Scene setter

- The Commission appreciates Google’s proactive approach to engage in a responsible dialogue with EU regulators and policymakers (including data protection and consumer protection authorities).
- The Commission will follow closely the investigation of the Irish DPA.
- From the perspective of consumer protection, BEUC raised a number of concerns about generative AI, including the risks for consumers’ mental health and high risk of unfair
commercial practices.

- It will be essential to **ensure full compliance with EU consumer law** if Google Bard is to be offered in Europe.

- The Commission and the CPC network will be in touch to discuss these concerns, and I am looking forward to our good cooperation in full transparency.

**AI regulation**

**LTT on the AI Act**

- The **AI Act** aims to ensure the **protection of fundamental rights and safety** of individuals. The proposal follows a **risk-based approach**. AI systems considered as high-risk\(^3\) should comply with a set of **requirements** before they can be put on the market and used, to enhance transparency and to minimise risks to safety and fundamental rights\(^4\).

- The new requirements will ensure that **possible breaches of fundamental rights** obligations can be **investigated** and addressed by national authorities and courts. To achieve this, the proposal includes requirements on **documentation and testing** of high-risk AI applications. It also provides for **human oversight** and **reliability and accuracy** of the systems.

- **Compliance with the future AI regulation does not mean that the use of a given AI system would be automatically lawful.** All other rules that would apply to the use continue to apply. For example, the AI Act **does not affect the EU data protection rules** which apply in full where providers and users of AI systems process personal data.

- **State of play:** EU legislators have adopted their position on the AI Act (the Council in December 2022 and the EP in June 2023) and entered into negotiations with the strong determination to adopt the final text before the end of the year.

**LTT on the AI Act and generative AI systems**

- **General Purpose AI systems**, including generative AI, have a multitude of potential applications, which may fall within various risk categories. To assess whether an AI-system is high-risk, the Act uses the concept of “**intended purpose**”, which is a common characteristic of EU product legislation.

- The provider of an AI system will have the responsibility to determine the purpose for which its product is intended to be used. As far as Bard can be directly used, including for high-risk applications, it would therefore have to fulfil the corresponding requirements for high-risk AI systems.

- In addition, the AI Act proposal provides for **specific transparency requirements** for systems used to **generate or manipulate image, audio or video content** that appreciably resembles authentic content. This includes an **obligation to disclose** that the content is generated through automated means, subject to exceptions for legitimate purposes (law enforcement, freedom of expression). This allows persons to make informed choices or step back from a given situation.

- The question of the regulation of generative AI will be a point of **discussion between the EU Co-legislators** and the **requirements might evolve in the final text**. In its position, the European Parliament proposed that **generative foundation models** would have to comply with

---

\(^3\) In areas such as education, employment, access to credits or public assistance benefits, law enforcement, migration and asylum, as well as the justice systems.

\(^4\) These obligations include risk assessment and mitigation systems, datasets governance, traceability, human oversight, robustness, security and accuracy. The requirements will be subject to standardisation.
additional requirements, like designing the model to prevent it from generating illegal content and publishing summaries of copyrighted data used for training.

*LTT on the AI Liability Directive in the context of generative AI*

- The AI Liability Directive (AILD, proposal adopted on 28 September 2022) seeks to ensure the protection of victims of damage caused by AI systems and legal certainty for businesses.
- It is important to increase trust in the technology to support its uptake.
- We want the same level of protection for victims of damages caused by AI than of other technologies.
- This is increasingly important in light of the recent developments in the field of AI, including applications like ChatGPT.
- It is important to have EU norms that promote trustworthy AI, which can then also help to formulate global norms and standards.

*Political advertising initiative*

- We are aware of the concerns you have raised in the context of the ongoing negotiations on the proposed EU regulation for transparency and targeting of political advertising.
- We all agree that we need to provide legal certainty and to ensure transparency and enhanced data protection, to strengthen accountability and deter interference.
- Political advertising can be a vector of disinformation, information manipulation and interference, in particular where the advertising does not disclose its political nature, the identity of its sponsors and the entities financing it, and where and how it was targeted.
• It is of utmost importance that the transparency and targeting requirements are put in place without undue delay, to effectively allow citizens to recognise political advertisements and exercise their democratic rights in an informed manner.

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

• 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.

• 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 as well.

• 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. All that is required is for Google to respond to the notification to inform the notifier about what it will do. It does not have to do anything else.

• 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.

Code of conduct on countering illegal hate speech online

LTT:

• 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.

• The Digital Services Act, entered into force in November 2022, 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 DSA
Meeting with Google

Brussels, 26 June 2023, 14:00

obligations. This includes the obligation to set up notice and action mechanisms, and the need to provide feedback to users.

- We are currently discussing with the IT companies how to update the Code towards a “DSA Code of conduct” to ensure it will add value to the new DSA provisions.

- In particular, we see the Code of conduct developing as a tool which is not only reactive (take down of content) but also supporting very large online platforms to anticipate and address specific systemic risks related to hate speech and freedom of expression online.

- The negotiation process started in March 2023 and is currently ongoing. We hope to be able to announce the new Code in the fall.

- We expect to maintain the most relevant commitments in the existing Code of conduct, notably on notice and action and in particular the turnaround of 24h for the review of notices.

- We also want to ensure that companies in the Code can report in a structured way additional measures they take to identify and address hate speech (e.g. through automatic detection tools).

- Most importantly, we are calling for joint efforts to establish a mechanism whereby platforms can receive timely information on trends and developments on hate speech or threats to freedom of expression on the ground, and react, if necessary, as part of their measures to mitigate systemic risks.

- The negotiation process started in March 2023 and is currently ongoing. We hope to be able to announce the new Code in the fall.

- We expect to maintain the most relevant commitments in the existing Code of conduct, notably on notice and action and in particular the turnaround of 24h for the review of notices.

- We also want to ensure that companies in the Code can report in a structured way additional measures they take to identify and address hate speech (e.g. through automatic detection tools).

- Most importantly, we are calling for joint efforts to establish a mechanism whereby platforms can receive timely information on trends and developments on hate speech or threats to freedom of expression on the ground, and react, if necessary, as part of their measures to mitigate systemic risks.

- Such information exchange would be fed by an EU wide network of stakeholders, including DSA trusted flaggers, civil society organisations and experts from academia. The multi-stakeholder cooperation approach established under the current Code of conduct represents good starting basis, but it needs to be reinforced.

- My services are reporting a very constructive attitude in the negotiations, and I trust it will continue that way. We are sure we can count on YouTube’s leadership, engagement and support to achieve our common ambitious goals.

Cookies Pledge

LTT

- Thank Google for its participation in the cookies pledge initiative and stress that the Commission counts on Google’s continued cooperation.

- The goal of this initiative is to address the issue of ‘cookie fatigue’ and to provide consumers with clearer information and a better understanding of digital advertising models.

- The identified solutions will be part of a pledge that will be voluntary and will not involve
changes to the existing laws.

**Geoblocking issue in Google Play Store**

- **Thank Google for its cooperation with the national consumer authorities**, within the context of the coordinated action of the CPC Network against the company (Google has agreed to address issues raised by the national consumer authorities and the Commission and to introduce changes in Google Store, Google Play Store, Google Hotels and Google Flights).

- **Remind Google that the issue of Geoblocking in Google Play Store remains unsolved.**

- **More specifically**, Google failed to remove restrictions to the use of different national versions of Google Play Store. It still prevents consumers from downloading content hosted in the Google Play Store of another EU country, even when such content should be accessible to them, such as in the case of cross-border travellers and tourists.

- **Urge Google to take all necessary steps and find technical solutions, in order to address this remaining issue and comply fully with the Geo-blocking Regulation.**

**c) Other topics that Google may raise:**

**GDPR enforcement**

- **COM is preparing a proposal** on enforcement of the GDPR in cross-border cases. The initiative aims to streamline cooperation between DPAs in cross-border cases by harmonising some aspects of the administrative procedure applied in such cases.

- **The initiative will not amend GDPR substantial rules** but will focus on harmonising certain procedural elements in order to support the smooth functioning of the GDPR cooperation mechanism and dispute resolution mechanism.

- **The proposal therefore fully maintains and supports the One-Stop-Shop mechanism.**

- **The initiative responds to** a list that the EDPB officially transmitted to COM in October 2022, identifying procedural aspects of the cooperation between DPAs that could be harmonised at EU level.

- **The initiative focuses on the following areas:**
  - Form of complaints and the position of complainants in the procedure;
  - Streamlining cooperation and dispute resolution;
  - Targeted harmonisation of procedural rights of parties under investigation in cross-border cases.

- **A public call for evidence** was issued on 24 February and closed on 24 March. COM has **consulted key stakeholders** through the GDPR Multi-stakeholder Group. In addition, COM has received input from DPAs through the EDPB and from MSs through the Member States GDPR Expert Group.

- **Indicative planning** is to adopt the proposal in **early July 2023.**

**EU-US Data Privacy Framework**

- **The adoption procedure** for the draft adequacy decision on the EU-US Data Privacy Framework is at an **advanced stage**. We are currently discussing the draft with a committee of representatives of EU Member States (comitology), which will have to vote on the draft.

- **We continue to work towards a possible adoption** of the final decision by the **Commission by**
next month, but that the timeline is not entirely in our hands: further work is also required on US side to implement the new safeguards (US intelligence agencies have to update their internal rules and procedures and the US has to ensure that EU citizens have access to the new redress mechanism).

- The draft adequacy decision will only enter into effect once the new legal framework is fully in place on US side.

- Importantly, the safeguards we have obtained will apply to all transatlantic data transfers, regardless of the transfer mechanism used: the future adequacy decision, Standard Contractual Clauses or other tools (e.g binding corporate rules, ad hoc contractual clauses etc.).
Meeting with Google
Brussels, 26 June 2023, 14:00

[Text of the meeting]

[Details of the meeting]

[Agenda or topics discussed]