berlaymont, Rue de la Loi, 200
Jean Rey, 1st Floor

European **Political Strategy** Centre

Report from the High Level-Hearing:

Preserving Democracy in the Digital Age

Introduction

'Fake news' and disinformation spread quickly in the digital age. By the time they can be exposed and skewed narratives corrected, our democratic fabric is already damaged. Trust in the very concepts of truth, fact and reality is undermined. Even worse, elections might be manipulated or swung. What are the steps that should be taken to contain the threat of disinformation? What is the role of public authorities, media outlets and social media companies? What is the ultimate goal of disinformation and how does it aide illiberal regimes and actors? And how can the emerging 'attention economy' be made compatible with quality media and well-informed citizens?

On 22 February 2018, the European Political Strategy Centre hosted five leading international experts for a High-Level Hearing on 'Preserving Democracy in the Digital Age' to intellectually accompany the European Commission's ongoing public consultation on 'fake news' and online disinformation. During the Hearing, the experts were asked to address a set of predetermined questions with the knowledge that a full transcript of the Hearing would be submitted as a public contribution to the consultation.

The experts included:

- **Anne Applebaum**, Pulitzer-Prize Winning Author, Columnist, Washington Post and Professor of Practice, London School of Economics
- **Philip Howard**, Professor of Internet Studies and Director of Research, Oxford Internet Institute, University of Oxford
- **Rasmus Kleis Nielsen**, Professor of Political Communication and Research Director, Reuters Institute for the Study of Journalism, University of Oxford
- **Philip Lelyveld**, Project Director on Immersive Experiences, Entertainment Technology Center, University of Southern California
- **Keir Giles**, Senior Consulting Fellow on Russia and Eurasia, Chatham House and Director, Conflict Studies Research Centre

The Hearing was moderated by **Ann Mettler,** Head of the European Political Strategy Centre, and **Ulrik Trolle Smed**, Policy Analyst at the European Political Strategy Centre.

The full replies can be found in the transcript. As a 'teaser', the first section will provide some highlights and quotes from each speaker in response to each question. These have been selected by the European Political Strategy Centre.

Contents

Hearing Questions and Structure

During the Hearing, the experts were prompted to reply to six main questions, including a number of sub-questions, and shared with the speakers ahead of the event. The questions were drafted by the European Political Strategy Centre for the purpose of stimulating the discussion. The questions provide no indication as to the European Commission's views on the subjects discussed.

Here are the questions:

1. Please state your name and affiliation; please flag any potential conflict of interest (e.g. if you are providing consulting services to a client potentially affected by the European Commission's initiative on 'building a European strategy to tackle 'fake news' and disinformation online', please state so). Please describe your background and your experience in dealing with 'fake news' from a public policy perspective.
2. What are your general views on global trends linked to the emergence of 'fake news' and related issues?
3. Based on your professional experience and research, what has caused the spread of 'fake news' online and what evidence do we have of its impact on democracies, societies and economies?
4. Based on your professional experience and research, which initiatives do you believe are necessary to tackle fake news online and its related issues?
5. Do you believe the European Commission's initiatives to tackle 'fake news' online and related issues are sufficient?
6. In a nutshell, what is your main message to the European Commission regarding what should (or should not) be done about 'fake news' and disinformation online?

Highlights from the Hearing

Highlights have been selected by the European Political Strategy Centre.

What are your general views on global trends linked to the emergence of 'fake news' and related issues?

Rasmus Kleis Nielsen

'I prefer the term 'disinformation' [...] to the term 'fake news', which is poorly defined, politicised and misleading. It is poorly defined, unless used in narrow sense – as false and fabricated content masquerading as news [...] the broader problems of disinformation, which I think of as intentionally misleading and often false or inaccurate information produced either for profit or for political purposes, must be understood in the political and media context.'

Anne Applebaum

'Disinformation campaigns can be run by anybody, by political parties, commercial companies [...] the rise of social media and anonymity on the internet have enabled large-scale disinformation campaigns which deliberately launder false information. Often, although not necessarily only, the campaigns seek to promulgate extremist ideas and then amplify them further using social media, trolls, bots and tricks designed to manipulate search engines.'

Philip Lelyveld

'We increasingly live in a constructed reality that blends the virtual and the real. This is not new. The telephone is a teleportation device for your voice. It delivers a disembodied virtual 'you' into someone else's reality, and vice-versa. Given enough stimuli, enough multisensory input, the virtual can become indistinguishable from the real.'

Keir Giles

'Let's go back just over 2,000 years and see what Cicero said about disseminators of fake news; he said: 'He speaks in accents familiar to his victims, wears their face and their arguments, rots the soul of a nation, and infects the body politic so that it can no longer resist.' I mention this because all of those terms are met in today's Russian doctrinal writing on the power of information warfare.'

Philip Howard

'The strategy was to seed multiple conflicting, even ridiculous, stories in a population in an uneven way with the goal of getting different people to believe different things [...] these conflicting messages essentially create an atmosphere of uncertainty and sufficient uncertainty to ever act [...] We were surprised to see the Russians practicing this communications technique in their neighbourhood, neighbouring countries [...] We were then surprised, again, to see politicians in the West using the same communication strategies on their own voters.'

Based on your professional experience and research, what has caused the spread of 'fake news' online and what evidence do we have of its impact on democracies, on societies and on economies?

Rasmus Kleis Nielsen

'Digital media has made it easier to publish and share any kind of information, including disinformation. So, we need to see the growth in the amount that disinformation is being published and circulate in our societies against the backdrop of a general exponential growth in the overall amount of all kinds of information circulating. Pedlars of disinformation are using often the very same digital media analogies that entirely legitimate political actors, news media publishers, civil society organisations, governments and private companies are using. The same tools are empowering various forms of hate groups as are powering the #MeToo movement and the Never Again movement.'

Anne Applebaum

'Whatever you think about their objectivity or lack of it, traditional newspapers and broadcasters created the possibility of a national conversation – a single debate as well as mechanisms to hold politicians to account. The disappearance of those news sources in a number of countries has led to polarisation and made political debate impossible.'

Philip Howard

'Consumption of 'junk news' is actually at the lowest amongst western democracies in Europe. In the US, we found a one-to-one ratio between 'junk news' and professional news shared over social media during the 2016 election. In France during the election there were seven pieces of professionally produced news for every piece of junk. In the German and UK elections it was about a four-to-one ratio. So, for the most part, 'junk news' does not find quite as large an audience in Europe as it does in other parts of the world.'

Keir Giles

'It is a key part now of Russian military doctrine and strategy for winning the conflict that they already perceive themselves to be in with the West in general - with NATO and the EU in particular. It's implemented by the very top hierarchy of the Russian leadership down through its media organisations to the very junior-most foot soldier in the Kremlin troll army. It doesn't necessarily need to be about targeting elections or referenda. Disinformation operations aim to undermine the whole system of liberal democracy and to sow and to amplify distrust in credible sources of information whether it is government or establishment mainstream media in order to influence the geopolitical direction of a country and of intergovernmental organisations.'

Philip Lelyveld

'Tools and techniques to engage our attention, and to understand and influence us, individually, on both a conscious and subconscious level, are being invented and refined in offices, test labs, and basements around the world. Expect to see them as either standalone products and services or embedded into other products and services – including entertainment experiences and advertising – as they prove useful.'

Based on your professional experience and research, which initiatives do you believe are necessary to tackle 'fake news' online and its related issues?

Rasmus Kleis Nielsen

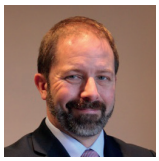
'We should remember in terms of professionally produced journalism, it is still the case that two thirds of investment in professionally produced journalism comes from print publishers. We need to renew these institutions to ensure that professional journalism can continue to play a vital role in our democracies moving forward.'

Philip Lelyveld

'Rather than try to stop 'fake news', I propose that we focus on mechanisms that identify, protect, and elevate what is most probably true and undistorted. To recognise and reward sources for being trustworthy. One approach would be to tie all posts back to their online identities [...] This approach won't directly take a person out of their personal echo chamber of ideas, but it could give them a sense of the trustworthiness of the sources.'

Anne Applebaum

'Without question, anonymity – whether it takes the form of about fake accounts or even non-human bots on Twitter or Facebook, or fake and misleading websites – gives almost complete freedom to people who are driven by anger or greed or ideology or financial interests. It's the primary tool that Russian and alt-right propagandists have used to create fake websites that echo and repeat stories or to artificially amplify false and damaging narratives.'



Keir Giles

'The first and most effective response to hostile subversive and destabilising activity is and always has been raising public awareness – and here the role of key leaders is absolutely crucial. Statements by senior figures like prime ministers and defence ministers recognising a state of conflict and the challenge have been shown in the front-line states to be an extremely powerful tool in empowering not only government but also society and media to take steps to protect themselves.'

Philip Howard

'We need a regular system of algorithmic audits. We audit video gambling machines, we audit financial trading algorithms, all in ways that don't violate the intellectual property of those technology firms. There is no other domain of business in which a company can design and build something, release it to the market and change the product only when somebody complains. A system of regular algorithmic audits would allow us all to restore trust in the social media systems that many of our citizens now value.'

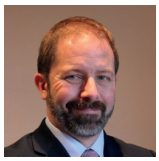
Do you believe the European Commission's initiatives to tackle 'fake news' online and related issues are sufficient?

Rasmus Kleis Nielsen

'It is striking how little we know from independent evidence-based research about the scale, scope and consequences of problems of disinformation and 'fake news' across Europe and I find it deeply disturbing that we are considering policymaking and intervention without actually first providing an evidence base of some sort.'

Philip Howard

'The greatest opportunity you probably already have is to set up data sharing arrangements between social media firms and the European Research Council. Facebook doesn't collaborate with researchers [...]. Researchers who do try to work with Facebook always sign non-disclosure agreements and can never publish replication data. The most important science journals require replication data so the most important social scientists with the biggest questions don't turn to the most important source of data.'



Keir Giles

'East StratCom. This is a critically important capability for responding to threats to democracy and our institutions, which at present appears scandalously under-resourced and under-empowered [...] Meanwhile, the opposition is throwing ever more resources and people into the kind of tactics and procedures that East StratCom is attempting to counter. Despite the constraints and despite the tiny budget and numbers, East StratCom does have a very high reputation among the expert community.'

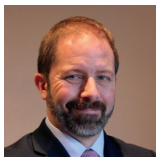
Anne Applebaum

'One possible solution might be to take East StratCom out of the EEAS, where it seems to be an uncomfortable fit with diplomats who have other interests and want to have different kinds of conversations about Russia, and move it into another part of the EU [...] Preferably this should be some part of the European Commission which deals more properly with matters of internal politics – either EU strategic communications or internal security bodies.'

Philip Lelyveld

'The storytelling arts and sciences have regularly evolved to keep up with the rising sophistication and expectations of our audiences. Similarly, if you are going to detect and respond to the outsider innovators and storytellers propagating targeted psychological manipulation tools including 'fake news', then you have to put in place technical and social processes that can also evolve to stay one step ahead of them, and that contribute to helping the average citizen make informed decisions based on reliable data.'

In a nutshell, what is your main message to the European Commission regarding what should (or should not) be done about 'fake news' and disinformation online?



Keir Giles

'First, recognise the threat – admit at the highest political level that there are hostile actors who wish to do us harm. Next, gather the evidence [...] find out what is working when they try to do us harm and what is not. Third, decide whether or not you want to win that fight or allow democracy and institutions to be fatally compromised by those adversary tactics that are actually succeeding. Next, in order to do that, adequately resource the response in terms of time, expertise, staff, political buy-in and support and endorsement of defensive measures (again at the highest level) and money over the long term because this is not a current crisis, this is a new reality.'

Anne Applebaum

'I believe that the European Union should focus on the problem of anonymity. Most disinformation campaigns operate thanks to anonymity, thanks to the fact that it's so easy to create fake websites, fake online personas, even armies of fake bots actually that aren't even people, they are computer code. The EU can take a really important step forward by investing in the ideas of online passports and online e-identities, as well as verified email and flags for anonymously created websites. The Commission can put pressure on the tech companies to create these products, and even sponsor them outright. These are measures that can enhance the lives of ordinary people, and could come to be seen as an advantage to European citizenship.'

Philip Howard

'I think if we want to do something positive for reinventing and reinvigorating our democratic cultures, guiding markets and how they should behave will be the softer-touch method that is preferable over content regulation. I would try to argue that guiding these markets involves creating a system for reporting the beneficiaries of data from our profiles and our technologies. A system of civic data donation so that we can express ourselves as citizens when we want to. We need a digital infrastructure that tithes for the collective good. We need to extend the non-profit rule and we need algorithmic audits before these technologies roll out into public life [...] To get us out of the democratic deficit we're in, we must make policy not just for the Internet we have, but for the one that is coming.'

Rasmus Kleis Nielsen

'If you want to renew our democracy for the digital age, I think we should focus on reinforcing our commitments to the fundamental values that characterise open societies and see what we can do to support the evolution of institutions that enable citizens to make the most of that freedom and those rights [...] This is not about neat, polite and genteel political debate. It is about fundamental rights and institutions that enable citizens to make the most of them. When we think about how respond to problems of disinformation. I think we should therefore first be cautious with regulation or the privatisation of policing of political speech that may compromise the very values we are trying to defend. We can consider these measures but we should be very cautious.'

Philip Lelyveld

'Innovation is never stifled. It is only redirected by regulation, the bottom-line imperatives of business, and societal forces. A good story captures and holds your attention. A great story creates 'sticky' memories by engaging your emotions. We are well on our way to developing and deploying the tools that will allow anyone to create and distribute personalised 'sticky' memories on a global scale. The tools don't care whether the story is fact or fiction, true or false. It may make more sense to create a system that identifies, elevates, and rewards a bounded set of data, information, and knowledge that we can verify to be true, reliable, and undistorted, than to try to detect and react to an unbounded flow of false, distorted, and fake content.'

Full Transcript of the Hearing

Highlights have been selected by the European Political Strategy Centre and approved by the speakers.

Welcome

Ann Mettler:

Good afternoon. It is my pleasure to welcome you to this Hearing on 'Preserving Democracy in the Digital Age'. My name is **Ann Mettler**, and I am the Head of the European Political Strategy Centre, the European Commission's in-house think tank. To my left, I am joined by **Ulrik Smed**, Policy Analyst in our foreign affairs team at the EPSC, who is also our lead on the topic of 'fake news' and online disinformation.

In November 2017, the European Commission opened a public consultation on 'fake news' and online disinformation and in January of this year launched a High-Level Expert Group on 'Fake News'.

Today's Hearing is very much an effort to contribute to these ongoing activities, and that is why I'm absolutely delighted to welcome such a high-level group of experts who will help us today shed light today on the challenge of 'fake news' and disinformation.

Before we start the Hearing, let me briefly give you some instructions and information:

The Hearing will last two hours until 5 o'clock. Each speaker will have a certain amount of time to address each question. Speakers were provided with an extended list of questions ahead of this meeting so that they could prepare.

The Hearing will be on the record and a full transcript of the Hearing will be submitted as an EPSC contribution to the public consultation on 'fake news' and online disinformation.

Given the format, I would appreciate if the audience would be in full listening mode – as no interaction with the speakers during the Hearing will be allowed. However, there will be an opportunity for an exchange of views after the Hearing is over, at 5 o'clock when we will be serving coffee outside of this room.

Two more announcements:

One minute before the time limit of a session expires, we will signal this by showing an orange card. Once, you have used up the maximum time allotted to a question, you will be shown the red card. Once that is shown, we ask you to conclude your remarks – or, if you take a bit longer in one question, we ask that you reduce your time accordingly in another question.

Also, please note we are rotating the order in which speakers are called on, so the order will be different for each question, so we do not always have the same people starting or concluding each question round.

We will now start with the Hearing.

Question 1: Introductions

Ann Mettler:

Please state your name and affiliation. Also, please flag any potential conflict of interest and please state if you are providing consulting services to a client potentially affected by the European Commission's initiative on 'Building a European Strategy to Tackle 'Fake News' and Disinformation Online'. Please describe your background and your experience in dealing with 'fake news' from a public policy perspective. You will have one minute maximum each.

And the first one to speak will please be Mr Giles.

Keir Giles:

Thank you, good afternoon. I am Keir Giles, I work with Chatham House in London and also with Conflict Studies Research Centre, which is a small group of subject matter experts which used to belong to the UK Ministry of Defence. I have no conflicts of interest, I have no consultancy; my background in journalism was 12 years with the BBC. My primary area of expertise now is Russia and how Russia projects power, including the use of information warfare and including within that what we are now referring to as 'fake news' and how it is used and abused. This is something I have been studying since Russian information warfare doctrine re-emerged in its current form just under a decade ago. I have published on the subject through Chatham House and through various parts of NATO describing what Russia is doing and also, in some cases, predicting what it is going to do next.

Ann Mettler:

Excellent, thank you. Professor Howard.

Philip Howard:

Thank you. My name is Philip Howard, I am a professor at the Oxford Internet Institute at Oxford University. I've been working in this domain for ten years or so, we have published several books several kinds of studies and our research has been funded by the European Research Council. In the last few years we have studied the role of automation and 'junk news' in the French election and the German election and the Brexit vote and then the UK election. We have done multiple studies on political learning in the United States and all in all have studied some 26 around the world investigating the role of government expenditures and political party expenditures in manipulating voters, both in their own countries and in the countries of their neighbours and countries around the world. I have no conflicts of interest and no consultancies to report. Thank you.

Ann Mettler:

Thank you so much. Professor Nielsen, please.

Rasmus Kleis Nielsen:

My name is Rasmus Kleis Nielsen, I am Director of Research at the Reuters Institute for the Study of Journalism and Professor of Political Communication at the University of Oxford. I lead a research team that works across issues in how citizens use news and media across the world; around how news organisations are adapting to an increasingly digital media environment; research on the role of platform companies in this environment and a new programme of research on disinformation online. Our research is supported by a wide variety of different actors that include media regulators, media companies, technology companies, non-profits and academic research councils.

Ann Mettler:

Thank you. Mr Lelyveld, please.

Philip Lelyveld:

My name is Philip Lelyveld, I have no conflicts of interest or consultancy conflicts to report. I run the Immersive Media initiative at the Entertainment Technology Center within the University of Southern California School of Cinematic Arts. Prior to joining the centre I spent 10 years leading initiatives related to the future of entertainment for the Walt Disney Company's corporate strategic planning group. I am here to discuss my current thoughts on how entertainment technology and the language of storytelling fit into the 'fake news' landscape and vice-versa.

Ann Mettler:

Thank you – and finally, Professor Applebaum, please.

Anne Applebaum:

Thank you. I am Anne Applebaum, I am a journalist and a historian, I have written several books about Soviet and East European history. A couple of years ago, in 2014, I began running a programme on 'New Forms of Propaganda' at a London think tank; I now run ARENA, which is a programme inside the London School of Economics, which looks at 21st century propaganda and disinformation campaigns, running projects that analyse how disinformation campaigns polarise societies and seeking ways to help journalists reach polarised audiences. Together with my co-director, Peter Pomerantsev, we have served informally as advisers on this issue to members of the US Congress and the UK Parliament, we have advised the US and British governments on counter-propaganda strategy, we have also advised senior officials, for example the US under-secretary for public diplomacy, and helped to shape programmes at the British Foreign Office, National Endowment for Democracy and European Endowment for democracy. I have no conflicts of interest and I do not serve as a consultant to any tech companies.

Ann Mettler:

Thank you so much, I will now hand over to Ulrik, please, for the second question.

Question 2: What are your general views on global trends linked to the emergence of 'fake news' and related issues?

Ulrik Trole Smed:

Thank you very much everyone, we are very happy to have you here. Now let us get started with the Hearing. Now we proceed to the second question on the context of 'fake news'.

What are your general views on global trends linked to the emergence of 'fake news' and related issues? You will have 5 minutes maximum each. The first one to speak will be Professor Applebaum. Please go ahead.

Anne Applebaum:

Thank you very much. 'Fake news' is an imprecise term which is now so overused that is unfortunately becoming meaningless. It can mean clickbait, rumour and gossip, which for economic reasons has replaced what used to be legitimate journalism in some outlets. It also now seems to mean genuine mistakes made by legitimate journalists.

What I am going to speak about in my brief remarks is something different, namely the way in which the rise of social media and anonymity on the internet have enabled large-scale disinformation campaigns which deliberately launder false information. Often, although not necessarily only, the campaigns seek to promulgate extremist ideas and then amplify them further using social media, trolls, bots and tricks designed to manipulate search engines. **Disinformation campaigns can be run by anybody, by political parties, commercial companies. The techniques that they use have been created by the advertising mechanisms that are an integral part of social media; by data collection; by algorithms that help create polarised audiences; by targeted and un-transparent advertising**. But since I am speaking here at the EU, I think it is important for this audience to

focus on one particular disinformation campaign, namely the one which currently targets the European Union, as an institution, and its core values. For the past decade, the Russian state has been seeking to undermine European solidarity and European democracy. Not just through online activity but through the funding of anti-European political parties, through the use of bribery and corruption to suborn centrist parties and more generally through the promotion of anti-European, anti-democratic (usually far-right, but sometimes also far-left) movements in almost every European country. More recently, they have sought to amplify the reach of these movements through social media, using both professional and internet trolls as well as automated networks of bots – computer code designed to mimic human interactions.

These are the same techniques that were used in the US election in 2016. Most of you will have seen the recent indictment of thirteen Russians from the St Petersburg troll factory, and this kind of activity of course takes place in Europe too. **Although we can debate about their sophistication, there is no doubt that Russia runs disinformation campaigns in nearly every European country, tailored to that country's politics, mostly promoting divisive messages designed to have an echo among particular groups**. As I have said, they take advantage of particular qualities of social media, which by its very nature polarises and divides society, provides opportunities for targeted advertising aimed at enervating or enraging particular groups, and offers multiple opportunities to create fake identities, bot armies, and computerised accounts which can give a false picture of reality.

In this endeavour, Russia does not act alone, it increasingly acts in concert with an international consortium of online alt-right activists, some of whom have connections to real-life far-right groups. It is not possible to describe this as coming from inside or outside of Europe since both of them now act in tandem. My team at the London School of Economics tracked their interaction, for example, during the German election campaign. We discovered Russian and alt-right professional trolls meeting in chat rooms and exchanging memes and tactics. They promoted one another's stories and narratives, sometimes completely independently. I would emphasise, though that it is a great mistake that these kinds of campaigns only matter during elections. In fact, they have much longer-term goals and they are operational all the time.

At the moment, this kind of disinformation comes from Russia, but it can come from somebody else next week. Any EU strategy– will have to deal with it on two levels. First, it will have to look critically and broadly at the structure of the platforms and their advertising tools in order to understand how these campaigns have been enabled. I am going to suggest in my later remarks a couple of things that I think the EU could do particularly. Secondly, I think it will have to focus on the particular nature of the Russian campaign, which has online and offline components, and I will offer more suggestions in later statements. Thank you.

Ulrik Trolle Smed:

Thank you very much, Professor Applebaum. Next will be Professor Howard – please go ahead.

Philip Howard:

Thank you. My team at Oxford University and I started studying the problem of 'fake news' – or, the term I will start to use is 'junk news' – in 2014. **As many of you may recall, this is the summer that the Malaysian Airlines flight was shot down over Ukraine.** I was living in Budapest at the time and noticed that my Hungarian friends were getting multiple conflicting messages – they felt – from Russian origins about what had happened when the plane was shot down.

The first of the stories was that democracy advocates in Ukraine shot the plane down because they thought Putin was on the plane and that he was flying from Holland to Malaysia. The second story was that Americans have shot the plane down – this was another story passing over Facebook's networks of friends and family amongst my Hungarian associates. The third story – easily my favourite – is the story of a lost World War 2 tank that had come out of the dark forests of Ukraine. Confused, it spotted the plane and shot the plane down.

It was clear at this moment, at the very early stages of our research, that the strategy was fairly deliberate. The strategy was to seed multiple conflicting, even ridiculous, stories in a population in an uneven way with the goal of getting different people to believe different things. And most of my Hungarian colleagues knew that these were Russian-origin stories, but **they worked in the sense that there was not one oppositional narrative for people to respond to – there were multiple narratives to respond to – and that these conflicting messages essentially create an atmosphere of uncertainty and sufficient uncertainty to ever act.**

Now what has come out of the last few years is a much more pernicious problem. **We were surprised to see the Russians practicing this communications technique in their neighbourhood, neighbouring countries. We were then surprised to see that these communication techniques were used by the Russians against voters in democracies in very direct ways in some of the world's strongest democracies. We were then surprised, again, to see politicians in the West using the same communication strategies on their own voters.**

So, this has very much become a problem that has leaked from Russia to other countries – certainly to other authoritarian regimes, but also to other democracies. That makes it a very difficult regulatory challenge for us and to help figure out what to do about it, my team and I has been working on trying to evaluate the impact of 'fake news'. It turns out to be very difficult to operationalise, to define 'fake news' – it is too hard to look at a piece of journalism and figure out how much fact-checking went into that article, went into that piece.

So, we have developed a five-point definition that is much more about evaluating the source of the news, the source of the information. We have five criteria:

1. professionalism;
2. style;
3. credibility;
4. bias; and
5. counterfeit.

The professionalism of a news outlet is fairly straightforward to evaluate in many cases. These outlets do not employ the standards and best practices of professional journalism. To decide what is not a professional outlet: they refrain from providing clear information about real authors, real editors, publishers and ownership structure. They lack transparency, accountability and do not publish corrections on debunked information.

The second point of evaluation for us is in style. These outlets use emotionally driven language with emotive expressions, swearwords, headlines in all-capital letters, hyperbole, *ad hominem* attacks, misleading headlines, unsafe generalisations, logical fallacies, moving images, graphic pictures and mobilising memes.

Our third criteria for defining 'junk news' involves credibility. **A low-credibility outlet relies on false information and conspiracy theories, which they often employ in strategic ways. They report without consulting multiple sources and they do not employ fact-checking methods. Bias appears in reporting from outlets that are ideologically skewed and hyper-partisan.**

The counterfeit examples are the most straightforward to identify: they are the ones that present news – or commentary as if it is news – in the BBC colours or in the New York Times font.

I want to conclude by saying that I think Europe is doing fairly well or is at least in a good position to address these things. The European Research Council has made several investments in several long term projects to study problem of 'junk news'; the EU is already showing leadership with these kinds of consultations, leadership that we do not see in other western governments. I believe there is a larger research community in the US looking into these problems, but I don't believe that they are further along in identifying the nature of the problem and defining it.

And in our comprehensive studies across multiple countries, we found that the consumption of 'junk news' is actually at the lowest amongst western democracies in Europe. In the US, we found a one-to-one ratio between 'junk news' and professional news shared over social media during the 2016 election. In France during the election there were seven pieces of professionally produced news for every piece of junk. In the German and UK elections it was about a four-to-one ratio. So, for the most part, 'junk news' does not find quite as large an audience in Europe as it does in other parts of the world.

Thank you.

Ulrik Trolle Smed:

Thank you very much. Next is Professor Nielsen.

Rasmus Kleis Nielsen:

Thank you very much. I think that we need to start from the top here.

This Hearing is about 'preserving democracy in the digital age', and before I turn to the issues of 'fake news' and disinformation, I want to be clear that the main challenges to democracy today are the erosion of the institutions that have historically enabled citizens to take part in popular government – political parties, member-based interest groups and news media – and the fact, secondly, that some ill-intentioned political actors, including foreign governments but sadly also some political actors in the European Union itself are not committed to the fundamental values that define democratic governments and open societies. And problems of disinformation must be understood in this context, and responses that are aimed at preserving, or rather even renewing, our democracy for the digital age need to tackle these broader issues and not only be narrowly related to disinformation.

I prefer the term 'disinformation', like many of the other panellists, to the term 'fake news', which is poorly defined, politicised and misleading. It is poorly defined, unless used in narrow sense – as false and fabricated content masquerading as news, which is a smaller subset of the wider problem that people are concerned with. It is politicised in the sense that it is a term that is used by politicians to attack and undermine the credibility of independent news media trying to hold them to account. And it is misleading because much of what we discuss under the headline of 'fake news' is neither fake – it can be genuine content put to malicious use, taken out of context, strategically deployed – and nor news for that matter. It can involve trolling, amplification, promotion, sharing and the like and it is news in any meaningful sense.

So, the broader problems of disinformation, which I think of as intentionally misleading and often false or inaccurate information produced either for profit or for political purposes, must be understood in the political and media context. That context today is one, politically, of low trust in many institutions across much of the European Union (there is significant variation, but we see low in many countries) and high levels of partisan polarisation in some, but not all, Member States. In this context, people do not know who to trust and they resort to motivated reasoning and self-selection, rather than taking part in joint discussions or trusting shared institutions. The media context is a move to an environment where people increasingly find news via third party platforms, products and services like search and social media. By now, two thirds of online news users regard search engines or social media or other forms of distributed discovery as their main way of finding news online. In this environment, people approach information with 'generalised scepticism' – they do not trust most of the institutions they rely on (we have copious amounts of evidence to document this) and often they do not even recognise or even remember the brands behind some of the information they come across, in particular when they come at it sideways via search or social.

The results of this change – low trust and the move towards a more distributed media environment where platforms lead people to content, sometimes content people do not know where it comes from – lead to an often rambunctious political and public sphere, but we should remember that does not necessarily mean that that rambunctiousness is a threat to democracy. No one ever promised us that our politics would be polite, or that public debate would be genteel.

Narrowly defined as for-profit or politically-motivated demonstrably false and fabricated content masquerading as news, so far research in Europe suggests that this has more limited reach than one might fear – especially on the open web – though it is clear that in France and Italy some false news pedlars generate a lot of engagement on social media, in particular on Facebook, so there are clearly issues that need to be confronted. But we need to get a sense of the scale and scope of the problem and not exaggerate this to further undermine citizens' confidence in our political and media institutions.

Much of this content is driven by political actors – foreign, but some of them domestic – some of it is driven by news media (clickbait, hyper-partisan opinion) and some if it by civil society. It is important to underline that much of this might be uncomfortable and undesirable, but it is not necessarily illegal, nor necessarily a threat to democracy, and it is not easily identified in an objective way. Because it is not simply a matter of true or false – it can also be wild exaggeration or highly opinionated opinions.

In my view, our best response to how we make sure that we can renew our democracies is to deal with these problems of disinformation that we face in this larger context of political threats and the erosion of some of our institutions is to protect our open societies by renewing our commitment to the fundamental rights that define the European Union, which includes the right to receive and impart information and views – also views we do not necessarily find comfortable or agree with – and then work to renew the institutions that enable citizens to make the most out of these fundamental rights, including news media. I will offer some concrete suggestions as to what can be done in that area.

Ulrik Trolle Smed:

Thank you very much, rich discussions already. Mr Lelyveld.

Philip Lelyveld:

Thank you. I am going to define 'fake news' as 1) verifiably false and 2) partially reported information taken out of its original context. I would like to mention two related terms; disinformation and propaganda. Law Professor Peter Kruger says disinformation is about changing the actual facts into fictional facts; propaganda is about getting you to ignore facts and make emotionally-biased conclusions. Disinformation is actual 'fake news'; propaganda is spin.

I am not going to discuss propaganda, but I am going to talk about the power of emotion as I discuss how we got here, from the storytelling perspective, in five points.

Point 1 – Historically the creation and distribution of tools for storytelling have been developed and refined for the professional market, then simplified and released to the consumer market. Think still cameras and movie cameras, camcorders, but also audio and video editing tools, filters and effects generators, etc. While originally developed to meet the special needs of a niche community, these tools have become general purpose tools useful for all sorts of unintended purposes; some constructive and some destructive to society. In addition to this, with the birth of the Maker Movement, we also have tools being developed at the grass roots level by citizen-inventors and creators that are adopted by the professional community. Innovation is alive and unconstrained.

Point 2 – **At the birth of the Internet, Mitch Kapor said: 'Architecture is politics.' The Internet was architecturally designed with a political intent; to be immune to any attempt by government or other forces to control it. An intended element of this is online anonymity. The founders wanted to protect free speech and political protest. As a result, on the internet nobody knows that you are a dog, or a bot, or one person masquerading as a crowd.** Associated with this, global online culture as reflected by the Creative Commons and Open Source movements strongly object to any efforts to embed Intellectual Property controls into the infrastructure of the Internet. The unconstrained flow of data, including valuable IP, helped steer innovation towards the use and monetisation of this data. Mashup Culture delivered yet another ecosystem of creative tools and resources to both the professional community and the global public.

Point 3 – Let us talk about business models and the attention economy. There are only three business models: I pay, you pay, they pay. I am not paying for you. You are not paying when you have been conditioned to expect things for free. They, the advertisers, are willing to pay in exchange for your willingness to give away a rapidly growing amount of your personal data. But they want your attention. **A good narrative, whether it is an ad, a fictional story, or news, creates 'sticky' memories when it engages you emotionally. Extremes in character, plot, and theme are more memorable and sticky, regardless of their rationality, reasonableness, or truthfulness.**

Point 4 – Quality Control has been discounted, or at least redefined, as the narratives we experience have gone real-time and we are presented with a continuous flood of new experiences to choose from. In the 24-hour news cycle we barely notice corrections.

Point 5 – **We increasingly live in a constructed reality that blends the virtual and the real. This is not new. The telephone is a teleportation device for your voice. It delivers a disembodied virtual 'you' into someone else's reality, and vice-versa. Given enough stimuli, enough multisensory input, the virtual can become indistinguishable from the real.** As the tools for creating alternate versions of the world and the people in it become widely available, we are left with Morpheus's line from The Matrix: 'Real is simply electrical signals interpreted by your brain.'

The open question that I suggest we focus on is, in a world where everything can be faked, and where everyone has the tools to create and distribute fake, how do we identify and protect the real?

Thank you.

Ulrik Trolle Smed:

Thank you very much, Mr Lelyveld. And finally, Mr Giles.

Keir Giles:

The term 'fake news' is a relatively recent invention. The problem it refers to of course is anything but new. I don't expect the term 'fake news' to be long lived. I think just like the phrase 'hybrid threats' before it, it's been so widely abused as to be effectively meaningless now. So, it is useful for urgently drawing attention to the problem, but the shelf life of the buzzword is going to be much shorter than the problem is going to last for. In a way it doesn't matter whether it is new or not. Just because it is presented sometimes as not a new problem is not a reason to ignore it. We might as well say that war has always existed therefore we need not pay attention to the danger of the outbreak of war. **Let's go back just over 2,000 years and see what Cicero said about disseminators of 'fake news'; he said: 'He speaks in accents familiar to his victims, wears their face and their arguments, rots the soul of a nation, and infects the body politic so that it can no longer resist.' I mention this because all of those terms are met in today's Russian doctrinal writing on the power of information warfare.** Now just as then, adversaries use this deliberately and in an organised manner. And unless this problem is addressed urgently, it is going to get worse fast. **It is surprising that we have not as yet seen widespread deployment of fake video and fake audio to authenticate news reports but we know that this is possible.**

So, in the case of Russia this may well again be stockpiling and preserving capabilities that are already in hand until a suitably important event comes along to deploy them, as we saw in advance of the US presidential elections. But we're already in a situation where we cannot take common acceptance of facts for granted. We're already in a space where events that we all recently lived through have to be proven again and again against a cacophony of disinformation.

It's not all about Russia. **We don't just have hostile actors from outside the EU space projecting disinformation and subversion into the EU area. There are also home-grown extremists who utilise the same techniques as for example Islamic State - now almost exclusively an online operation. But those**

problems that emanate from within our own countries are dwarfed by the organised campaigns coming from outside. That doesn't mean they don't use the same techniques. Russia, Islamic State, click-bait, marketers - for all of them, one key objective is to maximise dissemination of their messages, so sometimes the techniques are indistinguishable from online marketing. Russia has not invented all of the things that it is accused of - in some cases it just learns from marketing techniques elsewhere. In the same way as for example cybercrime and cyber espionage, carried out by different actors, share the same tactics, techniques and procedures and the same tools because the basic task is the same - in that case accessing information.

There are some instructive differences between how this problem is tackled in Europe and the United States. Despite the fact that some European countries have been aware of this problem and studied it for much longer than the United States, there is one very important difference which means that Americans already know a lot more about how these techniques are undertaken. And that is because US law enforcement agencies are visibly investigating it whereas European ones are not. The Netherlands for example do not have a current investigation into the Kremlin targeting of the EU Ukraine Association agreement vote. Same for the French, for the German elections, the Italian constitutional referendum 2016, Czech presidential elections etc. **The United States has come up with a lot of extremely important information and publicised some of the techniques that are being used to target democracy. And they have gone a step further with indictments and publicly identifying people and processes. This is emphatically not happening in Europe and most importantly of all, in the United States the investigations ongoing are keeping awareness up. Here awareness fades due to a shortage of institutional memory.** Some journalists, not all, are aware of the problem. Much more of the media space needs to be constantly reminded that it is being targeted and exploited in order to undermine democratic values and the civil societies they work within.

Ulrik Trolle Smed:

Thank you very much. Let me now hand back to Ann.

Question 3: Based on your professional experience and research, what has caused the spread of 'fake news' online and what evidence do we have of its impact on democracies, on societies and on economies?

Ann Mettler:

Thank you, Ulrik. So, thank you so much for introducing the subject. We will now proceed to the third question on the scope of 'fake news' and disinformation.

Based on your professional experience and research, what has caused the spread of 'fake news' online and what evidence do we have of its impact on democracies, on societies and on economies? You will have six minutes maximum each and the first one to speak will be. Professor Howard. Please go ahead.

Philip Howard:

Thank you. Over the last couple of years our team at Oxford University has been examining the distribution of poor-quality junk news and information across social networks. We have found that people in the US share more junk news than people in other advanced democracies, such as France, Germany and the UK. But we've also demonstrated that this junk news gets concentrated and has been concentrated in swing states, particularly during the 2016 election. More recently, we found that social media campaigns were targeting US military personnel, veterans and their families, for misinformation on national security issues. **The issue is never how much junk news, or 'fake news', flows within the country. The issue is whether this kind of junk content is concentrated at policymakers. Prominent female intellectuals, female politicians, feminist thinkers tend to be frequently targeted with these kinds of campaigns. They arise at times of social crisis, during a complex humanitarian disaster or a security crisis, and they seem to arise from the same place over and over again.** Social

media has become an important source for news and information, especially in the European theatre. An increasing number of users consider platforms such as Twitter and Facebook as a source of news. At important moments during these crises, social media users not only share substantial amounts of professional news, but also share extremist, sensationalist, conspiratorial, masked commentary, 'fake news' and other forms of junk news.

The problem has two ingredients. The first is the 'fake news' - the misleading information - the second are the proprietary algorithms held by social media firms. It is only the combination of these two things - the social media firms' algorithms and junk news - that makes for a misinformed electorate, political mistakes in decision making or an undermined electoral process.

Junk news in a sense is just a symptom - and I'm going to identify three levels of cause here. At the most macro level, the cause of the current problem is that significant amounts of valuable information about public life now reside within the private hands of a few technology companies. For centuries, churches kept the best records on public life. Then for several centuries governments and libraries kept the best records on public life. Now a handful of technology firms have the best data on us as individuals, on our networks, and on our public lives. They purposefully develop tools for exploiting those networks for their advertisers. They develop aggressive ways of taking pernicious advantage of our psychological predilections for selective exposure. We often choose to find information, to select information that reifies earlier choices, that supports the candidates we supported in the past and that prevents us from facing cognitive dissonance - the prospect that we've made a poor decision before. Social media platforms take advantage of our psychological structure by organising information in such a way as to prevent us from learning new things and exposing ourselves to difficult conversations. That is the most big-picture, macro-sense cause.

A more recent cause has to do with the failure of the business models of media and the journalism industry. Perhaps also the failure of higher education to teach people about the values of critical thinking, to teach people how to spot logical fallacies in a piece of news.

The most proximate cause of the problem we're here to address is that Facebook and Twitter serve large amounts of misinformation directly to voters in the 36 hours before they vote. That is the most direct cause of misinformation and the most direct threat to democracy. Foreign governments, industry lobbyists and political consultants within our democracies learn to manipulate, learn to take advantage of the affordances of these firms and these social media forms.

Let me say a little bit about what's on the horizon. I do believe the propaganda like this is not new, but certainly the distribution network and the newly sophisticated means by which we target this misinformation is new. **It's very important for us to plan for the Internet that is next, the internet that is ahead of us.** We have all lived with an Internet that is one we experience through browsers, where we control content to some degree. The next Internet, the Internet of Things, will be made up of between 30 and 50 billion devices by about 2020. To be on the Internet of Things you'll need a device with a battery pack, a sensor and an address on the Internet. **These devices will collect immense amounts of behavioural data. And when that data is matched with our social media data and matched with the targeting firms that work for consulting firms** that then work for political consultants who then work for political candidates or foreign governments, that **will create the ultimate political communication tool, a means of distributing direct and personalised political content to you in the 36 hours before you need to vote.**

We haven't seen true artificial intelligence behind the campaigns we've studied so far. What we've seen are sophisticated chat bots, simple scripts of content. But in the next few years, these scripts will get closer and closer to what machine learning experts describe as true AI. I also believe that in the next few years, the actors who use these technologies will switch from being interested mostly in elections and the sensitive moments for democracies to be interested mostly in issues, in interfering with our ability to make good policy in times of crisis.

Thank you.

Ann Mettler:

Thank you, Professor Howard. I am now turning to Professor Nielsen, please.

Rasmus Kleis Nielsen:

Thanks very much. **The starting point here I think has to be the recognition that digital media has made it easier to publish and share any kind of information, including disinformation. So, we need to see the growth in the amount that disinformation is being published and circulate in our societies against the backdrop of a general exponential growth in the overall amount of all kinds of information circulating.**

Pedlars of disinformation are using often the very same digital media analogies that entirely legitimate political actors, news media publishers, civil society organisations, governments and private companies are using. The same tools are empowering various forms of hate groups as are powering the #MeToo movement and the Never Again movement. And any response to problems of disinformation need to keep in mind that the same tools and technologies that can empower potentially harmful forms of disinformation also often empower entirely legitimate and benign forms of information, news and public engagement. It's clear that the rise of digital media is part and parcel of a profound shift in our political institutions and our media institutions. It's clear that there is much we don't know yet about the full implications of the shift that is unfolding around us. It's also clear that the implications will differ depending on the institutional context. The consequences will not be the same in Denmark where I am from as they will be in Bulgaria. But I think we can say a few things about what the basic implications are of the rise of digital media for information and disinformation.

The first one is that digital media has made it easier to publish this leads to a greater choice which in turn increases the information inequality between people who are most interested in seeking out high-quality information about public affairs and those who, while they care about public affairs, may care more about other things that are also made available to them easily and accessible. In highly polarised societies, this will be accompanied by partisan polarisation, where people self-select into consistent communities - but this is not in every society in Europe, but in some.

Secondly, it is clear that there are problems with the way in which digital media are being used by some citizens and some of these problems are compounded by the ways in which some platforms and services serve content, and this can sometimes create echo chambers or reinforce them. **But a growing amount of independent, evidence-based scientific research also documents that for most users, using social media and search engines lead people to a demonstrably more and more diverse information than they seek out of their own volition. It helps facilitate political participation and it helps facilitate civic engagement - and that these effects are particularly pronounced for young people and for people with limited interest in politics.** So, these companies have many imperfections, they have become platforms for many forms of abuse that we need to counter to protect and renew our democracies. But it is also clear that they are amongst the entities in our society that help counter some of the democratic problems we face.

Third, the rise of digital media has existentially challenged the business of news as we knew it from the 20th century. So, we have a world in which it is easier and easier to access information, more and more different sources are available. Many of these sources are amateurs or self-interested actors – companies, politicians, lobbyists of various sorts, whereas the business models that underpin professional journalism as we knew it is under tremendous pressure, because the market power it was premised on in the 20th century has disappeared and moved to platform companies that enable expression but do not fund professional journalism. This is particularly problematic at the local level. It is particularly problematic in small language markets, and it is particularly problematic in Member States of the European Union with no history of robust independent private sector media where this disruption is being felt very, very keenly and the profession of journalism and the business that sustained that historically is very threatened.

So, the move to digital media empowers us as individuals even as we also become dependent on these tools and technologies. It also empowered publishers to find new audiences connecting particularly younger people who don't seek out their content otherwise. But the publishers are also becoming dependent on these platforms with whom they are competing for attention and advertising. There's much we don't know yet about the scale and scope of the problem of disinformation, particularly in terms of how the impact is playing out in terms of citizens. **We see some research being conducted already**, including research by members of the panel that begins to shed light on this, **but I think at this stage we can suggest at least that we should expect to see that the main impact of sustained exposure to disinformation on citizens will be to undermine confidence in political institutions, media institutions and platform companies, to increase confusion around public affairs and to sow distrust and intensify polarisation around divisive issues.**

These are worrying risks, but we need to document them and to understand their scale and scope and intensity to be able to counter them. And to do so we need to keep in mind that so far most empirical research – in particular research from the United States, where, as Philip Howard pointed out, we have reason to believe this problem is more pronounced than in much, at least, of the Western Europe – most research suggests that 'fake news' narrowly defined as false and fabricated content has more limited reach than we might think. The best study I've seen so far – by Andrew Guess, Brendan Nyhan and Jason Reifler – suggests that 75 percent of Americans did not come across demonstrably false and fabricated information in the run up to the 2016 election. Of the 25 percent who did, on average they came across five stories in five weeks. And even the 10 percent who came across the most false and fabricated information came across 25 stories in the course of five weeks. **This is a problem and this problem can be serious for some communities or for some actors. But we need to be clear-eyed about what the evidence is for how serious this problem is so we don't play into the hands of our enemies by exaggerating their influence on our societies.**

Ann Mettler:

Thank you so much. And next is Mr Lelyveld please.

Philip Lelyveld:

Good storytelling draws you into a constructed world. The goal of entertainment technology and the language of storytelling is to construct an experience that will emotionally engage you. The best constructed experiences work to hide the limitations of their techniques so that the experience comes across as believably as possible.

I am sure you have all seen videos where the voice and image of world a leader or celebrity is manipulated to make it appear that they are making outrageous statements, or scenes where completely artificially constructed life forms interact seamlessly with live actors and the scene around them. Those are the easy lies, the transparent fakery in service of story that we recognise, accept, and enjoy.

But let me go a little deeper.

For over a decade tools like Dramatica have been used by scriptwriters to assess how well they have developed character, plot, and theme.

Market researchers use eye tracking, brainwave monitors, heart rate, and other bio-response data to design more effective ads. The ads are factually correct, but you must also recognise that the sound, image, pacing, and other artistic language elements are studiously designed to illicit a desired emotional impact. The data they use can also be gathered by properly equipped virtual and augmented reality consumer headsets and body computing devices like smart watches and fitness bands.

Affectiva, a company spun out of MIT, is one of a number of companies working to marry computer vision and deep learning to determine emotions from a person's nonverbal cues and facial expressions. The videogame company Flying Mollusk used Affectiva's software to produce a psychological thriller game whose difficulty changes with the player's level of fear.

Marketers hope these techniques will help them understand emotions well enough to tell when a person is open to a transaction. Imagine the potential uses, both good and bad, for all of the personal data you are releasing through the click license in exchange for the promise of a more personalised experience.

Facebook announced last summer that they were working on a brain-computer interface for typing and other interactions. Imagine other uses for the backchannel data; data that is necessarily gathered to make that work properly. Giving up this privacy is already now included in some click licenses. **Do we need to start thinking about a right to mental privacy?**

Virtual reality is often called an empathy engine. Because there is no frame, like the rectangle of a movie or TV screen, separating you from the sights and sounds of the experience, you are more likely to be emotionally and viscerally engaged. Fable Studio has developed an artificial intelligence character named Lucy. Lucy's wonderful story conceit is that you are Lucy's imaginary friend. She learns about you, gives you tasks, and stays with you, cross-platform, as you move through your day. Once you have bonded with her, imagine Lucy's power as a virtual trusted friend to influence you. Fable Studio's primary business is storytelling and world-building, not AI research. **But combine story with AI efforts to profile and predict individual human behaviour, and you have a powerful resource being developed with, at least until recently, little discussion of the ethics, risks, and unintended consequences.** I am aware of a number of 'ethics in technology' initiatives around the globe, and last month there were news stories about Harvard, MIT, and other schools developing courses on ethics related to computer science and artificial intelligence for people majoring in that topic, but I have not seen any of them gain traction yet. Should we have the right to understand the framework for an AI's personalised decision-making, including how it is filtering data?

To sum up, tools and techniques to engage our attention, and to understand and influence us, individually, on both a conscious and subconscious level, are being invented and refined in offices, test labs, and basements around the world. Expect to see them as either standalone products and services or embedded into other products and services – including entertainment experiences and advertising – as they prove useful.

Ann Mettler:

Thank you so much. Next up is Mr Giles.

Keir Giles:

The underlying approaches and principles of many of the organised disinformation activities we are seeing at the moment are broadly recognisable as reinvigorated subversion campaigns from the Cold War era and before. The key difference in implementation is the technological enablers that we've been Hearing about which enhance the reach, the speed and the precision of information operations but also vastly reduce their cost. Now, that, together with the changes in the information landscape and in western media behaviours, makes one of the key reasons why information operations have become so prominent in Russian strategy in the current decade. Since 2014 in particular, you see Russian military thought leaders talking about how information operations can deprive an adversary country of its sovereignty without the need for occupying its territory. They do this because they think it works.

However, as Rasmus has already said we don't have the evidence to support that. We don't know exactly which campaigning by the adversary has an impact and what does not. It is a critical deficiency in planning for responses to this challenge, that we don't know which adversary problem to target. It is possible to waste resources on chasing after things which actually have very little impact, while neglecting those problems that actually do reach deep into our societies to compromise them. In part this is because the disinformers have better knowledge about audiences than their own host nations do. They've had the time and the luxury to prepare their campaigns using trial and error. I would recommend to you a Wall Street Journal article from two days ago entitled 'Russian trolls tweeted disinformation long before U.S. election' for a look at exactly how that looks and feels, deconstructing these trial and reconnaissance efforts, but also providing indicators and warnings of future campaigns, if we watch carefully.
So, those states that decide to measure the success of pro-Kremlin disinformation or indeed from any other hostile actor need to do target audience analysis on their own population: targeted opinion polls which measure the spread and the effect of campaigns and their success among a particular audience. That includes focused audience analysis which should help identify which of the many available audiences are the most vulnerable and the most receptive to the disinformation campaign.

Just because we don't have the evidence at this point though does not mean we should not take disinformation campaigns with the utmost level of seriousness. **It is a key part now of Russian military doctrine and strategy for winning the conflict that they already perceive themselves to be in with the West in general - with NATO and the EU in particular. It's implemented by the very top hierarchy of the Russian leadership down through its media organisations to the very junior-most foot soldier in the Kremlin troll army. It doesn't necessarily need to be about targeting elections or referenda. Disinformation operations aim to undermine the whole system of liberal democracy and to sow and to amplify distrust in credible sources of information whether it is government or establishment mainstream media in order to influence the geopolitical direction of a country and of intergovernmental organisations.**

So, the objective can be strategic, including what amounts to regime change as we've seen in Russia's attempts to influence the outcomes of the US and French presidential and the German general elections. It can also be at a lower level of ambition; just to spread pro-Russian narratives in order to allow Russia greater freedom of movement in its choice of action and avoid the censure that comes with some of its more egregious international actions.
But at the very bottom level of ambition comes a broad based long-term weakening and undermining of adversary societies overall, and their institutions, without necessarily any specific short-term goal other than increasing Russia's relative strength in a classic zero-sum approach. If they erode and undermine our institutions, according to the logic of this confrontation this enhances their power without necessarily achieving any other effect on our societies.

Ann Mettler:

Thank you so much. Next up is Professor Applebaum, please.

Anne Applebaum:

Thank you very much, I am going to be a little shorter on this answer in order to expand further in the next question - on the question of what the EU should do. Let me just underline one of the reasons why disinformation campaigns are so successful now. As a number of people have said these tactics are not new, they've been tried before, we even know some of the mechanisms from Cicero. Two very important factors have led them to be more successful.

The first is the weakness and in some cases the actual disappearance of traditional media in some European countries. For a long time, we assumed that free markets in goods and services would always lead to a free market for information... But in the past decade both advertisers and readers have moved to the Internet. Free information easily available on cell phones has led to the sharp and maybe even irreversible decline in revenue for traditional journalism. In some smaller European countries, independent media has become very weak or has ceased to exist

entirely, having been replaced by media which is either controlled by the government and operated by the ruling party or by media controlled by business groups connected to the ruling party, and in some cases by Russian companies or others who seek to undermine democracy in those countries.

Secondly, the nature of social media – as some people have said and I won't repeat it – itself accelerates and accentuates this issue because its algorithms encourage people to see only the news and opinion that they want to hear. How does this affect democracy?

Whatever you think about their objectivity or lack of it, traditional newspapers and broadcasters created the possibility of a national conversation – a single debate as well as mechanisms to hold politicians to account. The disappearance of those news sources in a number of countries has led to polarisation and made political debate impossible. I witnessed this myself living in Poland over the last few years: the disappearance of a neutral centre ground meant that normal political conversation became almost impossible.

Polarisation, created by the collapse of traditional media and accelerated by social media, is also the source of other problems. **Polarisation by itself has created increased distrust for political and state institutions of all kinds**, both national civil servants and European civil servants – yourselves. Police, judiciary, government-run bodies of all kinds are now falling under suspicion on the part of very polarised groups, because one side or the other, or sometimes both, suspects that they have been captured by the opposing party. **Polarisation has another impact on democracy: A lot of studies have shown that highly polarised audiences are the ones which are most susceptible to conspiracy theories and disinformation campaigns.**

This is the context in which the massive Russian campaigns that we've all spoken of have been successful and it will be the basis on which other disinformation campaigns will be successful in the future. So while there is a specific Russian issue, I would encourage you when thinking about this problem, to think more generally about polarisation and how that's affecting our societies as well.

Ann Mettler:

Thank you very much, I will now hand back to Ulrik for the fourth question.

Question 4: Based on your professional experience and research, which initiatives do you believe are necessary to tackle 'fake news' online and its related issues?

Ulrik Trolle Smed:

Thank you very much for your assessments on the scope of 'fake news', we will now move on to the fourth question on how to address it.

Based on your professional experience and research, which initiatives do you believe are necessary to tackle 'fake news' online and its related issues? Please provide your assessment of which initiatives could be relevant and why. You will have 6 minutes each, maximum, and the first one to speak will be Professor Nielsen. Please, go ahead.

Rasmus Kleis Nielsen:

Thank you. I said from the outset I think our aim here should be to think about ways in which we can renew our democracies for the digital age, not simply protect what we've inherited from the past. I have suggested also that there were sort of two core sides to this. One is to protect our open societies and the other one is to develop institutions that enable citizens to make good use of the freedom and rights that these open societies provide. In terms of our response to 'fake news' and disinformation, I would start from these first principles and make three sort of types of suggestions.

The first concerns an area in which I think we need to show caution. The second one concerns an area in which I think we can think of narrow and precisely targeted responses. And the third one concerns how we can develop institutions and enhance our resilience to disinformation and also has a broader set of positive knock-on consequences for our democracies.

First on caution: **because 'fake news' and disinformation is hard to define clearly and objectively, we should be very careful with vaguely-worded legislation that leaves it to judges – or even worse the executive branch – to decide what may or may not constitute 'fake news', and thus can restrict free expression and the right to receive and impart information and views. Similarly we should also be very careful with political attempts to outsource to private companies the policing of acceptable speech** in ways that will almost certainly give these companies every incentive in the world to err on the side of caution – remove things and do so in ways that will not ensure due process or meaningful forms appeal for citizens who may feel they are being censored by governments who are forced to censor them by politicians. And again, free speech here includes information and ideas that may shock, offend or disturb us. This is not only about things we like. It is about what it means to be a free society and we need to be very, very cautious about how we act in that area because the very purpose of this exercise is to renew our democracies.

Secondly, how can we then think about targeted responses in the light of that caution and that commitment to our fundamental values. Direct interventions in my view should be used to address clearly and narrowly defined, identified problems. For example, **it is already illegal in many countries for foreign governments to meddle with the political process, just as hate speech, incitement to violence and the like is already illegal. So, this is a question of enforcement of existing legislation, more than about new legislation necessarily, and how we can make sure that existing laws are actually enforced and protect us the way they are intended to do so**. Similarly, when we turn from politically motivated false and fabricated information – sometimes from foreign states – to think about for-profit false and fabricated information, we need to put constant and public pressure on advertisers, ad-tech companies and platform companies that have enabled the monetisation of information that is potentially harmful for our democracies. They need to be encouraged, even pressured, to take seriously the responsibilities that come with being such a central part of infrastructure of free expression. Enabling this will necessitate new steps to increase algorithmic accountability, ensure an appropriate level of transparency, and make more data available to support parties that can independently assess the implications of these platform companies and the changes that they make on our democratic discourse.

Thirdly, strengthening our institutions. Four very quick points.

First of all, we need all Member States of the European Union, and ideally countries beyond the Union, to renew their commitment to protecting news and media against governments who are trying to use economic pressures or political pressures to control them and reduce their independence, against organised crime and extremist groups that are demonstrably threatening the practice of journalism all across the continent. Particularly in the south and parts of Eastern Europe, and, again, against politically mandated privatisation of the policing of free speech. It is indicative, for example, that all Member States have signed the Council of Europe recommendation on protection of journalists and their safety, but implementation has lacked somewhat, though this was signed in 2016. So, politicians need to step up here.

Second, creating an enabling environment for news media. **We should remember in terms of professionally produced journalism, it is still the case that two thirds of investment in professionally produced journalism comes from print publishers** operating across online and offline platforms, about 10 percent from commercial broadcasters and in those countries where it exists, like the UK, about 20 percent from public service media. **We need to renew these institutions to ensure that professional journalism can continue to play a vital role in our democracies moving forward. That will involve reforming existing forms of indirect and direct support for private sector media so that they continue to be politically independent but start to reward the future digital media rather than just the past** – print and broadcast – as they currently do. We need to support genuine

independent public service media – not organisations that are effectively state broadcasters or pro-government broadcasters – ensure they have autonomy and funding to deliver on their remit using all appropriate tools. We need to enable non-profit journalism by streamlining regulation to ease the creation of non-profit news organisations, incentivise support of these organisations and make support available for R&D and innovation in the news sector and in journalism. It is a sad state of affairs if advertisers and various forms of malicious actors are technologically ahead of legitimate news organisations, in part because these companies have not had much support in terms of renewing their industry across the Union.

Finally, it is important that we invest in media and information literacy efforts and also to think about the role that the European Commission and other relevant stakeholders can play in helping the journalistic profession build on the values and professional practices that has built up over the 20th century but also embrace skills for a digital media environment so that the journalists themselves can compete and ideally out-compete the malicious actors who are currently gaming an open and permissive media environment in ways that are endangering our political processes.

Thank you.

Ulrik Trolle Smed:
Thank you very much. Mr Lelyveld.

Philip Lelyveld:
Okay, from a very different perspective. I start from the position of immersive experiences, which include virtual, augmented and mixed reality. Those immersive experiences can include enhanced explorations of real places, people and events around the globe, imaginary places, people and events and any type of simulation in-between. Within those immersive experiences, we can have social interactions with avatars that are tele-presences of real humans, avatars driven purely by code, or actual human beings as 'avatars' or actors within the immersive experiences.

These immersive experiences are going to be informed by the Internet of Things which will feed data either directly into the experience or into the code that is creating the experience.

They will be informed by artificial intelligence that will create the most realistic elements of the experience for you and will respond in contextually logical ways to your actions.

No new entertainment medium ever replaces an old one. People just rebalance the entertainment mix that they seek out. So, we will add immersive experiences to text-based media, such as physical paper and digital platforms, personal passive and interactive audio-visual experiences like television, laptops etc. and group and virtual group audio-visual experiences like theatre, e-sporting events in both physical and virtual spaces activities.

All of these are channels that can be used to delivery data (raw elements), information (meaning), and knowledge (context).

For the most part these channels will deliver anything. The channels don't check for errors or distortions or lies.

There is a continuum between the absolutely true and undistorted, and the absolutely false and distorted. It is straightforward to check whether a sensor on the Internet of Things is sending true data or if it is malfunctioning. It is not nearly as straightforward to tell if a statement of opinion has been sampled or used in a manner that changes its original meaning.

In situations where there is uncertainty it may be easier and less risky to prove that something is not true than to prove something is not false.

So, rather than try to stop 'fake news', I propose that we focus on mechanisms that identify, protect, and elevate what is most probably true and undistorted. To recognize and reward sources for being trustworthy.

One approach would be to tie all posts back to their online identities. Fundamental to that approach is a mechanism that securely develops a reputation profile that is securely attached to the source's online identity. The profile would then be securely linked to any and all posts linked to that online identity, should the online identity choose to do so.

We can look to cryptography and the blockchain ledger infrastructure for ideas on how to do this.

By doing that, anyone viewing the posted material would be able to track back to the identity and make an informed determination of whether both the material and the source are credible or not credible, based on their own personal criteria. **This approach won't directly take a person out of their personal echo chamber of ideas, but it could give them a sense of the trustworthiness of the sources.**

A key aspect of this structure is that first-time posters, including fake identities and bots, would have low reliability ratings, and their contribution could be discounted accordingly. Also, contributions without a tie back to a reputation profile would be discounted and flagged as unverified or therefore of unknown reliability.

MetaCert is one company that has implemented a variant of this approach and released it as a browser add-on. They aggregate data about news sites from trusted fact checkers. They then crawl the web, find, and label social media accounts owned by those news sites. MetaCert is one company tracking a very limited number of news sites and their posts. I am suggesting expanding that approach to all online media from all sources.

The approach could be developed voluntary, allowing for self-regulation on an industry and societal level. A small group of key infrastructure players and influencers could come together and, assuming their intentions are aligned, they could create a beta version, trial and evolve it, and seed the infrastructure with it. The player's involvement could even be useful for their organisation's messaging. They would be working cooperatively to create a social good.

The approach won't cover all situations or completely solve the problem of lies and distortions masquerading as truth. But if it yields results that the market finds appealing, it could redefine the boundaries of trust within an open market.

Thank you.

Ulrik Trolle Smed:

Thank you very much. Mr Giles.

Keir Giles:

The first and most effective response to hostile subversive and destabilising activity is and always has been raising public awareness – and here the role of key leaders is absolutely crucial. Statements by senior figures like prime ministers and defence ministers recognising a state of conflict and the challenge have been shown in the front-line states to be an extremely powerful tool in empowering not only government but also society and media to take steps to protect themselves. As a subset of that, attacks must be publicised, especially those that seek to exploit societal divides. It is important to let the targets and the vectors of hostile information campaigning know that they have been duped. It won't address the underlying reason for their discontent. It will prevent them being leveraged by a hostile actor from outside.

Speed of reaction from trusted sources is another critical element and we have case studies again from the front-line states to see how this operates. I refer you to the case of the Lithuanian Lisa in 2016 or, earlier, the Estonian case of cyber-enabled disinformation attacks during a NATO exercise called Steadfast Jazz in 2013 and the response of the state and the media which neutralised any adverse effect from it. Speedy reactions are extremely important. The awareness and speed of reaction creates an environment where other measures can be taken, particularly enforcing the existing laws and regulations which are intended to ensure that media reporting is objective and accurate. Whether that is on a national level or supranational - now, as Rasmus said, **this is absolutely not policing what is acceptable speech, but pointing out that an individual or an organisation has repeated something which is untrue or sponsored by a hostile actor is not an attack on freedom of expression.**

Instead it is an absolutely integral part of ensuring freedom of expression. In addition, laws that are designed to counter the spread of hate speech should be applied to disinformation from Russia, whether it is on traditional or social media; it is another measure that can be empowered by creating an environment of awareness. Because many of the disinformation narratives are about inciting hatred toward a particular nation or a group of people or spreading false alarms stories about incidents or emergencies. **Awareness also allows public challenges to agents of influence - the politicians or the academics or the businessmen or the journalists who promote adversary interests and narratives. Whether it is through genuine belief or through ignorance or financial reward or because they have been induced to do so, their interventions can be questioned in an environment where you are aware that there is an overall campaign intended to erode your democracy.**

States should not leave this to individuals. What happens in that case is what we saw during the German Lisa case in January 2016 where it was an individual lawyer who actually undertook the investigation and launched legal proceedings against the instigators of the information attack and consequently received death threats. It's the lack of government initiatives which lead NGOs and dedicated individuals to take on the work - the work of surveying and debunking and countering disinformation, sharing information about ongoing campaigns. This only devolves to them because of a vacuum of initiative from governments and an abdication of responsibility based on a failure or a refusal to recognise the threat.

There are other policies on information which we can learn from. I present to you the Russian information security doctrine - not under any circumstances with the intent that it should be emulated, but instead we should study what they think they need to be protected against in order to understand the kind of hostile effect that they are seeking to project. Russia has always seen information security threats in content as well as cyber threats from code. We are now only catching up with their persistent assessment of the problem and we're only doing that because they are using information as a weapon against us. All this research and exposure and analysis should preferably be done both at national and at EU level with the closest possible coordination because disinformation strategies are tailored to individual countries, but they target us all and therefore the response should be as coordinated as possible, including situational awareness - sharing information about ongoing campaigns in order to empower this rapid reaction.

This could be a key role for East StratCom, the information sharing, although national governments would still need to lead on collecting information through monitoring of their own information channels whether it is traditional or mainstream or peripheral or social or private-channel media.

Finally, the critical point is ensuring that hostile disinformation does not cross from the public opinion space into the policy-making space. This can be done by means of monitoring and verification. Just as antivirus software protects a computer by ensuring that contaminated data introduced from outside doesn't affect core processes, so information security programmes should ensure that the sources of policy input are not corrupted by foreign influence.

Ulrik Trolle Smed:

Thank you very much. Professor Applebaum, please.

Anne Applebaum:

Thank you. When preparing for this session I thought a lot about what it is that the EU could do as opposed to what national governments could do, or what other actors can do. Both the specific problem of Russia, as well as the more deeper changes in the ways people get and process political information, will not have a silver bullet solution. There are going to be many solutions, there are going to be civil society solutions, journalistic solutions, and so on.

But what is it that the EU can do? The reinforcement of the independent media, while very necessary, seems to me beyond your competency. So is the very real problem of transparency in political advertising, and the need to enforce existing law on the Internet. Germany, for example, is looking at how to enforce its own hate speech laws on the Internet and is now making Facebook comply with them. All of those are very legitimate pursuits. But I'm not sure that that's what the EU should be doing; even if it's not intended to be censorship, any EU enforcement of national hate speech laws will look like that to somebody. In a situation where there is so little trust in EU institutions, I'm not sure that's the best idea. Instead, I'd like to use the short time allotted to me to focus on one particular issue: anonymity.

Without question, anonymity – whether it takes the form of about fake accounts or even non-human bots on Twitter or Facebook, or fake and misleading websites – gives almost complete freedom to people who are driven by anger or greed or ideology or financial interests. It's the primary tool that Russian and alt-right propagandists have used to create fake websites that echo and repeat stories or to artificially amplify false and damaging narratives. Yet, as we've just heard from Professor Lelyveld, technology around ending anonymity is beginning to evolve. Some systems for authenticating online anonymity already exist. Google's Gmail offers some business clients the option of having their outgoing e-mails endorsed with a golden key showing that the sender is real. Twitter issues a blue tick to accounts that it regards as verified, although the criteria for that right now is opaque and pretty arbitrary. Facebook has a similar scheme. **Why can't we make verification stronger, eventually making it a right and not a privilege?** Why can't everybody have a blue tick? Why can't everybody have verified email? That would, for example, eliminate the danger that by clicking on fake emails, we risk accidentally downloading a hostile computer programme. Why should that be a problem? Shouldn't we have some way of detecting it ourselves rather than being told about it afterwards by the FBI? **Most people would choose to read emails and engage on social media only with authenticated accounts, just as we're more likely in real life to debate people whose names we know. That doesn't mean that some people couldn't continue to communicate anonymously online if they wanted to, but for those who don't want to, this would be an important way to defend against disinformation.**

Social bots right now exist almost entirely for the purpose of creating fake amplification: it's as if someone in this room created an applause machine, so every time I speak lots of people clap and the rest of you pay more attention to me. That's what Twitter bots do right now online, they don't really have any other function. Just as the applause machine would give a false picture of this debate here in this room, it gives a false picture online. The practice of manipulating hundreds of thousands of fake supporters, whether for the purposes of selling soap or a political campaign, serves no socially useful purpose at all, it's just for deception.

The advantages of anonymity to dissidents and others need not necessarily be sacrificed. Again, if the tech platforms wanted to do so they could help create ways for people to prove that they are real, to link their social media presence or online Internet presence with a real person, without necessarily revealing their identities to all and sundry – you hinted at some of them just now. Perhaps we should be able to back up our email and social media accounts with other credentials - bank details, phone numbers, blockchain systems - and perhaps we should be able to do this without giving our details to tech giants. If they could simply issue an electronic token confirming that we want to use one identity to back up another then that should be enough.

There is an additional role for search engines such as Google to inform people who download anonymously created websites. Sometimes when you open a site you can get a warning: 'This site contains malware, open at your risk.' Why shouldn't Google also offer us another kind of warning: 'We don't know the origins of this website, it may have a false creator.' You can still download it if you want, and you can decide whether you want to open it or not.

We know why tech companies have refused to do this so far. Vast numbers of their accounts are fake – about 20 percent in the case of Facebook maybe up to half on Twitter. For that reason, **the European Commission might be able to offer something more than just pressure. In Estonia, the government has helped create a system that gives every resident of that country an online identity.** This is a totally secure online passport that gives people both rights and responsibilities online. And there is a huge opportunity here for the European Union to follow this example. Imagine if the EU could issue online e-citizenship to Europeans: that would both raise the tone of public debate and also give the EU a real and positive role in creating a more civilised online space. This is a concept that everybody can understand It could be optional, not compulsory. You have a paper passport in the real world – I had to show one to get into this building – **you have a digital passport in the online world, and it helps people establish that you're a real person. This could eventually come to be seen as a tangible advantage to European citizenship. It's something positive that you could do.** Rather than seeing the EU as a source of only negative ideas – as a source of censorship, or as the body burdened with defining "hate speech" – it would be very helpful if the EU offered something positive, something that would enhance the usefulness and validity of online debate.

Thank you.

Ulrik Trolle Smed:

Thank you very much. And finally, Professor Howard, please.

Philip Howard:

Thank you. I said earlier that I believed junk news to be just a symptom of an underlying disorder. I think our project should not be about the content that lobbyists or foreign governments generate - or social media platforms - we should actually use this as an opportunity to renew, as my colleague Rasmus says, renew our democracies. That means this should be about the flow of data within our democracies. It should be about presenting some new opportunities for Civic Engagement and Civic expression. Here are five policy initiatives that would allow the EU to renew democratic institutions in its Member States.

First, we need a system of mandatory reporting on the ultimate beneficiaries of data. Second, we need a system of citizen data donation. Third, we need information infrastructure that tithes. Fourth, we need to extend the non-profit rule for variables that data miners buy and sell. And fifth, we need a regular system of algorithmic audits. Now I'll address each of these in turn.

First, we need a mandatory system for reporting the ultimate beneficiaries of data. Citizens should be able to see which organisations are using their data making political inferences. Social media companies should be able to report back to users in a regularised way on which advertisers, which data mining firms, which political consulting firms have made use of their data. If I can make a political inference from something that you have watched on your smart television or from your location in space during a protest, that data should be revealable to citizens who own that device. The Internet of Things refrigerator or television should be required to reveal what political inferences are being made with the data from that device.

Second, we need a system of citizen data donation; we should be able as citizens in a modern democracy to be able to add to the list of organisations that do benefit from the data we generate. **Data is now the lifeblood of democracy. Social media firms effectively monopolise that data. Not everyone will express themselves in this way. Not every citizen will check to see where the data from their television is flowing around the world, but now, and more and more in the years ahead, this will be a wonderful opportunity for civic expression. A firm's monopoly control of publicly valuable data threatens democracy.**

Three, we need an information infrastructure that tithes. 10 percent of the ads on social media platforms should be for public service announcements. 10 percent of the data needs to flow in a secured way to public health researchers, to civil society groups, to journalists who do Computational Journalism, to political scientists and to public science agencies like the European Research Council. A 10-percent sample of the political ads bought on Facebook during elections should be publicly archived for everyone to see. My only footnote on that point is that in an AI world, in which the political ads are composed directly for each individual, 10 percent may not be the representative sample we want.

Fourth, we need to extend the non-profit rule for the kinds of variables that are traded by data mining firms. One of the few regulations that seem to consistently protect privacy over multiple jurisdictions is this rule that a firm can't profit by selling voter information files. A larger class of data types that is open and that private firms can't profit from in trading would help create a greater public pool of information that researchers and public health officials, policymakers like yourselves, can use to do constructive policymaking with.

Fifth, we need a regular system of algorithmic audits. We audit video gambling machines, we audit financial trading algorithms, all in ways that don't violate the intellectual property of those technology firms. There is no other domain of business in which a company can design and build something, release it to the market and change the product only when somebody complains. A system of regular algorithmic audits would allow us all to restore trust in the social media systems that many of our citizens now value.

Thank you.

Ulrik Trolle Smed:

Thank you very much, we will now move on to the fifth question.

Question 5: Do you believe the European Commission's initiatives to tackle 'fake news' online and related issues are sufficient?

Ann Mettler:

Thank you, thank you so much. You have now provided insights on how to address 'fake news' conceptually. Now we would like to draw your attention to the fifth question and the European Union's efforts to tackle the problem.

Do you believe the European Commission's initiatives to tackle 'fake news' online and related issues are sufficient? Please provide your assessment and indicate which areas of intervention could be improved and why.

You will have 5 minutes maximum each. The first one to speak will be Mr Lelyveld, please.

Philip Lelyveld:

If I can get you to remember one thing from my being here today, it would be this: innovation is never stifled.

Innovation is never stifled, it is only redirected by changes in the ecosystem that it operates within. Those changes can include regulation, the bottom-line imperatives of business and societal pressure, but innovation is never stifled.

The authors of 'fake news' are innovators. They will innovate around any technical, legal, or social obstacle you put in place in order to reach and build their audience. As you put up more obstacles they will find more sophisticated ways to bypass them. If you want to counter their efforts (and I say counter their efforts, because stopping them would require fundamental changes to the architecture and philosophical foundation of the Internet), **then you must understand their tools and techniques and out-play them. You need to identify their drivers and develop counter-drivers.**

On the technical, tactical, and granular level of the 'fake news' response, as I mentioned before, I suggest a technical approach that elevates what can be objectively graded as trusted or reliable, rather than taking on the gargantuan subjective task of grading for lies and distortions.

A gathering of key players whose interests in elevating reliable information sources are aligned could develop the definitions, screening criteria, policing and enforcement mechanisms and infrastructure of an alpha- or proof-of-concept release. If, through the usual fail fast and fix process, the approach proves out, then it would become the seed solution that others could contribute to and build on. This would be a 'seal of approval' system for good players.

Explaining why this approach was developed (to combat 'fake news'), how it works, and how it protects democratic processes without diminishing online freedoms, could become part of public education, media literacy, and other social actions that raise awareness of both the problem of 'fake news' and ongoing work to mitigate its impact.
The bigger question is: how do you identify, control or limit psychological manipulation by outside agents on a societal scale. One possible approach is to involve psychologists, sociologists, ethicists, etc. in the development of code (which could be artificial intelligence) that scours the web looking for evidence of social manipulation related to political issues.

The system would need ongoing human oversight to train and quality-control the process. It would also need human intervention when the code returns material that falls on the boundaries of its judgement criteria. Regular human involvement in the training and evolution of the algorithm's judgement framework is key.

In his article 'Build a Better Monster: Morality, Machine Learning, and Mass Surveillance', author Maciej Ceglowski writes: '[...] the algorithms have learned that users interested in politics respond more if they're provoked more, so they provoke.' When provocation stops working, the innovators will try other strategies.
As the 'fake news' generators change tactics, the detection and response systems need to be guided to respond to the new profile of the attack. Detecting social manipulation efforts by outsiders is an ongoing process, not a closed problem with a static deliverable.

The storytelling arts and sciences have regularly evolved to keep up with the rising sophistication and expectations of our audiences. Similarly, if you are going to detect and respond to the outsider innovators and storytellers propagating targeted psychological manipulation tools including 'fake news', then you have to put in place technical and social processes that can also evolve to stay one step ahead of them, and that contribute to helping the average citizen make informed decisions based on reliable data.

Thank you.

Ann Mettler:

Thank you so much. Next up is Mr Giles, please.

Keir Giles:

Viewed from the outside, initiatives that come from Brussels in this domain often look like addressing the symptoms and not the causes of the problem. Now, it might be that the cause is actually lying outside the EU's remit because you cannot deal with the problem that there is not a natural phenomenon giving rise to the 'fake news' problem but actual perpetrators and instigators without which it would not be an issue, and with whom you need to deal in order to address the fundamental problem. However, within that you asked us to look specifically at initiatives that were listed. I'm going to run through them in fairly rapid succession.

You asked us to consider the EU communications on online platforms from May 2016 and tackling illegal content online from September 2017. I haven't heard of either of those before you told me about them. So, I went off and looked them up. I read through the text and not knowing much about the status of an EU communication and

what exactly it does, I had to take them on face value. Assessed on that basis, I don't think they do very much. They are, as far as I can tell, aspirational documents - they are full of the words 'could' and 'should'. They are a communication not a regulation and as such something which can very easily be ignored. We've seen, particularly in the case of the United States, how voluntary efforts do not work against some of the key facilitators of 'fake news', until you actually get a big stick to hit them with.

Similarly, you asked us to comment on the Hybrid Fusion Centre. As far as I'm aware, that centre operates exclusively in the classified domain. We don't - there's really very little I can say about that, I'm afraid.

But let's go to the initiatives that can or will or already do work. I'd like to talk about InVID and verification of social media content, particularly in terms of video. This has enormous potential, especially when disinformation becomes exponentially more powerful with the addition of fake video. Yes, this has to be an EU initiative, not a national one, in order to avoid accusations of national bias. But it needs to be publicised. At the moment, again, very few people know that this exists and will eventually turn into a capability.

Next, East StratCom. This is a critically important capability for responding to threats to democracy and our institutions, which at present appears scandalously under-resourced and under-empowered. If I understand correctly, the staff of East StratCom currently consists of only 13 people, of whom the majority are focused on information policies towards the Eastern Partnership, instead of on the essential task of countermeasures to disinformation which affect the EU (and its Member States) itself. **Meanwhile, the opposition is throwing ever more resources and people into the kind of tactics and procedures that East StratCom is attempting to counter. Despite the constraints and despite the tiny budget and numbers, East StratCom does have a very high reputation among the expert community.** What is more difficult to explain is why it has such a relatively invisible media presence given the work that it is carrying out and how important it is to raise awareness of what is going on. I understand from journalist colleagues who are still in the trade that they are constrained from communicating directly with the media in order to publicise their findings. I think this is a fundamental mistake because we need to know this stuff. Surely the EU can do better, as this is a key part of the response. **If 'fake news' is a problem, let's empower the people who actually can do something about it and are best placed to advise on the next steps because they have studied the problem and collated studies of the problem. Other actors across the EU space can serve as a clearing house for studies of tools and techniques and, as Philip Lelyveld said, the drivers and how to counter them.**

Finally, you also asked us to comment on the US Congress passing a bill on countering foreign propaganda and disinformation, allocating 160 million US dollars - very approximately, 160 times the budget of East StratCom - in support of efforts to fight disinformation across three regions in Europe, including inside the EU. You said: 'What is your assessment of such an investment in general and in particular into the EU?' My assessment is: you should be embarrassed by this. The United States is doing this, because the EU isn't. I hold no brief for the US, but this is yet another example of America feeling that it needs to defend this continent from external aggression, because this continent can't be induced to take an interest in doing so itself.

Ann Mettler:

Thank you. Professor Applebaum, please.

Anne Applebaum:

Thank you. I won't repeat some of the things that Keir said. It's fairly clear that the voluntary efforts that have been undertaken so far by the EU haven't been successful, just as they aren't successful in most other places. **Cooperation with the tech companies works up to a point, but unless they're actually worried about their markets changing, they don't seem to change behaviour, Until now, they have not made any sweeping wholesale changes, just small attempts at patching up the problem.**

I'd like to elaborate further on two of the EU initiatives. One is the various small efforts to support and strengthen media. **It's important to remember that the whole concept of media freedom is pretty meaningless if there isn't an economic system to support independent media and if indeed media is being deliberately captured by ruling parties or by governments, as they have been, for example, in some countries in Central Europe.**

One thing to think about: one of the few sources of independent, verified information in our societies may eventually be neutral public broadcasters. The EU might therefore consider creating a Venice Commission for public broadcasters, an organisation which tries to define what they should be, which promotes high standards, which helps individual countries build them up, which tries to find models of neutrality and ways of creating and protecting a neutral public broadcaster. Such a commission would not tell countries what to do, but would rather create a reinforcement system.

I would also like to pay special attention to the East StratCom group. In addition to an active campaign to stop disinformation – one that might include, as I've said, the creation of a digital passport, as well as measures undertaken by individual nation states to tackle the regulation of political campaign advertising - the EU should have some forms of defence or response. The European Union needs a centre to track and identify disinformation narratives, a centre with proper funding and a proper mandate. I've just come from the Netherlands where I heard a lot about the trouble that the East StratCom group has recently had, legally - largely, I was told, because it didn't have enough Dutch speakers or experts. This kind of failure reflects the broader European failure to fund this group, which still relies mostly on voluntarily supplied information and which is operated mostly by people seconded from foreign ministries not employed by the EU. One possible solution might be to take East StratCom out of the EEAS, where it seems to be an uncomfortable fit with diplomats who have other interests and want to have different kinds of conversations about Russia, and move it into another part of the EU you will have to tell me which is the best part, you're the experts on how the European Commission works. Preferably this should be some part of the European Commission which deals more properly with matters of internal politics - either EU strategic communications or internal security bodies.

Understanding how Russian computational propaganda works is incredibly important. It's important for individual governments, it's extremely important - maybe of life and death of importance - for this body, for the European Commission, precisely because so much of it is targeted at you, and you need to understand what it is and how it works. But if it's not fitting well with the EEAS, if it's not working in that part of the European Commission, then perhaps consider moving it.

The US initiative, I agree with Keir Giles that this is a fantastic idea. I know some of the people who are working on planning that initiative, and a lot of it will be focused on Europe, although there's still a lot of argument about what it will do. Unfortunately, that money has not yet been allocated. It's not clear why it's been held up or why it's not being allocated or who in the White House exactly is preventing it from being spent, but it has not yet been spent. No director has yet been appointed to lead the organisation that is supposed to spend it. Apparently, Congress would like to spend it, other parts of the administration would not.

Ann Mettler:

Thank you. Next up is Professor Howard, please.

Philip Howard:

Thank you. Let me start off by identifying a couple of the programmes that were not on the list we were provided, that we were invited to evaluate, because I think it's important to recognise that you already have several good organisations that have been sending signals about these problems and there may be ways that you could more deeply listen to the signals you collect from them.

First, I want to make the point that **I believe quite firmly that we're past the moment of industry self-regulation. Industry has taken some steps and is doing some creative thinking around the political problems created over their platforms. They're trying different things, but they always try different things in different countries. We have no way of adding up the impact of industry-led initiatives, in a systematic way, on public life. Technology firms grudgingly cooperate with governments and democracies, they don't collaborate with researchers.** Facebook used to announce how many fake voters they culled from their networks before elections. They haven't done that in the last six months or so. At this point my research team and I have interviewed almost a hundred different political communication professionals, bot writers, software engineers, propagandists. I've spoken to Twitter and spoken to Twitter engineers, I've lectured at Facebook to Facebook engineers. And I'm constantly surprised at how - privately - these people who participate in our research want some public policy guidance. These are engineers who would like a gentle nudge, some signals of what to design to - and the worst of all situations for them is a lack of clarity. Engineers want some signals about what the public needs.

Now to the two domains in which I think you already have great capacity and should make better use. DG Connect has had for many years multiple media literacy initiatives, multiple good research networks. I benefited, through an affiliation with one in Budapest, for several years. I was working there, in fact, as we saw the media system get dismantled. And there were multiple signals, several different kinds of research projects, several different appeals, several different bodies of evidence, network data, survey data - that all showed a slow change in the ownership structure of Hungarian media. And there was a clear turning point, perhaps, the spring of 2014, in which the last independent media outlets were facing significant Internet-related taxes. Their audiences had diminished, Bertelsmann was no longer that interested in having too much of a heavy-handed steering of its properties in Hungary. So, you have a mechanism for watching a media system decay. But you didn't actually intervene in Hungary at the important moment where intervention might have made a difference. So, in the years ahead, as you notice the ownership structure of media systems in your Member States get seriously out of whack, you must intervene -with more than words and communications, but with the pull and push that you can have in markets.

The second thing: the opportunity, I think that you may have, is in research capacity. It's important - you might expect me to say - it's important to make long term investments in research capacity. But it is because of the European Research Councilthat the world knows of this problem and it's because of the European Research Councilprojects that we were able to collect large amounts of data to demonstrate that junk news takes advantage of social media algorithms to manipulate public life. I do not think that the EU should have to pay other organisations to fact-check content on Facebook. I don't think that working journalists or civil society groups should be responsible for fact-checking content on Facebook. But, clearly, supporting some creative initiatives among these kinds of actors will catch a few problems.

The greatest opportunity you probably already have is to set up data sharing arrangements between social media firms and the European Research Council. Facebook doesn't collaborate with researchers - I've said this multiple times in fora and once with a Facebook staffer nearby. He said: 'We collaborate with researchers - we hire them all the time!' That's not quite the collaboration I have in mind. **Researchers who do try to work with Facebook always sign non-disclosure agreements and can never publish replication data. The most important science journals require replication data so the most important social scientists with the biggest questions don't turn to the most important source of data. If a scholar can survive peer review and clear ethics protocols, which are tougher than Facebook's ethics protocols, and they are being financed by one of the world's great public agencies, they should be given access to the social media data that would help with significant public problems.**

Thank you.

Ann Mettler:

Thank you so much. And last, we go to Professor Nielsen, please.

Rasmus Kleis Nielsen:

Thanks very much. In line with my opening remarks about the importance of protecting open societies, I think it's important here to underline that perhaps the most important thing the European Commission is doing in tackling the issues facing all democracies in the digital age is aggressively confronting Member States who are not honouring the fundamental rights they're committed to in the convention and the charter.

Beyond that it's clear that the problems that we face around this innovation are multifaceted and complex, but there are also shared problems and it's important that the Commission work with Member States as well as other relevant stakeholders to develop shared responses to these shared problems.

I think some of the main things the Commission can do can be informed by some of the specific steps already taken. I think the communication on online platforms is useful in underlining the utility in embracing the democratic social and economic potential of the growth of digital media and in emphasising the need for a balanced and predictable regulatory and liability regime and in insisting on the importance of targeted and problem-driven approaches to specific identified problems.

Similarly, I think the communication on tackling illegal content online is useful in insisting on what is legal offline is also illegal online, for example foreign states meddling with our politics. Notions like 'trusted flaggers' are useful and I think could be relevant for discussions on disinformation, as are insistence on collaboration with law enforcement and the importance of transparency. And also of course here we need to recognise again that many of the things we discuss under the heading of disinformation is not actually illegal, so it's not covered by this particular set of initiatives.

But I am encouraged by the evaluation of this process by DG Justice, which has reported what they call 'significant progress' on the code of conduct on hate speech that is developed in collaboration with the platform companies. So it's clear that there is much yet that shall be done, must be done, also by the same companies. But it's encouraging to see that multi-stakeholder processes can actually deliver progress in an area where I think as I said before we need to be cautious before we turn to regulation, unless we have very clear definitions of what exactly it is we want to regulate.

What else can the commission do? I've underlined the importance of trying to strengthen the institutions that help citizens enjoy the benefits of open and free societies. **I think we need to look at the VAT harmonisation process to make sure that publishers are not punished for investing in the future and rewarded for investing in the past. It is baroque that privilege printed newspapers over online news distribution in 2018. We need to think about the state aid directive and whether Member States are unable to support independent media and what the role of public service media is in an increasingly digital media environment - and genuinely independent ones.**

You should think about whether the Commission can provide more support for the journalistic profession in terms of training, in terms of continuing education, upskilling and basic protection; need to think about whether the Commission can lead itself, but also encourage Member States to do more on making public data openly available in machine-readable formats for fact-checkers and other independent third parties and also when the commission needs to step in to ensure that those platform companies who do take seriously the responsibilities of providing an infrastructure of free expression are also protected from those who would push them to actively distort that debate or police acceptable speech.

Secondly, it is again perhaps unsurprising that a researcher says that more research is needed, but I have to say - given the gravity of the discussion we having today and the gravity of the discussions the Commission has led on and Commissioner Gabriel has led on, I have to say **it is striking how little we know from independent**

evidence-based research about the scale, scope and consequences of problems of disinformation and 'fake news' across Europe and I find it deeply disturbing that we are considering policymaking and intervention without actually first providing an evidence base of some sort.

We would never do in public health, we wouldn't do it in environmental impact assessment and it frightens me that we are considering doing this with democracy. I think the Commission can lead on this in ensuring that there is funding available, including other funders being incentivised to support independent evidence-based, timely and accessible work that can document the nature of the problem, assess the impact of it, assess the efficiency of interventions to counter it and help - or relevant parties - both counter it, but also help citizens understand it and journalists cover this.

As was rightly said before, we need a public discussion of this that has to be reality-based, rather than driven by alarmist speculation, as this is sometimes the case. We need to not exaggerate the problems we face – the problems are real, but that does not mean that they are everywhere or that there are pervasive or ubiquitous.

Thank you.

Ann Mettler:

Thank you so much. And now I am turning back to Ulrik for the sixth – and last – question.

Question 6: In a nutshell, what is your main message to the European Commission regarding what should (or should not) be done about 'fake news' and disinformation online?

Ulrik Trolle Smed:

Thank you very much, everyone. We are now almost there, after this tour de force on 'fake news'. This will be the sixth and final question and time for your main take-aways.

In a nutshell, what is your main message to the European Commission regarding what should (or should not) be done about 'fake news' and disinformation online?

You will have one minute each, maximum. The first one to speak will be again Mr Giles.

Keir Giles:

Five quick steps

First, recognise the threat - admit at the highest political level that there are hostile actors who wish to do us harm.

Next, gather the evidence. As Rasmus has just said, find out what is working when they try to do us harm and what is not.

Third, decide whether or not you want to win that fight or allow democracy and institutions to be fatally compromised by those adversary tactics that are actually succeeding.

Next, in order to do that, adequately resource the response in terms of time, expertise, staff, political buy-in and support and endorsement of defensive measures (again at the highest level) and money over the long term because this is not a current crisis, this is a new reality.

And finally, do what our experts are telling you. Not just in-house ones, but also from across civil society. You do not need another set of recommendations right now. You need to act on the ones that have been there for some time.

Ann Mettler:

Thank you so much. Professor Applebaum, please.

Anne Applebaum:

I would repeat: Concentrate on what the EU can do as the EU. What is in your competence as the European Commission.

Don't be distracted by the problems that are really the province of Member States, such as hate speech or online political advertising campaigns and how they should be regulated. Those are really issues for the Member States, each of which has its own laws on hate speech and political ads.

Do think about what you can do. As Keir Giles has stated, you should focus clearly and sharply on the Russian attempts to undermine European democracy, and I agree with his suggestions. In addition to that, I believe that the European Union should focus on the problem of anonymity. Most disinformation campaigns operate thanks to anonymity, thanks to the fact that it's so easy to create fake websites, fake online personas, even armies of fake bots actually that aren't even people, they are computer code. The EU can take a really important step forward by investing in the ideas of online passports and online e-identities, as well as verified email and flags for anonymously created websites. The Commission can put pressure on the tech companies to create these products, and even sponsor them outright. These are measures that can enhance the lives of ordinary people, and could come to be seen as an advantage to European citizenship.

Ulrik Trolle Smed:

Thank you very much. Professor Howard.

Philip Howard:

Thank you. To me the options for us fall into two buckets of possibilities: content regulation or market regulation. Both of them have negative consequences for public life. I think if we want to do something positive for reinventing and reinvigorating our democratic cultures, guiding markets and how they should behave will be the softer-touch method that is preferable over content regulation

I would try to argue that guiding these markets involves creating a system for reporting the beneficiaries of data from our profiles and our technologies. A system of civic data donation so that we can express ourselves as citizens when we want to. We need a digital infrastructure that tithes for the collective good. We need to extend the non-profit rule and we need algorithmic audits before these technologies roll out into public life. And we need the European Research Council to create a data repository that allows researchers to benefit from the collective wisdom that is emerging over platforms - networked technologies. To get us out of the democratic deficit we're in, we must make policy not just for the Internet we have, but for the one that is coming.

Ulrik Trolle Smed:

Thank you very much. Professor Nielsen.

Rasmus Kleis Nielsen:

Thank you. If you want to renew our democracy for the digital age, I think we should focus on reinforcing our commitments to the fundamental values that characterise open societies and see what we can do to support the evolution of institutions that enable citizens to make the most of that freedom and those rights that are provided.

We have to recognise that the societies in which we do this are irreducibly diverse. We do not agree on what the good life looks like and we will not agree on political matters and our democracies are therefore often disputatious. This is not about neat, polite and genteel political debate. It is about fundamental rights and institutions that enable citizens to make the most of them.

When we think about how respond to problems of disinformation. I think we should therefore first be cautious with regulation or the privatisation of policing of political speech that may compromise the very values we are trying to defend. We can consider these, measures but we should be very cautious.

Secondly, we can develop narrow targeted responses to identify specific problems of disinformation - whether those that are driven by foreign states or those that are driven by for-profit operations - and then invest in reinventing the institutions that enable popular government; in this case perhaps particularly importantly what can be done to help professional journalism and news media.

Our parents' generations build Europe from the ruins of empires, fascism and communism and I think it's clear that we can draw from the inspiration of that generation and have the same aspiration, if you will, to build a kinder and gentler form of democracy and capitalism than the one we see elsewhere in the West. I don't think we are the descendants of fearful men and women and I don't see why we should aspire to anything less than what people did before us.

Ulrik Trolle Smed:

Thank you very much. And, finally, Mr Lelyveld, please.

Philip Lelyveld:

Thank you.

Innovation is never stifled. It is only redirected by regulation, the bottom-line imperatives of business, and societal forces. A good story captures and holds your attention. A great story creates 'sticky' memories by engaging your emotions. We are well on our way to developing and deploying the tools that will allow anyone to create and distribute personalised 'sticky' memories on a global scale. The tools don't care whether the story is fact or fiction, true or false. It may make more sense to create a system that identifies, elevates, and rewards a bounded set of data, information, and knowledge that we can verify to be true, reliable, and undistorted, than to try to detect and react to an unbounded flow of false, distorted, and fake content.
Thank you.

Ulrik Trolle Smed:

Thank you very much. This was the closing of the Hearing. Now let me to pass it to Ann again.

Ann Mettler:

Okay – just for some closing remarks:

Thank you very much. We are delighted and very grateful that you have chosen to speak here today and to share your expertise and insights with us on this very important topic of preserving democracy in the digital age. We will now put these valuable insights onto paper and deliver it to Commissioner Gabriel as a contribution to the European Commission's public consultation on 'fake news' and disinformation online.

So, everything that was said here today will be transcribed, will be submitted and will be also put on the website of the European Political Strategy Centre in due course.

We now came to the end of the Hearing and we will now have an informal coffee just outside the room here to which I would invite all of you – the speakers but also the participants here in the room who have been very patient, who I am sure have some questions of their own.

But before we depart the room, may I ask my colleagues, and everyone present, to please give a warm round of applause to our speakers today.

[Applause].

Thank you so much, this concludes this Hearing.