Google presented its concerns stemming from the modifications introduced by the co-legislators to the Commission’s proposal to my services and cabinet.

The Commission’s proposal does two things: it provides a high standard of transparency for the provision of political advertising services in the internal market; and it provides for strengthened protections for the processing of personal data in the context of the targeting and amplification of political advertising.

The focus is not on personal political speech, such as private social media use, or journalism and editorial content – these activities are specifically excluded. The definition is based on objective criteria and the main responsibility for identifying political advertising resides with the sponsor – the originator of the message.
Meeting with [Name], Google's [Title]
Brussels, 6 March 2023, 17:00 – 18:00

- The proposal is clear that online platforms should not be required to monitor the content moving through their services to identify political advertising. No general monitoring obligation can be imposed, in line with the e-Commerce Directive and now the DSA.

- In other words, as regards data protection, when Google sells political advertising, or when it is indicated to it by a user uploading content that it is handling political advertising content, then it must treat it according to the political ads data protection regime.

- Google does not need to investigate or judge what is a political advertisement, but it may have to ask to its users to declare it if they upload such content on its services (as they do now for commercial advertising).

- When content on its services is notified to Google as not having been correctly identified as a political advertisement, this should be referred back to the user originating the content – the sponsor has the main responsibility for identifying and declaring the political nature of advertising content.

- The Commission will support the European co-legislators in finding an agreement to the political ads proposal in due time for the next EU elections.

- It will pay attention to support solutions that respect the essence of the proposal, including the carefully calibrated balance between effectiveness of the measures and workability for service providers.

LTT

- The Commission adopted the proposal for the AI Liability Directive, to ensure at the same time the protection of victims of damage caused by AI systems and legal certainty for the businesses active in this sector.

- The Proposal aims to increase trust in the technology. If victims of accidents will not get compensated because of a lack of adaptation of the liability rules to the specifics of AI, there will be a lack of trust in AI.

- The AI Liability Directive is a very targeted and proportionate instrument. The proposal only deals with aspects of liability rules challenged by AI specifics. All other points of liability claims are left to national law.

- In order to find out who the liable person could be or what went wrong, the proposed AI Liability Directive allows the victim to obtain information documented or recorded about high-risk AI systems, while protecting sensitive information like trade secrets by judicial safeguards.

- It avoids that the victim has to look into the ‘black-box’ of AI to prove its claim.

- The AI Liability Directive alleviates the victim’s burden of proof, to prevent that the victim needs to explain the inner workings of AI, by introducing a ‘rebuttable presumption’ of causality.
We will also give businesses, especially when operating cross-border, legal certainty about knowing their liability risks and being able to insure themselves against them.

**AI Act**

- This is world-wide the first comprehensive approach to the risks that AI creates.
- Proportionate and flexible rules address the specific risks, including to fundamental rights posed by AI systems.
- The AI Act provides for a technology-neutral definition of AI systems that is future-proof, to the extent that it can cover techniques and approaches which are not yet known or developed.
- It bans a few applications that are particularly risky from a fundamental rights perspective, such as general purpose social-scoring.
- For the rest, it is risk-based, since it focuses on so-called ‘high-risk’ AI use cases. Only these need to comply with a set of specifically designed requirements to enhance transparency and to minimise risks to safety and fundamental rights. These requirements will be subject to standardisation.
- It is effective, since high-risk AI systems must be assessed for conformity with these requirements before use.
- For the specific case of remote biometric identification systems (e.g. facial recognition tools to check passers-by in public spaces), the proposed regulation establishes an even stricter approach than for other high-risk AI use case.
- We expect a final agreement to be reached before the end of this year.

**b) Other topics that may be discussed:**

**Data protection**
Meeting with [PERSONA], Google's [FUNCTIONALITY]
Brussels, 6 March 2023, 17:00 – 18:00

EU-US Data Privacy Framework

LTT

- On 28 February 2023, the EDPB adopted its opinion on the draft adequacy decision, which concludes the first step of the adoption process.

- In its opinion, the EDPB welcomes a number of substantial improvements, in particular as regards the new necessity and proportionality requirements and the independence and powers of the new redress mechanism.

- At the same time, the EDPB points to some remaining concerns and requests the Commission to provide additional explanations in the draft adequacy decision.

- We will now carefully analyse the opinion and work to address the comments from the EDPB, before moving to the next phase of the adoption process: seeking the approval from a committee of EU Member States representatives (Comitology).

- A draft adequacy decision is also subject to the scrutiny of the European Parliament, which will express its position in the coming weeks.

- Once this procedure will be completed, the Commission will be able to adopt the final adequacy decision.

- Our expectation is that this decision could be adopted before the summer.

- At the same time, on the US side further work needs to be done to implement the Executive Order in the procedures and internal rules of the various agencies of the US Intelligence Community and to set up the new Data Protection Review Court.

- This is essential for the entry into force of the adequacy decision – which can only happen we all elements are in place. This will also inject further trust into the process while our institutional stakeholders are scrutinising the draft decision.

Hate speech online
Google/YouTube have been among the funders of the Code.

Over time, the Code has achieved fast progress.

After a slowdown in particular on removal rates in 2021, the latest evaluation shows that YouTube is performing well in terms of timely assessment of the user notifications and on the removal rates.

We encourage you to continue on this path of progress and ensure that YouTube’s performance during the monitoring exercises is not exceptional but rather standard throughout the year.

The Digital Services Act introduces a series of measures to reduce the prevalence of illegal content online.

The Code of conduct already represents a fast-track to compliance in relation to several obligations of the DSA. This includes the obligation to set up notice and action mechanisms, the reference to a 24h turnaround time [délai d’exécution] and the need to provide feedback to users.

The requirements of the Digital Services Act for very large online platforms like Google/YouTube are deemed to kick in the course of 2023.

We are therefore looking at further interplay between the DSA and the Code and how the Code can add value to the DSA provisions.

We see the Code of conduct developing as a tool that very large platforms can use to address the specific systemic risks related to the spread of hate speech as well as to limits to freedom of expression.

In this respect, the collaborative approach with civil society and academia should be exploited in full.

As an option we are considering additional commitments to establish a “rapid alert system” on threats on hate speech and freedom of expression which can provide you with alerts on risks happening in national contexts or on certain languages.

A formal consultation with all the platforms part of the Code has started since January 2023. Your preliminary views on this would be welcome.
Meeting with [Redacted], Google's [Redacted]

Brussels, 6 March 2023, 17:00 – 18:00

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
Meeting with [Name], Google’s
Brussels, 6 March 2023, 17:00 – 18:00
Meeting with [redacted], Google's [redacted]  
Brussels, 6 March 2023, 17:00 – 18:00
Meeting with Google's [Redacted]
Brussels, 6 March 2023, 17:00 – 18:00

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]
Meeting with [Name], Google's [Position]
Brussels, 6 March 2023, 17:00 – 18:00

- [Content]
- [Content]
- [Content]
- [Content]
- [Content]
- [Content]
- [Content]
- [Content]
- [Content]
Meeting with [Redacted], Google's [Redacted]

Brussels, 6 March 2023, 17:00 – 18:00
Meeting with [Name], Google's [Title]
Brussels, 6 March 2023, 17:00 – 18:00
Meeting with [redacted], Google's [redacted]
Brussels, 6 March 2023, 17:00 – 18:00

Curriculum vitae [redacted] Google's [redacted]

1 Sources, Google.com and Wikipedia
2 Source https://twitter.com/?lang=en