European Commission

COMMISSIONER VĚRA JOUROVÁ

MEETING WITH BRUSSELS REPRESENTATIVES OF FACEBOOK, GOOGLE, TWITTER AND SNAPCHAT

LOCATION: BERL 12/176 [OR IF EXTERNAL, ADD ADDRESS]

DATE AND TIME: [04/03/2019, 14H00]

MEETING OBJECTIVE: TO DISCUSS THEIR RESPONSIBILITIES IN THE CONTEXT OF THE EU ELECTIONS

MEMBER RESPONSIBLE: MONIKA LADMANOVA

DG CONTACT & TEL NO: [redacted]
DIRECTOR: MS MOOZOVA

VERSION: 18/09/2019 10:45

JUST/D3

PARTICIPANTS:

STEERING BRIEF

CONTEXT/SCENE SETTER

You will be meeting with the Brussels representatives of Facebook, Google, Twitter and Snapchat. The agenda for the meeting is as follows:

1. Info about the Elections package, its implementation and the follow-up Council conclusions;
2. Update on European elections network and its meetings:
3. Discussion about main gaps in the commitment to the integrity of election process and identification of key short-term actions.

On 27 February the European cooperation network on elections met for the second time to discuss monitoring and enforcement. The discussion showed that internet platforms and social media companies should do more:

- to raise awareness among users about online manipulation techniques;
- to engage equally with national authorities across the Union especially in this crucial period before the European elections;
- demonstrate more diligence to make available transparency tools which enable citizens to identify online advertising (including online repositories and clear marking, as already envisaged in the Code of Practice on disinformation),
- to take further measures to allow people flag suspected failures to comply with campaign norms (e.g. a "report content" button).

The elections package issued by the Commission on 12th September 2018 recommends to Member States to encourage transparency of paid political ads and communications and to engage with online platforms in awareness raising activities aimed at increasing the transparency of elections and building trust in electoral processes.

On 28 February the European Commission published reports by Facebook, Google and Twitter covering the progress made in January 2019 on their commitments to fight disinformation in the context of the implementation of the Code of practice. The Commission asked to receive detailed information to monitor progress on the scrutiny of ad placement, transparency of political advertising, closure of fake accounts and marking systems for automated bots. You and Commissioners Ansip, King and Gabriel delivered a joint statement calling for more progress on the commitments under the Code of Practice, details showing that new policies and tools are being deployed in a timely manner and with sufficient resources across all EU Member States, and more information on the actual results of the measures already taken.

OVERALL OBJECTIVES

The aim is to seek the commitment from the companies that they:

- comply with the national electoral laws and pay attention to the traditional principles that apply for offline environment;
- in particular, apply silence periods for political advertising in line with national rules;
- maintain communication channels with all Members States and national election networks and not only selected ones to support enforcement of the national rules.

IT platforms should also clarify how they ensure that citizens are enabled to identify online advertising and support the implementation of the Commission's September Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns, in particular regarding the transparency recommendations addressed at European and national political parties and campaign organisations (points (8),(9), (10)).

LINE TO TAKE

1. The Package

- The Commission has issued on 12 September 2018 an elections package including Guidance on data protection and a Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns.
- The elections package has been welcomed by both the European Parliament and the Council. Data Protection authorities are considering actions also in the framework of the European Data Protection Board. The European Data Protection Supervisor organised in February a conference on the topic covered by the Package.
- Platforms are bound by the GDPR and should be able to demonstrate how they comply with it as regards personal data linked to electoral processes. You need to have in place appropriate technical and organisational measures and be able to demonstrate that you complied with data protection requirements effectively.
- Platforms should support the implementation of the principles contained in the Recommendation of the Commission issued on 12 September and support enhanced transparency, the protection of the integrity of the European elections and building trust.

2. Update on European cooperation network on elections and its meetings

- The second meeting of the European cooperation network on elections took place last week on the 27/2.
- Issues discussed included among others:

  - data protection monitoring, the new mechanisms when data protection infringements are used in order to influence the outcome of European elections, and the role of data protection authorities in the new sanction procedure;

  - media plurality and the engagement of ERGA (bringing together national independent regulatory bodies in the field of Audiovisual Media services) in the implementation of the Action Plan on disinformation and the Code of Practice against disinformation;

  - law enforcement including cooperation with EUROPOL and examples of activities to take down organised crime online, Dark Web markets and their relevance in the electoral context.

  - participatory applications involving citizens in the monitoring elections by reporting instances of abuse;

  - fact-checking activities;

  - the mapping exercise conducted by COM on the situation in the Member States;

  - exchange of specific best practices;

  - experience of cooperation with online platforms, with some Member States reporting that no engagement has taken place so far;

- The envisaged table top exercise on cybersecurity.

All relevant information is published on our website.

3. Main gaps in the commitment to the integrity of the election process and key short-term actions

- A key objective of the elections package is to promote the transparency of paid online political advertisements and communications. Such transparency concerns the political party, political campaign or political support group **behind** paid online political advertisements and communications, information on the **source** of funding and on campaign **expenditures** for online activities, and **targeting criteria** being used. Citizens should be able to easily recognise online political advertisements and communications and who is behind them. Member States are encouraged to engage with platforms in this context and apply sanctions as appropriate.
- Last week the Commission published reports by Facebook, Google and Twitter covering the progress made in January 2019 on commitments under the Code of Practice on disinformation.
- Commissioners Ansip, King and Gabriel and I issued a joint statement demanding more progress on commitments, more detail on new policies and tools, and specific benchmarks to enable the tracking and measurement of progress.
- During the second meeting of the European cooperation network on elections, Member States were clear that they needed greater engagement and reassurance that social media platforms were aware of national laws and procedures in the context of elections, and that they were **taking steps to ensure that their activities would be in compliance with these rules**. Platforms should support the application of **electoral safeguards like silence periods for political advertising** (in line with national rules).
- They sought more clarity at a national level about the exact timeline when the platforms would be implementing their commitments under the Code of Practice, and whether further steps would be taken to support them in their own efforts in implementing the September Recommendation, in particular regarding the transparency recommendations addressed at European and national political parties and campaign organisations.
- A commonly expressed concern is that **engagement and cooperation should be afforded to all Member States on equal terms**. I urge you to do this.
- I would suggest you to **seek the political advertisers using your services to declare that they comply with national rules and that they have considered the Commission's September Recommendation as regards transparency to be ensured in the electoral context.**
- A strengthened engagement with relevant actors is necessary to promote transparency, and platforms should support Member States in achieving this.
- I would like you to **clarify how you intend to roll out tools in all Member States which enable citizens to identify online advertising and understand who is paying for it, and also to consider going further and empowering citizens to flag failure to comply with national rules relevant to the**

electoral context. Information could be shared with national authorities, as appropriate.

BACKGROUND

Regarding the elections package

The Commission adopted a package of measures in September 2018 to promote free and fair elections in Europe. The package includes:

- Data protection guidance;
- a Communication on securing fair and free European elections;
- a Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns;
- and proposal to amend Regulation 1141/2014 on the statute and funding of European political parties and foundations.

The European Parliament welcomed this package in its Resolution on the Facebook-Cambridge Analytica case adopted on 25 October 2018.

On 19 February the Council adopted Conclusions on the September election package welcoming the Commission's initiative and establishing detailed commitments from the Member States for actions in support of the main elements of the package, in particular the formation of elections cooperation networks and the initiatives to support greater transparency in campaign financing and advertising, strengthening citizens awareness and resilience, compliance with European data protection norms, and combating disinformation and cyberattacks. Among others, these Conclusions underline that free, reliable and pluralistic media underpin effective and healthy democracy and that it the same vein, open, secure and accessible internet and online platforms can facilitate participatory, transparent and effective democracy. They also recall the importance of guaranteeing to citizens an open public sphere and of ensuring a level playing field for political campaigning and electoral processes that citizens can trust.

They stress the need for urgent action to protect the Union and the Member States, their bodies and policies from targeted disinformation campaigns, which are likely to increase in the run up to the 2019 European Parliament elections and call for awareness-raising activities aimed at protecting the integrity of the electoral process in cooperation with platforms.

On 27 February the European cooperation network on elections met for the second time. It included discussions on monitoring and enforcement of activities relevant to the electoral context, on specific steps to ensure transparency of paid political advertising and communications and of funding, and on awareness raising activities, also jointly with the media and online platforms.

Member States expressed concerns at the lack of clarity form the platforms regarding the timetable for the implementation of commitments by the platforms of commitments under the Code of Practice, and sought greater engagement from them in supporting Member States monitoring and enforcement activity in the context of the elections. Following this meeting, the Commission proposed a strengthened engagement with relevant actors to promote transparency, and

called on the platforms to support Member States in achieving this.

You presented the elections package to the European Data Protection Board last year. Some data protection authorities have undertaken specific actions. The IE data protection authority intervened during the second meeting of the European Cooperation Network on elections on 27/2 underlining the need for an holistic approach to activities which indicate that voters are being influenced. We understand that the EDPB intends to adopt a joint statement on data protection in elections, which sets out detailed advice to Member State data protection authorities.

The European cooperation network on elections will meet next a priori for the last time before the European elections on 4 April, with discussions including awareness raising campaigns for citizens, political parties and the media, Member State reflections on the contribution of the media platforms to implementing election package recommendations to promote transparency, and the role of the network in supporting proactive electoral monitoring, including on the basis of risk scenarios studies. A table-top exercise to explore cybersecurity risk scenarios and solutions is being organised for the network on 5 April.

A key part of the Recommendation is taking steps to promote transparency in political advertising ahead of the elections to the European Parliament. Points 8, 9 and 10 ask national political parties, foundations and campaign organisations to:

- ensure that citizens of the Union can easily recognise online paid political advertisements and communications and the party, foundation or organisation behind them;
- make available on their websites information on their expenditure for online activities, including paid online political advertisements and communications, as well as information on any targeting criteria used in the dissemination of such advertisements and communications;
- make available on their websites their paid online political advertisements and communications or links to them.

This reflects the importance of increasing the transparency of elections processes, at the same time increasing the accountability of political parties participating in the electoral process in the Union, monitoring and oversight and voters' trust in that process, which underpins the Recommendation. It also aligns with a previous amendment to Regulation 1141/2014 on the statute and funding of European political parties and foundations, adopted in 2017, which included the introduction of a requirement on European political parties to ensure that the national political parties which affiliate with them make this affiliation clear in their websites, as a condition for the European political party's access to European funding.

Point 11 of the Recommendation asks Member States to apply appropriate sanctions on political parties and foundations at national and regional level for cases of infringements of data protection rules being used to deliberately influence or attempt to influence the outcome of European elections. The Recommendation also asks national data protection supervisory authorities, in compliance with their obligations under Union and national law, to inform the Authority for European political parties and foundations of any data protection

infringement decision, where it follows from that decision or there are otherwise reasonable grounds to believe that the infringement is linked to European political party or foundation political activities with a view to influencing European elections. Such information is necessary in order to ensure a proper functioning of the sanctions on the European political parties and foundations, proposed by the amendment to the Regulation 1141/2014 on the statute and funding of the European political parties.

Finally, point 15 of the Recommendation asks national political parties, foundations and campaign organisations to implement specific and appropriate measures to prevent cyber incidents and protect themselves against cyberattacks. The Member States are separately called upon to provide support for such activities as appropriate, and we are aware from our contacts with Member State electoral and cyber-security authorities through the European cooperation network on elections that such support is being provided in some states.

You are writing to national political parties and foundations to draw their attention to elements of the Recommendation addressed to them.

Mapping of national electoral campaign rules and rules governing political parties funding and spending

In the context of the European network on elections, the Commission undertook a mapping of electoral campaign rules and rules governing political parties funding and spending, which is a living document and will be updated in contact with the Member States on an ongoing basis. The first results of the Commission's mapping have revealed a number of differences among the Member States as well as gaps and areas where the overall system could be strengthened, particularly from a European perspective.

Given the democratic principle that no electoral law changes should be made in the 12-month period preceding an election, some of the identified gaps in legislation will need to be addressed more fully in the longer term. Promotion of enhanced compliance among the relevant actors – such as political parties and social media providers – is something the Member States should focus on in the remaining period before May European elections.

When it comes to transparency of political advertising, only a half of the Member States have requirements for transparency of paid political advertisements and communications, and only a few of those have specific rules applying to social media.

More concretely:

-Requirement to disclosure source of the political ad: BG, CZ, DE. FI, FR, HU, LT, LV, PL, SI, SK

-Outright prohibition of publishing anonymous ads: BG, LT

-In some MS, registration number with election authority must be also visible on the ad (CZ, RO)

-In many cases there are no special mention of social media in the legislation, but the law is applied also in this context

-Social media is explicitly included in some legislations: CZ, FR, PT, DE (for illegal hate speech), RO (included with regards to limits to campaign spending)

Regarding the Code of Practice

In October 2018, online platforms and the advertising industry agreed on a self-regulatory Code of Practice on Disinformation. The Code includes several commitments structured around five main areas of intervention:

- Scrutiny of ad placements;
- Political advertising and issued based advertising;
- Integrity of the services;
- Empowering consumers;
- Empowering the research community.

The Code is expected to help provide more transparency on sponsored political advertising, so that online users will be able to easily distinguish paid-for content from journalistic content. It should also contribute to effectively demonetise websites used to spread disinformation online. Advertisers will receive the necessary information to decide whether they place or not their ads in certain pages and sites that have been identified as purveyors of disinformation.

The Code should also bring about a reduction of fake accounts and automated bots that can be used to manipulate the public opinion by spreading and amplifying disinformation.

In line with the Action Plan on disinformation, the Commission has received Monthly Reports from Google, Facebook and Twitter addressing actions taken during January 2019 towards implementation of the commitments on electoral integrity. In a statement issued on 28th of February, the Commission, while acknowledging the benefits of the policies that the platforms are rolling out to support the integrity of elections (better scrutiny of advertisement placements, transparency tools for political advertising, and measures to identify and block inauthentic behaviours on their services), has indicated that it would need to see rapid progress on the commitments made by the platforms that there is room for improvement for all signatories. The concerns expressed by the Commission relate to the absence of details showing that new policies and tools are being deployed in a timely manner and with sufficient resources across all EU Member States. The reports issued by the platforms also provide too little information on the actual results of the measures already taken. Furthermore, the platforms have failed to identify specific benchmarks that would enable the tracking and measurement of progress.

Google has reported on actions taken during January to improve scrutiny of ad placements in the EU. Facebook and Twitter did not.

Google published its new policy for "election ads" on 29 January; it is available in 25 EU languages. Advertisers seeking to run such ads must be verified and document that the they are an EU-based entity or citizen of a Member State. Facebook's pan-EU archive for political and issue advertising will be available in March 2019. This was considered as very late by some Member States during the last meeting of the European Cooperation Network on elections as the campaign has already started in some Member States.

Google reports that it is staffing dedicated elections teams to prevent election-related abuse of its services, clamp down on malicious behaviour and react to

breaking threats. It does not, however, provide detail. Facebook and Twitter provided some information in this area, but with little detail.

Regarding prior engagement with these companies

There have been a number of meetings between the Commission and the companies over the past months.

Most recently, in early February, Facebook wrote to the Commission, seeking approval for an approach to providing advertising services in the context of the elections, which would restrict the ability to place political adverts targeted at users from a particular Member State to residents of that state, during the campaign period.

The Commission did not take a position in its reply as it is not its responsibility to facilitate the compliance of social media platforms with national electoral and advertising rules. The reply from the Commission made clear that the monitoring and enforcement of elections falls within the remit of national authorities, with an obligation of those taking part in advertising and campaign activities in the context of elections to ensure compliance with relevant national rules applicable to electoral matters while at the same time respecting any rule applicable to companies operating in the internal market. Political parties, foundations and campaign organisations are also required to comply with specific national rules in an election context.

Facebook replied on 27 February, stating that the decision was made to only allow people to run advertisements in a Member State if they have passed an authorisation process that will include checking they are resident in that Member State.

A meeting with Facebook, or with more of the providers, on this point at technical level is being considered but has not been committed to.

DEFENSIVES

What has been the follow-up of the meetings of the European cooperation network on elections?

- The European cooperation network on elections met for the second time last week. These meetings serve to continue meaningful exchanges with the Member States on all aspects of the package on securing free and fair elections, in particular on monitoring and enforcement related topics.

- This includes steps to ensure transparency of paid political advertising and communications and of funding, and awareness raising activities including with the media and platforms. The first results of the Commission's mapping of national electoral campaign rules and rules governing political parties funding and spending have been presented and will continue to be discussed with the Member States.

What is your position on the decision of Facebook to restrict the ability to place political adverts targeted at users from a particular Member State only to residents of that state?

- It is your responsibility to ensure compliance with national and EU law.
- Imposing limitations based on residence considerations could raise questions of compliance with national law and EU law regarding voting rights of mobile EU citizens.
- Mobile EU citizens have a right to vote and stand as a candidate in municipal elections and in elections to the European Parliament in the Member State of their residence, under the same conditions as nationals of that state (Articles 20 and 22 TFEU).
- This right implies not only the formal suppression of the nationality requirement as a condition for EU citizens to stand as candidates in municipal and in European elections, but requires every Member State to ensure that all EU citizens who reside in that State are put on equal footing with the nationals as regards the conditions for exercising this right. Ensuring full enjoyment of this right encompasses, for example, possibility of fully making use of the essential instruments and infrastructure in the electoral process.

Contact point: [redacted]

Director: Irena MOOZOVA

From: [redacted]
To: MOOZOVA Irena (JUST);
Cc: [redacted] JUST D3
Subject: Flash 04/03 - Meeting Commissioner Jourova with IT Platforms
Date: mardi 5 mars 2019 11:19:14

Flash 04/03 - Meeting with IT Platforms (Facebook, Google, Snapchat, Microsoft, Twitter): Commissioner Jourova, Daniel Braun, Monika Ladmanova, [redacted]

- Commissioner underlined again the importance of guaranteeing free and fair elections and that the platforms should comply with national legislation, as well as with EU initiatives (Election package, Code of Practice etc.)
- COM also reported briefly on the last meeting of the European cooperation network on elections, where the Member States discussed all aspects of the Recommendations: data protection (including sanctions), electoral laws (it is clear that these rules are fragmented); cybersecurity table top exercise, as well as transparency and advertising. For the latter, the Member States asked for more information from the platforms on their initiatives.
- Commissioner framed the discussion as a process leading up to and beyond the elections, with certain actions being needed immediately, where the focus is on delivering free and fair elections while preserving rights, and the in the longer term, where the focus should be on achieving a balanced regulatory environment.

Short-term actions with the focus on European elections

- The platforms reported to be already engaging with national authorities, but were supportive of reaching out to the national networks in particular **and have asked for contacts of the representatives of national election networks, which COM agreed to provide**.
- In terms of transparency tools, FB and Google are due to roll out their transparency of political ads in March. Most platforms will implement compartmentalisation (in other words, you can advertise only where you have residence). The verification method mentioned by several platforms involved a proof of identity (ID card), plus performing a search check of the data provided by an advertiser.
- Some negative feedback has also been received. E.g. in DK Snapchat oblige people to demonstrate residence in DK, and have received complaints that this rule does not exist nationally and that they are introducing regulation.
- A vital part of transparency is also publicly available repository of all ads. FB said that they will run a public repository where advertisements are associated with a party, and can be checked on their page (Google also maintains such a repository).
- Some platforms (including Google) announced they have updated their policies to require that the advertisers declare their compliance with the national election rules.
- Microsoft raised the importance of cybersecurity and cyber incidents they have discovered and asked where they could report their findings, especially in view of the Rapid Alerts System to be set up. Daniel Braun will facilitate contact with RAS team. Member States should be primary input, but platforms should also contribute.
- FB reminded that besides foreign interference, they have observed in some cases also domestic actors trying to interfere.
- Snapchat is in touch with voters via the EP to recommend participation in the elections. FB, Google are also doing this.

Longer-term, after European elections

- Commissioner noted that efforts for protecting the integrity of European elections are not only solving an adhoc problem, but also testing a potential (self)regulatory model. She suggested that all actors unscientifically assess after May whether our efforts were proportionate and effective.
- Most platforms called for involving civil society in this reflection, which has strong parallels to Code of Conduct, as well as more platforms/other companies. The work on this does not end with these elections. Wants to make this work more inclusive of other companies. Some of them also said that we should also consider whether there this scope for EU law in this area, providing guidance for what to do and how to actually produce "transparency" and what their commitment should be.
- **COM: will carefully raise at JHA that the IT companies** are asking for greater clarity regarding any gaps in electoral rules, and what contribution is desired by the Member States from them.

3

COMMISSIONER JOUROVÁ

TECHNOLOGY & DEMOCRATIC FREEDOMS: MOVING FORWARD WITH NEW LAWS @MICROSOFT CENTRE

DATE AND TIME: 21/01/2019 13:00-14:00

MEETING OBJECTIVE: TO DISCUSS THE RULES THAT SHOULD GOVERN THE DEVELOPMENT AND USE OF AI-ENABLED TECHNOLOGIES

MEMBER RESPONSIBLE: DANIEL AND WOJTEK

AI

TABLE OF CONTENTS

STEERING BRIEF

CONTEXT/SCENE SETTER

You will be participating to this event organised by Microsoft Centre to discuss the rules that should govern the development and use of AI-enabled facial recognition technologies.

You will give keynote remarks. Brad Smith, President and Chief Legal Officer of Microsoft, will also provide keynote remarks. It will be followed by a panel discussion moderated by Bojana Bellamy, President of Hunton Andrews Kurth LLP's Centre for Information Policy Leadership.

OVERALL OBJECTIVES

- Underline that the Commission is very aware of the sensitivities including opportunities and challenges of the use of facial recognition technologies.
- Underline that such technologies of course have to be developed and deployed in full respect of EU law, including the GDPR and consumer acquis.
- Inform about the Commissions work to ensure an ethics and Fundamental rights approach to the development of AI in general and facial recognition on particular (notably through the High Level Expert Group on Artificial Intelligence that are currently)
- Comment on how the Commission will assess the need for possible further regulatory action.

SPEECH TECHNOLOGY AND DEMOCRATIC FREEDOMS

Introduction

Thank you, Brad, for inviting me here and for today's debate on Technology and Democratic Freedoms.

Technology and digitalisation have changed our lives beyond recognition; it revolutionised the way we work and travel, the way we learn about things. It offers no doubt many opportunities for society and for economic innovation.

But recently, last year in particular, we have become acutely aware of the challenges that digitalisation and technology pose to the rule of law, democracy and fairness. Regularly we see shocking revelations, whether in relation to Cambridge Analytica, foreign meddling in elections or a hacking attacks on personal data of German politicians. If all this is not a wake-up call for us all, I don't know what is.

And it had an impact on the private sector and the regulators alike. We have reached a moment where it has become clear to everyone that the dialogue between politics and technology is not only unavoidable. It is absolutely needed and desired.

I would like to start by sharing with you my thoughts about some of the problems amplified by digitisation for our societies, before I offer some ideas about what we could do about it.

But, as this event is about tech meetings politics, let me share something personal with you. I don't think of myself as a very

'techy' person. I am certainly no coder or engineer. I even deleted my Facebook account a few years ago because I like to communicate –but the constant stream of hateful comments I was getting was not communication. I do use an iPad though.

Although a politician, I am also a sociologist and a lawyer by training and this background is shaping my views and my actions.

Promise of better future but with negative side effects

As a sociologist I am very mindful of the effects digitisation has on our society.

Think of Artificial Intelligence and automation for example. I know Microsoft has been thinking about it a lot and even released a book on Artificial Intelligence and its role in society a year ago.

We all have high hopes about the impact of AI. Autonomous cars, smart cities, modern concepts of mobility, progress in medicine, education or transport... But on the other hand, it raises plenty of legal and ethical questions about fundamental rights, trust, liability and the role of humans in an economy driven by AI.

On top of this, a recent study estimates that up to 800 million jobs could disappear by 2030. I read that Microsoft imagines that by 2038 personal digital assistants will be trained to anticipate our needs, help manage our schedule, prepare us for meetings, reply to and route communications, and drive cars.

But this means that the jobs of three or four of my colleagues will disappear.

New jobs will be created, I'm sure, but it is clear that all these things bring huge societal change and challenge, not only for the labour market but to our lives in general.

We have to watch out on the effects on society, whether a new type of digital poverty and social exclusion will be created by all this.

Especially, that I think the trust to those that lead this revolution today, including to some extent our hosts today, has eroded and created a lot of anxiety rather than enthusiasm.

Today many are closer to believing a dystopian vision scarily captured in the episodes of Black Mirror rather than a prosperous future.

Values

The pace of technological revolution is so huge that it is difficult to catch up. In cases like this, we should always go back to the basics. And the EU and its Member States have been built on a solid foundation of democracy, freedom, fairness and the rule of law.

Digital or not - for values this should not matter. Technology is a means to an end, not an end itself. It should serve the people.

Yet, many of the tech champions were labelled as the disruptors. They wanted to 'move fast and break things' often disregarding those core values.

These things started to change, but the only long-term solution I see is for a democratic society to take control of this process and put people at the centre of the technological revolution. And the politicians and indeed the tech companies have their roles to play to make that happen.

Privacy of data

On the regulatory side in Europe we decided to adopt a set of modern rules on data protection known as GDPR. The new regulation aimed to reconcile two key things: give people more control to restore trust to digitalisation whilst opening channels for modern innovation following the principle of privacy by design.

It is an advantage for the EU to be advanced on modem privacy rules. Because we must not ignore lost confidence in the tech revolution. Two-thirds of Europeans (67%) are concerned about not having complete control over the information they provide online. This mistrust will have an impact not only on the future of digital technology, but also on development of artificial intelligence or any type of big data research such facial recognition.

GDPR is a wide-reaching regulation. The way we thought about it is that it should be technologically neutral. So, it doesn't matter if we talk about Artificial Intelligence or facial recognition. The principles of the GDPR should apply to all of this.

This was a step in a right direction, even though when we strated this process in 2012 many people thought we were "foolish".

Now, as our knowledge about how data can be used is growing, thanks to numerous scandals, like the Facebook / Cambridge Analytica one, many people, including tech CEOs themselves, admit that the hands-off approach to privacy might not be the best. And we see that many countries in the world are discussing horizontal privacy rules, including the US.

I understand there are concerns about the impact on innovation of the GDPR, especially for SMEs and start-ups and we have to watch it. In fact I am organising an event in June dedicated to this issue. But it's clear that data protection is not a luxury; it's a necessity.

Online content and responsibility of platforms

But legislation is not the only thing the EU can do. And again, let me share something with you which may come as a surprise to those who see the Commission as a regulating monster.

I don't have a knee-jerk reaction that regulation is the best way to solve all the problems. It could be, but we have to explore all the options available on the menu.

That is exactly the approach we took to illegal online content. We adapted our response to different types of content. The bigger the potential harm for the people, the faster and stronger the reaction should be. That's why we proposed the legislation to remove terrorist content within one hour from when the content is flagged.

Then, you have the self-regulatory approach relating to illegal hate speech such as racism and xenophobia. The Code of Conduct

I agreed with the platforms, including Microsoft, two years ago brought very good results, very quickly and rallied all actors around the common understanding of the fact that some things are simply illegal – offline as well as in the online environment. And this approach proved to be effective.

Artificial Intelligence and Facial Recognition

We also try to have a similar approach to AI. On the one hand, we want to embrace the fantastic opportunities and make sure Europe is a good place for research and investment in this technology and does not lag behind others, in particular the US and China.

On the other hand, we have to ensure that people trust it and we must address people's concerns.

In this context, the use of facial recognition technologies is a challenge.

While such technologies can help improve criminal law investigations by helping to identify suspects, improve security for instance at border controls and in banking to prevent fraud, it can also be misused and adversely affect our privacy.

How many of us would feel comfortable when facial recognition is combined with sentiment analysis indicating our reaction to an event in terms of being happy, sad, bored or excited in order to through automation subsequently provide us with content or suggestions that fits with that emotion?

In Japan, I visited a futuristic bedroom prepared by Panasonic with a mirror that does exactly that. For me this was a rather disturbing experience.

The GDPR already provides some of the answers to this challenge. It prohibits in principle the use of automated decision-making, such as in AI, except where this is done on the basis of a law or with the explicit consent of the people.

The use of facial recognition technologies for purpose of uniquely identifying a natural person is only allowed where it fulfils strict conditions.

But the GDPR alone will not answer all the questions. That's why we have started thinking what else we can do, starting not by regulation, but by bringing people to the table. we need to follow the results of the work of the High Level Expert Group on Artificial Intelligence that is currently working on developing AI ethics guidelines. We expect that this work will be ambitious and go beyond guiding principles and rather form a concrete operational tool for industry for the development and use of IA.

Once we have seen how far the guidelines take us the Commission and the Member States must, as a second step, stand ready to monitor developments, including at national level.

We are also looking into liability in the AI context. In March last year a first pedestrian was killed in Arizona by an autonomous car. Once this technology is in full swing, the costumers and citizens must know who is liable. The car owner? Manufacturer? Or one of many software providers?

The way forward

The main purpose of today's discussion is not only to assess what has been done. I actually think we tried to address the most urgent issues and we have started a number of very important debates across many policy areas, including also competition policy.

But as European politics is turning slowly to election mode and the discussion about the future of Europe will hopefully move also to public squares, I would like to discuss a number of ideas we should be considering.

And I find it timely, because I see in the public debate some questions appear that in my view miss the real issues.

To break up Facebook or not – is not the right question.

To regulate tech or not – is also not the right question.

They are too narrow and won't solve the issues that that are ignited by the tech revolution.

The big question we should try to answer is what place tech should have in our society.

I believe we need to change our mind-set and apply the rules that we have for the offline world in the online environment. That is what I have pushed throughout my mandate, the Code of Conduct on illegal hate speech being one example of this.

Also, we need to go beyond the headline grabbing questions. We need to have a systematic approach to decide where and for which aspects we need regulation, and if we do, whether it's better to focus on self-regulation and how to agree on a system of compliance with our values.

An architect needs to respect and comply with the building code and a number of safety legislations. For the digital world we should think of a similar system, a mix of ethical, legal and societal norms that would ensure continuing trust in the greatest revolution of our lifetimes.

Here are some ideas that in my view we should be focusing on also in the next mandate of the European Commission.

First of all, we should continue to follow 'the people's first' approach. Technology should be predominantly for the people, not for profit or growth. I don't believe these have to be exclusive, though.

Two – we should find the way to better understand the impact of tech regulation or the lack thereof in our lives. When we talk about regulation, we do environment or economic impact assessments. Yet, the discussions we are having are about the impact of tech on democracy and the rule of law. In my view, it is time to consider the impact on fundamental rights, values, democracy.

Third, closely linked to that, we should think how to implement the 'values by design' approach by companies, similar to our privacy by design approach in the GDPR. This would mean for

example ensuring that programmers think from the start of building algorithms about how this could affect our fundamental rights.

Forth, we should not be afraid to have a serious discussion about accountability in the online environment. The e-commerce directive serves its purpose and I am not saying necessarily 'let's open it'. But we have to talk about it in the future, also in the new context of AI.

Speaking of AI, as I mentioned, we have to be very careful if and how to regulate. We have our fundaments, GDPR, and I don't think we need another huge legislation specific to AI only. Given that AI could be applied in almost any field, like the Internet, we should analyse and reflect carefully before creating specific set of rules for AI alone. Rather we should now look into adopting the existing rules on for example, product safety, data, discrimination or cars to take into account new developments.

Fifth, we need to assure algorithm transparency and accountability to allow for the tracing of and prevention of bias, discrimination or any use of algorithms that would be contrary to individual rights.

We should think of installing black boxes, like on the planes, which can record everything happening in the AI system like in the autonomous cars, so we can work out what happened if things go wrong.

Sixth, I would also want to make sure that Europe is a place that embraces innovation and allows for ideas to grow. There are

places in Europe that champion fintech or biotech, but when it comes to AI we are lagging behind the US, and more and more China.

We have to find a way to allow start-ups to innovate and to grow in a more strict regulatory environment in Europe. We could think of lessons we learn from the fintech industry and think of regulatory sandbox for start-ups when it comes to privacy or data not to scare people away from Europe.

And whatever regulation we come up with, we have to get better in assessing its impact on SMEs.

I want to play an active role in the last year of my mandate to prepare the ground for this discussion – I hope today is the important part of this process.

Conclusion

I have spent quite some time discussing the negative aspects of the tech revolution. I think this is a crucial conversation we need to have in order not to sleep-walk into another huge crisis that would impact a lot of people.

Our role, the role of politicians, is to make sure that we will bring people and companies and civil society together, and that we will facilitate finding the right answers to these challenges.

This is really a crucial time, given that we are also very worried about potential impact of disinformation and online manipulation ahead of European Elections in May 2018.

We have to work hard, the online platforms, the regulators and the enforcers to ensure that the elections are free from foreign interference and from unfair manipulation.

The democratic process in Europe is already being undermined and I expect the tech companies to step up their efforts ahead of the European elections.

The answers we offer to digital challenges are a great opportunity to prove that we can embrace people's uncertainties and that we in fact also work for the people.

This is the only way to defend our values, not only in the digital, but also in offline world.

BACKGROUND ON AI

The new EU initiative on AI, published on 25 April 2018 in the Communication on Artificial Intelligence for Europe, has three dimensions: (1) boosting the EU's technological and industrial capacity and AI uptake across the economy, (2) preparing for socio-economic changes brought about by AI, and (3) ensuring an appropriate ethical and legal framework.

On the third dimension, the Commission's services have set up a dedicated Expert Group on liability and new technologies that has already started working. This Expert Group will (i) work on guidance on the interpretation of the Product Liability Directive (PLD) and (ii) assess to which extent liability regimes at EU and national levels can address new challenges raised by new technologies. As a result, the Commission plans to provide (i) guidance on the interpretation of the Product Liability Directive and (ii) a report on the broader implications for, potential gaps in and orientations for, the liability and safety frameworks for AI, the Internet of Things and robotics by mid-2019.

LINE TO TAKE

- For the Commission, it is important to achieve two goals: the take-up and development of the technology within the EU as well as the effective protection of our citizens. These goals are linked: for ensuring the take up, we have to ensure that users – citizens, consumers, but also firms using AI – have trust in the technologies.

- The Commission's aim is to ensure effective redress mechanisms for victims and legal certainty for producers with regard to potential damages caused by AI, taking into account the specific characteristics of this technology.

- Alongside the wider AI Alliance and its High Level Expert Group, the Commission has set up an Expert Group working on liability issues for emerging digital technologies.

- The group is looking into the existing Product Liability Directive and beyond, i.e. into the broader challenges brought by these technologies and potential gaps in existing EU and national rules. It will also assist the Commission in setting out possible future orientations on liability, in a report due by mid-2019 that will also look at the safety of these technologies.

(4)

From: BRAUN Daniel (CAB-JOUROVA)
To: LADMANOVA Monika (CAB-JOUROVA); TALKO Wojtek (CAB-JOUROVA); CONSTANTIN Simona (CAB-JOUROVA); HULICIUS Eduard (CAB-JOUROVA); O'CONNELL Kevin (CAB-JOUROVA); NIKOLAY Renate (CAB-JOUROVA)
Cc: [redacted] CAB JOUROVA ARCHIVES; [redacted]
Subject: flash report from Microsoft event "Technology & Democratic freedoms", 21/1
Date: lundi 21 janvier 2019 18:38:08
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png

Bilateral with B. Smith

[redacted]

Privacy is spreading across US, other states will pass privacy laws, which will put pressure on the Congress. Microsoft are pushing for that to be as close to GDPR as possible. Cssr proposed that Microsoft presents at the GDPR one-year-after event. They suggested to look at the date again as 3 June is G20 meeting in Japan focused on data.

Panel discussion

Commissioner delivered the keynote speech with some additional thoughts at the beginning. There she repeated the "Let's not panic" philosophy. She added that we need to look at the rules that apply offline. We need to maintain rule of law and fundamental rights, and want to set world standards. She advocated for cooperation with the tech sector in the Western world with shared values. The rest was the speech as in our briefing.

Brad Smith then had a presentation on how computers can do more and more but what do we want computers to do is a question only humans can answer. This has to start with ethical principles - ethics, bias, inclusiveness, privacy, accountability.

He argued that we need a "regulatory floor" under the market. He said there is a role for self-regulation but not for everything.

1) Privacy: GDPR is the fundamental building block, thanks to it people have a choice
2) Bias

- Implement a new law that requires tech companies to document their capabilities and limitations in view of bias and create a process whereby citizens can understand this
- enable third-party testing for accuracy
- "high stakes scenario" events: only qualified people can use the results, human review

3) Democratic freedoms

This concerns the balance of safety and fundamental rights. Need to limit government surveillance - court order requirement etc.

Q&A

What is human-centric tech?

Cssr talked about exclusion and the feeling of anxiety. People are concerned about uncertainty, inequality and quick changes. Technology has to serve humans and not the other way around.

Does China have a competitive advantage because they do not regulate privacy?

Cssr assessed that in the short term yes but in the long term we are doing it right, the principle that every human matters, this is Europe.

B. Smith thought Europe is the nurturer of privacy in the world, influencing i.a. the state of privacy protection in the US by design. Positive words on GDPR.

How do you apply the offline-online principle with territoriality etc.?

B. Smith emphasised that laws must be technology-neutral way. Territoriality indeed makes things more difficult.

Daniel, Wojtek

Daniel Braun

Deputy Head of Cabinet

European Commission

Cabinet of Commissioner Vera Jourová

Justice, Consumers & Gender Equality

[redacted]

ec.europa.eu

Follow us on:

@VeraJourova

5

[redacted]

From: [redacted]@microsoft.com>
Sent: jeudi 18 octobre 2018 12:04
To: [redacted]
Cc: [redacted]
Subject: Meeting Request with Kevin O'Connell

[redacted]

I'm writing on behalf of Mr. John Frank, Microsoft Vice-President for EU Government Affairs, to inquire whether it would be possible to schedule a meeting next week with Mr. O'Connell.
The purpose is to discuss e-evidence.

Please find below some suitable slots:

- Oct 24, at 9am or 12h00 or 12:30,
- Oct 25, afternoon before 17:00,
- Oct 26, morning.

In case none of these slots would be suitable, please feel free to make other proposals.
Thank you in advance. Looking forward to your reply.

Kind Regards,

[redacted]

[redacted]

[redacted] EU Government Affairs
Corporate, External and Legal Affairs

[redacted]

Microsoft

Enterprise number : 0437910359 – RPR-RPM Brussels

(6)

Meeting with IT companies to explain the Terrorist content Regulation and the Elections Package

17 September 2018 at 16.30

Visitors:
[redacted](G+) and [redacted]
[redacted] EMEA from YouTube
[redacted] and Thomas Myrup Kristensen (Managing Director, Head of EU Affairs)from Facebook
John Frank (Vice-President EU Government Affairs) and [redacted] from Microsoft

Scene setter and objective

In the State of the Union address, 12 September 2018, the president presented two initiatives of high importance to DG JUST in the context of the work that we do with platforms, notably the Regulation on Terrorist online content as well as the Elections Package.

The purpose of today's meeting is to:

- Explain the Terrorist content Regulation and the importance for the IT companies to continue delivering progress under the Code of Conduct on hate speech
- Explain the Elections Package and the important role and responsibility of platforms in the democratic processes

Speaking points

Terrorist Content and the Code of Content on hate speech

[On the rationale behind legislation for terrorism and not for hate speech]

- When we last met, the Commission was assessing the need for further regulatory measures to tackle illegal content online. We had several options ranging from no measures at all, measures to tackle specific types of illegal content such as terrorism, hate speech or child sexual abuse, or more horizontal measures that would apply to all kinds of illegal content.

- **We has been very active in this assessment**

- Our **objective** in this context has **been twofold:**
  - **Firstly** and as the Cabinet in charge of the Fundamental rights portfolio, we have worked closely with our colleagues in the relevant Cabinets and DGs to ensure that all measures that were contemplated were accompanied by a **solid assessment in terms of impacts on fundamental rights.**
  - **Secondly,** and as the Cabinet in charge of sectorial initiatives and collaboration on illegal content in the field of **consumer protection** and **illegal hate speech**, we have of course made sure that experiences and results from our dialogues have been fully taken into account when deciding and assessing the next steps in respect of illegal content. **We have paid the utmost attention to the need to ensure a results oriented approach**. For consumer protection and hate speech we want to ensure that we pick an option that makes concrete difference on the ground which is not necessarily the one that appears the most forceful on paper.

- You will have seen that the Commission has finalized the assessment and **has proposed legally binding measures to tackle the spread of terrorist content online.**

- More specifically, it was found the while voluntary measures, including the work in the EU internet Forum, had yielded important results, this is an area where urgent action is needed and more needs to be done by all platforms.

- By **contrast, in the field of hate speech the assessment did not conclude that there is a need for regulatory measures** at this point in time for the following reasons
  - Our common work under the code of conduct on countering illegal hate speech has yielded quick results and has effectively tackled the problem. Our monitoring of your work shows that you now remove 70% of content reported to them compared to only 28% 1.5 years

- Since determining what constitutes illegal hate speech requires contextualization and knowledge of the historical, semantic and local context in which it was produced, effective measures to tackle illegal hate speech require a collaborative approach between yourselves, civil society and Member State authorities. We have achieved this under our Dialogue. This collaboration has developed through the gradual development of trust that stems from collaboration and, which cannot be created through legislation.
- Of course, we now need to continue to ensure that other platforms sees the benefit and the economies of scale in this process and we are happy to see that since January, 4 platforms have joined our dialogue and will continue working with onboarding more companies.
- Unlike in the field of terrorist content, proactive and automatized tools to detect illegal hate speech are still from reality. We do not have evidence that present state of the art technology would be at the level that its imposition would be reasonable, neither in terms of costs to the platforms, nor in terms of the impact on freedom of expression that could be envisaged if using tools that are too blunt and that yield a high number of false positives
- Lastly, tackling illegal hate speech requires action in the whole enforcement chain. We are currently working with Member States in a very concrete way to support investigations, prosecutions and sentencing of hate speech. We expect to present comprehensive guidance's to this effect this fall and will proceed to working close to the market on these issues with law enforcement and victim's support organizations in the coming years.

[Next steps Code of Conduct]

- So does this mean that we don't need to continue working on hate speech? Of course not. On the contrary **we need to make**

continues progress to demonstrate that this is the way forward to tackle illegal hate speech.

- To this end we see the following next steps
  - **A 4th monitoring** to be carried out during the end of the year
  - Continued **collaboration with NGO's on streamlining the notification process** as well as continued mutual learning and exchanges to help assessing the contextual aspects of illegal hate speech.
  - Continued **collaboration with NGO's on counternarratives.** We were very impressed of the synergies, the creativity and productivity that you all showed in the meeting in Dublin in June and we look forward to seeing how this work will develop
  - Continued progress on **transparency and user feedback** as a follow up to the Commission's recommendation on illegal content of 3 March.

- We fully trust that you fully share our vision for the continued work.

[The terrorist Regulation – substance and fundamental Rights]

- Returning to the terrorist regulation I would also like to take this opportunity to **walk you through what the new rules implies in practice and how we have ensured that fundamental rights are protected in the proposal.**

- The measures identified within the Regulation focus on those identified as a priority by stakeholders to stem the dissemination of terrorist content.

- This include:

  - the introduction of **removal orders** by competent authorities, requesting companies to remove terrorist content within one

hour. This deadline is reasonable since it will constitute a decision by a MS authority or a court and where the IT platform does not have to assess the merits of the order. The order can be challenged in a court both by the Platform and by the Content provider

- the duty to assess **referrals** from competent national authorities and by Europol as a matter of priority and to give feedback (but no rules or deadlines for removal)

- Furthermore companies affected will need to take **proactive measures** including the deployment of automated detection tools. Here, the Commission has carefully assessed the impact on freedom to conduct a business and freedom of expression to ensure that the measures are calibrated so as to not impose a disproportionate burden on the platforms and so as not to lead to the removal of legal content that is protected by the right to freedom of expression.

- Several **safeguards h**ave been put in place to ensure that the provision on **pro-active measures** is fundamental rights compliant.

  - To ensure that the measures does not unduly affect **freedom to conduct a business,** proactive measures should be proportionate to the risk of exposure to terrorist content. Since **absence of removal orders and referrals to a platform is an indication of a low risk**, the companies that are affected by the need to apply such measures are limited to what is strictly necessary. Furthermore, the **resources of companies** that have been called to put in place such measures, **should be taken into account** by the competent authority that have requested such measures when assessing whether measures are effective and appropriate.
  - As concerns **freedom of expression**, the Regulation underlines the need for the platforms to assess not only

whether the proactive measures are effective in terms of identifying terrorist content but also that they are expected to act in a diligent, proportionate and non-discriminatory manner in respect of content that they store.
    - Where the hosting service providers use **automated means** to identify and remove terrorist content, they must ensure that any such decisions are accurate, well-founded and subject to human oversight and verification.

- Beyond the safeguards that have been put in place in respect of proactive measures, the Regulation includes other **general provisions that are aimed at safeguarding user's ability to freely exchange ideas online,** including requirements for companies to:
    - inform content providers when content is removed
    - establish user-friendly complaint mechanisms so that content providers can complain if they consider that their content was erroneously removed and,
    - increased transparency regarding the hosting service providers' policies as well as reporting to public authorities, will ensure effective control and accountability.

The election package

- The Regulation on terrorist content was however not the only initiative of interest to you in the State of the Union address.

- In his speech, the Commission's president stressed the importance the Commission places on safeguarding democracy in the EU. Key element of that is increasing the transparency of elections and building trust in the electoral processes.

- The Commission recommends actions in several areas to secure free and fair elections: national and European election

cooperation networks, transparency of political advertising online and fighting disinformation campaigns, data protection and cyber security.

- **Cooperation networks:** Each Member State should set up a national election network, involving national authorities with competence for electoral matters and authorities in charge of monitoring and enforcing rules related to online activities relevant to the electoral context. Member States are encouraged to meet, with the support of the Commission, in a European coordination network on the elections to the European Parliament, as soon as possible to be able to be best prepared to protect the 2019 elections.

- **Transparency and fighting disinformation:** The Commission is fully behind the Code of Practice on Disinformation which is about to be completed this month and where I know that some of you have participated actively. This is the key document in this regard. The Recommendation on free and fair elections adds some elements. We want to ensure the active disclosure to citizens of the Union of information on the political party, political campaign or political support group behind paid online political advertisements and communications. Member States should also encourage the disclosure of information on campaign expenditure for online activities, including paid online political advertisements and communications, as well as information on any targeting criteria used in the dissemination of such advertisements and communications.

- **Data protection** – the Commission has published a guidance document for actors involved in the electoral context - such as national electoral authorities, political parties, data brokers and analysts, social media platforms and online ad networks. The objective is to draw the attention of those stakeholders to the provisions of the General Data Protection Regulation (applicable since May) which are of particular relevance in the electoral context and which were singled out in the ICO

preliminary findings in the Facebook/Cambridge Analytica case (proper legal ground for processing, transparency, etc.). This document is of course not exhaustive and does not interfere with the guidelines on key GDPR provisions issued by the European Data Protection Board. In line with the principle of accountability, it is for data controllers to ensure compliance with all provisions of the GDPR and the national electoral legislation – and to turn if necessary to their national data protection authorities for advice.

- **Cyber security** - the Recommendation calls on the Member States to put in place the necessary procedures to prevent, detect, manage and respond to cyberattacks, aiming to minimise their impact, and guarantee a swift exchange of information at all relevant levels, from technical to operational and political.

Background - Measures proposed in the Terrorist Regulation:

Many of the recent attacks within the EU have exposed terrorists' use of the internet to plan attacks, and there is continuing concern about the role of the internet in allowing terrorist organisations to radicalise, recruit, train, facilitate and direct terrorist activity. The European Parliament and the European Council called on the Commission in 2017 and again in 2018 to present proposals to address these issues. These calls were echoed by statements issued by the leaders of the G7 and G20 in 2017 as part of the shared effort to tackle terrorism both offline and online.

While positive results have been achieved from voluntary initiatives, including under the EU Internet Forum, terrorist propaganda continues to be easily accessible online and the level and pace of response continues to vary. In some cases, internet platforms have not engaged in voluntary efforts or did not take sufficiently robust action to reduce access to terrorist content online. In addition, different procedures and in some cases regulatory actions across Member States limit the effectiveness and efficiency of cooperation between authorities and hosting service providers.

This is why the Commission is proposing a legislation on terrorist content which will harmonise rules for companies offering services across Europe.

The most important features of the Regulation includes the following:

1. **Removal orders**

The removal orders, issued by national authorities requesting hosting service providers to remove terrorist content online or disable access to it, must be carried out within 1 hour. Failure to comply with a removal order may result in financial penalties. Removal orders will be an important tool for Member States that may also wish to continue using existing

voluntary referral arrangements, particularly where hosting service providers do not respond swiftly and effectively to referrals.

2. Duty of care obligation and proactive measures

The new rules require hosting service providers to take proactive measures including the deployment of automated detection tools where appropriate and when they are exposed to the risk of hosting terrorist content. Service providers should also report on the proactive measures put in place after having received a removal order to the relevant authorities.

These proactive measures should be proportionate to the risk and the economic capacity of hosting service providers. They might comprise measures to prevent the re-upload of removed terrorist content or tools to identify new terrorist content, whilst recognising the need for oversight and human assessment to ensure that legal content is not removed. Such measures should be decided primarily by the hosting service providers themselves and, if necessary, in dialogue with national authorities. National authorities may, as a last resort, impose specific proactive measures where the measures in place by hosting service providers prove insufficient.

3. Strong safeguards

The new rules will require hosting service providers to put in place effective safeguards to ensure full respect of fundamental rights, such as freedom of expression and information. In addition to possibilities of judicial redress for hosting service providers and content providers to contest a removal order, such safeguards will include the possibility of user-friendly complaint mechanisms for content providers where hosting service providers have taken down content unjustifiably.

4. Increased cooperation

Hosting service providers and Member States will be obliged to nominate points of contact to facilitate the swift handling of removal orders and referrals. This will help improve co-operation between Member States and the companies, where outreach efforts have at times been difficult. A hosting service provider's point of contact does not have to be located in the EU but should be available 24/7 to ensure that terrorist content is removed, or access to it is disabled, within 1 hour of receiving a removal order. Cooperation with Europol, Member States and hosting service providers is encouraged and will be further enhanced when transmitting removal orders and referrals.

5. Transparency and accountability

The new rules will provide for greater accountability and transparency. Companies and Member States will be required to report on their efforts and the Commission will establish a detailed programme for monitoring the results and impact of the new rules. To enhance transparency and accountability towards their users, online platforms will also publish annual transparency reports explaining how they address terrorist content on their services.

6. Penalties

Member States will have to put in place effective, proportionate and dissuasive penalties for not complying with orders to remove online terrorist content. In the event of systematic failures to remove such content within 1 hour following removal orders, a service provider could face financial penalties of up to 4% of its global turnover for the last business year.

(7)

From: BRAUN Daniel (CAB-JOUROVA)
Sent: 18 September 2018 17:05
To: NIKOLAY Renate (CAB-JOUROVA); CONSTANTIN Simona (CAB-JOUROVA); LADMANOVA Monika (CAB-JOUROVA); TALKO Wojtek (CAB-JOUROVA); HULICIUS Eduard (CAB-JOUROVA); O'CONNELL Kevin (CAB-JOUROVA)
Cc:

Subject: FW: Flash of the meeting between CAB and IT Companies - 17 September

Follow Up Flag: Follow up
Flag Status: Completed

fyi

From: [redacted]
Sent: Tuesday, September 18, 2018 5:01 PM
To: BRAUN Daniel (CAB-JOUROVA); CRABIT Emmanuel (JUST)
Cc: [redacted]
Subject: Flash of the meeting between CAB and IT Companies - 17 September

FLASH REPORT / Meeting JOUROVA CAB and the IT Companies in the Code of conduct

Date: 17 September, 2018
Attended by: Renate Nikolay and Daniel Braun (CAB Jourova), [redacted] (DG JUST C2), [redacted] (Facebook), [redacted]

Aim: to present the recent COM initiatives on preventing dissemination of terrorist content online and election package and next steps on the Code of conduct on countering illegal hate speech online

Renate Nikolay and Daniel Braun ran through the two initiatives announced during 2018 SOTEU, their logic, the approach taken from our policy perspective, in particular to ensure balance with fundamental rights. For the regulation on terrorist content, RN and DB stressed the important role had in confining the scope to terrorist content: illegal hate speech can continue on voluntary setting given good results achieved in the Code and the complexities linked with detection and removal of hate speech vs. protection of freedom of expression. Continued progress, in particular regarding transparency and feedback to users, and further expansion of the Code of conduct is now expected in order to reinforce such approach.

IT companies expressed a substantial satisfaction with the balance found with the regulation on terrorist content online, expressing few concerns on its edges (e.g. on future of the EU Internet Forum, possible fragmentation of national competent authorities in charge of removal orders, data preservation for proactive measures, approach to sanctions, tight timeline for implementation). General satisfaction was expressed for the election package too: IT companies wondered how they should further contribute apart from the work on the Code of practice. RN and DB invited to share knowledge on tech

developments on their platforms and actively engage into next upcoming events (Cybersecurity conference and Annual Colloquium on FR)

European Commission

COMMISSIONER VĚRA JOUROVÁ

MEETING WITH AMAZON WEB SERVICES

LOCATION: BERL 12/176

DATE AND TIME: 11/07/2018, 14H00

Meeting Objective: to discuss – E-commerce product safety, New Deal for consumers, Data protection / Data flows, Illegal content on the internet

VERSION: 13/11/2018 11:37

JUST/1198

Participants: Ms Barbara Scarafia - VP &; Associate General Counsel, International Consumer Legal, Amazon, Mr James Waterworth - Director of EU Public Policy, Amazon, Mr Stephane Ducable - Director of EU Public Policy, Amazon Web Services

DATA PROTECTION - GDPR

CONTEXT

HoC Nikolay met with AMAZON Europe Vice-President and Associate General Counsel on 22 November 2017, discussing data protection, consumer rights and enforcement and product safety.

This meeting offers the opportunity to inform Amazon representatives of the main elements of the Communication of 15 May 2018 on 'Completing a Trusted Digital Single Market for all' and about the next steps following the entry into application of the GDPR.

The Communication underlines that the protection of personal data is key in building confidence in the digital economy. It reminds Member States of the importance of having their national legislation in place for the effective application of the GDPR and of equipping the data protection authorities with all the resources necessary to ensure a full and efficient application of the GDPR.

Amazon Web Services (AWS) has become a member of the Association of Cloud Infrastructure Services Providers in Europe (CISPE). CISPE submitted to the Article 29 Working Party its Data Protection Code of Conduct for Cloud Infrastructure Providers. On 23 February 2018, the WP29 sent a letter with comments on the Code to CISPE. CISPE is currently amending the Code in view of the comments received, and will need to resubmit the Code for approval to a DPA in accordance with GDPR.

OBJECTIVE(S)

The objectives of your meeting would be to:

- Stress the importance of GDPR in the light of recent events (such as Facebook/Cambridge Analytica) and the importance of a proper application of GDPR.

- Refer to the Commission Communication of 15 May on Completing a trusted Digital Single Market for all.

LINE TO TAKE

- The New European Union data protection regulation – the General Data Protection Regulation (GDPR), is applicable as of 25 May 2018. The new legislation modifies and updates data protection rules at EU level to make Europe fit for the digital age.

- The Facebook / Cambridge Analytica case highlights if necessary the relevance of the new EU-wide data protection rules set by the General Data Protection Regulation (GDPR).

- The GDPR reinforces principles and rules, it clarifies and harmonises the notion of consent and further develops transparency obligations. It requires the implementation of data protection by design from the outset. As part of the accountability principle, controllers must implement measures appropriate to the risks. In our recent Communication on Completing a trusted Digital Single Market for all, we have underlined the importance of protecting personal data for building confidence in the digital economy.

- GDPR also reinforces the role of national data protection authorities, the enforcers of the EU data protection rules. It gives them better means of cooperation, clearly divides the

competences between the DPAs in cross-border cases and harmonises the enforcement powers, in particular the power to impose fines.

- It is important to keep in mind that the GDPR, as a Regulation, is directly applicable throughout the EU from 25 May. At the same time, we are monitoring the adoption of national laws by the Member States. So far [13] Member States have adopted their national legislation [(AT, DE, FR, HR, NL, SE, SK, DK, UK, PL, IE, MT, LT)]. The others are at different stage of the procedures (including discussion in national parliaments). On 25 May, the Commission sent letters to the Member States to remind those who are not yet ready of the need to adopt their national laws without delay.

- We are continuing to engage with the European Data Protection Board. As you are well aware, the then Article 29 Working Party already issued ten guidelines to assist with implementation and interpretation of new legislation (on data portability, data protection officers, lead supervisory authority, data protection impact assessments administrative fines, urgency procedures, data breach notifications, profiling, consent and transparency). The EDPB work is ongoing on guidelines on accreditation (public consultation closed on 30 March), on certification (public consultation closing on 12/07), and on Codes of Conduct. Following our request, all guidelines are subject to a six weeks public consultation process. We encourage you to make your views known in the context of those public consultations.

Next steps

- We now need to ensure that the new rules are properly applied on the ground. We all have our roles to play: the Commission, the Member States, the Data Protection Authorities individually and in the form of the European Data Protection Board, the companies and the civil society.

- As guardian of the Treaties, the Commission will monitor the proper application of the GDPR. We have a battery of actions to carry out from now on:

    - We will continue our work with the Member States and closely monitor the application of the Regulation in Member States. We will take appropriate actions as necessary, including the recourse to infringement actions.

    - We have allocated grants to support Data Protection Authorities by co-financing their awareness-raising activities. These activities will start in the second half of this year and will continue in 2019.

    - We will continue our work with stakeholders to explain the GDPR, including through our participation to events both in Brussels and in Member States, and through the GDPR multi-stakeholder group we have established.

    - We will assess the need to make use of our power to adopt delegated or implementing acts, if we establish that there is a clear added-value and request from stakeholders.

    - In one year's time from now, in May 2019, we will take stock of the Regulation implementation, and we will report on the application of the new rules in 2020.

- The EU has set up a strong data protection framework on which a dynamic digital Europe can be built. The EU is well equipped to deal effectively with the new data challenges, provided all actors work closely together in effectively implementing and applying the new tools to protect the rights to privacy and data protection of individuals.

DEFENSIVES

What will the Commission do if Member States' actions are late or not in compliance with the GDPR?

- Where Member States do not take the necessary actions required under the Regulation, are late in taking them or make use of the specification clauses provided for under the Regulation in a manner contrary to the Regulation, the Commission will make use of all the tools it has at its disposal, including recourse to the infringement procedure.

What is the Commission position on the guidelines recently published by the Article 29 Working Party/EDPB?

- The guidelines of the Article 29 Working Party/EDPB are very important to provide increased legal certainty to stakeholders since they will guide the data protection authorities when implementing the GDPR.

- The Commission supports the work of the Article 29 Working Party/EDPB and share with its members its views and expertise on the provisions of the GDPR. It also strongly encouraged the Working party to conduct public consultation on the draft guidelines.

- However, the Article 29 Working Party/EDPB is an independent body and therefore the content of the guidelines are their responsibility.

What is the procedure for the approval of Codes of Conduct under the GDPR? What happens to Codes approved under the Directive?

- According to Article 40 GDPR, a Code of Conduct must be submitted to the competent supervisory authority at national level for its approval. Where it relates to processing activities in several Member States, the EDPB must be consulted and provide an Opinion on the compliance of the Code with the GDPR. The competent supervisory authority must approve the Code following this opinion. The Commission may then give a particular Code general validity within the Union.

- The EDPB is currently working on Guidelines to describe the procedure for submitting Codes of Conduct to supervisory authorities under Article 40 GDPR.

- Codes approved under the Directive will need to be updated by industry to conform them to the GDPR. The GDPR does not as such provide for a transition regime of currently approved Codes. Updates and amendments of current Codes to bring them in line with the GDPR will need to be submitted to the competent supervisory authority for its approval.

One-stop-shop mechanism

- The new rules provide for a "one-stop-shop" mechanism. This means that companies conducting cross-border processing activities only have to deal with one national data protection supervisory authority. Previously, companies had to deal with different decisions from different national data protection authorities.

- A co-operation and consistency mechanism allows for a coordinated approach between all the data protection authorities involved.

- Both controllers and individuals benefit from the "one-stop-shop". Controllers only have to deal with one single supervisory authority, making it simpler and cheaper for companies to do business in the European Union. At the same time, it is easier for citizens to get their personal data protected since they only have to deal with the data protection authority in their Member State, in their own language.

What about the European Data Protection Board? What does it do?

- Similarly to the current "Article 29 Working Party", the European Data Protection Board includes the data protection authority of each Member State, and the European Data Protection Supervisor (EDPS).

- The tasks of the European Data Protection Board are listed in the Regulation (Article 66). It shall, for example, monitor the correct application of the Regulation, advice the Commission on any relevant issue, issue opinions, guidelines or best practices on a variety of topics.

- The main difference is that the European Data Protection Board will not only issue opinions, but also binding decisions regarding some cross-border cases (e.g. if there are conflicting views between several concerned supervisory authorities). The objective is to ensure a consistent application of the Regulation.

What are the upcoming plans of the new Chair of the European Data Protection Board?

- We very much congratulate Ms Jelinek on her recent confirmation on 25 May 2018 as the Chair of the European Data Protection Board.

- Ms Jelinek has stressed that the EDPB shall continue its already ongoing work streams to ensure the successful application of the new legislation.

- The new Chair is currently reflecting on further activities (including guidance) of the EDPB.

Background

The General Data Protection Regulation together with the Data Protection Directive for Police and Criminal Justice Authorities ("Police Directive") form the **"data protection reform" package.** The GDPR entered into force on 24 May 2016 and shall apply from 25 May 2018. The Police Directive entered into force on 5 May 2016 and EU Member States had to transpose it into their national law by 6 May 2018.

The Commission has established an **Expert Group with Member States** to prepare the implementation of the GDPR and the transposition of the Police and Criminal Justice Authorities Directive. The Expert Group meets each month alternatively on the two pieces of legislation. The last meeting of the Expert Group took place on 20 February.

The Commission has launched a study on **certification mechanisms** in order to assess whether it would make sense to make use of Commission empowerments for delegated and implementing acts. Moreover, at the request of the Parliament, we also conduct a pilot project aimed at providing a Fundamental rights review of EU data collection instruments and Programmes.

The Article 29 Working Party (now **European Data Protection Board**) has adopted a **number of guidelines** on key aspects of the GDPR and will pursue this task in the coming months.

Guidelines/working documents by the European Data Protection Board in view of the entry into application of the Regulation[1]	
Right to data portability	Adopted on 4-5 April 2017
Data protection officers	
Designation of the lead Supervisory Authority	
Data protection impact assessment	Adopted on 3-4 October 2017
Administrative fines	
Profiling	Adopted on 6-7 February 2018
Data breach	
Adequacy referential	
Binding corporate rules for controllers	
Binding corporate rules for processors	
Consent	Adopted on 10-11 April 2018
Transparency	

[1] All adopted guidelines are available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Certification	Preliminary draft adopted on 25 May and public consultation ongoing until 12 July 2018
Accreditation	Work ongoing (following public consultation)
Derogations for international transfers	Work ongoing (following public consultation)

The group will work on the update of other existing opinions, as well as on the European Data Protection Board rules of procedure. The work will continue under the **new Chair** who was elected on 7 February 2018 (Ms Jelinek from the Austrian data protection authority), and confirmed as Chair of the European Data Protection Board on 25 May 2018.

In line with the Letter of Intent accompanying President Juncker's State of the Union speech, we have developed **practical guidance for individuals and citizens**. It is a practical tool launched on 24 January aimed at business (especially SMEs), public authorities and citizens, which are available on the web and in all EU languages. It also entails a chapeau communication presenting the Commission's action to ensure a proper application of the new data protection rules. It was supplemented since then by additional communication materials aimed in particular to SMEs and individuals. The Communication of 15 May on Completing a trusted Digital Single Market for all urges Member States to adopt the necessary national legislation and equip their national data protection authorities to properly enforce the GDPR.

[redacted]

PROTECTION OF PERSONAL DATA AND DATA FLOWS (INPUT OF C4)

CONTEXT

Amazon and certain of its affiliates participate in the EU-US Privacy Shield Framework. This concerns also Amazon Web Services, which are included in the Amazon Privacy Shield certification since 20 October 2017. Amazon has thus an economic interest in the sustainability of the EU-US Privacy Shield Framework.

LINE TO TAKE

- The participation of companies like Amazon, but also that of many small and medium sized enterprises, confirms the (commercial) interest in the program, which facilitates transfers and reduces costs.
- At the same time, the Privacy Shield strengthens the level of protection of the personal data transferred to companies in the U.S. that are certified under the framework, which is important for maintaining the trust of consumers in Europe.
- Last autumn, the Commission conducted the first annual review of the Privacy Shield, an important milestone and key element of the framework.
- The outcome of this first annual review was positive; the Commission was able to conclude that the U.S. continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield.
- At the same time, the Commission has formulated a number of recommendations on how to improve the practical implementation of the safeguards provided in the Privacy Shield.
- In autumn this year, we will have the second annual review. As one of the major U.S. companies certified under the framework, I count on you to support the sustainability of the Privacy Shield.

BACKGROUND

Amazon has certified with the Department of Commerce and thus adheres to the Privacy Shield Principles. If Amazon does not resolve a complaint relating to the Privacy Shield, a customer in the EU can submit a complaint to a US dispute resolution company (TRUSTe), which provides a third-party dispute resolution service based in the US. If neither Amazon nor TRUSTe resolves the complaint, a customer in Europe may pursue binding arbitration through the Privacy Shield Panel. Amazon is of course also subject to the investigatory and enforcement powers of the Federal Trade Commission.

[redacted]

SAFETY OF PRODUCTS SOLD ONLINE

CONTEXT

On 25 June 2018 Amazon, together with three other online marketplaces (Alibaba, Ebay and Rakuten France), signed a Product Safety Pledge with the objective of increasing the safety of products sold online by third party sellers. This initiative sets out specific voluntary actions that go beyond what is already established in the EU legislation.

The commitments include among others: response to notifications on dangerous products by Member State authorities within 2 working days and to other notices within 5 working days; to consult RAPEX and take action when the products can be identified on their websites; and to take measures to prevent the reappearance of dangerous product listings.

This initiative, which is the first one of its kind in the product safety area, is part of the general dialogue with platforms on illegal content online (similarly to the Code of Conduct on Hate Speech or the MoU on Counterfeit Goods).

OBJECTIVE(S)

- To inform that the Commission welcomes the signature of the Product Safety Pledge by Amazon, whose goal is to increase the safety of products sold online.
- To inform them that the Commission will monitor the progress of the Pledge to assess if further actions are needed.

LINE TO TAKE

- To inform that the Commission welcomes the signature of the Product Safety Pledge by Amazon. Ensuring that consumers are protected when they buy online or offline is of paramount importance. Proactive measures from online intermediaries such as the ones included in the Pledge go in the right direction to achieve our common goal of protecting consumers. Setting good practices can also encourage the rest of market players to follow their example.
- To inform that the Commission will closely monitor the progress made on the commitments publishing a report every six months.

BACKGROUND

More and more consumers shop online. Online sales in the EU represented 20% of the total sales in 2016, and this percentage is expected to increase in the coming years. Online shopping is convenient for consumers but it poses certain challenges from the point of view of product safety.

Controlling the safety of products sold online can be also problematic for public authorities. For this reason, last year (1 August 2017) the Commission issued a **Notice on the market surveillance of product sold online** to help authorities with their work. The Notice clarifies the responsibilities of online actors, including platforms and their notice and action obligations to remove illegal content, i.e. dangerous products.

The **e-Commerce Directive** (Article 14) states that online intermediaries are not liable for the illegal content they host (including dangerous product listings), provided that they do not have knowledge of the illegal activity or information or, upon obtaining such knowledge or awareness, they act expeditiously to remove it. The directive does not specify the timing.

DEFENSIVES

Goods Package

LTT:

- In 2013 the Commission tabled proposals to group under one single legal framework the regulatory provisions on product safety and on market surveillance for both harmonized and non-harmonized products.

[redacted]

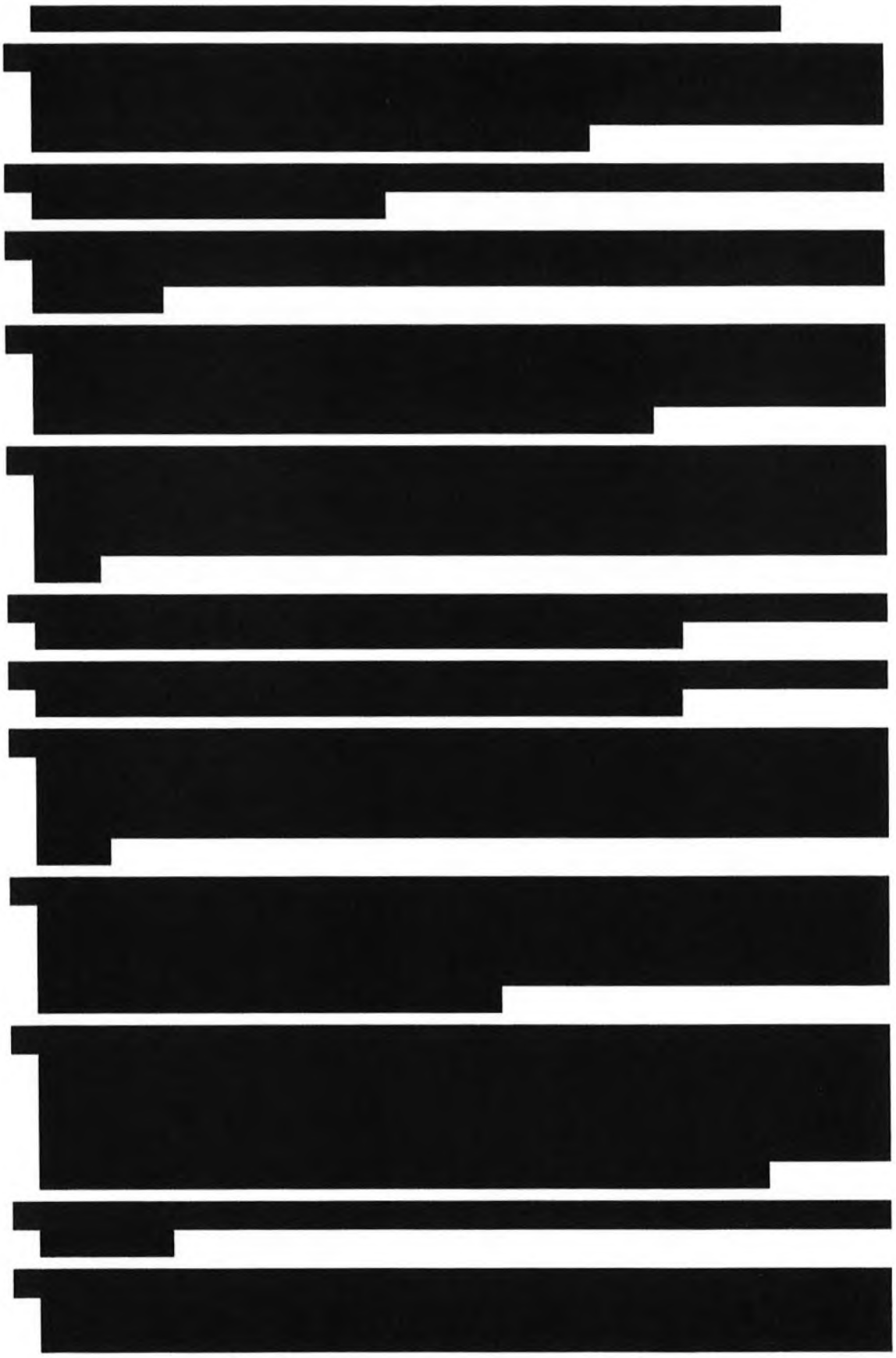
Role and responsibilities of fulfilment service providers

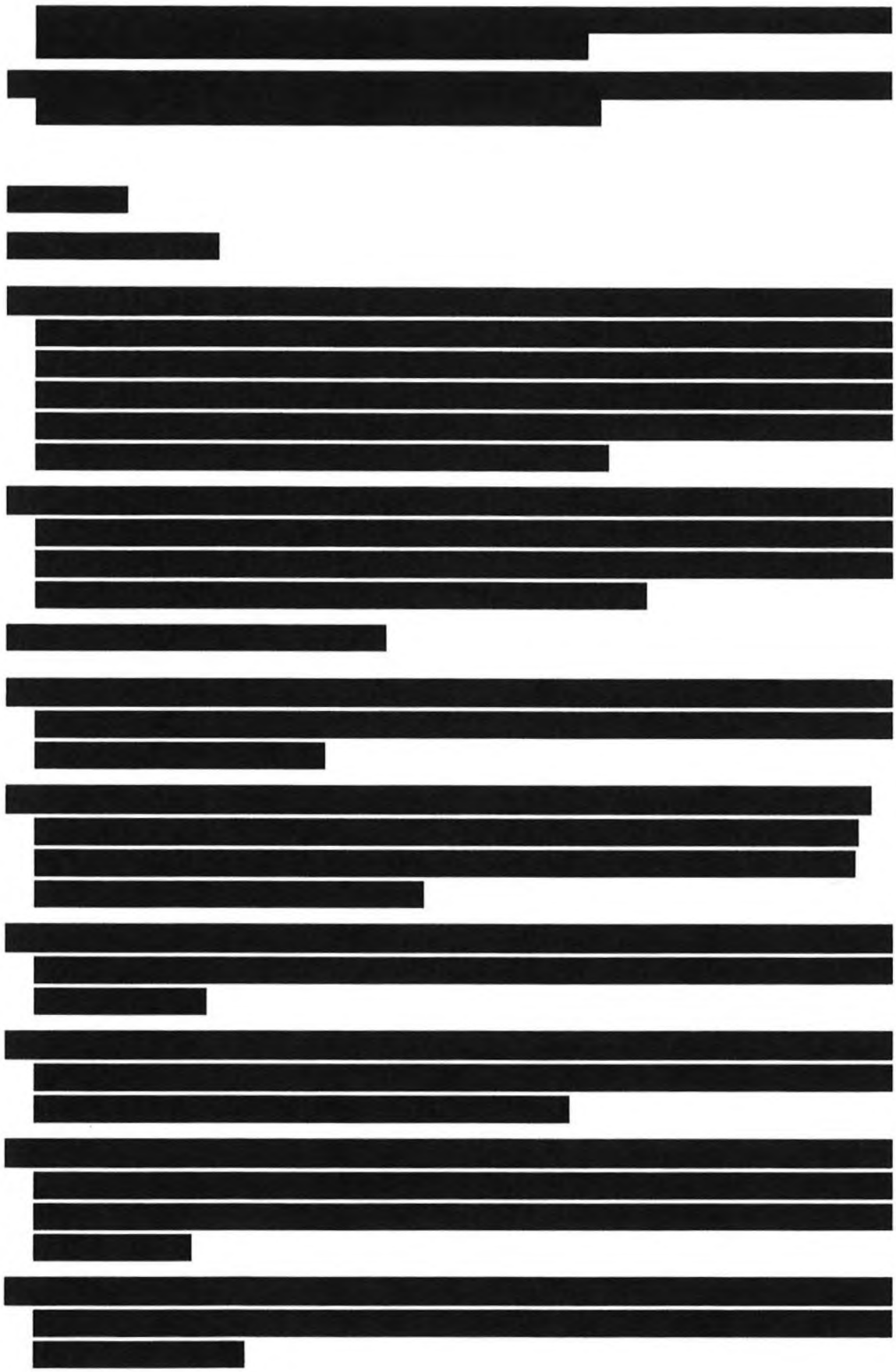
LTT:

- We believe that the interpretation is a balanced one taking into consideration the role fulfilment houses have in the supply chain. In the business model where fulfilment houses are used, the product reaches the consumer with the active participation of these service providers. These economic operators profit from e-commerce and their responsibilities need to be assessed accordingly.
- All actors in the online supply chain have to take part, in a balanced way, in ensuring that products sold to European consumers are safe.

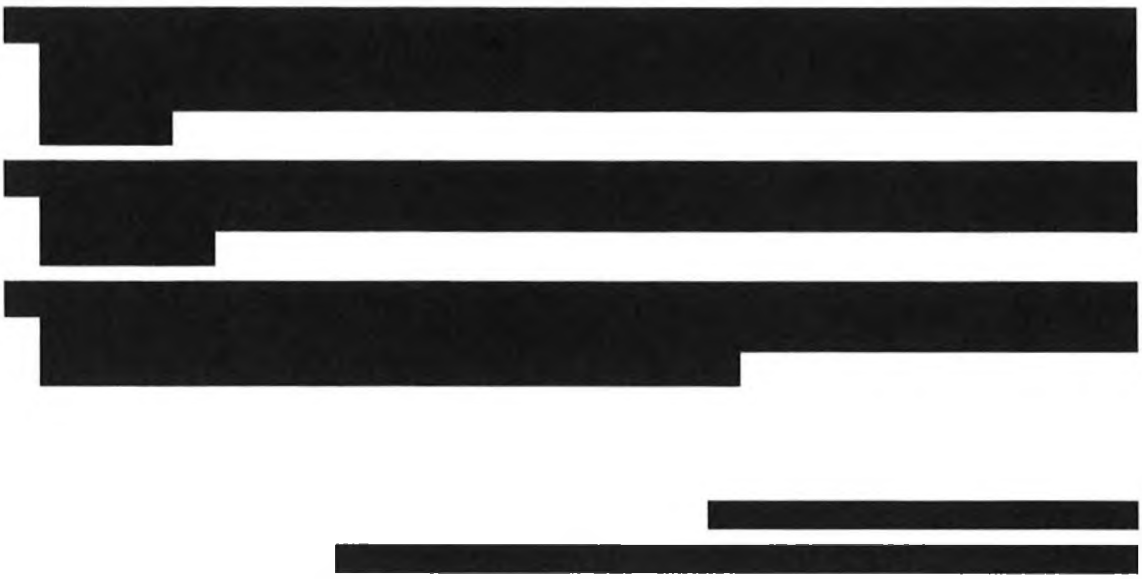
[redacted]

[redacted]





[redacted]



ANNEX

Subject: Meeting with Ms Barbara Scarafia, Amazon Vice President & Associate General Counsel (EH)

Participants: Amazon: Barbara Scarafia, [redacted]
CAB: Renate Nikolay (RN), Eduard Hulicius (EH), DG JUST: [redacted]

Date: 22.11.2017

Objective: The meeting was requested by Amazon for an introduction of Ms. Barbara Scarafia, Amazon Vice President & Associate General Counsel. Main topics discussed: data protection, consumers rights and enforcement, product safety.

Key points:

- Ms. Scarafia from Amazon thanked for receiving them. She expressed that Amazon is a big fan of the Digital Single Market and other EU initiatives, such as geo-blocking, digital contracts and data flows. Amazon is currently working with DG JUST on product safety as well as with DG GROW on counterfeit goods.
- Data Protection:
    - Amazon is working on the implementation of the GDPR and they are interested on e-privacy (because of their advertisement business). Amazon faces challenges to explain to sellers the new EU legal framework on data protection. Amazon does not disagree in principle with the GDPR or e-privacy, but they call the Commission to not force platforms to make things twice: if the e-privacy initiative is going to add extra obligations to platforms than the ones established in the GDPR, then it would be better to go directly to the final solution.
    - Mr. Ducable from Amazon presented a "Code of Conduct for Cloud Infrastructure Service Providers". This Code of Conduct has been prepared between Amazon and other competitors and it is the first Code "GDPR native". The Code has been submitted to the Article 29 Working Party last March and it has been recently considered admissible for review.
    - RN welcomed the initiative of Amazon of the Code of Conduct, foreseen under the GDPR. It comes in a good timing, as Commissioner Jourova is meeting the plenary of the Article 29 Working Party next week. The Commission is now in a crucial phase for the implementation of the GDPR, which has been an excellent example of how proactive implementation should work. This process has been done in three branches. First, through the active involvement on Member States, such as Germany. Second, with the work carried out by the Article 29 Working Party. And third, by additional guidance, mentioned in the speech of President Juncker of the State of the Union. Additional work can be done, such as campaigns for citizens and

working with platforms such as Amazon in cross-linking efforts. Regarding e-privacy, RN supports Amazon's call of need for coherence with existent legislation.

- Consumer Rights and enforcement
  - Ms. Scarafia stated that Amazon is a consumer friendly company, which complies with consumers' rights legislation. Amazon calls the Commission to help them to keep promoting innovation that can help consumers, such as their devices Alexa or dash buttons.
  - RN expressed that the position of Commissioner Jourova is not being over-protective on consumers policy, but consumers should have the same rights online and offline. The Commission is working in a New Deal for Consumers, coming as a result of a REFIT of consumers legislation. The main conclusion of the REFIT is that the level of protection of consumers is high in the EU, but enforcement is still behind. The Commission wants to strengthen the CPCs, to act in a faster way. The Commission is also reviewing legislation on injunctions.
  - MPB explained that CPCs up to now have worked in a corrective manner, but what it would be ideal if they also have a preventive role. MPB asked Amazon to participate in a dialogue with other platforms, CPCs and the Commission to review the state of play and to assess if things put on place are acceptable. For instance, regarding innovation and the new apps designed for Amazon, there could be a dialogue to discuss about these innovations. Amazon reacted positively, although they expressed that they would need to better understand Commission's plans on this.
- Product Safety
  - Ms. Scarafia expressed willingness to keep working on product safety issues with the Commission. They defend a risk based approach. Ms. Scarafia highlighted the positive aspects that innovation could bring to product safety, such as machine learning, artificial intelligence, databases and big data.
  - RN thanked Amazon for their work on product safety. RN informed about the new key initiative on Artificial Intelligence to be launched during first half of 2018. RN also informed about the Trilateral Summit in June next year and its possible focus on platforms.
  - Ms. Zafeiratou explained that Amazon is also following the Goods Package and expressed their concerns if the new package regulates the role of fulfilment houses. If new legislation comes that forces providers of fulfilment houses (such as Amazon) to change their business model, then it would be difficult to keep working on voluntary code of conducts such as the one on product safety.
- Transparency of platforms and Online Dispute Resolution
  - EH asked if Amazon considers that there is enough transparency of online platforms. Ms. Scarafia said that every marketplace is different. MPB explained that the challenge is to find the right balance between a flexible legislation and proper enforcement.
  - EH commented on the withdrawal of one of Amazon's companies of the Online Dispute Resolution system. Ms. Scarafia did not have knowledge of that withdrawal and asked to have the official letter (action for JUST E.3).

Hi Eduard,

Please find below some points of the meeting of the Commissioner with Amazon that and me have prepared.

Best,

Flash report - Meeting of Commissioner Jourova with Ms Barbara Scarafia (VP of Amazon) and James Waterworth and - 11 July 2018 - Brussels

Participants: EC: Commissioner Jourova, Eduard Hulicius, Emmanuel Crabit (JUST.C), [redacted]

Barbara Scarafia, James Waterworth

Objective: Exchange of views on data protection, illegal content, product safety, and New Deal for Consumers.

Main discussion:

- **Data Protection**: Commissioner Jourova explained that an assessment of the GDPR will be prepared one year after its adoption. The assessment will focus on the influence of the regulation on innovation, unnecessary costs (especially for SMEs), and proportionality. Amazon said that they are working to ensure that their procedures are compliant with the regulation. They showed their concerns regarding the proposal for the e-privacy regulation.

- **Product Safety**: Commissioner Jourova welcomed the signature of the Product Safety Pledge. Amazon is very happy with the voluntary commitments from the industry, such as the MoU on counterfeit goods. From now on they will work on its implementation, which they say as a learning process from both sides.

- **Illegal Content**: Commissioner Jourova explained that the Commission is currently assessing the need of taking specific actions related to counterterrorism and not to other types of illegal content. Amazon welcome this approach of considering each topic separately, and they asked if the new instrument will included a definition on terrorist content, as they wouldn't like to become judges of what is terrorist content or not. Commissioner explained that the instrument being discussed will provided a narrow definition which will not allow an extensive interpretation of the concept.

- **New Deal for Consumers**: Amazon overall showed support for the New Deal legislative proposals. They are in favour of increased transparency for online marketplaces and welcomed the technology neutral approach of the New Deal. [redacted]

[redacted]

- Finally, Amazon invited the Commissioner to participate as a speaker in an event to be organized in 26th September in Brussels; Commissioner Jourova promised to check her availability.

10

[redacted]

From: John Frank (CELA) @microsoft.com>
Sent: mercredi 4 avril 2018 16:47
To: [redacted](CAB-JOUROVA)
Cc: [redacted]
Subject: Re: US legislative proposal on lawful access, the CLOUD Act

Yes, that time can work.

Thx
John

Get Outlook for iOS

From:[redacted]@ec.europa.eu
Sent: Wednesday, April 4, 2018 3:40:39 PM
To: John Frank (CELA)
Cc:[redacted]
Subject: RE: US legislative proposal on lawful access, the CLOUD Act
Many thanks for your prompt reply. Monday at 16h00 suits you?
BR,
[redacted]

From: John Frank (CELA) [mailto: @microsoft.com]
Sent: Wednesday, April 04, 2018 4:35 PM
To:[redacted](CAB-JOUROVA)
Cc:[redacted]
Subject: Re: US legislative proposal on lawful access, the CLOUD Act
[redacted]
I am away on vacation this week but I will be back in Brussels all of next week. Monday to Wednesday my schedule is better, if a time then is possible.
Thx
John
Get Outlook for iOS

From:[redacted]@ec.europa.eu <[redacted]@ec.europa.eu>
Sent: Wednesday, April 4, 2018 3:15:02 PM
To: John Frank (CELA)
Cc:[redacted]
Subject: RE: US legislative proposal on lawful access, the CLOUD Act
Dear Mr Frank,
Renate and Kevin would be available for the meeting on Friday 6/4 at 11h00. Does it suit you?
Best Regards,
[redacted]

European Commission
Cabinet of Commissioner Věra Jourová
Commissioner for the Justice, Consumers and Gender Equality
[redacted]

[redacted]

Follow us on:
@VeraJourova @EU_Justice
@EU_Consumers EU Justice and Consumers

From: John Frank (CELA) [mailto @microsoft.com]
Sent: Wednesday, March 28, 2018 12:10 PM
To: NIKOLAY Renate (CAB-JOUROVA); O'CONNELL Kevin (CAB-JOUROVA)
Cc: [redacted]
Subject: RE: US legislative proposal on lawful access, the CLOUD Act

Hi Renate and Kevin, I would like to schedule a call or a meeting to discuss the Cloud Act and the international agreements it contemplates. Would you be available for a discussion?
Thanks
John

From: John Frank (CELA)
Sent: Tuesday, February 6, 2018 2:04 PM
To: @ec.europa.eu' @ec.europa.eu>;
@ec.europa.eu' @ec.europa.eu>
Subject: US legislative proposal on lawful access, the CLOUD Act

Dear Renate and Kevin,

I am writing about a relevant legislative development in the U.S. Today, we understand that members of U.S. Congress will introduce the Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018 to address cross-border access to electronic evidence. This compromise proposal grows out of efforts over the past two years regarding the draft International Communications Privacy Act. The proposal was previewed yesterday by Senator Hatch, and will be formally introduced today. We are unsure at this stage of the prospects for its adoption, but it does have bipartisan sponsors in both the Senate and House.

The CLOUD Act appropriately recognizes that formal government-to-government cooperation is the only lasting solution for cross border data transfers to address international privacy concerns and conflicting foreign law. The bill incentivizes bilateral frameworks for cross-border crime investigations, starting with the proposed US-UK agreement. Senator Hatch specifically encouraged the U.S. government to "expeditiously implement a similar bilateral data sharing agreement with the EU and other allies in protecting consumers around the world and facilitating legitimate law enforcement investigations."

I am attaching the text of the proposal, and a section-by-section summary. On balance, Microsoft views this as a positive step forward, paving the way for further steps that need to follow. The proposal would revise the outdated Stored Communications Act of 1986, and create a concrete path for the U.S. government to enter into modern bilateral agreements with other governments, with specified conditions for such agreements. The legislation would amend U.S. law so that U.S. warrants and other legal process issued for data held by communications providers may reach data stored overseas – importantly, however, the reach of U.S. warrants and legal process would be limited by international comity. Conversely, the legislation would also make clear that lawful demands from other countries (which enter into bilateral agreements) can reach data stored within the U.S., thus enabling exceptions to the blocking statute that currently exists.

There are a number of important features of the proposed legislation, regarding its scope and the conditions for the negotiation of bilateral agreements, that we know will interest you. We would be happy to discuss at your convenience, particularly regarding our mutual interest in an EU-US agreement and how to pursue this in light of the proposed changes to U.S. law.

Best regards,
John