

From: [REDACTED]
To: MOOZOVA Irena (JUST); [REDACTED]
Cc: [REDACTED] JUST
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.



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 in 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 from 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 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: Thomas Myrup Kristensen @fb.com>
Sent: mercredi 9 janvier 2019 12:01
To: CAB JOUROVA CONTACT
Cc: NIKOLAY Renate (CAB-JOUROVA); BRAUN Daniel (CAB-JOUROVA);
Subject: Meeting request from Nick Clegg, Facebook

Dear Commissioner Jourová,

Nick Clegg, Facebook's Vice President, Global Affairs and Communications, will be in Brussels end of January. We would be grateful if you would be available for a meeting on **Monday 28 January** to discuss issues of common interest.

Nick would appreciate the opportunity to discuss how together we can ensure that a strong digital agenda is set for the next five years. Furthermore, we would like to set out the actions we are undertaking to confront some of the biggest challenges of the digital age, particularly ahead of the forthcoming European Parliament elections.

Please don't hesitate to reach out to me should you have any further questions regarding the meeting request and we look forward to being in touch with your office shortly.

Kind regards,

Thomas

Thomas Myrup Kristensen
Managing Director EU Affairs, Head of Office

M:
E: _____ fb.com



COMMISSIONER VĚRA JOUROVÁ

MEETING WITH N. CLEGG, VICE PRESIDENT OF FACEBOOK

LOCATION: BERL 12/176

DATE AND TIME: 28/01/2019, 16H00

MEETING OBJECTIVE: TO DISCUSS: (I) GDPR; (II) ILLEGAL CONTENT ONLINE; (III) EP ELECTIONS; (IV) DISINFORMATION

MEMBER RESPONSIBLE: WOJTEK TALKO

DG CONTACT & TEL No: [REDACTED]
DIRECTOR: EMMANUEL CRABIT

VERSION: 18/09/2019 11:11

JUST/123

PARTICIPANTS:

TABLE OF CONTENTS

STEERING BRIEF	3
TOPICS	4
TOPIC 1: DATA PROTECTION	4
TOPIC 2: CODE OF CONDUCT ON ILLEGAL HATE SPEECH / ILLEGAL CONTENT ONLINE	13
TOPIC 3: EP ELECTIONS	19
Topic 4: Disinformation.....	26
ANNEX: NICK CLEGG, CV	28
ANNEX – LATEST MEDIA COVERGE ON FACEBOOK/NICK CLEGG	29

STEERING BRIEF

CONTEXT

On a yearly basis and towards the beginning of each year, Facebook's highest officials conduct a courtesy call.

On 23 Jan 2018, you met Sheryl Sandberg, Facebook's COO. During this meeting, you exchanged views on the following topics: (i) hate speech; (ii) data protection- GDPR & the Privacy Shield; (iii) e-evidence. On 2 March 2017, you met Nick Clegg's predecessor, Mr. Elliot Schrage. During this meeting, you exchanged views on the following topics: (i) online hate; (ii) CPC action on social media; (iii) Privacy Shield; (iv) Implementation of GDPR.

This meeting comes as Facebook is trying to reverse a long period of serious problems at the company – these include, amongst others, the Cambridge Analytica scandal, serious allegations of permitting alleged interference in a number of elections, and accusations of "slow and ineffective responses" to the use of Facebook in support of the "genocidal intent" during the Rohingya crises. Facebook has been at the heart of the "tech-lash". The year 2018 for Facebook has been labelled as 'complicated' or *annus horribilis*.

Facebook's general response to the scandals has been to acknowledge the problems, apologise, and to promise "to fix it", as well as to publicly welcome "practical" regulatory efforts in principle.

The company has hired some 20.000 staff for content moderation, developed new rules and technologies to limit fraudulent ads, implemented stricter policing of data protection, published detailed transparency reports and invested in technology tools, notably to detect terrorist content on its services. It has also sought to improve its governance through collaboration with US academics, a civil and human rights audit, and a proposed external oversight mechanism.

VP Ansip will be meeting Nick Clegg earlier in the day (meeting scheduled at 09:00).

OVERALL OBJECTIVES

- Discuss and enquire on the state of play of the different data breaches under the GDPR involving Facebook;
- Secure the continued commitment by Facebook on tackling illegal hate speech through the Code of Conduct on illegal Hate speech and provide information on the next steps envisaged by the Commission on combating illegal content online;
- On EP elections and disinformation: inform Facebook on Commission's actions to raise participation in EP elections, as well as ensure free and fair elections; enquire about Facebook's actions undertaken in these areas;

TOPICS

TOPIC 1: DATA PROTECTION

CONTEXT

Your meeting is taking place roughly 8 months after the entry into application of the General Data Protection Regulation (GDPR). The Commission has underlined its approach to the application of GDPR in two communications: the Communication on GDPR guidance on 24 January 2018 and the Communication on 'Completing a trusted Digital Single Market for all' on 15 May 2018. In particular, the Commission has called on Member States to implement all actions necessary in a timely manner and to equip the data protection authorities with sufficient resources. On 12 September, the Commission has issued an electoral package including GDPR guidance in the electoral context.

OBJECTIVE

- Discuss state of play on the FB/Cambridge Analytica scandal.
- With respect to the different data breaches involving Facebook: ask Facebook on the progress of their analysis of the nature of the breach and in implementing the necessary measures. Reiterate the line expressed publicly in the context of the September data breach that we expect Facebook to provide more information on the breach and to fully cooperate with the Irish Data Protection Commissioner.
- Discuss state of play of complaints and investigations against FB in Europe.

LINE TO TAKE

[The FB/Cambridge Analytica scandal State of Play]

This case highlights the relevance of the new EU-wide data protection rules set by the GDPR. These rules focus on making companies more accountable, more responsible in how they deal with our data.

- The Commission is in close contact with both the Chair of the EDPB and the Chair of the UK ICO (the UK data protection authority) who has been leading the investigation on Cambridge Analytica since this company is based in the UK. We fully support the coordinated response of the EU data protection authorities.
- We take note that the ICO released in October its full report and imposed a maximum £500,000 fine on Facebook for two breaches of the Data Protection Act 1998. We understand that Facebook has appealed the fine and the case is now pending before the UK Court of Appeal. [Facebook argues that the core of the ICO's enforcement is now broader than the simple questions raised in the Cambridge Analytica case, owing to the lack of harm to British citizens from that scandal.] We are awaiting the Court's decision in this case.

- As part of the electoral package adopted by the Commission in September, we have issued a Guidance on the use of personal data in the electoral context to remind all actors involved in the electoral process a number of key data protection principles.

[September & November 2018 Data Breach]

- In October 2018, following the Facebook September Data Breach, the Irish Data Protection Commission formally commenced an investigation to examine Facebook's compliance with the relevant provisions of the GDPR.
- In December 2018, following the Facebook November Data Breach, the Irish Data Protection Commission formally commenced an investigation to examine Facebook's compliance with the relevant provisions of the GDPR.
- As I underlined in the context of the September breach, we expect Facebook to provide all necessary information on the persons affected in the EU. Have you made progress in analysing the nature of the breach and implementing the necessary measures?
- We are fully supportive of the work of the Irish Data Protection Commissioner and would like to encourage you to fully cooperate with her services.

[Other pending cases in Europe against Facebook]

- There has been an increase in the number of complaints received by Data Protection Authorities since the entry into application of GDPR. NGOs active in the field of data protection have started to make use of the possibility to bring collective actions before data protection authorities and courts, in particular against the GAFAM.
- We note that Facebook is the subject of several of these collective actions, with complaints filed notably in France, Austria and Germany. These cases must be handled by DPAs under the new cooperation mechanisms established by the GDPR, with the Irish DPA acting as the Lead supervisory authority. Before issuing its decision in a complaint, the Lead supervisory authority must consult with all concerned authorities. In case of a disagreement between the DPAs, the matter will be escalated to the European Data Protection Board who can issue a binding decision. The new cooperation mechanisms in GDPR will ensure a consistent application of the GDPR across Europe.

DEFENSIVES

What will the Commission do if Member States' actions are late or not in compliance with the General Data Protection Regulation?

- 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.

One-stop-shop mechanism

- The new rules provide for a "one-stop-shop" mechanism. This means that companies conducting cross-border processing activities will only have to deal with one national data protection supervisory authority. Currently, companies must deal with different decisions from different national data protection authorities.
- A co-operation and consistency mechanism will allow for a coordinated approach between all the data protection authorities involved.
- Both controllers and individuals will benefit from the "one-stop-shop". Controllers will 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 will be easier for citizens to get their personal data protected since they will 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 former "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, advise 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 not only issues 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 sanctions foreseen in the GDPR?

- What we have learned from the many recent scandals (Uber data breach, Facebook Cambridge Analytica) is that violations of privacy rules can be very harmful for individuals and for the society as a whole. We need to get serious about data protection compliance and enforcement. As in other areas of law, this requires credible and sufficiently deterrent sanctions.
- The GDPR establishes a range of enforcement tools, from warning to penalties and fines. All these tools must be effective, proportionate and dissuasive. The agreement on fines ensures that they are a deterrent. Each case must be determined in light of its specific circumstances and taking into account 11 different factors listed in the Regulation, including the :
 - gravity/ duration of the violation;
 - number of data subjects affected and level of damage suffered by them;

- intentional character of the infringement;
 - any actions taken to mitigate the damage;
 - degree of co-operation with the supervisory authority.
- The GDPR sets out two main categories of ceilings of fines for infringements of the Regulation, depending on the gravity of the infringements (2% or 4% of worldwide turnover). These ceilings, as there are expressed in percentage of the company's turnover, ensure that the fine will always be proportionate to the economic weight of the concerned company.
 - These are ceilings, meaning maximum amounts. There will therefore apply only to the most serious violations which have taken place over a long period of time, have affected a large number of individuals etc.
 - Finally, credible sanctions give value to compliance (compared to a situation where only symbolic sanctions meant that complying or not with data protection rules did not really matter) and avoid situation of free riders (which has just relying on and benefiting from the compliance efforts of others).

Will the opening clauses in the General Data Protection Regulation lead to fragmentation in the application of data protection rules in the EU?

- The Regulation gives Member States the possibility to further specify the application of data protection rules in specific fields, for example public sector, employment and social security, preventive and occupational medicine, public health, scientific or historical research purposes or statistical purposes, etc. In addition, for genetic data, biometric data and data concerning health, the Regulation empowers Member States to maintain or introduce further conditions, including limitations.
- However Member States' actions are framed by two elements: Article 8 of the Charter, and Article 16(2) TFEU under which national legislation cannot impinge on the free flow of personal data within the EU.
- When adapting their national legislation, Member States have to take into account the fact that any national measures which would have the result of creating an obstacle to the direct effect of the Regulation and of jeopardising its simultaneous and uniform application in the whole of the EU are contrary to the Treaties.
- In the summer 2018, we launched a study to look into the use of some of the specification clauses of the GDPR by the Member States (such as the specification clauses in the field of health or scientific research). The results of the study are expected by the end of 2019.

BACKGROUND

Background on Facebook September data breach

Facebook is already subject to an official investigation from the Irish DPA for a previous data breach in September, which may have affected 50m people. Facebook accounts were compromised by an attack that gave hackers the ability to take over users' accounts. According to the information available 10% of those are European accounts.

On 3 October 2018, the Data Protection Commission formally commenced an investigation into this case. The investigation will examine Facebook's compliance "with its obligation under the GDPR to implement technical and organisational measures to ensure the security and safeguarding of the personal data it processes. Facebook has informed the DPC that their internal investigation is continuing and that the company continues to take remedial actions to mitigate the potential risk to users."

You had a telephone conversation with the Head of the Irish Data Protection Commissioner, Helen Dixon on 3 October and publicly urged Facebook to provide more information on the breach and the persons affected, and to fully cooperate with the Irish DPC.

Background on Facebook November Data Breach

Facebook admitted in a blog post on 14 December another data breach, possibly affecting 7m people. The bug may have allowed up to 1,500 apps get access to private photos held by users on the social site for 12 days between September 13 and September 25, 2018.

The Irish Data Protection Commissioner announced in December a fresh investigation into the social media giant and has commenced a statutory inquiry examining Facebook's compliance with the relevant provisions of GDPR.

In the meantime, Facebook announced that it would roll out tools for app developers that allow them to determine which people using their app might be impacted by this bug. Facebook is working with those developers to delete the photos from impacted users. Facebook also announced that it would notify people potentially impacted by this bug via an alert on Facebook.

Under new EU GDPR rules, a company can be fined up to 4% of its annual turnover. In Facebook's case, this could amount to around €1.5bn.

Background on the other pending cases in Europe against Facebook

There has been an increase in the number of complaints received by Data Protection Authorities since the entry into application of GDPR. NGOs active in the field of data protection have started to make use of the possibility to bring collective actions before data protection authorities and courts, in particular against the GAFAM.

Facebook is the subject of the following complaints:

- La Quadrature du Net (submitted to the French DPA): the complaint concerns the requirement to obtain valid consent under GDPR. La Quadrature du Net (LQDN has been mandated by 10 000 citizens) also filed similar complaints against, Google (Gmail, YouTube and Search), Apple, Amazon and LinkedIn. With regards to the complaint by LQDN against Google, CNIL, on 21 January 2019, issued a EUR 50 million fine. CNIL concluded that Google's ads personalization breached the GDPR (lack of transparency, inadequate information and lack of valid consent regarding the ads personalization)
- Schrems/NOYB (submitted to the Austrian DPA): NOYB argues that FB forced users into agreeing to new terms of service, in breach of the requirement in the law that such consent should be freely given.
- Frankfurter Allgemeine Sonntagszeitung reports that Federal Minister of Justice and Consumer Protection Katarina Barley has launched a master lawsuit against Twitter and Facebook after the cyberattack against German politicians. Affected customers can collectively launch a lawsuit "if there are liability claims against companies in connection with the data leak," Ms. Barley has noted. "The one-for-all lawsuit" is an instrument that makes it possible to sue large corporations. The data theft affected above all MPs whose mobile phone numbers and other private data were published. The links to the data were shared via accounts on Twitter and Facebook.

The Irish Data Protection Commission is the Lead supervisory authority for Facebook. Under the consistency mechanism, the national authorities having received the complaints must forward them to the Lead supervisory authority. We understand that both the Austrian and the French DPAs have referred the complaints against Facebook to the Irish DPA, who is investigating the matters.

Next to these complaints, the New York Times published in December 2018 revelations that Facebook entered into data sharing agreements with several third parties (including Apple, Netflix, Spotify, Amazon, and Yahoo!). The documents obtained from the NYT date from 2017, so prior to the entry into application of the GDPR.

Background on GDPR

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 applies 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 European Data Protection Board (previously known as 'Article 29 Working Party') 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 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	
Data breach	Adopted on 6-7 February 2018
Adequacy referential	
Binding corporate rules for controllers	
Binding corporate rules for processors	
Consent	
Transparency	Adopted on 10-11 April 2018
Certification	
Accreditation	Adopted on 4 December 2018 – Annex subject to public consultation until 1 st February 2019
Derogations for international transfers	Adopted on 25 May 2018
Territorial scope of the GDPR (Article 3)	Preliminary adoption on 23 November 2018 – subject to public consultation until 18 January 2019

In line with the Letter of Intent accompanying President Juncker's State of the Union speech, we have developed practical guidance for SMEs and citizens. It is

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

a practical tool launched on 24 January 2018 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 General Data Protection Regulation. Specific Guidance on the application of data protection rules in the electoral context have been issued in September as part of the electoral package. They have been inspired in particular by the Facebook/Cambridge Analytica case.

GPDR statistics

Statistics in the Member States

Nearly all national data protection authorities report higher (in some cases doubled) workload since the new data protection rules came into force on 25 May.

- Since then, EU citizens submitted at least **45 500 data protection complaints** to the national authorities.
- There were at least **18 500 data breaches** notifications across the EU.
- **Fines** are starting to be imposed: by DPA in the German state of North Rhine-Westphalia, by Austrian DPA, by UK DPA (ICO).
- Only a few codes of conduct have been officially submitted to Data Protection Authorities pursuant to Article 40 of the GDPR.

Complaints by countries from 25 May 2018 to 25 October 2018:

- France: 3767 complaints
- Germany: 6555 complaints
- Ireland: 448 complaints
- Poland: 2833 complaints
- Sweden: 48 complaints
- Italy: 2547 complaints
- Romania: 1643 complaints
- UK: 14996 complaints
- Netherlands: 9661 complaints

Note that the data from the different countries are not entirely comparable, for instance some DPAs reported all kinds of actions taken and not only complaints received.

[Source: GDPR today, edited by panoptikon.org, available at <https://www.gdprtoday.org/category/charts/>, 25/10/2018, and Dutch DPA at <https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/bijna-10000-mensen-dienen-privacyklacht-bij-autoriteit-persoonsgegevens>]

EDPB cooperation mechanisms

There are currently **255 cooperation cross-border cases in the case register**. The breakdown of these is below:

- **176** have been initiated as a result of a complaint;
- **79** cases originating from other sources such as an investigation, a SA initiative, a legal obligation, a media report etc.

From the above cases, the following procedures have been triggered:

- **397** procedures relating to **Mutual Assistance** (Art 61). These procedures may lead in the future to One-stop-shop procedures;
- **43 One-stop-shop procedures** (Art 60) from which **2** are **Final Decision**, **20 Draft Decisions**, **1 Revised Draft Decision** and **20 Informal Consultations**;
- **25 Local Case Requests** (Art 56.2);
- **Consistency procedures**: **30** Art.64 procedures, **29** of them concern the DPIA lists.

In addition, **574** procedures have been launched to **identify the lead and concerned SAs** (Art 56.1) (**300** ongoing, **274** closed). The number of Article 56 procedures is less relevant, because at this stage it is still not concluded that a case exists (it may also be possible that several parallel procedures to find a Lead SA will combine into 1 single case; or that a procedure will lead to no case at all (i.e. absence of cross border dimension)).

[Source: EDPB, state of play 08/01/2019]

COM Eurobarometer on data protection in elections

Data protection will remain one of the key aspects of the next year's elections. The results of the Eurobarometer show that more than two thirds (67%) of respondents are concerned that the personal data people leave on the Internet could be used to target the political messages they see. 26% are 'very concerned' about this.

[Source: COM press release, 23/11/2018]

Contact: [REDACTED]

Quality and language control: [REDACTED]

TOPIC 2: CODE OF CONDUCT ON ILLEGAL HATE SPEECH / ILLEGAL CONTENT ONLINE

CONTEXT

Facebook has shown leadership from the outset in terms of the establishment and running of the dialogue on countering illegal hate speech, in the context of the Code of conduct. Facebook has been performing better than all the other IT companies on notice and take down, as proven by Commission's most recent monitoring exercises. Facebook has ensured Instagram's swift participation to the Code of conduct after acquiring it.

Preliminary data on latest monitoring exercise (to be released in early February 2019) seem to confirm the positive trends on the response by IT companies to notices on illegal hate speech.

The Commission key messages to IT Companies over the last year have been focusing on the need to ensure continued progress on the Code in order to confirm the validity of the self regulatory approach and feed into the assessment regarding measures to be taken on illegal content online.

IT Companies in the Code of conduct and civil society organisations working against hate speech has continuously improved their cooperation, under the leadership of the industry. The platforms hosted a series of workshops in Dublin to foster such collaboration and to work together e.g on spreading positive narratives (latest workshops: 21 January 2019 hosted by Twitter; 27 June 2018 hosted by Facebook).

On illegal content more broadly, Facebook may (mildly) criticise the recent legislative proposal to tackle terrorist content in particular as concerns the requirement to remove terrorist content within one hour and to take proactive measures.

OBJECTIVES

- Underline that the concrete progress on the ground and the fact that the Code of conduct has yielded quick results were imperative to the Commission's assessment that legislative measures were not needed to tackle hate speech
- Underline the need for continuous progress. Facebook's performance on the commitment in the Code of conduct are extremely good. Instagram can further progress on notice and action after recent participation. Generally, efforts on spreading positive narratives through campaigns online will be very helpful.
- Ask them to have figures on trends of hate speech notices over time (we asked many times and never got it).

LINE TO TAKE

- The Commission has been 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.

- My objective in this context has been twofold:
 - Firstly, I worked very closely with the colleagues Commissioners responsible of other portfolios to ensure that all measures on the table were accompanied by a solid assessment in terms of impacts on fundamental rights.
 - Secondly, given my competence on illegal content in the field of consumer protection and illegal hate speech, I had to make sure that experiences and results from our dialogues were fully taken into account when deciding and assessing the next steps. 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 finalised the assessment and has proposed legally binding measures to tackle the spread of terrorist content online.
- More specifically, it was found, that 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 and this is mostly thanks to the positive results in the implementation of the Code of conduct.
- This work has yielded quick results and has effectively tackled the problem, in a context of multi-stakeholder cooperation. Our monitoring shows that platforms remove about 70% of content reported to them compared to only 28% 2 years ago. The preliminary results we have from the most recent monitoring seem to indicate a trend of stability on removal, and improvement on the 24h turnaround time for reviewing the notices.
- So does this mean that we don't need to continue working on hate speech? Of course not. On the contrary we need to intensify the efforts because the fight against illegal hate speech is not won. Continuing the path of progress would demonstrate that this is the way forward to tackle illegal hate speech.
- To this end we envisage the following next steps:
 - The results of the most recent monitoring hate speech online will be launched soon, my staff is in contact with yours to get the data ready.
 - Continued collaboration with trusted reporters in civil society on streamlining the notification process as well as continued mutual learning and exchanges to help assessing the contextual aspects of illegal hate speech.

- Continued progress on transparency and user feedback as a follow up to the Commission's recommendation on illegal content of 3 March 2018
 - Continued onboarding of new companies. Efforts from Facebook to identify other services or help recruiting other companies to join the Code will of course be greatly appreciated.
 - Continued collaboration with NGOs on counter-narratives. We were very impressed of the synergies, the creativity and productivity that you all showed in the meeting organised by Facebook in Dublin in June and we look forward to seeing how this work will develop.
- Also we would appreciate to receive figures on trends of hate speech notices over time from you. (We asked many times and never got it).

DEFENSIVE LINES

How were fundamental rights taken into account in the terrorist Regulation?

- 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 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 not to 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** have been put in place to ensure that the provision on **pro-active measures** is fundamental rights compliant.
 - To ensure that the measures do 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
 - the right of judicial review in respect of all decisions by authorities in respect of the application of the Regulation.
 - 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, which will ensure effective control and accountability.

BACKGROUND (ONLINE TERRORISM PROPOSAL)

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.

Contact: [REDACTED]

Quality and language control: [REDACTED]

TOPIC 3: EP ELECTIONS

OBJECTIVE

- Inform about our actions to raise participation in EP elections, as well as ensure free and fair elections; enquire about Facebook's actions undertaken in these areas.

LINE TO TAKE

- The Commission is dedicated to both promoting participation in the upcoming European elections and securing free and fair elections, in full respect of fundamental rights and the rule of law.
- No single actor can achieve these goals alone. Furthermore, platforms such as Facebook must take their responsibility for ensuring free and fair elections

(On Participation):

- The Commission is working with the European Parliament to support the general participation of citizens in the elections to the European Parliament.
- In terms of promoting participation, the Commission recognises the important role social media and platforms like Facebook can play, and is aware that a number of platforms are taking steps to promote participation, including Facebook and Google. *(Facebook actions in increasing voter participation: In several countries, Facebook rolled out the "I voted" / "I am a voter" button that appears on users' home page and is shared in their friends' newsfeed. One study found that this button could have a positive effect on voter turnout. Although questions were raised if all voters in a certain country had the possibility to use the button and at what time they were given this possibility, as this can have an impact on the impartiality of such a campaign. Google is planning a number of services, including tailored information boxes on elections subjects in Google search).*
- The Commission is concerned to ensure that in all cases a level political playing field is maintained, and that citizens' fundamental rights are guaranteed, including in particular the freedoms of speech and association, and the right to a hearing.
- **Does Facebook plan anything similar in relation to the European elections 2019? Will it ensure that any voter participation activities are rolled out in line with national election laws and respecting equal treatment of all EU voters?**

(On Free and fair elections):

- The Commission has adopted a number of initiatives aimed at protecting the integrity of the upcoming elections. Most notably, the Election package of 12 September 2018, the Code of Practice on Disinformation and the Action Plan on Disinformation.

- Facebook should **cooperate with all national authorities** to ensure that rules related to online activities relevant to the electoral context are respected.
- **Does Facebook intend to set up special teams for covering European elections 2019 and how will these teams cooperate with national election networks?** *(At the meeting with DG JUST on 29/11/18, FB explained that they set-up a cross-functional team dealing with elections, but could not answer the question on special team for European elections. The recent media report have shown that FB is setting up such teams for large member states (e.g. Facebook had struck a new partnership with Germany's federal cyber-security office to help to uphold the integrity of elections in Germany) but it is unclear whether they would do the same for smaller ones).*
- **Transparency of political advertising** is a crucial element in all these initiatives. Facebook should ensure that citizens of the Union can easily recognise online paid political advertisements and communications and the party, foundation or organisation behind them, as well as information on any targeting criteria used in the dissemination of such advertisements and communications. Information on expenditure/funding related to online activities should also be published. *(At the meeting with DG JUST on 10/10/18, FB gave an overview of their planned transparency measures to be rolled out before EP elections, which include: possibility to see who the advertiser is, the actions from a particular advertiser - and see therefore whether this advertiser does fragmented advertising, i.e. differentiated according to target groups. The recent media reports reveal that FB will also introduce a measure which require political advertisers to authenticate their identity before buying an ad and that there would be public archives of political ads available for seven years after the publishing of an ad)*
- **Will the transparency of political ads be fully in place in time for the EP election campaigns and will cover all EU member states? What progress is being made on an online registry of ads? How will Facebook authenticate the identity of buyers of political ad space?**
- **Disinformation** – Facebook has joined the Code of Practice on disinformation and submitted its first report, which is currently being assessed by CNECT. *(At the Meeting with DG JUST on 10/10/18 – FB stressed their commitment to the Code of Practice. They said that they recognised they have to engage with regulators and authorities. FB also relies on 3rd party fact-checkers. Problematic pages are either taken down, marked as misleading, or linked to alternative articles providing a different viewpoint.)*
- **What are Facebook's policies for fighting disinformation in the context of European elections 2019? How does Facebook intend to balance its policies against disinformation with the freedom of expression?**

DEFENSIVE LINES

The Recommendation on elections goes beyond the European elections – how do you envisage the work of this network going forward?

- We should meet three times before the elections, and we will consider our preparedness from a number of perspectives, including in the context of elections in some Member States, where the European elections will be held on the same day or in the same period as local and national elections.
- This process will form the basis of our future work. The purpose of this network is to support resilience in our electoral processes, which is a long term project which will no doubt evolve.
- The Commission will prepare a post-election report after the elections.
- We will also be engaging and coordinating as appropriate with other networks, including the EPDB, the fact checkers and the Rapid alert system.
- The network may also serve to facilitate the dialogue between the national election networks and online platforms.

With six months left before the European elections, what can the Commission hope to achieve in this area?

- Work to combat disinformation and securing fair and free elections is urgent, but we are not starting from scratch.
- A key tool is the EU's strong data protection rules, whose value have already been demonstrated in the Facebook/Cambridge Analytica scandal.
- The EU Institutions and the Member States have long established collaboration in the area of cybersecurity, and notably the Network and Information Security cooperation group recently issued a Compendium on Cyber Security of Election Technology.
- The Code of Practice on disinformation, which emerged from the Commissions April 2018 Communication on Tackling online disinformation, is a set of industry self-regulatory standards to fight disinformation on a voluntary basis, which all the major online platforms have signed up to.
- The Commission's package of measures on securing free and fair elections issued on 12 September 2018 addresses the Member States, and national and European political parties and foundations, providing concrete measures to address the challenge of disinformation and securing fair and free elections in Europe.
- The Action Plan of 5 December of the European Commission and the High Representative provides further specific proposals for a coordinated EU response to the challenge of disinformation.

- Online platforms, such as Facebook, must take on their share of responsibility in ensuring free and fair elections.

Who should oversee efforts to improve transparency?

The Commission will monitor progress being made and report in the post elections report.

Will the Commission's report on the Code of Practice be issued in time for the network meeting?

- No. The signatories were requested to provide updated information on policies and practices taken as of year-end 2018 to implement the Code of Practice by 10 Jan. However, the trade association signatories have asked for an extension and it will not be possible to issue the report before 21 January. Information received will be published without substantive comment.
- It could be for the second meeting in February.

There have been allegations that online platforms are aggressively removing online political discussion in an effort to avoid being held responsible for the spread of disinformation. Aren't the European measures to combat disinformation liable to make this worse, and is the Commission comfortable with the potential impact on democracy?

- When assessing content published on their platforms, IT companies have to assess it, not only against their rules and community guidelines, but, where necessary, against applicable law and fundamental rights, including the freedom of expression. A priori, the content that is illegal offline should not be allowed to remain legal online.
- The European Commission is continuously monitoring the implementation of its Code of Conduct on countering illegal hate speech online to which many IT companies have signed up.
- The Commission will also carry out a comprehensive assessment of the implementation of the Code of Practice on Disinformation in its first 12 months at the end of 2019. Should the implementation and the impact of the Code of Practice prove unsatisfactory, the Commission may propose further measures, including of a regulatory nature.

What is in the Code of Practice on disinformation?

- The signatories commit to disrupt advertising revenue to go to accounts and websites that misrepresent material information about themselves and to provide advertisers with adequate brand safety tools and information about websites purveying disinformation.

- The signatories will enable public disclosure of political advertising and make effort towards disclosing issue-based advertising. For example, political ads in election campaigns will be clearly marked as such.
- The platforms will have clear and publicly available policy on identity and online bots and take measures to close fake accounts.
- The platforms will provide information and tools to help people make informed decisions when they encounter online news that may be false. They will also make it easier for people to find diverse perspectives about topics of public interest, while giving prominence to reliable sources on their services.
- The platforms will provide privacy-compliant access to data to researchers in order to track and better understand the spread and impact of disinformation.
- By implementing the commitments included in the Code, the signatories will increase transparency for European citizens about political and issue-based advertising and will limit manipulation techniques such as the malicious use of bots and fake accounts.
- The Code should contribute to countering mass online disinformation campaigns that polarise public opinion or sow distrust in the European institutions.

How can the Commission support increased turnout in elections?

- Following the 2014 elections to the European Parliament, the Commission had pledged in its 2015 post-election report to identify ways of further enhancing the European dimension and the democratic legitimacy of the Union decision-making process, and to examine further, and seek to address, the reasons for the persistently low turnout in some Member States.
- In February 2018, the Commission called for early and ongoing engagement with citizens in debates on European issues, an earlier start to political parties' campaigns for the elections to the European Parliament, including those of their candidates for President of the European Commission, more transparency about the links between national and European political parties and the promotion by Member States of the right to vote, in particular for underrepresented groups.
- We expect from, the platforms, such as Facebook to contribute to increased voter engagement and participation. This should be done on an equal basis for all groups of voters and across all Member States.

BACKGROUND

On the Commission Recommendation from 12 September 2018

- On 12 September 2018, the Commission issued a Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament, in line with its priority to ensure fair and free elections to the European Parliament in 2019.
- It recommends in particular the establishment of cooperation networks in each Member State, which should involve in particular national authorities with competence for electoral matters, for cybersecurity, media and data protection.
- Additionally, a European coordination network on elections is envisaged with representatives from Member States liaising at the European level. The objective is to jointly quickly detect potential threats and gaps, sharing findings and expertise, exchange information and ensure a swift and well-coordinated response including by liaising on the application and enforcement of relevant rules in the online environment.
- The Recommendation also elaborates on improving transparency, whereby European and national political parties foundations and campaign organizations and other stakeholders are asked to take appropriate steps to ensure that information is actively disclosed to citizens 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.
- Furthermore, the Recommendation calls on the Member States to put in place the necessary procedures to prevent, detect, manage and respond to cyberattacks, as well as to play a role in raising awareness of the above mentioned issues in advance of the elections.

April Communication on disinformation

- The Commission is implementing the actions to counter disinformation announced in its *Communication on Tackling online disinformation*, adopted in April 2018.
- One key initiative is the Code of Practice on Disinformation for online platforms and the online advertising sector. This is a self-regulatory instrument, developed by industry stakeholders.
- On 16 October, initial signatories subscribed to the Code of Practice. These include the three major platforms (Facebook, Google, Twitter) and Mozilla, plus trade associations representing other online platforms and the online advertising sector.
- The Code includes 15 commitments centred around five chapters: (1) Scrutiny of ad placements; (2) Political advertising and issue-based advertising; (3) Integrity of services; (4) Empowering consumers; and (5) Empowering the research community. Participants identify the commitments relevant to their services and the policies and actions they will take to implement their commitments.

- We are also making progress on other actions, including supporting the development of an independent European network of fact-checkers, support to quality journalism and new initiatives to promote media literacy.
- The Commission issued a Progress Report on these actions in December.

Action Plan

- In response to a June 2018 request, on 5 December 2018 the Commission and the High Representative adopted an Action Plan with further specific proposals for a coordinated EU response to the challenge of disinformation. It was requested and has been endorsed by the European Council. Among other things, it proposes actions to ensure that industry delivers on the Code of Practice on Disinformation as well as actions to raise awareness about disinformation, empower consumers, and support media literacy.

Contact: [REDACTED]

Topic 4: Disinformation

OBJECTIVE

- to establish a direct high-level contact with Nick Clegg as the likely channel to convey the Commission's concerns to the leadership of Facebook in the future

LINE TO TAKE

- Facebook's problems have been at the core of the global push-back against technology companies.
- Sustained, credible, and verifiable action is needed to regain the trust of many parts of the population. The impacts of Facebook's scandals have tarnished the whole industry in many ways. This is bigger than Facebook alone.
- We acknowledge and welcome the many actions Facebook has taken to redress the balance, in particular on terrorist content and on disinformation.
- We especially welcome the efforts around the hash-sharing database for terrorist content, and the high quality reporting under the code of practice for disinformation.
- Facebook needs to continue along this path, and must be open to continued constructive and transparent cooperation with the European Commission, to monitor and improve the integrity of its service.

BACKGROUND

Positions on illegal content online

- **Facebook's view** is that they have already done a lot to fight illegal content. This includes hiring and training several thousand content moderators, compliance with the DE law on hate-speech, running and hosting the hash-sharing data-base to fight terrorist content. They have also carried out a "public consultation" on hard questions, including on censorship online. While Mark Zuckerberg acknowledges that Facebook needs a significant change in operations, they refuse the label of media company which is increasingly thrust upon them.
- **Our view** is that Facebook needs to do much more to win back the trust of European regulators. A diligent implementation of the illegal content recommendation would be a useful step.

Positions on disinformation

- **Facebook's view** is that it is seriously tackling the problem of disinformation, including through its commitments under the Code of Practice. Facebook has provided a quality first implementation report under this code.
- **Our view** is that this is a first constructive step in the right direction, but that success will be determined on the ground, over time and industry wide. They need to continue to co-operate, while also remaining responsive and transparent to new threats.

Position on platform regulation in general

- **Facebook's public view** is that it welcomes well designed, practical regulation. Internal documents revealed by the New York Times, however, seem to reveal that internally the company remains generally opposed to calls for regulation, including in response to George Soros' 2018 Davos speech, in which he attacked Facebook and Google. Facebook has been critical the German Hate Speech law, and the Terrorist Content Regulation, without publically opposing these rules.
- **Our view** is that we tackle specific problems on the basis of evidence, rather than providing for any overarching horizontal regulation. At present we are finalising the negotiations on the Platform-to-Business Regulation, which provides transparency and redress for companies doing business on Facebook. This college has decided not to modify the E-Commerce Directive.

Contacts:

(illegal content)

[REDACTED] (online disinformation)

ANNEX: NICK CLEGG, CV

Nick Clegg grew up in Buckinghamshire with his two brothers and sister. His mother is Dutch and his father is half Russian, which influenced Nick's internationalist outlook and linguistic ability – he speaks French, German, Spanish and Dutch.

Nick studied Social Anthropology at Cambridge and afterwards continued his postgraduate studies at the University of Minnesota and the College of Europe in Bruges – where he met his wife, Miriam, with whom he now has three sons. Nick then spent some time in New York, working as a trainee journalist with Christopher Hitchens, as a consultant in London, and in Budapest writing about economic reform having won a prize from the Financial Times. Later Nick moved to Brussels where he worked for five years for the European Commission. His job included managing aid projects in Central Asia following the collapse of communism and acting as a trade negotiator with China and Russia as a senior member of Leon Brittan's office, then Vice President of the EC.

In 1999 Nick was elected Member of the European Parliament for the East Midlands - the first liberal Parliamentarian in the whole region since the 1930s. As an MEP, he co-founded the Campaign for Parliamentary Reform, which led calls for reforms to expenses, transparency and accountability in the European Parliament. He was also the Trade and Industry Spokesman for the Liberal group of MEPs and piloted a radical new law breaking up telecoms monopolies.

Nick lectured part-time at Sheffield and Cambridge Universities before being elected as Member of Parliament for Sheffield Hallam in 2005.

He became Europe spokesman in Charles Kennedy's shadow cabinet, acting as deputy to Menzies (Ming) Campbell. When Ming won the 2006 leadership election, he became Shadow Home Secretary. In this position, Nick led the Liberal Democrats' defence of civil liberties, proposing a Freedom Bill to repeal unnecessary and illiberal legislation, campaigned against ID Cards and the retention of innocent people's DNA, and argued against excessive counter-terrorism legislation.

Nick was elected leader of the Liberal Democrats in December 2007. Following the election in 2010, Nick took the party into government as part of the first Coalition in the UK since the Second World War, where he put Liberal Democrat policies into practice for the first time – the £800 income tax cut, the £2.5b pupil premium, legislating for gay marriage, introducing shared parental leave, the list goes on and on.

Nick stood down as leader in 2015, after which Tim Farron was elected.

(Source: https://www.libdems.org.uk/nick_clegg)

ANNEX – LATEST MEDIA COVERGE ON FACEBOOK/NICK CLEGG

Why Facebook hired Nick Clegg

By Wired

Facebook should hope that, this time around, Clegg will be able to deliver on his admirable sentiments. It's important not just for Mark Zuckerberg – but for all of us.

You've had a bad year. Actually, a year where the default corporate setting has been 'acute crisis'. You've been implicated in undermining democracy, the founders of one of your most successful divisions have quit the company, your messaging service has been linked to incitement of violence, you've demonstrated that the core element of your business model – private data – is not safe in your hands, your products have been used as a tool for bad actors and criminals, research has suggested that your products have a negative influence on users' well-being, your founder has been summoned to appear in front of a Senate committee and lawmakers across the globe are engaged in examining your excessive influence and questionable tax arrangements.

So, what do you do? Who do you turn to? Well, it's obvious isn't it? Nick Clegg.

Clegg knows about bad years, of course. He promised to hold the Conservative party to account during the coalition government of 2010 to 2015, but will be remembered principally for his U-turn in 2010 on his promise to eradicate tuition fees, a change of heart that, along with the Lib Dems being consigned to a marginal role in the coalition, led to a devastating rout of the party at the 2015 general election in which it lost 49 seats, leaving it with only eight MPs.

Two years later, during the snap election of 2017, Clegg lost his own seat, Sheffield Hallam, after an increased number of first-time voters ensured that there would be no forgiveness for the tuition fee betrayal. That night #Cleggsit trended on Twitter.

Since then, Clegg has been an advocate for another referendum on Brexit and has founded a think tank, Open Reason, to promote liberalism. On the organisation's website, the section devoted to Clegg's pro-Europeanism nestles next to another of his interests: technology, particularly artificial intelligence. Here is where we get to the crux of why his appointment to head Facebook's global affairs and communications team should not come as a shock.

The main challenge to Facebook is coming from the European Union (EU), and Clegg – who was an MEP from 1999 to 2004 – knows his way around Brussels. As the EU Commission begins to discuss the possibility of regulating Facebook like a teleco, or Margrethe Vestager – the competition commissioner whose term ends in 2019 and has been a formidable force in reining in the power of American technology companies – examines Facebook's tax arrangements, who better than a former MEP to lobby and navigate the Byzantine interests and structures of Brussels?

In a Facebook post published the day of his appointment, Clegg offered a sense of what his brief will be by emphasising that his role will be more than deal-making with legislators – it will involve shifting corporate culture at a company whose founder announced earlier this year he would “fix” it. The sensibility of a politician who believes in consensus, rather than that of an engineer seeking to eradicate a bug, might be exactly what Facebook needs.

“Facebook, WhatsApp, Messenger, Oculus and Instagram are at the heart of so many people’s everyday lives – but also at the heart of some of the most complex and difficult questions we face as a society: the privacy of the individual; the integrity of our democratic process; the tensions between local cultures and the global internet; the balance between free speech and prohibited content; the power and concerns around artificial intelligence; and the wellbeing of our children,” Clegg writes.

“I believe that Facebook must continue to play a role in finding answers to those questions – not by acting alone in Silicon Valley, but by working with people, organisations, governments and regulators around the world to ensure that technology is a force for good.”

To do this, of course, Clegg will have to be more than a lobbyist. He will need to grapple meaningfully with the issues he has chosen to highlight, and to demonstrate that Facebook is willing to make decisions that are in the best interests of society, not just its shareholders. The company can no longer afford the tin ear that has become its hallmark. If Clegg is to prove that he really means what he says, he will have to deal with issues such as corporate tax avoidance – an issue that he highlighted during his tenure as deputy prime minister.

A year ago, at an event organised by Campaign, Clegg already sounded like a Silicon Valley employee. While conceding that Big Tech companies had much to do to prove that they are “good global citizens”, he argued that, “in other areas they’re being unfairly caricatured, often by a print media that has an ulterior motive to discredit social media because of its success in attracting online advertising revenues that otherwise might be spent on newspapers.”

Claiming that the failures of Big Tech are being “unfairly caricatured” is, of course, specious. Clegg has long argued for the rights of citizens to be paramount in decision-making – it is to be hoped that this sentiment is still central to his thinking as he glad-hands lawmakers in Washington, Brussels and Beijing on behalf of the fifth most valuable company in the world. In government, Clegg was principled but pragmatic. He will need to emphasise the former of these qualities if he is to change the current perception of his new employer.

Facebook should hope that, this time around, Clegg will be able to deliver on his admirable sentiments. It’s important not just for Mark Zuckerberg – but for all of us.

Facebook Cracks Down on Networks of Fake Pages and Groups

By Wired

Pages and groups are the tools Facebook misinformation peddlers love the most. Creating a network of anonymous pages is one of the easiest ways to quickly spread fake news or propaganda on the social network. This tactic has most famously been used by Russian trolls—even long after the 2016 presidential election. Earlier this month, Facebook took down a cohort of deceptive pages linked to Russian state media. Now, the social network has changed its policies to better enable cracking down not just on individual pages, but on entire networks of fraudulent pages and groups.

Facebook has historically played Whac-a-Mole when it comes to systems of fraudulent pages, even when they're run by the same person. If a troll runs two fake news pages but only one of them violates Facebook's policies, the company can't take down the other until it breaks the rules as well. That loophole has allowed propagandists to simply shift their efforts to other existing pages after Facebook closes down one arm of their operation. But starting today, the social network will begin removing entire factions of pages and groups, even when not all of them have individually met Facebook's criteria to be removed.

In a blog post announcing the change, Facebook said it "may now also remove other Pages and Groups with similar names that are maintained by the same person, even if that specific Page or Group has not met the threshold to be unpublished on its own."

In some situations, the social network has already gotten more aggressive with networked pages; in August of last year for example, Facebook expunged a band of inauthentic pages that appeared to have originated in Iran. It has also repeatedly removed coordinated trolling efforts from Russia. But under the new policy, the company won't need to demonstrate infractions from every single page to justify a sweeping takedown.

Facebook will also launch a new control panel Thursday for page managers, designed to make it easier for them to understand when their posts have breached Facebook's Community Standards. The Page Quality tab will display content that Facebook recently removed and will cite the rule it broke. For example, it might inform a page manager that their video was taken down for going against the social network's rules forbidding hate speech. The menu won't display all policy violations, but it does include things like graphic violence, harassment, bullying, nudity, and sexual activity. Notable omissions include spam, clickbait, and intellectual property violations.

Page Quality will also show page managers when their content has been rated "False," "False Headline," or "Mixture" (primarily misleading, but contains some true information) by third-party fact-checkers like the Associated Press or Politifact. When fact-checkers give posts these kinds of negative feedback, Facebook reduces how many people see them in their News Feed.

Facebook has historically played Whac-a-Mole when it comes to systems of fraudulent pages.

Internal Facebook documents leaked to Motherboard last year indicated that the social network has different deletion thresholds for pages depending on the type of content violation they commit. For example, if a page manager receives five “strikes” for hate speech in a 90 day period, Facebook instructs moderators to delete their page. If a page or group has more than two “elements” of sexual solicitation, it gets deleted. That covers the page’s description, photo, or title, for instance. (It’s possible these policies have since been revised, but they help color how Facebook thinks about policing pages and groups.)

The Page Quality tab will likely reduce some of the confusion page managers experience on Facebook, where it can be difficult to understand how or why the social network is moderating content. If you don’t know that a fact-checker labeled your post fake news, it’s easy to think Facebook isn’t showing it to people for more sinister reasons. The tool makes these kinds of actions more transparent, especially for those who are in charge of pages with large followings that generate hundreds of notifications a day. But it likely won’t mean much for bad actors who already intend to skirt Facebook’s rules in the first place.

These new features and updates are part of wider changes Facebook has made over the past two years, which are designed to make it harder to spread misinformation and propaganda on its platform. Many of those actions have focused on tightening its advertising policies; the social network now has strict requirements for organizations that want to run so-called issue ads, for instance. These new tweaks take aim at another problem: fraudulent pages and groups that don’t need to rely on paid advertising to reach an audience.

There’s one issue, however, that Facebook has yet to address: It’s still possible to run Facebook pages anonymously. Pages can then create their own affiliated groups, allowing bad actors to erect entire communities without revealing their identity. Facebook gives page managers the ability to list their “Team Members,” but the functionality is optional. It’s understandable why the platform works this way; the social media manager for a nonprofit or publication might not want their work connected to their personal Facebook profile, for instance. But it makes it almost impossible for users to understand where a page or group came from. In July for example, a Facebook group that purported to be a safe space for sexual assault survivors was taken over by trolls who harassed its members. The group was run by an anonymous Facebook page, so the victims had no way to discern the identity of their harassers.

Facebook has made pages more transparent by disclosing the date they were created and whether their name has been recently changed, but so far it has stopped short of requiring users to disclose when they create them. That loophole will continue to make it easy for bad actors to construct networks of fraudulent pages, but at least now Facebook has given itself the authority to take them all out in one swoop.

DAVOS-Sandberg says Facebook must earn back trust

By CNBC

DAVOS, Switzerland, Jan 23 (Reuters) - Facebook Inc's operations chief Sheryl Sandberg said on Wednesday that the world's largest social network needed to win back public trust after facing scandals for violating its users' privacy.

The social media platform is investing billions of dollars a year to improve the security of its network, Sandberg said in an interview hosted by German newspaper Die Zeit and UK law firm CMS at the World Economic Forum in Davos, Switzerland.

"We did not anticipate all of the risks from connecting so many people," Sandberg said, adding that the site had added features that give users greater control over their personal information.

The 15-year-old technology company has been a darling of California's Silicon Valley, making stars out of its founder, chief executive and chairman Mark Zuckerberg, and Sandberg, known for her feminist manifesto "Lean In". But its shares have fallen roughly 33 percent since July to \$144 due to concerns about user privacy.

Last year, the company was buffeted by revelations that UK consultancy Cambridge Analytica had improperly acquired data on millions of its U.S. users to target election advertising.

"We need to earn back trust," Sandberg said.

Some of Facebook's major shareholders have pushed for Zuckerberg, who has majority control of the company, to step down as chairman.

Sandberg said he should remain both chair and CEO. She said that she also plans to remain at Facebook, where she has worked since 2008.

"I think I have a job to do," she said. "It's a job I really want to do."

Sandberg said that if Facebook had to change its business model and charge users a subscription fee instead of collecting advertising revenue, far fewer people would be able to use it.

"Fundamentally disallowing our business model would harm a lot of people all over the world."

She said her grassroots women's movement, spurred by the publication of "Lean In", was still going strong. But, asked if she was considering a run for U.S. president in the 2020 election, she replied : "It's not on my agenda." (Editing by Mark Trevelyan)

Why Sheryl Sandberg, Facebook's 'adult in the room', may pay the price for its failings

By The Guardian

After months of revelations about the firm, the executive is being talked of as a sacrifice, not founder Mark Zuckerberg

Facebook's already terrible year is ending on a new low, as Mark Zuckerberg and his beleaguered executive team battle another share price slide, this time triggered by new revelations about the company's relaxed attitude to the privacy of its 2.2 billion customers' data.

Shares dropped more than 7% on Tuesday after it was revealed that the company had bent its own data rules for clients including Netflix, Spotify, Amazon, Microsoft and Sony.

The latest damaging report, published by the New York Times on the back of a District of Columbia lawsuit accusing the social media giant of exposing residents to political manipulation by "failing to protect" user data during the 2016 US presidential election, will surely be disagreeable to Zuckerberg, Facebook's 34-year-old founder, chief executive and controlling stockholder.

But it is Sheryl Sandberg, former chief of staff at the US treasury under Larry Summers and the woman brought in a decade ago to be the "adult" in Facebook's executive ranks, who is largely taking the heat for the company's mounting operational, financial, political and public relations challenges.

Facebook contractors faced Christmas ultimatum: accept wage offer or lose jobs

Clearly, Sandberg has much to account for as chief operating officer. Facebook's travails, which have seen it shares drop nearly 40% since their July peak, are not Sandberg's alone to carry, though on some days it appears the 49-year-old has been doing much of the heavy lifting.

"There's little doubt the company is facing critical challenges and has made some egregious mistakes," says Kathryn Kolbert of the Athena Centre for Leadership Studies. "The fact that Sandberg was brought in to be the adult in the room does not absolve Zuckerberg of responsibility.

"Mark Zuckerberg is the CEO of a multibillion-dollar company, and he's been at it a while. He's a grown-up. He ought to be responsible. But from what I see, there isn't the sense that both should be accountable."

Five weeks ago, Sandberg's key role in shaping the company's response to multiple crises was exposed, again by the New York Times. These have included the revelations of Russian interference in the 2016 election, the Cambridge Analytica scandal, and the

decision to hire a rightwing opposition research company, Definers Public Affairs, to apply aggressive political campaign tactics to Facebook's PR and to look into the finances of high-profile investor George Soros days after he publicly criticised the big US technology companies.

Facebook claimed that the research into Soros "was already under way when Sheryl sent an email asking if Mr Soros had shorted Facebook's stock".

However, the backlash against Sandberg, until recently a figurehead for tech-branded progressive feminism, has barely relented.

The bestselling author, who just a year ago was riding high on the success of *Option B*, a follow-up to her empowerment manual *Lean In*, is taking hits from all sides.

Sandberg, as the executive who helped develop Google's ad-supported business strategy before joining Facebook, was in the firing line in September when the company became the focus of an American Civil Liberties Union complaint alleging that its advertising system allows employers to target job ads based on gender.

Three weeks ago, before a sold-out audience at the Barclays Centre indoor arena in Brooklyn, former first lady Michelle Obama said Sandberg's belief that women can always "have it all" if they assert themselves across their personal and professional lives – a key tenet of Sandberg's *Lean In* philosophy – is "a lie".

"It's not always enough to lean in because that shit doesn't work all the time," Obama reportedly said.

Then last week the civil rights group NAACP launched a week-long boycott of Facebook after a report it had commissioned highlighted concerns over voter suppression, ad targeting and the company's own issue with workplace diversity.

"We know that we need to do more: to listen, look deeper and take action to respect fundamental rights," Sandberg said in a conciliatory statement.

Mark Zuckerberg, chief executive officer and founder of Facebook, at a technology gathering in Paris in May.

Mark Zuckerberg, chief executive officer and founder of Facebook, at a technology gathering in Paris in May. Photograph: Christophe Morin/IP3/Getty Images

According to Nathalie Molina Niño, author of *Leapfrog: The New Revolution for Women Entrepreneurs*, part of the hostility aimed at Sandberg is certainly related to her gender. "The higher a woman gets in terms of success, the greater the culture that enjoys taking her down," Niño says. Indeed, negative posts on Sandberg's own Facebook page are largely written by men.

At the same time, Niño points out, *Lean In* missed the mark because it failed to reflect the experience of most women who are balancing work and family.

As a result, Sandberg has become synonymous with a particular brand of female empowerment that is considered out of touch with notions of inclusiveness.

"It's applicable only to women in the corporate world and that's a fairly small, marginal group," Niño says. What Lean In showed, in fact, "is in contrast to what is true for most women, and the backlash against Sandberg is a reflection of that reality".

But Sandberg is not standing back. It is a measure of her resilience, as well as solid support from Zuckerberg and Facebook's board, that she has stayed put.

In an interview with the news network CNN, Zuckerberg said: "Sheryl is a really important part of this company and is leading a lot of the efforts to address a lot of the biggest issues that we have. She's been an important partner for me for 10 years ... I hope that we work together for decades more to come."

While Sandberg is taking the heat for Facebook's problems, Zuckerberg appears to be relatively unscathed. "The company is facing incredible challenges and has made egregious mistakes, so Zuckerberg should bear primary responsibility," says Charles Elson, expert in corporate governance at the University of Delaware.

Forcing Sandberg out, he says, would solve the perception that the company is taking action, but achieve nothing in terms of resolving the seemingly insurmountable issue of policing the user content of a global social network.

The company has made egregious mistakes and so Zuckerberg should bear primary responsibility

Charles Elson, University of Delaware

"The public wants somebody to take the fall, and since Zuckerberg is the owner he's not going to do it. So they've come to the view that Sandberg is the next best thing."

But that risks a potential new PR backlash by pushing Sandberg out without solving any of the company's data privacy and political manipulation issues.

If Sandberg departs, her brand too tarnished to be of further use to Facebook, the decision will be Zuckerberg's to make. "As the majority voting shareholder, he calls the shots," Elson points out.

Facebook's terrible year

17 March

The Observer and New York Times reveal that Facebook accidentally allowed consulting firm Cambridge Analytica to gather members' data for political purposes. The number of users is later put at 87 million.

10-11 April

Founder Mark Zuckerberg testifies before the Senate judiciary and commerce committees. He says Facebook “didn’t take a broad enough view of our responsibility, and that was a big mistake”.

3 June

The New York Times reports that Facebook struck agreements allowing phone-makers including Apple, Amazon, BlackBerry, Microsoft and Samsung to access users’ personal information.

26 July

Facebook’s share price plunges 20%, wiping \$17bn off the value of Zuckerberg’s stock, after the company reveals that 3 million European users have quit.

5 September

Sandberg testifies before the Senate intelligence committee regarding efforts to prevent foreign states from spreading false information on social media.

28 September

Facebook announces that hackers used 400,000 accounts under their control to gain the access tokens of nearly 50 million Facebook users, in the firm’s largest data breach.

14 November

The New York Times reports alleged tactics by the firm to block scrutiny of Russian disinformation and hate speech distributed via Facebook.

15 November

Facebook creates an independent body to monitor offensive content. Zuckerberg says he now believes that Facebook “should not make so many important decisions about free expression and safety on our own”.

21 November

Facebook confirms it hired rightwing political research firm Definers Public Affairs to attack George Soros and undermine critics by publicising their links to him. Zuckerberg and Sandberg deny knowledge of the arrangement.

30 November

The New York Times reports that Sandberg asked Facebook communications staff to research Soros’s financial interests after he describes social media, and Facebook in particular – as “a menace to society”.

18 December

to the business of being Facebook—a multi-billion-dollar profit machine with a growing user base. This was because, for years, there were no consequences for Facebook's deleterious actions. No matter how much the company pillaged your privacy or ignored the rules, nothing changed for Facebook, except that its stock price kept going up.

After a bumpy public offering in May 2012, Facebook's stock rose steadily from a low near \$18 to an all-time high of about \$218 in July 2018, giving the company a market capitalization of more than \$600 billion. User growth shot up faster than any other social-media company in history, adding more than a billion new users, most of whom used the service on a daily basis. Revenue was pouring in, too. Facebook's annualized revenue per user increased from \$16 a person in the first quarter of 2015 to a whopping \$34 a person just three years later. Facebook, to borrow a quote from a certain president, could have gone out on Fifth Avenue and shot someone, and people would still sign up for the service and investors would continue to buy its stock.

For most of that time, Sandberg was celebrated in the press as a deity among the business elite. Her résumé is indeed astounding: Sandberg has served on the board of the Walt Disney Company, Women for Women International, Starbucks, and countless others. Her book, *Lean In: Women, Work, and the Will to Lead*, literally created a cultural movement. She has appeared on *Fortune* magazine's "Most Powerful Women in Business" list nearly a dozen times; the *Time* 100 list; and the *Jerusalem Post*'s "World's 50 Most Influential Jews" list. The list (sorry, pun intended) could go on.

When the mood turned, and the scandals began piling up—Cambridge Analytica, fake Russian accounts, security breaches, a *New York Times* investigation that alleged Facebook hid evidence of election interference on its platform—Sandberg's reputation fell along with Facebook's stock. Today, the company is worth about \$200 billion less than it was in July, and Sandberg is desperate to resuscitate their fortunes.

Reading the most recent responses by Facebook and Sandberg, you have to wonder if a fresh apology is going to resonate with users or the media, or if this is just another Silicon Valley public-relations exercise. My theory is: no apology tour will matter until there is meaningful change in leadership at Facebook, which is still run by most of the same executives that were in place when the Cambridge Analytica scandal began. Sandberg is still C.O.O., Zuckerberg is still chairman and C.E.O., Chris Cox is still C.P.O., Mike Schroepfer is still C.T.O., Dave Wehner is still C.F.O., and people like Andrew "Boz" Bosworth—who sent the now-infamous memo that suggested user growth was more important than human lives—still works for Facebook. The company's board, too, is still the same. The only senior person who has left the company is the former vice president of global communications, Elliot Schrage—possibly the most thoughtful and nuanced of all the senior managers there, and one of the few who appeared to grapple honestly with Facebook's failures.

I'm not saying that Sandberg should be fired. I'm not saying Cox, Schroepfer, or Zuckerberg need to resign, either. But I am saying that something has to change at the company at the top. Simply wheeling out a new P.R. campaign that says "we're a different company" isn't sufficient. The first time there's another scandal—and there

will be one, if not a dozen, as we head into the next presidential election—that corporate messaging is going to melt away like the snow in summer.

I understand why Sandberg is trying to lower the temperature in the media, especially the rhetoric about her role. Some news coverage has been harsh, some justified, most somewhere in the middle. But the very reason people pounced on Sandberg the first chance they got was the very reason the company finds itself in its present situation. For more than a decade, people have demanded that Zuckerberg stop being so shady with their personal information, that he change aspects of the site that felt intrusive, that Facebook try to do better. Each time, it fell on deaf ears, was ignored, or laughed at. Then, when it became clear that Sandberg was just like Zuckerberg, the cannons turned toward her. If Sandberg really wants to change how she's perceived in the press today, she shouldn't be trying to tell people outside the company that it's time for change, but rather pushing for it inside Facebook.

Facebook is the most 'vulnerable' big tech firm facing disruption, top VC says

By CNBC

- Facebook is the most vulnerable big technology firm when it comes to facing disruption, Rebeca Hwang, co-founder and managing director of Rivet Ventures, tells CNBC at Davos.
- Hwang also says large technology firms could be challenged by start-ups.
- Phil Chen, managing director at venture firm Presence Capital and decentralized chief officer at HTC, says blockchain technology could take some power away from big tech firms.

Mark Zuckerberg, chief executive officer and founder of Facebook Inc., listens during the Viva Technology conference in Paris, France, on Thursday, May 24, 2018.

Marlene Awaad | Bloomberg | Getty Images

Mark Zuckerberg, chief executive officer and founder of Facebook Inc., listens during the Viva Technology conference in Paris, France, on Thursday, May 24, 2018.

Facebook is the most vulnerable large technology company when it comes to facing disruption, a prominent venture capitalist told CNBC on Tuesday, amid ongoing concerns around privacy.

The social media giant had a rough 2018. It kicked off after revelations that the data of 87 million Facebook users had been harvested by a political consultancy that ended up working with President Donald Trump's campaign. Then came reports about Russian-backed attempts to influence American elections and news that 50 million Facebook

accounts were compromised in a cyberattack, in addition to the resignation of Instagram's founders.

Rebeca Hwang, co-founder and managing director of Rivet Ventures, said backlash from users toward social media firms has left Facebook in a tough place.

"I do think Facebook is in a very vulnerable place right now. Both seen from the perspective of the consumer reaction ... but also from the perspective of the deal flow that I see and the types of companies that are trying to become the disruptors of a Facebook," Hwang said during a CNBC-hosted panel at the Davos Sanctuary.

"In my opinion, they have to take very strong actions to maintain their position."

Facebook was not immediately available for comment when contacted by CNBC.

Part of the discussion on the panel focused on the power of the world's largest technology firms and whether they are too powerful to face disruption. Hwang said that the heightened sensitivity among consumers toward data privacy could provide an opportunity for start-ups.

"I think the ones that have become dominant, especially with younger generations, it's also very challenging having that status. And so I don't necessarily see a future where all of these giants will continue dominating forever. I think there will be disruptors in some of these areas by new players," Hwang told CNBC.

Blockchain disruption?

Phil Chen, managing director at venture firm Presence Capital and decentralized chief officer at HTC, said blockchain technology could take some power away from big tech firms.

Blockchain is the technology that underpins the cryptocurrency bitcoin. It is a public ledger of transactions in bitcoin that is decentralized, meaning it is not owned by any one person. Instead, it is maintained by many participants.

Chen argues that companies like Facebook hold data on users in a central database that is owned by the company.

But blockchain technology could decentralize databases, allowing users to own their own data, and taking the power away from large companies.

"That's the hope, that's the thesis. At the end of the day today, the big corporates, they have big central servers that hold everybody's data. I think what bitcoin and blockchain really allows ... is empowering people to own their own keys," Chen told CNBC.

A key is a unique cryptographic address that allows someone to own their own cryptocurrency. Chen argues that this unique key could also allow users to own their own data.

"Once you start owning your own keys, which is the means in which you own the cryptocurrency, then you start owning your identity, then you start owning your data, and that needs the whole crowd and the people to participate," Chen said.

Inside Facebook's fight against European regulation

By Politico

Dozens of Commission documents show how the tech giant pushed back against rules on issues ranging from copyright to privacy.

We don't need no regulation.

That was the message from Facebook to the European Commission over a period of four years, according to dozens of emails and written accounts of arguments made by the social media company in private meetings with Commission officials.

The documents show that the company's representatives pushed back against almost any form of regulation of its businesses in the EU.

"The industry does not need a regulatory push to improve," the company told the Commission in March 2016, according to the Commission's written summary of the meeting.

The internal Commission documents, dated from 2015 to early 2018, were obtained through a freedom of information request by Corporate Europe Observatory, a lobbying watchdog.

They include summaries of meetings held with Commission Vice President Andrus Ansip, Commissioner for Justice Věra Jourová, their respective Cabinets, DG CNECT Director General Roberto Viola and his deputy Claire Bury, among other Commission officials. Most of the meetings were organized at Facebook's request.

The message the tech giant delivered was not one the Commission was primed to accept, according to lobbyists and officials who have followed the growing effort in Brussels to regulate tech companies.

"Facebook has consistently been tone-deaf about major concerns brought to their attention," said Marietje Schaake, a Dutch liberal member of the European Parliament who specializes in tech issues. "From their impact on election outcomes, to spreading of conspiracies and hate speech, the consistent message has been that regulation would stifle innovation. This is a losing strategy in Brussels."

On a range of legislation, ranging from privacy protection to copyright reform to rules governing responsibility for illegal content uploaded to internet platforms, the Silicon

Valley tech giant's arguments seem to have fallen flat — as European Union officials moved forward with regulation the company was warning against.

While lobbying is a normal part of the legislative process, the documents underscore a disconnect between Facebook's arguments and the EU's philosophical approach to lawmaking.

Some U.S. legislators might be sympathetic to the idea that tech companies be left free to innovate or that consumers are best placed to decide whom to trust with their data. Among European policymakers, the instinct is to write protections into law.

"Facebook's strategy is not adapted to dealing with the European Union," said Damir Filipovic, a former tech lobbyist who is now director at the Brussels-based consultancy firm Europa Insights. "You cannot come to Brussels with a Washington story about not wanting regulation for the tech sector."

A spokesperson for the European Commission said it is "always ready to receive input from citizens and various stakeholders, such as think tanks and business and civil society representatives, in order to make informed political choices."

'Private law'

Facebook's views on regulation led to tension with the European Commission starting in 2016, when tech companies, including Google and Facebook, worked with the institution on a code of conduct to fight online hate speech.

The code aimed, among other things, to clarify how tech firms should decide whether or not to remove content flagged by users. Tech companies, including Facebook, wanted to be free to refer to their terms and conditions instead of EU legislation, according to an April 2016 meeting summary with the Cabinet of Commissioner for Justice Jourová.

The Commission "urged [them] to reconsider" this position and argued that the tech companies should make their decisions using "national law implementing the Framework Decision on racism and xenophobia" — EU legislation that encourages national governments to introduce criminal penalties for some racist and xenophobic acts.

The final text, adopted in May 2016, was a compromise between Facebook and the Commission's position.

Upon receipt of a valid removal notification, the IT companies [commit] to review such requests against their rules and community guidelines and where necessary national laws," the final code of conduct reads.

Nonetheless, in subsequent meetings Facebook continued to press its case, trying to convince the Commission that its internal rules should take precedence over EU legislation or national law.

In January 2017, Facebook referred only to its terms of service when explaining decisions on whether or not to remove content, the documents show. "Facebook explained that referring to the terms of services allows faster action but are open to consider changes," a Commission summary report from then reads.

"Facebook considers there are two sets of laws: private law (Facebook community standards) and public law (defined by governments)," the company told the Commission, according to Commission minutes of an April 2017 meeting.

"Facebook discouraged regulation," reads a Commission memo summarizing a September 2017 meeting with the company.

The decision to press forward with the argument is unusual, said Margarida Silva, a researcher and campaigner at Corporate Europe Observatory. "You don't see that many companies so openly asking for self-regulation, even going to the extent of defending private law."

Facebook says it has taken the Commission's concerns into account. "When people sign up to our terms of service, they commit to not sharing anything that breaks these policies, but also any content that is unlawful," the company told POLITICO. "When governments or law enforcement believe that something on Facebook violates their laws, even if it doesn't violate our standards, they may contact us to restrict access to that content."

When it comes to fighting online terrorist propaganda, however, that argument was not enough to win over the Commission. The Commission has put forward a legislation forcing platforms to take down flagged terrorist content within one hour.

"We cannot rely on self-regulatory methods for terrorist content," Commissioner Jourová said at a conference this week.

The proposal is being considered by the European Parliament and Council of the EU.

'A service expected by users'

Another focus of Facebook's lobbying was the so-called e-Privacy Regulation — a Commission proposal the social media giant has described as a "threat" to its business model, which relies on online advertising.

Presented by the Commission in 2017, the regulation would require companies to request their users' consent to access and use personal communications.

The measure is something the European public is demanding, according to the Commission, which regularly cites a 2016 Eurobarometer survey, in which 92 percent of respondents said they find it "important that the confidentiality of their e-mails and online instant messaging is guaranteed."

"Should I not be asked before my emails are accessed and used? Don't you think the same? Is this asking too much?" Vice President Andrus Ansip tweeted in October 2017, when the Commission faced a fierce lobbying campaign by tech giants like Facebook and Google, as well as European media companies, telecom providers and advertisers.

Facebook repeatedly told the European Commission in 2017 and 2018 it did not want to be forced to collect users' consent to process their communications.

In different sessions with Commission officials during that time period, gathering users' consent was described as "too rigid, disproportionately cumbersome, extremely burdensome and not user-friendly," according to minutes of the meetings. "Transparency and choice" is more important than consent, Facebook argued.

Facebook tried to convince the Commission there is "no need for a regulation" at all.

In a March 2017 meeting, the company argued the public is free to use other services on the market if they don't agree with Facebook's privacy policy.

In an effort to be excluded from the regulation's scope, the tech giant also argued that Facebook Messenger is "not a messaging service." It added: "It is much more than that because it can notify you about an event which was mentioned during a conversation, it can suggest new friends based on the content of discussions."

In January 2018, Facebook told the Commission that the processing of communications is "expected by users, and even more — a value because of which people sign up for," referring to suggestions for friends, events, replies and others.

"Facebook claims this is not a privacy violation but a service expected by users," the meeting minutes read.

The company's arguments failed to sway the Commission, which has continued to insist that companies obtain consent for the use of personal information.

The Commission's proposal has received the endorsement of the European Parliament, but the Council of the EU — where national governments have their say — has yet to adopt a position. The three institutions must agree on any final legislation.

Meanwhile, Facebook continues to argue that it should be able to process personal data on the basis of so-called legitimate interest — which doesn't necessarily require a user's explicit consent. The British data protection authority describes legitimate interest as the "most flexible lawful basis for processing" personal data.

"As recognized in [the EU's General Data Protection Regulation], other legal bases for data processing, such as legitimate interest or contractual necessity, might be more effective in promoting transparency and control than consent," the company told POLITICO in response to questions for this article.

'Technology, not legislation'

Another area of concern for Facebook is the possibility of rules that would make it liable for content users upload to its platform, including hate speech, terrorist content and copyrighted material.

“Facebook [is] concerned about a possible change in the liability for intermediaries under [the] Digital Single Market,” Commission minutes from an April 2015 meeting read.

The EU law governing responsibility for content on social media platforms is the 2000 e-commerce directive, which does not hold companies like Google and Facebook liable for illegal content posted by their users.

Companies must take down illegal content once it has been flagged as such, but they are not required to actively prevent it from being uploaded.

“Additional liability would be a barrier to Facebook and the new business models on the platform,” the company said in July 2016.

European Commission President Jean-Claude Juncker elected not to reopen the e-Commerce Directive during his mandate. But other legislation, including a reform of copyright laws winding its way through Brussels, could make Facebook liable for some of the content on its platform.

On copyright, the arguments Facebook made publicly differed sharply from what it told the Commission behind closed doors.

In public statements critical of the reform, trade associations representing Facebook, such as CCIA Europe or EDiMA, largely played down the issue of liability. They focused instead on a proposal that would require internet platforms to use so-called upload filters that would automate the analysis of content, blocking anything that was illegal.

These, argued the trade associations, are tantamount to censorship. “Filtering before upload will censor EU citizens online,” EDiMA’s campaign slogan read in September 2018.

At the same time as trade associations representing Facebook were warning against “upload filters,” the company itself was touting its filtering technology in meeting with the Commission as an attempt to head off measures that would make it liable for the content on its platform.

Referring to content protected by copyright, Facebook also told the Commission in April 2015 that “every content uploaded by users is filtered through Audible Magic software before actual upload. The measures taken are kept at the level that would allow them to keep their status as a hosting provider.”

According to the Commission’s minutes of a March 2016 meeting, Facebook said it had “invested important resources to develop filtering mechanisms (copyright, bullying, terrorism, hate speech).”

In September 2017, one year after the copyright reform was presented, the social media giant told the Commission it preferred “collaborating and relying on technology rather than complex legislation that risks being implemented in a diverse manner in member states.”

“It’s very common for the Silicon Valley to push against regulation at all,” said Margarida Silva, of Corporate Europe Observatory. “But those emails show very clearly that they have specific non-public policy positions they are lobbying on,” Silva added, referring to the internal Commission documents.

The European Parliament and EU national governments are still in negotiations over copyright reform.

If the text currently on the table, which is not final, were to be adopted, Facebook would become liable for copyrighted content on its platform and would be required to strike licensing deals with rights-holders who want them.

When asked by POLITICO about the emails, Facebook argued the company is “transparent about the technology [they] use.”

‘The right regulation’

Over the course of the last year, Facebook seems to have switched tack on regulation, at least in its public statements.

In March 2018, the Guardian reported that the British political consulting firm Cambridge Analytica had harvested the data of millions of Facebook’s users in Europe and the U.S. for political purposes without their knowledge.

Confronted by furious lawmakers on both sides of the Atlantic, Facebook CEO Mark Zuckerberg did not push back against the idea that the company should be regulated. Instead, he asked policymakers consider what the “right regulation” should be.

It’s a shift in tone the company has widely adopted. “Governments have a right and a duty to set rules and boundaries, and we are supportive of the right regulation,” Facebook Chief Operating Officer Sheryl Sandberg said at the DLD conference in Munich this week. “Governments have to set standards, and companies have to work with them to make sure we can meet them.”

For Brussels, that was never in doubt.

“Whether or not we should regulate tech is not the right question [to ask],” Commissioner Jourová told a Brussels crowd this week. “The question is what place tech should have in our society.”

From: TALKO Wojtek (CAB-JOUROVA)
Sent: jeudi 28 février 2019 09:00
To: CAB JOUROVA ARCHIVES
Subject: FW: flash report from meeting Nick Clegg - for your approval

Follow Up Flag: Follow up
Flag Status: Flagged

Here is the flash.

Best,

Wojtek

From: TALKO Wojtek (CAB-JOUROVA)
Sent: Wednesday, January 30, 2019 4:58 PM
To: NIKOLAY Renate (CAB-JOUROVA) @ec.europa.eu>
Cc: ...
Subject: flash report from meeting Nick Clegg - for your approval

Flash report from meeting with VP of Facebook, Nick Clegg

Date:

On the request of Facebook, Commissioner Jourová (with HoC Renate Nikolay and Wojtek Talko) met with new VP for Global Affairs & Communications Clegg (accompanied by

Thomas Myrup Kristensen, Head of Brussels Office).

Nick Clegg (NK) presented the latest developments on the platform, especially when it comes to the ads transparency tools. He announced that Facebook will roll out a number of features ahead of EU elections, including:

- Public archive of all the ads, with detailed information on who paid for them, who was targeted and what was the reach of the ads.

- Verification of people / organisations that want to post the political and issue ads with an ID.
- The verification will take place on the national level, as there are different national laws when it comes to political ads. This means that pan-EU political campaign on FB will not be possible. Verification will have to take place on national level.

On the issue ads, NK explained that despite difficulties in establishing a coherent definition, they decided to do it because this has been the most common channel of advertising in the US elections. FB is working with a group of academics to try to define what will be an issue ad in electoral context.

In the Q&A about the new features, it transpired that FB is still working on closing loopholes that were discovered during the US midterm elections, but the main idea behind all these tools is increased transparency.

NK then spoke about removing content and fake accounts. FB is increasingly relying on AI to shut down fake accounts, even before they appear on the platform. The same goes for terrorist content.

On hate speech, FB hired 30,000 people to review the content. NK expects that AI will also be helpful in this task, as early studies show that AI might be more efficient and consistent than humans. It is FB view that the regulators and politicians should assume their responsibility as private companies should not be the judges of what is allowed online.

Commissioner Jourová thanked FB for their commitment to the CoC and stressed that FB, like any other company, has to respect the law, also when it comes to illegal speech. She reiterated that for her the freedom of speech is extremely important, so nothing that platforms do should limit it. She appreciated new human resources employed by FB.

FB also reiterated its commitment to the Code of Practice on disinformation. NK explained they are trying to promote news content which is not sensationalist and click-bait by giving it less relevance in the news feed. He stressed they don't intend to remove anything from the platform and that news in any case is only 4% of all the posts.

NK also explained the business model of FB insisting it is not about selling data to third parties, but using the data to show relevant advertising to users. He said a lot of other websites, including the sites of the newspapers track the behaviour of its users.

Commissioner Jourová stressed that GDPR must be respected and FB should be clear and transparent vis-à-vis its users on how it collects the data and how it uses it.

From: [REDACTED]
 Sent: Tuesday, January 29, 2019 9:50 AM
 To: CRABIT Emmanuel (JUST) ; [REDACTED] (JUST) ; BRAUN Daniel (CAB-JOUROVA) ; [REDACTED]
 Cc: JUST C2 ; JUST C DIR ; [REDACTED]
 Subject: FLASH REPORT: Meeting of 28.01.2019 with IT Companies in the Code of conduct

Dear all,

A short summary of the meeting had yesterday at CAB with IT Companies on the implementation of the Code of conduct on countering illegal hate speech online.

Happy to address any comment or question,

Best,

[REDACTED]

FLASH REPORT

Meeting CAB Jourová with IT Companies in the Code of conduct – 28 January 2019

Attended by: Renate Nikolay, Daniel Braun and Monika Ladmanova – Cabinet Jourová;

[REDACTED] – JUST C2
 [REDACTED] (Facebook/Instagram), [REDACTED]
 [REDACTED] (Google/YouTube), [REDACTED]
 [REDACTED]

Aim:

- to discuss the upcoming launch of the results of the 4th monitoring exercise and share views on next steps on countering hate speech online.
- To have an exchange of views on how IT companies could address violence against women and misogyny online.

Key messages by CAB:

- The Code is delivering sustainable results on notice-and-action and the results to be announced on 4th February will be in line with previous monitoring, showing also some further progress. Twitter seem to have lower take down rates. Encouraging to see consistency in the assessment: the more intense hate content is, the higher the take down. This is an indicator of due attention to free speech.
- There is a need to progress on transparency reports (e.g. breakdown on EU/country data or on number of hate speech flags) and feedback to users.
- Good that new companies have showed interest and have come on board, need to make an effort about getting even more players, so the Code can cover 100% of the market.
- Commissioner will announce the upcoming campaign to promote tolerant speech during the elections which is resulting from the joint work between IT platforms and the network of trusted flaggers.
- CAB asked for a round of views on a) what IT platforms do to address gender base violence and how can this strand of work be efficiently looped into the work of the

Code and b) what are the views on next years' policy developments regarding illegal content online.

A *tour de table* followed, in a general positive spirit. All companies highlighted the important dynamics (also internally within their teams) achieved thanks to the dialogue set by the Code, the good results and the need to continue delivering. There was a general engagement on the envisaged campaign, highlighting this is the result of the growing cooperation with civil society organisations / trusted flaggers. IT companies mentioned several initiatives (e.g. trainings or awareness raising actions) they have in place to address gender based violence and harassment online. In general terms, substantial agreement to COM approach until now on separating the discussions and measures depending on the types of content, given the specificities of each

Key additional points raised by individual companies:

- [REDACTED] announced that they will send data on number of hate speech flags received as requested by CAB, with the caveat that the trends showed by such figures are not necessarily an indication of increased amount of hateful content (it is also due to an enlarged network of trusted flaggers). [REDACTED] flagged the importance of measures such as limiting the features of the videos which complement removals and de facto obtain similar results.
- [REDACTED] informed that the team of reviewers has now reached 15 000 people worldwide and that FB intends to continue the improvements on the transparency reports.

[REDACTED]

CAB concluded by thanking all for the good work, summarising the spin of the upcoming press conference and signalling openness to have joint communication / messages. The call for data on training of IT companies staff on hate speech content was reiterated. The results of the monitoring will also be presented in the context of the next meeting of the Justice ministers in March.

[REDACTED]



European Commission
DG Justice and Consumers
Fundamental Rights Policy

[REDACTED]

 facebook

Yours sincerely,



European Commission
Directorate-General for Justice and Consumers



[REDACTED]
[REDACTED], DG for Justice and Consumers

[REDACTED]
[REDACTED], DGCCRF

BY EMAIL

18 October 2018

Updates to Facebook Terms of Service

Dear [REDACTED]

Thank you for taking the time to meet with us on 18 September (the "**Meeting**") to discuss proposed updates to Facebook's Terms of Service ("**Terms**").

As agreed between us at the Meeting, we are pleased to provide for your consideration in **Annex 1** to this letter our proposed amendments to the Terms addressing the issues raised by your Network. A summary of the proposed amendments is provided at **Annex 2**.

We trust that these proposals will adequately address your Network's concerns, and we remain available to discuss them further. Similarly should have any questions in relation to the above, please do not hesitate to contact us.

We look forward to hearing from you.

Yours sincerely

[REDACTED]
[REDACTED]
[REDACTED]
Facebook Ireland Limited

facebook

[REDACTED]
[REDACTED]

ANNEX 2

Summary of proposed amendments to Terms

Sections 1 & new Section 2 – Describing Facebook’s business model

We propose to add a new section that clearly explains to consumers how Facebook generates revenue from advertising, which enables Facebook to provide the service to users without charge. This section also makes clear to users that Facebook does not sell their data, but that their data is used to personalise the ads they see.

The reference and hyperlink to the Data Policy, and the explanation that we use personal data to provide the Facebook service, is also moved to a prominent position at the top of the terms to increase transparency.

Please note that, in particular as we are concerned to ensure this section clear and easy for consumers to understand whilst also describing the key elements of our business model, our teams are continuing to iterate on this precise wording. To the extent we consider further amendments are needed to this language we will provide that as quickly as possible, but did not want that to hold up provision of the attached in the interests of moving forward in a timely manner.

Section 1 – Research activities

We have included more information about the specific research efforts conducted by Facebook for the purposes of developing and improving our products and services. This reflects information already provided in the Data Policy about how users’ personal data is processed for this purpose. As such, we also propose to add another hyperlink to the Data Policy explaining this, for ease of reference.

Section 3.2.1 – Content removals; Section 4.2 – Account suspensions and removals

We have simplified the language explaining when we can remove content. Furthermore, we have added clearer, more specific language explaining that we will notify consumers and provide a right of appeal when content is removed for violation of our Community Standards, subject to clear, proportionate and specific exceptions.

This approach has also been reflected in section 4.2 relating to account suspensions and terminations.

Section 3.1 – Intellectual property licence

[REDACTED]

facebook

[REDACTED]

Section 3.3.3 – Software updates


We have simplified the language to make clear to users that this clause relates merely to technical updates to relevant software.

Section 4.2 – Surviving clauses

We have amended this section to limit the number of clauses that continue to have effect after termination of the contract, namely the IP licence and clauses relating to disputes. This change is made in conjunction with the amendment to section 3.1 above which clarifies the circumstances in which the IP licence can be terminated, and/or may continue in limited cases where relevant content persists on our servers.

Clause 4.3 – Limitation of liability

We have removed the last sentence of this section to avoid the double-negative statement, as discussed at the Meeting. In light of the amendments described above including in particular the clarification as to the scope of section 3.1, we consider that this clause is otherwise clear and fair to consumers in the context of the remainder of the contract.

From: 
Sent: mardi 12 février 2019 08:47
To: CAB JOUROVA ARCHIVES
Cc: TALKO Wojtek (CAB-JOUROVA)
Subject: FW: notes from FB meeting

Follow Up Flag: Follow up
Flag Status: Completed

For registration. Thanks.

Flash note, meeting with Facebook 10 Oct 2018

Participants:
 Commission: T. Zerdick (CAB FVP), W. Talko (CAB Jourova)

Facebook:

- Markus Reinisch, VP Public Policy, EMEA
- Thomas Myrup Kristensen, Managing Director EU Affairs and Northern Europe, Head of Office Brussels

On the request of Facebook we met to understand better the latest steps FB has taken to contribute to election integrity and fight with disinformation online.

FB stressed that they are working to address this issue globally (US-midterms, elections in Europe, Brazil, India, etc.). They explained the following:

- Increasing transparency in political advertising on the platform. Such measures could include a depository of every ad issued on the platform, transparency on who paid for it. Also, as an example FB used the Irish referendum, where FB allowed only organisations in Ireland to purchase the ads related to the referendum on abortion, because they noticed some increased activity on the issue from outside Ireland.
- Fight against fake accounts. FB has a real-name policy and there is a link between fake accounts and disinformation. FB, thanks to AI, closed half a billion of fake accounts in first quarter of 2018.
- Misinformation – FB described different approaches they are testing (flagging content as 'suspicious' or 'disputed' didn't bring good results, for instance). FB also observed that most of the fake news on the platform is generated for commercial purposes, not political ones. FB also works with NGOs and independent fact-checkers. More news on this issue to come later on.
- FB stressed they would want to continue their work on civil engagement, like promoting high quality content or helping people to find the polling station or raise awareness about the voting date. In this context, there was a mention of 'I vote' button active during the election period.

There was not much time for Q&A, but we asked about FB commitments to EU initiatives (FB fully committed; stressing the need to regulatory clarity on what is allowed and what is not, especially that in Europe there is fragmented regulatory landscape).

From: [REDACTED]
Sent: mardi 12 février 2019 08:46
To: CAB JOUROVA ARCHIVES
Cc: TALKO Wojtek (CAB-JOUROVA)
Subject: FW: meeting with Facebook 27 September 2018

Follow Up Flag: Follow up
Flag Status: Flagged

For registration. Thanks.

From: TALKO Wojtek (CAB-JOUROVA) dec.europa.eu
Sent: Monday, February 11, 2019 4:48 PM
To: [REDACTED]
Subject: meeting with Facebook 27 September 2018

This is the flash note from the meeting of 27 Sept

Flash note meeting with Facebook 27 Sept 2018

Participants: W. Talko (CAB Jourova) Thomas Myrup (FB), (FB via video link)

On the request of FB we met to follow up the meeting with Commissioner Jourová which took place the week before on the CPC action. FB aim was to explain better the points the Commissioner made in her public statements and on Twitter. FB main message was that they are fully committed to working on the issues in Terms and Conditions identified by the CPC and the Commission, but it is important to have a full clarity what is expected and what are the concerns. In substance, the same points were raised as in meetings the previous week. I thanked FB for their outreach and said that we were hoping to see the same level of engagement on the technical level when dealing with CPC and the Commission experts.

ANNEX I

Email addresses dedicated to the "Notice and action" procedure

CPC Authority	Email address
Austrian Federal Ministry of Labour, Social Affairs and Consumer Protection	[REDACTED]
Belgian Federal Public Service Economy - DG for Economic Inspection	[REDACTED]
Cypriot Consumer Protection Service - Ministry of Energy, Commerce, Industry and Tourism	[REDACTED]
Ministry of Industry and Trade of the Czech Republic	[REDACTED]
Danish Consumer Ombudsman	[REDACTED]
Consumer Protection Board of Estonia	[REDACTED]
Finnish Competition and Consumer Authority	[REDACTED]
Directorate for Competition Policy, Consumer Affairs and Fraud Control of France	[REDACTED]
German Federal Ministry of Justice and Consumer Protection	[REDACTED]
Hungarian Competition Authority	[REDACTED]
Icelandic Consumer Agency	[REDACTED]
Irish Competition and Consumer Protection Commission	[REDACTED]
Italian Competition Authority (AGCM) - Directorate B Consumer Protection	[REDACTED]
Consumer Rights Protection Centre of Latvia	[REDACTED]
State Consumer Rights Protection Authority of Lithuania	[REDACTED]
Ministry of Economy of Luxembourg - Directorate for internal market and consumers	[REDACTED]
Malta Competition and Consumer Affairs Authority	[REDACTED]

Netherlands Authority for Consumers and Markets	[REDACTED]
Norwegian Consumer Authority	[REDACTED]
Polish Office of Competition and Consumer Protection	[REDACTED]
National Authority for Consumer Protection of Romania	[REDACTED]
Slovak Trade Inspection	[REDACTED]
Market Inspectorate of Republic of Slovenia	[REDACTED]
Spanish Agency for Consumer Affairs Food Safety and Nutrition (AECOSAN)	[REDACTED]
Swedish Consumer Agency	[REDACTED]
UK Competition and Markets Authority (UK CMA)	[REDACTED]

ANNEX II

New Facebook Terms – Outstanding Issues

- 1, page 1

[REDACTED]

- 3rd paragraph, page 2

"Research way to make our services better: We engage in research and collaborate with others to improve our Products. One way we do this is by analysing the data we have and understanding how people use our Products. You can learn more about some of our research efforts."

[REDACTED]

- 3.2, page 3

"We can remove content you share in violation of these provisions and, if applicable, we may take action against your account, for the reasons described below. We may also disable your account if you repeatedly infringe other people's intellectual property rights.

Where appropriate, we will take steps to notify you when we remove your content for violating our Community Standards. We may not be able to provide notice in all cases, for example if we are prohibited from doing so by law or where it might harm our community or the integrity of our Products."

[REDACTED]

- 3.3, page 4

[REDACTED]

- 3.3.1, 2nd paragraph, page 4

"Specifically, when you share, post, or upload content that is covered by intellectual property rights (like photos or videos) on or in connection with our Products, you grant us a non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings)."

The German version includes the sentence: *"This license is only for the purpose of making our Products available to you"* [REDACTED]

- 4.1 page 5

"We work constantly to improve our services and develop new features to make our Products better for you and our community. As a result, we may need to update these Terms from time to time to accurately reflect our services and practices."

The German version includes the sentence: *"We will only make changes if the provisions are not appropriate anymore or if they are incomplete, and only if the changes are reasonable for you in consideration to your interests"* [REDACTED]

- 4.2 page 5

"If we determine that you have clearly, seriously, or repeatedly violated our terms or policies, including in particular our Community Standards, we may suspend or permanently disable access to your account. We may also suspend or disable your account if we required to do so by law. Where appropriate, we will notify you about your account the next time you try to access it. You can learn more about what you can do if your account has been disabled and how to contact us if you think we have disabled your account by mistake."

[REDACTED]

- 4.2 page 5

"If you delete or we disable your account, these Terms shall terminate as an agreement between you and us, but the following provisions remain in place: 3, 4.2-4.5."

[REDACTED]

- 4.3 page 5

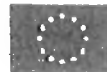
"Provided we have acted with reasonable skill and care, we do not accept responsibility for: losses not caused by our breach of these Terms or otherwise by our acts".

[REDACTED]

- 4.3 page 6

"It also does not exclude or limit our liability for any other things where the law does not permit us to do so".

[REDACTED]



Brussels.

FACEBOOK IRELAND LTD

On the other hand, in the view of CPC authorities, the new terms raise additional concerns, especially taking into account that the recent Cambridge Analytica events have demonstrated the need for social media operators and platforms in general, to provide more transparency on their business model and be more inclusive on their liability, especially in relation to third party activities. This would enable consumers to better understand what they can expect from the usage of your services.

[REDACTED]

[REDACTED]

A more detailed list of concerns in relation to the new proposed set of terms is included in Annex II to this letter.

[REDACTED]

We ask Facebook to review and address as soon as possible the concerns described above and listed in Annex II. In view of implementing rapidly the necessary adaptations to Facebook terms, we confirm our availability to meet you, possibly still in the month of July to discuss a rapid solution to this matter.

CPC Authorities may decide to take enforcement measures as appropriate to address outstanding issues of non-compliance with consumer protection requirements, although we hope that this will not become necessary.

Please note that the assessment above is made on the basis of the consumer protection legislation and is without prejudice to any assessment of the compliance with the applicable EU legislation on data protection.

Sincerely,

[REDACTED]

[REDACTED]

DG Justice and Consumers

[REDACTED]

DG CCRF

From: [REDACTED]@fb.com>
Sent: lundi 23 juillet 2018 12:23
To: JUST [REDACTED]
Cc: [REDACTED] (JUST); [REDACTED] (JUST); [REDACTED] (JUST); [REDACTED]@dgcrf.finances.gouv.fr
Subject: Re: Follow-up on CPC Social Media Action
Attachments: CPC letter 23 July 2018 .pdf

Dear Sirs

Please see attached letter from Facebook Ireland Limited.

Kind regards
[REDACTED]

[REDACTED] | facebook

From: "JUST [REDACTED]@ec.europa.eu"
Date: Friday, 6 July 2018 at 15:32
To: [REDACTED]@fb.com>
Cc: [REDACTED]

Subject: Follow-up on CPC Social Media Action

Dear [REDACTED],

Please find here enclosed an electronic copy of the letter addressed to Facebook.

For any further inquiries please send your correspondence to the functional mailbox of [REDACTED]

[REDACTED] Directorate General for Justice & Consumers [REDACTED]

[REDACTED], copying the officials in charge [REDACTED]

[REDACTED]@ec.europa.eu), or [REDACTED]
[REDACTED]@ec.europa.eu).



European Commission

Directorate-General for Justice and Consumers

██████████, DG for Justice and Consumers

[REDACTED], DGCCRF

BY EMAIL

23 July 2018

Recent updates to Facebook Terms of Service

Dear [REDACTED]

Thank you for your letter of 6 July 2018.

Thank you for your comments on our recently updated Terms of Service ("**Terms**"). As we informed you in our letter of 4 April, we introduced these Terms as part of a larger coordinated update to other terms and policies, most notably our Data Policy, to coincide with the coming into force of the GDPR. As we previously advised, the updated Terms reflect the substance of the changes we had already made to the previous SRR as a result of our cooperation with your Network.

We are therefore disappointed to learn of your Network's concerns regarding the new Terms notwithstanding our previous engagement, and would be grateful for the opportunity to meet with you to discuss these issues in more detail. In the meantime I hope to offer some clarification on some of the main points raised in your covering letter.

[illegible]

facebook

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

facebook



I hope that the above provides some clarification on the key points that you have raised. We would be very grateful for the opportunity to meet with you to discuss these issues and the other points raised in your letter in more detail. Unfortunately due to absences of key personnel over the Summer recess we regret that we will be unable to meet with you in July; however we would be happy to arrange a meeting at your convenience in early September. If this is acceptable to you, we should be grateful if you could confirm by return and we can then make necessary arrangements.

Yours sincerely

[Redacted signature]

[Redacted name]

[Redacted title]

Facebook Ireland Limited

facebook





EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE and CONSUMERS

[REDACTED]

Brussels,
[REDACTED]

[REDACTED]
FACEBOOK IRELAND LTD
[REDACTED]

Dear [REDACTED],

I am writing to you regarding your letter of 23 July 2018 in my capacity as [REDACTED] [REDACTED] for facilitation of the CPC Network operations under Regulation 2006/2004 EC on Consumer Protection Cooperation.

CPC authorities welcome Facebook's commitment to proceed with the full functioning of a "notice and action procedure" dedicated to them and the pledge to fully collaborate with them. Nevertheless, your observations and statements would need to be confirmed by concrete proposals of terms of service to ascertain their compliance with the CPC common position of 9 November 2016 and in particular with reference to the outstanding issues raised by the CPC Authorities in their letter of 6 July 2018.

In this connection, we would like to invite you to a meeting with high level national representatives of the CPC network in Brussels on 18 September 2018 at our headquarter building, the Berlaymont. Once you have confirmed the availability of experts from your company, we will provide the exact location and timing. This meeting will be an opportunity to discuss in detail your submission with CPC Authorities and eventual questions that you may raise in advance.

Please let us know, as soon as possible, if this date is feasible, in order for national competent authorities to prepare their travel arrangement.

Yours sincerely,
[REDACTED]

[REDACTED]



EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE and CONSUMERS

[REDACTED]

Brussels,
[REDACTED]

[REDACTED]

FACEBOOK IRELAND LTD
[REDACTED]

Dear [REDACTED],

Following my letter of 22 August 2018, I now confirm our invitation to a meeting with CPC Authorities on Tuesday 18 September 2018 at 15:30. Please note that our Commissioner for Justice Consumers and Gender Equality Věra Jourová will open the meeting.

I kindly ask you to indicate the name, function and contact details of the person(s) who will attend from your company. Due to security measures in Commission buildings please provide the date of birth, nationality, ID card number and expiry date of the ID card of the person(s).

[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED], DG for Justice and Consumers

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED], DGCCRF

BY EMAIL

14 September 2018

Recent updates to Facebook Terms of Service

Dear [REDACTED]

Thank you for your recent letters regarding the updates to Facebook's Terms of Service.

Facebook is committed to upholding the consumer protection rights of its EU users and to making further changes to its Terms of Service to address the CPC's remaining concerns, as necessary.

We welcome the opportunity to meet with you on 18 September to discuss these concerns and potential revisions in more detail.

With this in mind and in the spirit of cooperation, we set out in the Annex to this letter some preliminary responses to each of the specific issues set out in your letter. We hope that this can serve as a useful initial basis for discussion in the meeting.

We wish to thank you again for the constructive cooperation with your Network to date and look forward to meeting with you on 18 September.

Yours sincerely

[REDACTED]
[REDACTED]
[REDACTED]
Facebook Ireland Limited

CONFIDENTIAL

Facebook Terms of Service – Proposed amendments

Section 1: Our Services

As explained in our letter of 23 July, the description of the Facebook service under Section 1 of the Terms is one of the most significant updates from previous versions (formerly known as the 'SRR'). The purpose of this section is to make clear to consumers each of the core aspects of the Facebook service that forms the main subject matter of the contract. This section sets out in clear and easily intelligible language the core aspects of the Facebook service including, *inter alia*, the fact that Facebook uses data to show users ads, and that it engages in research activities to improve its products.

We note from your letter of 6 July that the CPC considers these aspects should be clarified further. As the CPC will note, Article 4(2) Directive 93/13/EEC provides that an assessment of the unfair nature of a contractual term shall not extend to the definition of the main subject matter of the contract. Nevertheless, we are always open to constructive feedback on how we can improve the clarity of our Terms in the interests of users.

Accordingly, we suggest the following proposed amendments and would welcome the opportunity to discuss these with you:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Finally, we should note that Facebook's Data Policy provides extensive information to users about how Facebook processes their personal data and the choices they have. Section 2 of the Terms prominently directs users to the Data Policy and provides a hyperlink if consumers wish to understand more about Facebook's use of data specifically.

Sections 3.2 & 4.2 – Removal of content and account terminations

We acknowledge the issues raised by your Network with regard to notifying users when we remove user-generated content and/or terminate accounts, and providing a means of appeal in each case.

As we have previously explained, Facebook does notify users and provide a means of appeal in many cases, and we are continually working to expand this functionality to improve the user experience. However, there is a wide variety of cases where doing so is neither appropriate nor technically feasible (for example, in cases of

facebook

[REDACTED]

[REDACTED]

CONFIDENTIAL

repeat violations, serious violations or illegal activity). It is therefore not possible to provide an absolute contractual right to notification and appeal in every instance, nor is it easy to describe the limitations of this right in language that is both comprehensive and easy for consumers to understand. It is essential that Facebook maintains the necessary flexibility in this respect to ensure it can continue to keep users safe and protect consumers from bad actors on the platform.

The recent changes to these sections were drafted with the objective of making this clear to users without giving the misleading impression that users are entitled to an absolute right in all cases, per our previous discussions with your Network. We would welcome the opportunity to work further with your Network to agree upon what further modifications to this clause may be possible in order to address these concerns and we hope to discuss this with you in the meeting on 18 September.

Section 3.3 – User permissions

The primary purpose of section 3.3, specifically 3.3.1 and 3.3.2, is to obtain appropriate intellectual property licences necessary to provide the Facebook service to the contracting user and all other Facebook users. We should be grateful if you could provide further details on what specific clarifications your Network considers necessary and would be keen to discuss this with you in our meeting on 18 September.

Sections 3.3.1 and 4.1 – Additional language in German versions

As you will appreciate, whilst we strive to achieve a consistent position across all 28 Member States, in some instances it is necessary to make changes that are responsive to legal or regulatory requirements that are specific to one jurisdiction. The additional language used in the German version of sections 3.3.1 and 4.1 of the Terms was introduced as part of separate legal arrangements that are limited to Germany.

[REDACTED]

Section 4.2 – Clauses remaining in effect after termination

The Terms make clear that users are free to delete their Facebook account and terminate the contract at any time, for no cost. As is typical for contracts of this nature, it is necessary for certain clauses to survive termination in the event of a later dispute.

It is also necessary for Facebook to retain a licence over certain content for technical reasons in order to be able to continue to provide the service. For this reason, the Terms note that *“any content that you delete may persist for a limited period of time in backup copies (though it will not be visible to other users). In addition, content that you delete may continue to appear if you have shared it with others and they have not deleted it.”*

We acknowledge the concerns raised in your letter to 6 July and would be keen to discuss with you how Facebook can make this language clearer and/or more prominent to users.

Section 4.3 – Limitation of liability

Section 4.3 is intended to make clear to consumers that Facebook does not accept responsibility for losses caused by the actions of a third party, where Facebook itself is not at fault and has acted with reasonable skill

facebook

[REDACTED]

CONFIDENTIAL

and care. The clause expressly does not purport to exclude liability for Facebook's own acts or breaches of the Terms. We consider that this clause is clear and consistent with the requirements of EU law.

Section 4.3 also makes clear that, in addition to liability for death, personal injury or fraudulent misrepresentation, Facebook also does not attempt to exclude liability for anything else where doing so may be prohibited by applicable Member State law. This clause is for the benefit of consumers.

We should be grateful if you could provide further details on what specific clarifications your Network considers necessary and would be keen to discuss this with you in our meeting on 18 September.

facebook





COMMISSIONER VĚRA JOUROVÁ

MEETING WITH FACEBOOK

(Participants from Facebook: [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED])

LOCATION: [REDACTED]

DATE AND TIME: 18/09/2018, 14:45H

MEETING OBJECTIVE: TO DISCUSS THE CPC SOCIAL MEDIA ACTION

DG CONTACT & TEL NO: [REDACTED]
[REDACTED]

ACTING DIRECTOR: [REDACTED]

VERSION: 14/12/2018 15:16

STEERING

The meeting will be a good opportunity to insist with Facebook that they must comply with the demands of CPC authorities and to emphasise that we expect a rapid solution to this case.

Topic 1: CPC Joint Action on Social Media

Context

Following the common position of the CPC Authorities that was sent to Facebook on 9 November 2016 and a long dialogue process, Facebook agreed to modify certain of its terms of service (in order to comply with the CPC requirements) and to establish a "notice and action" procedure dedicated to the CPC Authorities for reporting illegal content. The results were presented by the Commission through a press release on 15 February 2018.

The revelation of the Cambridge/Analytica Scandal and the adoption of new terms of service by Facebook on 19 April 2018, led to a new assessment by the CPC Authorities on the compliance of Facebook's terms with EU consumer law. As a result, a letter was sent to Facebook on 6 July 2018 with a list of the outstanding issues concerning its terms of service. CPC Authorities requested from Facebook to be more transparent on the characteristics of its services and to be more inclusive on its liability, especially in relation to third parties activities, and explained in detail the shortcomings of its new terms (see background for a summary of the issues). Facebook sent two replies on 23 July 2018 and on 14 September 2018



[REDACTED]

The EU Consumer Protection Cooperation (CPC) Regulation links national consumer authorities in a pan-European enforcement network. The cooperation is applicable to consumer rules covering various areas, such as the Unfair Commercial Practices Directive, the E-commerce Directive, the Consumer Rights Directive or the Unfair Contract Terms Directive.

LTT

- Emphasise that it is time that Facebook fully cooperates with the CPC Network and that it brings their terms and practices in full compliance with EU consumer legislation.

- [REDACTED]

- 
-
- 
- Especially after Cambridge Analytica events, consumers deserve clarity on how their data is used and Facebook should also stop declining responsibility for the actions of third parties with whom it shares consumers' data.
 - A positive note is that a "notice and action" procedure has already been agreed, which will allow CPC Authorities to notify wrongdoings detected on the platform and ask Facebook to remove illegal content. We count on Facebook to expeditiously review all notifications received by CPC authorities and to take action as appropriate.
 - Conclude by encouraging Facebook to use today's meeting with CPC authorities as an opportunity to receive further advice from the authorities on how to comply with EU legislation.
 - Then emphasise that you expect the company to show responsibility to EU consumers by proceeding as quickly as possible with the necessary modifications. Achieving compliance rapidly will allow the company to avoid enforcement measures.

Defensives

Why has the CPC Joint action reopened?

- The action was never closed, since Facebook kept certain terms that were identified by CPC Authorities as infringing EU

Consumer Law.

- Moreover the Cambridge/Analytica scandal revealed the need for more transparency on Facebook's business model; equally, the need for better protection of consumers rights against third parties who engage in actions through Facebook's platform.
- In addition, Facebook introduced new terms of service on 19 April 2018, which were examined by CPC Authorities anew and were found to be partly incompliant with the CPC Network's requirement.

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- Especially after Cambridge Analytica events, there needs to be clarity on these issues and the company should also stop declining responsibility for the actions of third parties with whom it shares consumers' data.

Why should Facebook comply with CPC Network's requirements?

- CPC authorities offer a dialogue at the EU level in view of a common solution that will be valid across the EU, instead of potentially 28 national formal enforcement actions, such as the one initiated by the Italian authority AGCM on 28 October 2016 against the terms of Whatsapp (a company that belongs to Facebook) or the one initiated by French authorities.
- Therefore, it is in the interest of Facebook to establish effective cooperation with the CPC Network. This can reduce compliance costs and generate more legal certainty.
- More in particular, by complying, Facebook will avoid imminent enforcement measures by national authorities. [REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

What is the objective of this dialogue?

- The objective of this dialogue, is to ensure that Facebook's Terms of Service are fair for EU Consumers and that consumers are not misled on the key characteristics of Facebook's services.

BACKGROUND

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Annexes

1. Outstanding issues with Facebook

Contact:

[REDACTED]

ANNEX I: OUTSTANDING ISSUES WITH FACEBOOK

[illegible]

<p>Policy</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>
---------------	-------------------	-------------------

		<div>[REDACTED]</div>
Presentation of Data Policy <div>[REDACTED]</div>	<div>[REDACTED]</div>	<div>[REDACTED]</div>

		<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
<p>Presentation of Research Policy 3rd paragraph, page 2</p> <p>"Research way to make our services better: We engage in research and collaborate with others to improve our Products. One way we do this is by analysing the data we have and understanding how people use our Products. You can learn more about some of our research efforts."</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
<p>Permissions granted by the users 3.3, page 4</p> <p>[REDACTED]</p>	<p>No reply in Facebook's letter of 23 July</p>	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>

<p>[REDACTED] [REDACTED]</p> <p>3.3.1, 2nd paragraph, page 4</p> <p>"Specifically, when you share, post, or upload content that is covered by intellectual property rights (like photos or videos) on or in connection with our Products, you grant us a non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings)."</p> <p>The German version includes the sentence: "This license is only for the purpose of making our Products available to you" [REDACTED] [REDACTED]</p>		<p>[REDACTED] [REDACTED] [REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]</p>
<p>Removal of user generated content</p> <p>3.2, page 3</p> <p><i>"We can remove content you share in violation of these provisions and, if applicable, we may take action against your account, for the reasons described below. We may also disable your account if you repeatedly infringe other people's intellectual property rights.</i></p> <p><i>Where appropriate, we will take steps to notify you when we remove your content for violating our Community Standards. We may not be able to provide notice in all cases, for example if we are prohibited from doing so by law or where it might harm our community or the integrity of our Products."</i></p>	<p>No reply in Facebook's letter of 23 July.</p> <p>Facebook generally argues that, for security reasons, it is not obliged to notify the users for the removal of content.</p>	<p>[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]</p>

		<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
<p>Power to suspend or terminate an account 4.2 page 5</p> <p>"If we determine that you have clearly, seriously, or repeatedly violated our terms or policies, including in particular our Community Standards, we may suspend or permanently disable access to your account. We may also suspend or disable your account if we required to do so by law. Where appropriate, we will notify you about your account the next time you try to access it. You can learn more about what you can do if your account has been disabled and how to contact us if you think we have disabled your account by mistake."</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	No reply in Facebook's letter of 23 July.	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
<p>Survival of terms 4.2 page 5</p> <p>"If you delete or we disable your account, these</p>	No reply in Facebook's letter of 23 July.	<p>[REDACTED]</p> <p>[REDACTED]</p>

<p><i>Terms shall terminate as an agreement between you and us, but the following provisions remain in place: 3, 4.2-4.5."</i></p> <p>[REDACTED]</p>		<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
<p>Limitations of liability 4.3 page 5 "Provided we have acted with reasonable skill and care, we do not accept responsibility for: losses not caused by our breach of these Terms or otherwise by our acts".</p> <p>[REDACTED]</p>	<p>No reply in Facebook's letter of 23 July.</p>	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>

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)

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]
[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** have 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.

From: @fb.com>
Sent: mardi 8 mai 2018 13:44
To: (JUST); (JUST)
Cc:
Subject: (JUST),
 Re: MCC case- Irish High Court appeal

Hi ,

Of course, not a problem. Let us come back to you with some proposed times on the 15th and 16th May.

Best,

From: " " @ec.europa.eu" < @ec.europa.eu>
Date: Monday, May 7, 2018 at 11:39 AM
To: < @fb.com>, " " @ec.europa.eu"
 < @ec.europa.eu>
Cc: < @fb.com>, < @fb.com>, < @fb.com>, < @fb.com>, " " @ec.europa.eu" < @ec.europa.eu>, < @fb.com>
Subject: RE: MCC case- Irish High Court appeal

Dear ,

This week will be difficult because of the holidays and too much work – could we perhaps have a call on 15 or 16 May?

Best wishes,

From: [mailto: @fb.com]
Sent: Thursday, May 03, 2018 6:00 PM
To: (JUST); (JUST)
Cc:
 (JUST);
Subject: Re: MCC case- Irish High Court appeal

Dear ,

Apologies for my delayed reply. We wanted to suggest setting up a call next week when we'll have more information to share. We can send over some proposed days and times if that works for you?

Thank you,

From: " " @ec.europa.eu" < @ec.europa.eu>
Date: Thursday, May 3, 2018 at 10:43 AM
To: < @fb.com>, " " @ec.europa.eu"
 < @ec.europa.eu>
Cc: < @fb.com>,

< @fb.com>, < @fb.com>,
< @fb.com>, " @ec.europa.eu" < @ec.europa.eu>,
< @fb.com>

Subject: Re: MCC case- Irish High Court appeal

Dear ,

May I ask what happens then? What effect would a pending case before the Supreme Court have for the reference for a preliminary ruling to the CJEU? Would the former only become relevant if the Supreme Court would annul the decision from the High Court (ahead of the ruling by the CJEU)?

Best regards,

Sent from Email+ secured by MobileIron

From: " " < @fb.com>
Date: Thursday, 3 May 2018 at 09:50:13
To: " (JUST)" < @ec.europa.eu>
Cc: " " < @fb.com>, " " < @fb.com>, " " < @fb.com>,
" " < @fb.com>, " " < @fb.com>, " (JUST)"
< @ec.europa.eu>, " (JUST)" < @ec.europa.eu>, " "
" < @fb.com>
Subject: Re: MCC case- Irish High Court appeal

Hi ,

My understanding is that it has not been sent yet, but will be sent imminently- likely today.

Best,

> On May 2, 2018, at 10:55 PM, "f @ec.europa.eu" < @ec.europa.eu> wrote:

>
> Thank you for the update, .

> But does it mean that the reference has been made, has been actually sent by the High Court to Luxembourg?

>
> Best,

> _____
> From: [@fb.com]

> Sent: 02 May 2018 23:52

> To: (JUST)

> Cc: (JUST);

> (JUST);

> Subject: Re: MCC case- Irish High Court appeal

>

> Hi ,

>

> A brief update on our side: while the judge didn't grant a stay in the MCC case today, we intend to appeal the case in front of the Irish Supreme Court next week.

>

> Please let us know if you have any questions.

>

> Best,

>

> On Apr 30, 2018, at 6:59 PM, "[@ec.europa.eu](mailto: @ec.europa.eu)<<mailto: @ec.europa.eu>>"
 < [@ec.europa.eu](mailto: @ec.europa.eu)<<mailto: @ec.europa.eu>>> wrote:
 >
 > Thank you.
 >
 > Have a nice evening,
 >
 >
 >
 > From: " " (<mailto: @fb.com>)
 > Sent: Monday, April 30, 2018 7:22 PM
 > To: (JUST)
 > Cc: ; ; (JUST);
 > Subject: Re: MCC case- Irish High Court appeal
 >
 > Hi ,
 >
 > We wanted to provide another quick update—the judge did not make a decision today in court as to whether to stay the case, saying she'll take it away to consider further. We may hear from her by the end of the week; she's not planning to give a written decision on this matter.
 >
 > In court she heard from us that we're appealing, in part, on the grounds that (1) the case is moot post-GDPR (May 25th) and there are questions as to the judgement's interpretation of US law.
 >
 > We'll provide more updates as they come.
 >
 > Best,
 >
 >
 > From: " " ([@ec.europa.eu](mailto: @ec.europa.eu)<<mailto: @ec.europa.eu>>"
 < [@ec.europa.eu](mailto: @ec.europa.eu)<<mailto: @ec.europa.eu>>>
 > Date: Monday, April 30, 2018 at 2:50 PM
 > To: < [@fb.com](mailto: @fb.com)<<mailto: @fb.com>>>
 > Cc: < [@fb.com](mailto: @fb.com)<<mailto: @fb.com>>>, [@fb.com](mailto: @fb.com)<<mailto: @fb.com>>>, [@fb.com](mailto: @fb.com)<<mailto: @fb.com>>>, [@fb.com](mailto: @fb.com)<<mailto: @fb.com>>>, [@fb.com](mailto: @fb.com)<<mailto: @fb.com>>>
 < [@fb.com](mailto: @fb.com)<<mailto: @fb.com>>>, " " ([@ec.europa.eu](mailto: @ec.europa.eu)<<mailto: @ec.europa.eu>>"
 < [@ec.europa.eu](mailto: @ec.europa.eu)<<mailto: @ec.europa.eu>>>, [@ec.europa.eu](mailto: @ec.europa.eu)<<mailto: @ec.europa.eu>>>
 ' [@ec.europa.eu](mailto: @ec.europa.eu)<<mailto: @ec.europa.eu>>"
 ' [@ec.europa.eu](mailto: @ec.europa.eu)<<mailto: @ec.europa.eu>>>
 > Subject: RE: MCC case- Irish High Court appeal
 >
 > Thank you very much for the update, ! . Much appreciated. Best,
 >
 > From: " " (<mailto: @fb.com>)
 > Sent: Monday, April 30, 2018 2:35 PM
 > To: (JUST)
 > Cc: ; ;
 > Subject: MCC case- Irish High Court appeal
 >
 > Hi ,
 >
 > Thank you again for your time last week. We wanted to let you know that we will be at the Irish High Court today and will notify the court of our intent to appeal the MCC case.
 >
 > We will send more details shortly, but wanted to share this update with you as soon as possible.
 >
 > Please let us know if you have any questions.
 >
 > Best,
 > |

From: (CAB-JOUROVA)
Sent: 28 June 2018 14:51
To: CAB JOUROVA ARCHIVES
Subject: FW: Flash Facebook 26 April

Dear

For registration and info for and
Thank you

From: TALKO Wojtek (CAB-JOUROVA)
Sent: Thursday, June 28, 2018 1:39 PM
To: (CAB-JOUROVA)
Cc: (CAB-JOUROVA)
Subject: Flash Facebook 26 April

Flash report - meeting with Facebook 26 April

Participants: Wojtek Talko, ' (HoU DG Just), (DG Just),
Thomas Myrup, '

On the request of Facebook (FB), we met representatives of Facebook to discuss their compliance work on the GDPR. The meeting was mainly a presentation from FB showing the print screens of the real consent process that people have to go through.. FB argued that they will implement some elements of the GDPR globally. FB presented how they intend to comply with the GDPR, including the establishment of a DPO for FB Ireland. FB also presented the technical change in the interface for FB users and face-recognition function. We had a number of questions on compliance with the GDPR of different features presented.

From: (CAB-JOUROVA) on behalf of JOUROVA Vera (CAB-JOUROVA)
Sent: 06 April 2018 12:57
To: CAB JOUROVA ARCHIVES
Cc: (CAB-JOUROVA)
Subject: FW: Letter for the attention of Ms Sheryl Sandberg, COO Facebook
Attachments: Commissioner Jourova 4.5.18.pdf

Follow Up Flag: Follow up
Flag Status: Flagged

To register ☺ thanks,

From: Sheryl Sandberg [mailto:sheryl.sandberg@fb.com]
Sent: Thursday, April 05, 2018 9:45 PM
To: JOUROVA Vera (CAB-JOUROVA)
Cc:
Subject: RE: Letter for the attention of Ms Sheryl Sandberg, COO Facebook

Commissioner Jourová,

Thank you for your letter. What happened with Cambridge Analytica represents a breach of trust, and we are very sorry this happened. Please find in the attached letter a response outlining our plan for addressing the issues you raise.

My very best,
Sheryl

sheryl.sandberg | chief operating officer | facebook
1 facebook way
[fb.com](https://www.facebook.com/sheryl.sandberg)

From: sheryl.sandberg@ec.europa.eu <sheryl.sandberg@ec.europa.eu>
Sent: Monday, March 26, 2018 9:27:56 AM
To: Sheryl Sandberg
Subject: Letter for the attention of Ms Sheryl Sandberg, COO Facebook

Dear Ms Sandberg

For your attention, please find the attached letter.

Best Regards

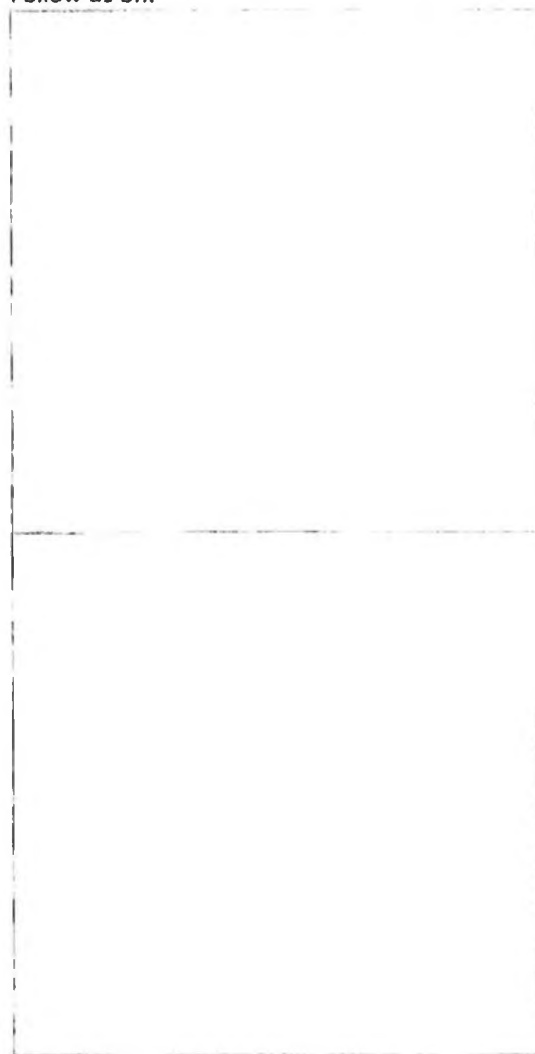
Věra Jourová

Commissioner for Justice, Consumers and Gender Equality

European Commission

<https://ec.europa.eu/commission/commissioners/2014-2019/jourova>

Follow us on:



@VeraJourova



@EU_JUSTICE

Commissioner Jourová,

Thank you for your letter and for giving me the opportunity to answer your questions.

What happened with Cambridge Analytica represents a breach of trust, and we are very sorry. It is now clear to us that there's more that we could have done, and as Mark Zuckerberg said, we are working hard to tackle past abuse and are committed to letting people know if their data was inappropriately accessed or misused.

Before responding to your questions, I'm including some of the details about the timeline of events here for your reference:

In 2013, Dr. Kogan - a researcher at Cambridge University - created the third-party app "thisisyourdigitallife" and launched it on the Facebook Platform. People who installed the app gave permission to access some of their data, as well as some data about their Facebook-friends if the friends' privacy settings allowed for such sharing.

Although Dr. Kogan gained access to the information from our users in accordance with the policies in place for developers at that time, he did not subsequently abide by the terms of those policies. By passing on information to a third party, including SCL/Cambridge Analytica and Mr. Wylie of Eunoia Technologies, he violated our platform policies.

When we learned of this violation, we removed his app from Facebook and demanded certifications from Dr. Kogan and all parties he had given data to that the information had been destroyed. SCL/ Cambridge Analytica, Dr. Kogan, and Mr. Wylie all certified to us that they had destroyed the data in question in 2015.

Three weeks ago, we received reports from media that, contrary to the certifications we were given, not all data was deleted. Cambridge Analytica have confirmed publicly that they no longer have the data, though others are challenging this assertion. We are determined to find out the facts.

We have hired a digital forensics firm, Stroz Friedberg, to conduct a comprehensive audit of Cambridge Analytica to verify the deletion certification they provided us. Cambridge Analytica has agreed to comply and afford the firm complete access to their servers and systems. In accordance with the request of the UK Information Commissioner, we have refrained from conducting a forensic investigation until the Information Commissioner has conducted her own examination of the premises and systems of Cambridge Analytica. We have approached the other parties involved — Mr. Wylie and Dr. Kogan — and asked them to submit to an audit as well. Dr. Kogan has given his verbal agreement to do so. Mr. Wylie thus far has declined.

Last year, the UK's Information Commissioner opened a formal sector inquiry into the use of data analytics for political purposes, and this has involved the ICO consulting with a range of organizations. We have been assisting the Information Commissioner with that inquiry, including questions in relation to Cambridge Analytica and Dr. Kogan. We remain in regular contact with the ICO to assist them with their inquiries.

facebook

Address: 1 Hacker Way
Menlo Park, CA 94025

The Irish DPC conducted two audits of Facebook in 2011 and 2012 and made a number of recommendations, including in relation to our platform and our privacy settings. Likewise, the Federal Trade Commission investigated Facebook's platform practices in 2010 and issued a Complaint and Consent Order in 2011 following this investigation.

Based on feedback we received from the IDPC, FTC and other regulators, we made a number of changes to our platform practices between 2012 and 2014. These changes were focused on providing people with prominent in-product notification about the kinds of data their friends could share about them, engineering clear and specific disclosures about each field of data an app could access before a user granted permission, restricting the data that apps could access all together, and providing per-app controls over who could view information posted by apps on people's behalf.

Due to these changes, had Dr. Kogan connected his app to Facebook today, he would not get access to the level of information about friends that he did in 2013. On Facebook, apps can no longer ask for information about people's friends unless their friends have also authorized the app. We also now have a stricter app review process. When a developer creates an app that asks for certain user information, we require developers to justify the data they are looking to collect and how they're going to use it – before they are allowed to even ask people's permission for it. We then review whether the developer has a legitimate use for the data in light of how the app functions. We have been rejecting a significant number of apps through this process.

Two weeks ago, Mark Zuckerberg announced several steps to further lock down our platform and prevent bad actors from accessing people's information. This week, we shared an update on the progress we've made. We're dramatically reducing the information people can share with apps and shutting down other ways data is shared through Groups, Events, Pages, and Search. We're rolling out a tool at the top of News Feed to show people the apps they've connected with and providing them with an easy way to delete them. We will also let people know if their data may have been shared with Cambridge Analytica. In total, we believe the Facebook information of up to 87 million people – majority in the US, but 2.7 million in the EU – may have been improperly shared. Using as expansive a methodology as possible, this is our best estimate of the maximum number of unique accounts that directly installed the 'thisisyourdigitallife' app as well as those whose data may have been shared with the app by their friends.

These are just the latest steps. This is a long-term effort and we will continue to share updates. We are liaising with the UK's Information Commissioner, the Irish Data Protection Commissioner, the Chair of the Article 29 Working Party, and all EU data protection authorities.

You also asked how we intend to apply principles enshrined in EU privacy laws. The principles of purpose limitation, data minimization and transparency are essential to users' trust, and we remain fully committed to them. In preparing for the forthcoming GDPR, we have assembled the largest cross-functional team in the company's history to conduct an entire review of the way we manage EU citizens' data. That review remains ongoing and is an integral part of the product development cycle. We will abide by the GDPR and the principles of data minimization and purpose limitation by ensuring that we have a clear purpose for the data we collect, and a clear legal basis for processing.

The Facebook logo, consisting of the word "facebook" in a white, lowercase, sans-serif font, is positioned on the left side of a dark grey rectangular background.

Address: 1 Hacker Way
Menlo Park, CA 94025

Starting this week, we are making a series of announcements about our changes regarding privacy and data protection, including new tools to enhance transparency and control over data for people on Facebook. It is important to emphasize that many of these changes and updates are designed specifically to comply with the GDPR although the underlying controls and protections will in many cases be launched globally. These changes have been in preparation for many months, but the events of the past few weeks underscore their importance and timeliness.

Over the last year, we have proactively approached many of Europe's data protection authorities to explain the steps we are taking to comply with the GDPR. We have also had the privilege of presenting to a meeting of the Article 29 Working Party in January of this year on some of the important changes we are making to prepare for GDPR. We will continue engaging with Europe's authorities in this spirit going forward.

Finally, I want to underline that we remain deeply committed to helping protect the integrity of the electoral process on Facebook. We have, for instance, launched a pilot ads transparency tool in Canada and we have announced verification for political ads to provide increased transparency. We will continue to work with regulators, our industry partners and our community to better ensure transparency and accountability in our advertising products.

As Mark Zuckerberg said, this was a breach of trust, and we must do better. The changes we are making to prepare for compliance with the GDPR are a continuation of our efforts to make a better community for our users. We are committed to protecting people's personal data and respecting the rights of everyone who uses Facebook.

My team in Europe is available to meet with you at your earliest convenience. Thomas Myrup Kristensen (Managing Director EU Affairs) is the right person to connect with, and has confirmed he is already in touch with your office. I would also be grateful for the opportunity to speak to you personally when your schedule allows.

Sincerely,

Sheryl Sandberg
Chief Operating Officer
Facebook, Inc.

The Facebook logo, consisting of the word "facebook" in a white, lowercase, sans-serif font, is positioned on the left side of a dark gray rectangular bar.

Address: 1 Hacker Way
Menlo Park, CA 94025

Brussels,
RN(2018)

Dear Sheryl,

I write to you to better understand how data of Facebook users, including possibly that of EU citizens, got into the hands of third parties without their knowledge or consent. I would also like to learn about your plans to address these recent revelations. As you know, the enforcement of data protection rules in Europe is the responsibility of European Data Protection Authorities. They have my unequivocal support and I expect Facebook to fully cooperate with them in the context of their investigations. As you know the GDPR becomes applicable on 25 May. It not only changes the law but introduces a number of principles of particular concern for you and your company.

I am also following with interest the work by the FTC in the US on the matter, in particular with regard to the 2011 Consent Order. They will keep me informed of any enforcement steps they will take. This also matters for the Privacy Shield. It is crucial to address all concerns relating to the respect of EU and US law.

In my view, the concerns raised recently have much broader consequences for the democratic processes.

I regret that Facebook's official statements, including those of CEO Zuckerberg, have not alleviated my concerns.

This is particularly disappointing given our efforts to build a relationship based on trust with you and your colleagues. We have worked together well on a number of issues, in particular on the Code of Conduct on illegal hate speech and our dialogue in the context of the Privacy Shield. This trust is now diminished.

It is clear that your network has great influence and offers great potential for people, advertisers and other businesses. But with great power comes great responsibility. Facebook needs to take steps to regain the trust of its users and to meet its obligation to society.

Democracy requires an open debate. Your platform has been used for many years now as a vehicle for political marketing, but recent news indicates that a lack of transparency and abuse of personal data could also have negative impact on the quality of this debate and even on our electoral processes.

In view of the above I would like to ask you some questions:

- 1) How do you intend to apply the principles enshrined in EU privacy laws, such as purpose limitation and data minimisation on Facebook and among the Facebook family?
- 2) Have any data of EU citizens been affected by the recent scandal? If this is the case, how do you intend to inform the authorities and users about it?
- 3) Are you absolutely certain that such a scenario as with Dr Kogan/Spectre's app and Cambridge Analytica couldn't be repeated today?
- 4) Is there a need for stricter rules for platforms like those that exist for traditional media?
- 5) Do you intend to change anything in your approach to corporate social responsibility, especially when it comes to transparency towards your users and regulators?

I would appreciate a reply within the next 2 weeks.

Regards,

Vera Jourová



COMMISSIOBNER VĚRA JOUROVÁ

MEETING WITH MEETING SHERYL SANDBERG, COO, FACEBOOK

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

DATE AND TIME: 23/01/2018 15:00

**MEETING OBJECTIVE: TO DISCUSS 1.HATE SPEECH, 2A) DATA PROTECTION –
GDPR, 2B) PRIVACY SHIELD, 3.E-EVIDENCE**

MEMBER RESPONSIBLE: BRAUN DANIEL

DG CONTACT & TEL NO:

DIRECTOR:

VERSION: 08/11/2018 13:06

JUST/123

TABLE OF CONTENTS

STEERING BRIEF	3
TOPICS	4
TOPIC 2 A) GDPR	8
TOPIC 2B) PRIVACY SHIELD	13
TOPIC 3 E-EVIDENCE	19
TOPIC 4 CYBER VIOLENCE AGAINST WOMEN AND GIRLS	23
ANNEXE	24

STEERING BRIEF

CONTEXT/SCENE SETTER

This visit from Sheryl Sandberg is a follow up to a previous discussion in California. She will be accompanied by:

- Richard Allan, Vice President EMEA Public Policy, Facebook
- Thomas Myrup Kristensen, Managing Director EU Affairs, Facebook
- Joel Kaplan, Vice President Global Public Policy, Facebook

She is also meeting VP Ansip and Commissioner Moedas on the same day to discuss the future of the digital single market, Platforms, illegal content online, E-Privacy and Fake news. She has attended the Macro 'do business in France' initiative at Versailles and will move to DavoS;

OVERALL OBJECTIVES

- Secure the continued commitment by Facebook on tackling illegal hate speech through the **Code of Conduct on illegal Hate speech**
- Inquire about **addressing cyber-violence against women** in a similar way as illegal hate speech targeting minorities.
- Promote the benefits of the **GDPR** and inform about and promote the functioning of the **Privacy Shield**
- On **e-evidence**, encourage support for ongoing Commission initiatives to support practical measures on e-evidence and the forthcoming legislative proposal.

TOPICS

HATE SPEECH

CONTEXT

On 31 May 2016 the European Commission together with Facebook, Microsoft, Twitter and YouTube announced the Code of Conduct on Countering Illegal Online Hate Speech, which includes a series of voluntary commitments to combat the spread of such content in Europe. The four platforms agreed to assess the majority of users' notifications in 24h for illegal hate speech as defined in relevant national legislation implementing EU law and committed to remove, if necessary, those messages when considered illegal. The four companies also committed to improving the support to civil society as well as the coordination with national authorities.

On 28 September, the Commission adopted a Communication which provides for guidance to platforms on notice-and-action procedures to tackle illegal content online. The importance of sectorial dialogues including the one countering illegal hate speech online and the need to continue working with the implementation of the Code of Conduct are featuring prominently in this guidance document.

The Communication announced that the Commission will monitor the progress of the IT Companies and assess, by May 2018, impacts of actions to see if additional (including legislative) measures would be needed.

As a follow up to the Communication, several Commissioners met with representatives of online platforms on 9 January 2018 to discuss progress made in tackling the spread of illegal content online

On 19 January, the Commission published the results of the third round of monitoring of the implementation of the code of conduct. The results showed a significant improvement of the level of implementation in comparison to the first and second monitoring published in December 2016 and June 2017, will feed into to the impact assessment actions to see if additional (including legislative) measures would be needed.

OBJECTIVE(S)

- Commend Facebook for showing leadership on this file while underlining the need for continued engagement and progress.
- Discuss follow up to the September Communication on Illegal Content

LINE TO TAKE

- Through the Code of Conduct on Countering Illegal Hate speech Facebook along with Microsoft, YouTube and Facebook agreed to assess the majority of users' notifications of in 24h also respecting national legislation implementing EU law on hate speech.
- The work in the code of conduct was important in terms of feeding into the Commissions Communication of 28 September which provides for guidance to platforms on notice-and-action procedures.
- One of the strongest features of the Code of Conduct is the monitoring process, which allows us to continuously assess progress and the difference we make on the ground.
- As you know, we have just finalised the third monitoring of the implementation of the code of conduct and the results are very good.
- On average, the IT Companies responded by removing more than 70% of the deemed manifestly illegal content notified compared to 59% six months ago and only 28% one year ago.
- The amount of notifications reviewed within 24 hours has also significantly improved and all the IT Companies now fully meet the target of reviewing the majority of the notifications within the day.
- In terms of rate of removal and time to removal, Facebook was in the lead, removing 80,8% of the notified content and assessing notifications within one day in 89,2% of the cases.
- Together with the other IT Companies, Civil Society and Member States, Facebook has shown that the collaborative approach of the Code of Conduct works. By creating an alliance between all the relevant actors, It Companies, civil society Member States and law

enforcement, you have managed create a process of converging interests where we are all working together to achieve the dual objective of ensuring effective removal of illegal racists and xenophobic hate speech while respecting freedom of expression online.

- The results will be very important to the Commission when we assess see if additional measures would be needed to tackle illegal content and, if so, which ones.
- While it is too early to give an indication on the outcome of the assessment, I want to fully preserve the Code of Conduct and its progress.
- Still, work remains to be done, in particular in relation to reporting (public transparency) and user transparency, which is an important guarantee for freedom of expression online. However, I also note that Facebook was the best performing company in terms of feedback to users.
- Another area which needs to be developed further is how to address the cyber violence against women. It is a phenomenon which I want to focus during my dialogue with IT companies.
- We have shown that the code is an efficient way to obtain results and we should now focus attention on ensuring its status as an industry standard that allow for the "onboarding" of as many relevant social media platforms as possible.
- I count on Facebook to continue showing leadership on the efforts to prevent racism and xenophobia and apply rules that apply offline also online.
- Your communication to other companies about the experience of working with the code from an industry perspective is of course very important and appreciated. Our next challenge is to demonstrate that this form of collaboration is a sustainable model not only for large platforms but also for small SME's and

start ups.

Background

After three rounds of monitoring, regularly carried out since its adoption, the Code of Conduct on countering illegal hate speech online has contributed to achieve important results through a path of continuous progress. According to the latest data:

- On average, the IT Companies responded by removing more than 70% of the deemed manifestly illegal content notified. Facebook removed 80,8% of the content YouTube 75,2% and Twitter 45,6%. This corresponds to a steady improvement to the removal rate of 59% recorded in the second monitoring exercise ended in May 2017, which in turn doubled the removal rate of the first monitoring exercise of December 2016, where only 28% of the notifications led to the removal of the notified content.
- The amount of notifications reviewed within 24 hours has largely improved, reaching an average of more than 81%, considerably higher than the 40% and 51% registered one year and six months ago respectively. The third monitoring round shows that all IT Companies now fully meet the target of reviewing the majority of the notifications within the day, Facebook reviewed within the day 89,2% of notifications, YouTube 62,8%. The improvement in time of assessment of Twitter was particularly striking moving from 39% in May 2017 to 79,9% in this third exercise

[REDACTED]

TOPIC 2 A) GDPR

CONTEXT

You are meeting with Sheryl Sandberg, COO at Facebook.

In 2017, you had a meeting with MR. Elliot SCHRAGE, Facebook's Global VP for Policy and Communications.

The reaction of Facebook to the GDPR was not entirely positive. European Digital Media (EDiMA), where Facebook is a member, expressed some concerns after the adoption of the GDPR. According to those, GDPR failed to strike the balance between protecting the citizens' fundamental right to protection of personal data and allowing the business in Europe to grow. On the contrary, it "undermines the ability of businesses in Europe to innovate, operate efficiently and grow". However, the company is pragmatic and ready to make the new legislative framework workable. That is why it called for an open and transparent implementation process and wide consultations with all relevant stakeholders, including the industry.

Note also that Facebook 'Custom Audiences' tool has been the subject of investigation in Germany by the Bavarian DPA. With this tool Facebook promises advertisers to target both existing and potential customers directly. In a press release of 4/10/2017, the Bavarian DPA considers that the permissibility of using Custom Audiences from customer lists must depend on consent having been granted within the meaning of Section 4a of the Federal Data Protection Act (BDSG). Despite the use of the hashing process, it argues that the data transmitted are at least personal for Facebook, which is why the procedure requires justification from a data protection perspective. It found no evidence of any legal basis for such activities.¹ [Comment: with the GDPR in place, Facebook must also find a legal basis under Article 6 GDPR for the processing of personal data, and any further processing must meet the compatibility test in Article 6(4) GDPR.]

OBJECTIVE(S)

The objectives of your meeting would be to:

- Promote the benefits of the GDPR;
- Explain the Commission's priorities during the transition period;
- Reassure that businesses have an opportunity to be actively involved in actions conducted during the transition period.
- To find out how they will communicate about new GDPR Rules.

¹ <https://www.spiritlegal.com/en/news/details/facebook-custom-audiences-and-data-protection-law.html>

LINE TO TAKE

- The New European Union data protection regulation – the General Data Protection Regulation (GDPR), will be applicable from 25 May 2018. The new legislation modifies and updates data protection rules at EU level to make Europe fit for the digital age.
- The GDPR is a competitive advantage a trust-enabler and a key instrument to ensure level-playing field for all companies operating in the EU market. Increased trust from consumers will provide further business opportunities and chances for innovation. Companies will also have easier access to the whole EU market, with the current 28 national legislations being replaced by one, simple and clear legal framework. The GDPR is not a revolution; it simplifies the legal landscape for businesses and brings enhanced legal certainty for their operations.
- Commission is working closely with Member States to accompany them in the process of adapting or repealing their existing laws as necessary. We are fully aware that one of the main concerns of business is that measures taken at national level must not lead to any new fragmentation.
- We are also supporting the work of the Data Protection Authorities who have a key role in ensuring coherent interpretation and enforcement of the new rules. The Article 29 Working Party is playing an active role in preparing guidelines for companies and other stakeholders.
- Article 29 Working Party has already issued six 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, and on urgency procedures). It has adopted guidelines on data breach

notifications and profiling which were subject to public consultation until 28 November and are currently being finalised. At its last plenary meeting on 28-29 November, the Article 29 Working Party adopted guidelines on consent and transparency which are now subject to public consultation (until 23 January 2018). Businesses are strongly encouraged to take advantage from the current consultation and provide their views.

- We also want to maintain an open dialogue with other stakeholders, notably businesses, to ensure they are aware of their obligations and also dispel doubts about the application of the new rules. For instance, we held our first multi-stakeholder expert group on 19 October to support the application of the GDPR in view of opinions of its members, including academia, legal practitioners, civil society and business representatives.
- As announced in the letter of intent following President Juncker's State of the Union speech, the Commission will provide guidance to businesses, especially SMEs, and individuals so as to raise their understanding of the new rules in view of their application as of May 2018. This guidance will take the form of a practical online toolkit. We will have it ready by the data protection day on 28 January. We are also supporting financially awareness-raising activities carried out at national level, including by Data Protection Authorities.

DEFENSIVES

How is the Commission planning to ensure that citizens and business are aware of new legislation?

- We consider it essential to foster a uniform interpretation of the GDPR across Member States, hence our active work with national authorities either bilaterally or in the GDPR expert group, and our support to the work of Article 29 Working Party to produce a comprehensive set of guidelines. Existing national guidelines should be brought into compliance with those EU level WP29 guidelines since we are well aware of industry's concerns regarding the risk of inconsistent application.
- As already mentioned, EU grants are being allocated for training of DPAs and national authorities (including the production of materials), others in the coming months will more specifically target awareness-raising among SMEs and the general public. Building on this and to accompany these various actions, we have developed guidance, in the form of a toolkit, in order to prepare business and citizens about the new rights and obligations under the GDPR. This will be launched on our website by Data Protection Day on 28 January.
- We continue our open dialogue with all stakeholders, including civil society and businesses, to ensure that they are aware of their obligations and to dispel any doubts they may have about the application of the new rules.
 - We held our first multi-stakeholder expert group on 19 October to support the application of the GDPR in view of opinions of its members, including academia / legal practitioners / civil society and business representatives.
 - We also have regular exchanges to discuss about the GDPR and the sector specific issues. On 23 October, the Commission services held a workshop with more than 150 stakeholders active in the health sector.
 - On 27 November we held a workshop with the EU umbrella federation of SMEs and their national members to better understand the specific needs of SMEs.
 - On 1st February we will hold a workshop with the consumer organisations (BEUC and member organisations).

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

- The guidelines of the Article 29 Working Party 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 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 (and after May 2018 the European Data Protection Board) is an independent body and therefore the content of the guidelines are their responsibility.

[REDACTED]

TOPIC 2B) PRIVACY SHIELD

CONTEXT

Facebook is certified under the Privacy Shield. Transfers of personal data from Facebook Ireland Ltd to Facebook servers located in the U.S. were the subject of the proceedings between privacy activist Max Schrems and the Irish Data Protection Commissioner which led to the invalidation of the Privacy Shield's predecessor, the Safe Harbor framework, by the Court of Justice in its *Schrems* ruling. The so-called Schrems II case (see defensives) is equally based on a complaint by Mr Schrems against data transfers by Facebook, this time on the basis of so-called "Standard Contractual Clauses".

The Commission conducted the first annual review of the Privacy Shield mid-September 2017 and published its report on 18 October 2017. At the end of November 2017, the EU data protection authorities adopted their own report on the first annual review, which in many aspects is aligned with the Commission's views but also contains more critical language, in particular as regards surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA) and the powers and independence of the Ombudsperson. The data protection authorities call for improvements to be made by the next annual review, but want to see the appointment of a permanent Ombudsperson and a clarification of the Ombudsperson's rules of procedure before the end of May 2018. If their concerns are not addressed within the indicated timeframes, the data protection authorities threaten to take action, including possibly by challenging the Privacy Shield decision before national courts.



OBJECTIVES

- Inform about the outcome of the first annual review of the functioning of the Privacy Shield and the follow-up to the Commission's report.
- Invite Facebook to support the sustainability of the Privacy Shield framework, in particular by arguing in favour of a swift implementation of the Commission's recommendations.

LINE TO TAKE

- Since the launch of the Privacy Shield (on 1 August 2016), more than 2,600 companies have joined.
- The participation of companies like Facebook, Google, IBM and Microsoft, 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 U.S. companies certified under the Shield, 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.
- We have seen a number of improvements compared to the old Safe Harbour framework. In particular, the Department of Commerce now manages more tightly the certification process and carries out closer checks the applications for certification.
- But the Commission also formulated a number of recommendations on how to improve the practical implementation of the safeguards provided in the Privacy Shield.
- Some of these recommendations are of an operational nature (e.g. compliance monitoring by the Department of Commerce) and we are confident that these issues can be addressed rather easily.
- My staff is in contact with the Department of Commerce (which is in charge of the administration of the Shield) on

this but it would be important that you also pass the message that this is important to show some movement and some progress following our recommendations.

- This is all the more important as also the data protection authorities in the EU who participated in the annual review want to see certain improvements without delay. They have threatened to take action – including bringing the Privacy Shield before national courts – if their concerns are not addressed in time.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- As one of the major U.S. tech companies, I count on you to support the sustainability of the Privacy Shield by arguing in favour of a swift implementation of our recommendations in your contacts with the U.S. administration and with Congress.

BACKGROUND

The Privacy Shield provides for a review to be conducted on an annual basis. The purpose of the review is to carefully assess the proper functioning, implementation, supervision and enforcement of the Privacy Shield framework. This concerns all aspects of the framework: both compliance by companies and by U.S. authorities, including in the field of national security access to personal data.

The first annual review took place on 18-19 September in Washington, DC. On 18 October, the Commission adopted and published its Report to the European Parliament and Council on the first annual review of the functioning of the EU-U.S. Privacy Shield, which was presented to the EP's LIBE Committee on 6 November and presented to Member States in the Council on 21 November.

While the Report concludes that the U.S. does continue to ensure an adequate level of protection for personal data transferred under the Privacy Shield, it also identifies a number of areas where the implementation of the framework should be improved. To this end, it makes a number of recommendations:

In the commercial area, the Commission recommends

- that companies should not be allowed to publicly announce that they are Privacy Shield-certified until the Department of Commerce has finalised the certification;
- that the Department of Commerce conducts regular searches for companies falsely claiming participation in the Privacy Shield;
- that the Department of Commerce conducts compliance checks on a regular basis;
- that the Department of Commerce and the Data Protection Authorities work together to develop guidance on the legal interpretation of certain concepts in the Privacy Shield (e.g. with regard to the principle of accountability for onward transfers and the definition of human resources data);
- that the Department of Commerce and the EU Data Protection Authorities strengthen their awareness raising efforts (e.g. to inform individuals about how to exercise their rights under the Privacy Shield).

In the area of national security,

- the Commission would welcome if the U.S. Congress would consider favourably enshrining in the Foreign Intelligence Surveillance Act the protections for non-Americans offered by Presidential Policy Directive 28 (PPD-28);
- the Commission calls on the U.S. administration to swiftly appoint a permanent Privacy Shield Ombudsperson, as well as the missing members of the Privacy and Civil Liberties Oversight Board (PCLOB);
- the Commission calls for the public release of the PCLOB's report on the implementation of PPD-28.

In both the commercial and national security areas, the Commission also calls on

the U.S. authorities to proactively fulfil their commitment to provide timely and comprehensive information about any development that could raise questions about the functioning of the Privacy Shield.

DEFENSIVES

Two actions for annulment have been brought against the Privacy Shield.

- Two actions for annulment of the Privacy Shield decision (one brought by Digital Rights Ireland and one by La Quadrature du Net) have been lodged with the General Court. The case of Digital Rights Ireland has recently been declared inadmissible by the Court.
- While we cannot of course predict the outcome of the other case – like in any other proceedings before the Court – we are confident that the adequacy decision will withstand judicial scrutiny. We strongly believe that the decision is lawful and in particular fulfils the requirements stipulated by the Court in the *Schrems* ruling. Otherwise, the Commission would not have adopted the decision in the first place. Neither would we have received overwhelming support from the Member States.
- This being said, the commitments made under the Privacy Shield are not the only thing that matters. It will also be important that the U.S. honours its commitments in practice and fully implements the framework. This is yet another reason why the Annual Review was so important, but this now has to be followed-up by action on the recommendations that the Commission and the data protection authorities have issued.
- *[NB: In the case lodged by La Quadrature du Net, the Commission has submitted its defence in September. The applicant had until late December to file its reply (second round of written pleadings). Several Member States as well as a number of private entities have requested and received permission to intervene in the case in support of the Commission. They filed their submission in mid-December. We expect an oral hearing at the earliest in late 2018 and the judgment not before mid-2019.]*


[REDACTED]

[REDACTED]

[REDACTED]



The EU DPA's represented in the Article 29 Working Party may decide to suspend transfers based on the Privacy Shield if their concerns are not addressed on time.

- It is the purpose of the annual review mechanism to address issues before they become problems. This is why we are working with our U.S. partners on the implementation of our recommendations and we are confident that such a scenario can be avoided.
- 

TOPIC 3 E-EVIDENCE

CONTEXT

Facebook is a key company with regard to access to electronic evidence. It has set up an online platform to receive (non-content data) law enforcement requests which has been positively received by Member States law enforcement end users and could even possibly serve as a model for others. Facebook is ready to cooperate with EU law enforcement on legitimate requests, but does not want to hand over data to some non-EU third countries in order to protect the rights and freedoms of customers.

In recent stakeholder consultations, Facebook has emphasised the need to avoid **conflicts of law** between EU and US legislation. Facebook is also aligned with Google and Microsoft in emphasising that if the service provider is providing solutions for corporate customers, the primary target of a Law Enforcement production order should be the corporate user of the service and not the service provider.

Facebook was critical regarding a common legal framework for direct access, which is no longer in the scope of the draft initiative.

In your meeting with Facebook Vice-Presidents (Schrage, Allen, Beringer) and Privacy lead Deadman last September, Facebook expressed support for practical measures on e-evidence (single points of contact, training on mutual legal assistance), but raised concerns about legislative measures that could create conflicts of laws for companies.

Facebook has been proactively involved in consultation for the forthcoming legislative proposal on e-evidence, including a recent meeting with Kevin O'Connell and DG Justice (meeting report in background).

OBJECTIVE

- Encourage support for ongoing Commission initiatives to support practical measures on e-evidence and the forthcoming legislative proposal.

LINE TO TAKE

- I am grateful for Facebook's proactive engagement in the stakeholder consultation for our forthcoming proposal on e-evidence, as well as on the ongoing practical measures to improve cross-border access to e-evidence, which we discussed when I visited Silicon Valley in September.
- Work is ongoing on our envisaged proposal, due to be adopted in February. It would introduce a cross-border European Production Order, for the disclosure by service providers such as Facebook of information stored in

electronic form that could serve as evidence in the framework of criminal investigations or proceedings.

- This proposal will be drafted in full accordance with EU data protection rules and respect of fundamental rights. It will also address conflict of law situations.
- The feedback we received from service providers has been extremely useful for us. It has helped us to shape our proposal in order to find a good balance between all interests at stake.
- I am grateful for your ongoing support in this initiative that will deliver a standardised EU approach and more legal certainty for all concerned.

DEFENSIVES

Costs for service providers will be huge and the administrative burden disproportionate

The Impact Assessment has assessed the burden for service providers linked to the proposal. It concludes that the introduction of a European Production Order, even if combined with the obligation to designate a legal representative within the EU, will even generate savings for them, notably because it will establish a clear legal framework compared to the current practice of voluntary cooperation, with clear rights and obligations on both sides. This is also why several service providers, including Facebook, support the introduction of a mandatory framework.

Conflicts of laws – you will force us into something illegal under U.S. law

A clause on ensuring international comity will be included in the proposal. Its aim is also to prevent that service providers are faced with situations of conflicts of law, as is more and more the case today. This is also a very important issue for the Commission, in particular in view of reciprocal responses by third countries which could affect fundamental rights of persons protected by EU law, such as the data protection acquis. A procedure will be set up, whereby the service provider can raise such conflicts of law with the issuing authority, and which can also involve the third country.

There is a lack of standard of what legitimate access looks like

The proposal contains a set of conditions and safeguards which aim to ensure respect for proportionality and fundamental rights while at the same time making sure the instrument remains an effective tool for law enforcement and judicial authorities. This includes thresholds delimiting the scope, notification requirements and judicial remedies for persons affected and even rights for service providers that exceed by far what exists in domestic legislation in the Member States.

BACKGROUND

Meeting on 10 January 2018 between CAB JOUROVA and Facebook

- Facebook (FB) highlighted its work on the non-legislative side of law enforcement access to data requests, notably trying to clarify what authorities may or may not access.
- FB welcomed the constructive and open working relationship with HOME and JUST services as part of the public consultation.
- This proposal is an opportunity for the EU to show leadership, since access to data by law enforcement is a global issue and the harmonisation in the EU space is necessary, given the different procedures in place in the MS for accessing data.
- On the US side, Congress is constantly pushing EU's law enforcement authorities back, because there's a lack of standards on "what good

(legitimate) access looks like".

- FB's biggest concern is the conflicts of law issue, notably between EU and US laws. They noted that US ISPs have different modus operandi when dealing with requests. For FB, the place where data is stored should not matter. What is essential is the safeguarding of data protection standards, the place where the receiving company is incorporated and, most importantly, the jurisdiction where the user is.
- US Congress has traditionally seen this as an internal affair, linked to the Stored Communications Act. FB has actively engaged with Congress to show the matter has an external dimension, since foreign law enforcement authorities have a need to access US providers' databases. FB is pushing the DoJ to enter into agreements with 3rd countries, but there are no criteria yet for what said countries have to comply with to get such an agreement.
- FB expressed concern that the forthcoming proposal isn't based on the assumption that an agreement between EU-US for companies to provide data to foreign law enforcement authorities is in place.
- FB receives 75.000 requests a year from law enforcement, EU authorities being among the most active (Latest Transparency Report published 22 December 2017)
- FB wants to encourage other ISPs (like instant messaging services) to be cooperative with law enforcement. Maybe a collaborative/knowledge transfer platform between ISPs would help. They noted the possibility that companies who don't want to be cooperative will ultimately withdraw their establishment from the EU.



TOPIC 4 CYBER VIOLENCE AGAINST WOMEN AND GIRLS

Background on cyber violence against women and girls

The Commission recognises cyber violence as a form of gender-based violence, which it is committed to eliminating as part of its work to promote gender equality in the EU. In 2017, the Commission launched focused actions to combat violence against women, providing support for projects tackling the problem. A number of these initiatives aim to increase reporting of online sexual harassment, as well as awareness of sexism online.

The Commission co-funds the European Safer Internet Centres , in order to raise awareness, among minors and their carers, of risks online and protection methods. This includes sexual violence, harassment and child sexual abuse images online, which affects mostly girls.

The European Institute for Gender Equality has issued a recent report on cyber VAWG showing national initiatives, such as provisions criminalising revenge porn in the U.K., France, Germany or Malta.

EU Member States that have ratified the Istanbul Convention must establish, in their national law, offences on stalking and sexual harassment. The Convention encourages cooperation with the private sector and the media to tackle this problem. The EU is in the process of acceding the Istanbul Convention which will help to streamline national approaches to combat VAWG, including cyber violence. The Commission continues to encourage Member States to consider ratification of this Convention.

Legal protection for victims of cyber violence is included in the Victims' Rights Directive and the Directive on trafficking in human beings. The Victims' Rights Directive ensures that victims get access to general and specialised support services, responding to their individual needs and providing for emotional assistance and counselling. Cybercrime is also a priority for Europol, through the European Cybercrime Centre (EC3) to improve law enforcement cooperation on online sexual coercion and extortion against minors.

The Commission is also addressing cyber violence and hate speech under initiatives creating the Digital Single Market. The Electronic Commerce Directive provides basis for notice and takedown in response to court orders or allegations of illegal content. Moreover, the proposed revision of the Audiovisual Media Services Directive contains strong provisions for internet platforms to set a flagging system. The Commission is also working with platforms through the Code of Conduct against online hate speech to increase reporting and takedown of harmful content. The Commission's work on platforms and data economy will further clarify the issue of liability of intermediaries.

ANNEXE

Curriculum Vitae - Sheryl Sandberg (source Bloomberg²)

Ms. Sheryl K. Sandberg has been the Chief Operating Officer of Facebook, Inc. since March 24, 2008.

Ms. Sandberg is responsible for helping Facebook scale its operations and expand its presence globally and also managed sales, marketing, business development, legal, human resources, public policy, privacy and communications.

Ms. Sandberg served as a Vice President of Global Online Sales & Operations at Google Inc. from November 2001 to March 2008. She joined Google Inc. in 2001.

Ms. Sandberg served as the Chief of Staff for the United States Treasury Department under President Bill Clinton, where she helped lead its work on forgiving debt in the developing world. She served as a Management Consultant with McKinsey & Company, Inc. and as an Economist with The World Bank, where she worked on eradicating leprosy in India.

She has been an Independent Director of The Walt Disney Company since March 2010.

She has been an Independent Director of Facebook, Inc. since June 25, 2012 and SurveyMonkey Inc. since July 2015. She serves on the board of the Center for Global Development. She served as a Director of The Advertising Council, Inc. She served as a Director at Starbucks Corporation from March 2009 to March 21, 2012 and eHealth, Inc. from May 2006 to December 17, 2008. She serves as a Director at One Campaign and Leadership Public Schools.

She is Director of Google.org/the Google Foundation and directs the Google Grants program. She serves as a Director of The Brookings Institution, The AdCouncil, Women for Women International and V-Day.

In 2008, she was named as one of the "50 Most Powerful Women in Business" by Fortune and one of the "50 Women to Watch" by The Wall Street Journal.

Ms. Sandberg holds a.B. in Economics from Harvard University and was awarded the John H. Williams Prize as the top graduating student in Economics. She was a Baker and Ford Scholar at Harvard Business School, where she earned an MBA with highest distinction.

2

<https://www.bloomberg.com/research/stocks/people/person.asp?personId=27544173&privcapId=29096>

From: (CAB-JOUROVA)
Sent: 28 June 2018 16:25
To: CAB JOUROVA ARCHIVES
Subject: FW: Flash - Meeting with Facebook 23 January 2018

From: (CAB-JOUROVA)
Sent: Thursday, June 28, 2018 3:03 PM
To: CAB JOUROVA ARCHIVES
Cc: (CAB-JOUROVA)
Subject: FW: Flash - Meeting with Facebook 23 January 2018

Dear
Please register.
Thank you

From: TALKO Wojtek (CAB-JOUROVA)
Sent: Thursday, June 28, 2018 2:58 PM
To: (CAB-JOUROVA); (CAB-JOUROVA)
Subject: Flash - Meeting with Facebook 23 January 2018

- Meeting with Facebook 23 January 2018:
- Commissioner Jourová, W. Talko, M. Ladmanova; S. Sandberg, T. Myrup
- During the meeting Facebook has offered its views on a number of issues:

1. E-evidence

- Facebook welcomed the fact that the EU is working on e-evidence proposal. From their point of view this is needed for the tech sector.
- FB's biggest concern is the conflicts of law issue, notably between EU and US laws. For FB, the place where data is stored should not matter. What is essential is the safeguarding of data protection standards, the place where the receiving company is incorporated and, most importantly, the jurisdiction where the user is.
- US Congress has traditionally seen this as an internal affair, linked to the Stored Communications Act. FB has actively engaged with Congress to show the matter has an external dimension, since foreign law enforcement authorities have a need to access US providers' databases.
- FB gets 75.000 requests a year by law enforcement, the EU authorities are amongst the most active (Transparency Report, published 22nd December 2017)

- Fb wants to encourage other platforms to be cooperative with law enforcement. They feel that companies who don't want to be cooperative will ultimately withdraw their establishment from the EU

2. Section 702 FISA and other Privacy-Shield related subjects

- FB has told the Commission that Section 702 has been extended until 31st December 2023.
- FB suggested that some changes that apply to US citizens could have a positive impact on the Commission's assessment of the adequacy of the data protection level in the US.
FB said that in their dialogue with the US Administration it seems that there won't be any acts contrary to the commitments assumed in the Privacy Shield
- FB also informed us that they would welcome the appointment of missing members of the PCLOB and for the enactment of PPD-28 safeguards as an act

3. Illegal hate speech

- FB informed the Commission about its continued efforts to improve removal of illegal content. They hired more people and the results are improving. They offered their commitment to this exercise and potentially to help other smaller firms by know-how sharing.

4. GDPR

- FB said that they are working full speed to introduce necessary changes to be compliant with the GDPR on time. They have set-up the biggest cross-departmental group to do this exercise and assured the Commission that they see this also as an opportunity to re-commit to privacy of their users.
- FB couldn't offer concrete detail at this stage, but offered to come back with more information once they are ready.

Wojtek Talko
Member of Cabinet



European Commission

Cabinet of Commissioner Vera Jourová
Justice, Consumers & Gender Equality



Follow us on:



@VeraJourova



@EU_Justice



@EU_Consumers



EU Justice and Consumers

