MEETING WITH [redacted]

Google [redacted]

Scene setter

- You are meeting [redacted] Google [redacted].

Data flows

- **US companies are increasingly putting pressure** ([redacted]) to agree on a successor arrangement to the Privacy Shield as soon as possible. This is fuelled in particular by fear of **upcoming enforcement action by European data protection authorities** (DPAs) after the Schrems II judgment. In the past months, we have started to see the first "post-Schrems II" cases, e.g. the suspension by the Portuguese DPA of the transfer of census data from a Portuguese public authority to the US and cases before the Belgian and French Council of States (insisting on the importance of specific protections, such as encryption).
- The **EDPB is currently also finalising its work on the investigations into the use of** [redacted] by European companies (which were triggered by complaints from [redacted]. Moreover, while it seems that the investigation of the Irish DPA into Facebook's data transfers (which were the subject of the national proceedings that led to the Schrems II judgment) is taking more time than expected, its decision is expected in the coming months.
- **Certain DPAs have also started to issue specific guidance** on the Schrems II judgment. Companies have for instance criticised recent guidance from the Berlin DPA, where it advises companies to switch to providers (referring in particular to cloud service providers) in the EU or countries benefiting from an adequacy decision, and to move personal data stored in the US back to the EU.

Political ads initiative

- You will discuss the proposal for a Regulation on transparency and targeting of political advertising, adopted by the Commission on 25 November 2021.
- Google made some contributions to the consultation for the European Democracy Action Plan and to the transparency initiative.
- Google implements a fairly narrow definition of political ads based on content related to candidates or elections, and pushed for such an approach to be implemented. Its position centred on promoting "in ad" transparency rather than limits or restrictions, though the scope of the transparency it pushed for was quite limited in substance and in scope (it omits organically shared previously paid for content, such as when a person shares a paid-for article or other advert to her friends on social media).
- Google provides limited access to information about political ads at the moment through its ad report[1]. It requires some verification to place a political ad, but it does not have single MS policy like Facebook in 2019.

[1] https://transparencyreport.google.com/political-ads/region/EU

- Google's current policy political ads does not cover all the requirements envisaged under the proposed Regulation. In particular, to comply with the proposal:
  - Google would need to change its approach to include all political actors and a broader range of political advertising liable to affect the outcome of elections, referenda and legislation;
  - Google's policy on the information to be published concerning each ad includes some but not all elements included in the transparency requirements, notably regarding the amounts spent and the targeting information are missing;
  - Google currently permits contextual targeting (which is based on searches and content being accessed eg via its new app). This could be caught by the prohibition. This will be a sensitive point for Google.

Hate speech

- You will present the Commission's response to illegal hate speech online.
- It will be an opportunity to refer to the upcoming Commission initiative to extend the list of "EU crimes" to hate speech and hate crime.
- You may also refer to the Digital Services Act, in particular its interplay with voluntary Codes of the conduct and in the light of the recent revelations by the Facebook whistleblower Frances Haugen.
- You can refer to Google/YouTube's involvement in the Code of conduct on countering hate speech online and their results in the latest evaluation of the Code. YouTube has been a strong supporter of the Code.

Consumer protection cooperation (CPC) action on Google)

- The Commission and Consumer Protection Cooperation (CPC) Authorities, sent a common position to Google in July 2021. They mainly requested more transparency (on its business model, search results and reviews policy) and more clarity on prices and essential pre-contractual information that Google provides to consumers in its various products (Google Hotels and Flights, Google Store, Google Play, Google Search and Ads).
- Welcome that Google engaged in a dialogue with the CPC Authorities and the Commission and sent its reply in October 2021 with proposed changes that could bring its practices in line with EU consumer law. Google's suggestions are currently under assessment and while they seem to go to the right direction, there still leave some points open for further discussion.
- Stress that the Commission expects Google, to take the necessary steps in order to address all the issues raised by the CPC Authorities and contribute to the successful conclusion of this action, as it has also done in the past with the rogue traders action. Otherwise, CPC authorities could enter into a formal procedure under the CPC Regulation.

Product Safety Pledge

- You might use this meeting to invite Google to consider whether their Google Store or the Shop/Ads could qualify to be covered by the Product Safety Pledge.

LTT

Data flows

- The Commission **remains firmly committed to facilitating trusted data transfers**.
- I am thinking for instance of the **adequacy negotiations we recently concluded** with the UK and South Korea – two years after creating with Japan the world's largest area of free and safe data flows.
- We are currently having si**milar talks with a number of partners**, in particular in Asia and Latin America.
- This commitment to international data flows is **also reflected in our approach to trade negotiations**. We are systematically including in the digital trade chapter of all our trade agreements a straightforward prohibition of data localisation requirements. This is what we did for instance in the Trade and Cooperation agreement we concluded at the very end of last year with the UK.
- In other words, we want to make clear that genuine data protection, on the one hand, and digital protectionism, on the other hand, are two very different things.
- **On 4 June 2021, we adopted modernised standard contractual clauses** (SCCs) for international data transfers. These have been fully aligned with the general data protection Regulation (GDPR) and adapted to modern business realities. They also take into account the requirements of the Schrems II judgment and operationalise the clarifications offered by the Court of Justice of the European Union.
- Through their standardisation and pre-approval, these clauses provide companies, especially SMEs, **a practical tool to assist them in complying with the GDPR**.
- Of course, these Clauses **have to be used in accordance with the case-law of the Court of Justice of the EU**, including its Schrems II judgment, and the guidance of the EDPB.
- That is **why we worked closely with the Board to ensure consistency between our respective worksteams**. This is reflected in the final guidance of the EDPB that was also adopted in June, which is better aligned with the approach of the standard contractual clauses (compared to previous EDPB drafts).
- To further facilitate the use of the SCCS, we are **developing a Q&A addressing implementation issues, providing further clarifications etc.** This will be a dynamic, online source of information that will be regularly updated.
- **We are doing this in close cooperation with stakeholders** as we want this to be an as practical as possible tool – based on "real life" situations. For example, we met with a so-called 'multi-stakeholder' expert group established under the GDPR on 29 October to discuss what the Q&A should focus on.
- **With respect to transatlantic data flows**, the most comprehensive solution remains a new adequacy decision, which would allow data to flow without the need for any further authorisation or transfer instrument.
- The **EU and US have been engaged in intense negotiations** in the past months and weeks. I was in Washington DC last months to take stock of the talks.

- We have entered into the substance of the issues [redacted] and are discussing the details of possible solutions.
- What is at stake here are **complex and sensitive issues** that relate to the delicate balance between national security and privacy, **but we have made good progress even if we are not yet there**.
- This **remains a top priority** in Brussels and in Washington DC.
- At the same time, **we will only agree to a new arrangement that is fully compliant** with the Schrems II judgment.
- This is also the **only way to develop a durable solution**, one that ensures the stability and legal certainty that stakeholders expect on both sides of the Atlantic.

Political ads initiative

- Political advertising services in the EU are developing. National regulation of political advertising imposes obligations on providers of political advertising services which condition the availability of political advertising and determine elements of its content to provide specific transparency. Member States 'approach is fragmented creating barriers in the internal market (eg compliance costs etc).
- The overall growth and particularly significant increase in relevant online services, in a context of unevenly enforced and fragmented regulation, has prompted concerns that the internal market is not currently equipped to provide political advertising to a high standard of transparency to ensure a fair and open democratic process in all Member States.
- High transparency standards are necessary to preserve the essential balance in the political process in the face of transformative changes in the provision of such services and in the ways that political actors communicate with the electorate.
- The Commission proposed on 25 November legislation on transparency of sponsored content in a political context ('political advertising'), as part of a package of measures on electoral resilience and democratic participation.
- It complements the Digital Services Act proposal and the existing data protection acquis.
- It provides for a high, harmonised standard of transparency for the provision of political ads services in the EU internal market, and harmonised rules to on the use of targeting and amplification techniques in the context of the publication, dissemination or promotion of political advertising.
- Transparency requirements are addressed to providers of political advertising services, including online platforms, advertising publishers and political consultancies, clarifying their respective responsibilities and providing legal certainty.
- It is based on a broad common definition of political advertising, which includes messages by or on behalf of a range of political actors, as well as messages which are liable to influence the outcome of an election or referendum, a legislative or regulatory process or voting behaviour.
- It covers all kinds of advertising, from traditional offline media like print, radio and television, to streaming video, social media and even influencers. It does not cover purely personal or purely commercial messagesfrom a political actor.
- Transparency requirements apply when a political advertising service is involved in the political ad. This excludes situations where an online intermediary service is used without payment, such as a person posting to an online blog. But if that person is paid to do so, then the transparency obligations are involved.
- When service providers provide services connected to political ads, they will need to retain certain essential information about their services, and to provide these to publishers, and, on request, to specific interested entities and national authorities.
- The transparency requirements require political ad publishers to ensure that all political advertising is marked as such and accompanied by a transparency notice, to enable the wider context of the political advertisement and its aims to be understood –

this includes information about the sums of money paid for the advertising and their sources, as well as information about targeting.

- Once an advertisement is indicated as being political advertising, this should be clearly indicated to other service providers involved and, its further dissemination should still comply with transparency requirements.
- Very large online platforms will also need to retain the ads and the transparency notices in the repositories foreseen by the DSA.
- These measures will support the development of the internal market in such services, enable cross-border campaigning, and ensure a high standard of transparency to support oversight and accountability.
- Personal data is increasingly used in the context of political advertising. It can be used in targeting and amplification techniques and can have certain specific negative effects on individuals, especially when used untransparently and on the basis of sensitive data.
- The proposed Regulation will prohibit the targeting and amplification of political advertising using sensitive personal data, except in two specific conditions (the explicit consent of the data subject, or for certain bodies such as political parties for their members or persons they are in regular contact with).
- It will also provide additional safeguards compared to the existing acquis. When using personal data in the context of targeting or amplifying political ads, data controllers will have to provide data subjects with specific information about the sources and types of data used, the nature and purpose of the targeting and logic used, including the size of the audience and the criteria used, and information about the exercise of their data protection rights, including effective means to refuse and withdraw consent.
- Political ad publishers will need to also make sure that this information is included in transparency notices published with the ads.
- These measures should encourage transparent and compliant use of personal data in this context, empower citizens, strengthen monitoring and enforcement and support accountability. They should discourage manipulative technologies and interference.
- Further, Citizens will be empowered to indicate to publishers when they encounter political ads which are problematic. Publishers of political advertising will need to provide a mechanism to support this, and to take reasonable steps to respond.
- In order to support their oversight function, Member State authorities and vetted/auhorised interested parties will be empowered to request relevant information from service providers about the political advertising services they provide. Member State authorities will also be supported in cooperating in cross-border monitoring and enforcement, including through single points of contact and a strengthened European Cooperation Network on Elections.

Hate speech

- The fight against racism and xenophobia and its manifestations of hate speech is a key priority for this Commission.
- Hate speech is illegal according to EU law and what is illegal off line should have no place online.
- The 2008 Framework Decision criminalises public incitement to violence or hatred on grounds of race, colour, religion, descent or national or ethnic origin.
- In December, the Commission will adopt an initiative which aims to trigger a Council Decision extending the current list of so-called 'EU crimes' in the Treaty to hate crime and hate speech.
- This would enable the Commission, in a second stage, to propose a strong common legal framework to tackle hate speech and hate crime across the EU.
- In addition, the Commission's hate speech toolbox also contains effective policy measures.
- As an example, and to face the challenges of online hatred, in 2016 the Commission has initiated a voluntary Code of conduct.
- Google/YouTube have been among the funders of the Code.
- Over time, the Code has achieved fast progress on removing online hate speech. We have seen removal rates go up from only 28% in our first monitoring in 2016 to a removal rate around 70%. A large majority of the notices are reviewed within the 24h prescribed by the Code.
- According to the latest evaluation published in October 2021, YouTube is performing very well in terms of timely assessment of the user notifications.
- Yet, we have noticed a decrease in the take down rate [from nearly 80% to 59%] and we have a dialogue in place with YouTube to understand the reasons of this and address any needed improvement.
- As you probably know, the Code has also created spaces of cooperation and dialogue between IT Companies and civil society fostering in particular trusted flagger programmes and joint awareness raising campaigns against hate speech online.
- We intend to reinforce in the coming months the exchange and cooperation between NGO/trusted flaggers and the platforms' trust and safety teams.
- As we have heard from the Facebook whistle-blower Frances Haugen, there is room to improve content moderation and to address risks of amplifying illegal content and algorithms producing harm to our democratic processes.
- She also called for strong EU legislation in the field of illegal content online.
- In December 2020 the Commission has adopted a proposal for the Digital Services Act.
- The Digital Services Act proposal introduces a series of measures to reduce the prevalence of illegal content online. Users and trusted flaggers will be empowered to report illegal content, in an easy and effective way.

- Very large online platforms will need to fix their vulnerabilities for amplifying harmful behaviours, in particular against vulnerable groups.
- We have also proposed measures to increase transparency and mechanisms for users to complain against the decisions of the platforms on content moderation.
- And – importantly - these horizontal rules against illegal content are carefully calibrated and accompanied by robust safeguards to respect freedom of expression and an effective right of redress.
- We are currently having constructive discussions with the participants in the Code on how to make the tool fit for the current challenges on countering hate speech online and the possible provisions of the DSA.

DEFENSIVES

Data flows

The Commission and the US should agree on a new framework as soon as possible, to ensure continuity of transatlantic data transfers.

- The Commission and the US Department of Commerce are engaged in discussions on developing a successor arrangement, in full compliance with the Schrems II judgment.
- We are ready to discuss (creative) ways to comply with the requirements of the Court, but we also have to recognise that the judgment raises complex issues. Moreover, we need to get this right if we want to develop a sustainable framework for EU-US data flows. This is in our mutual interest. What therefore matters for us is that any possible solution is in full compliance with the Court's judgement. This is a question of respect for the rule of law and it is an essential condition to create legal certainty for companies on both sides.

For the new arrangement for transatlantic data flows solutions that would not require legislative change in the US should be relied upon.

- The Schrems II judgment provides the Commission's mandate for the negotiations with the US.
- This means that any possible solution will need to have in place limitations on the collection of data, ensure access to court and provide for enforceable individual rights.
- What matters for us is the outcome. Regardless of the type of solution, and whether or not it requires legislative reforms, it should be clear that it must be in full compliance with all requirements of the judgment.

We are concerned about calls for data localisation.

- We have repeatedly confirmed the Commission's commitment to facilitate data flows. This is reflected in our ambitious agenda on facilitating trusted data transfers.
- For instance, we recently concluded adequacy negotiations with South Korea and the UK, two years after having created the world's largest area of free and safe data flows with Japan. We are in talks with several other countries, in particular in Asia and Latin America.
- We actually believe that there are many more opportunities today than even a few years ago to promoted trusted data flows. This is a direct result of the (upward) convergence trend in privacy we are observing in many parts of the world. It's much easier to facilitate data flows between systems that speak a similar (not an identical) language.
- Our commitment to data flows is also reflected in the approach we are taking in our trade negotiations, at both the bilateral (current FTA negotiations with countries such as Australia, New Zealand, Indonesia, Chile, Tunisia etc.) and multilateral (ecommerce negotiations at the WTO) level.
- For example, in the trade agreement with the UK, we included a straightforward prohibition of data localisation requirements and an emphasis on the importance of data flows.
- We want to make very clear that genuine data protection, on the one hand, and digital

protectionism, on the other hand, are two very different things.

- Developing strong privacy safeguards and promoting the free flow of data are not opposite objectives but complementary.
- The EU is also actively participating in the multilateral conversation on data flows – in the OECD; the G7 and the G20. The latter in particular under Japan's leadership and under the Osaka track with 'data free flow with trust' as the central underlying concept.

We are concerned about the uncertainty created by the Schrems II judgment, which is further fuelled by the very strict guidance of the data protection authorities

- We understand the need for practical guidance and therefore worked closely with the EDPB, which issued detailed guidance on 18 June 2021.
- In our own work on standard contractual clauses, which are the most used tool for international data transfers, we have operationalised some of the clarifications provided by the Court, which we believe provide a helpful toolbox to assist companies in their compliance efforts.
- While we were finalising the clauses, we also worked closely together with the EDPB to ensure consistency between our approaches.

Political ads initiative

Will citizens see a difference to political ads?

- Yes they will. With every advertisement citizens will hear or see:
    - A clear statement that the advertisement is political;
    - the identity of the sponsor of the political advertisement, including any the entity controlling the sponsor;
    - a transparency notice or a clear indication of where it can be easily retrieved.
- The transparency notice is an important element as it will include information, which will allow people to understand the wider context of the political advertisement and its aims. It will include:
    - the identity of the sponsor and contact details;
    - the period during which the political advertisement is intended to be published and disseminated;
    - information on the aggregated amounts spent or other benefits received in part or full exchange for the preparation, placement, promotion, publication and dissemination of the relevant advertisement, and of the political advertising campaign where relevant, and their sources;
    - where applicable, an indication of elections or referendums with which the advertisement is linked;
    - where applicable, links to online repositories of advertisements;
    - information on the mechanism for citizens to indicate political advertising which may not comply with the Regulation;
    - where applicable, information about how the advertising is targeted and amplified
- Citizens will also be empowered to indicate when they encounter problematic political advertisements not complying with the Regulation

How will people know they are looking at a political ad and why?

- This initiative aims to establish high standards of transparency in the provision of political advertising services, and to strengthen the protection of fundamental rights in this activity.
- Specifically, this means that with every advertisement citizens will hear or see:
    - A clear statement that the advertisement is political
    - the identity of the sponsor of the political advertisement, including any the entity controlling the sponsor
    - a transparency notice or a clear indication of where it can be easily retrieved
- The transparency notice is an important element in the transparency to be provided to citizens. It will include information to enable the wider context of the political advertisement and its aims to be understood. It will include:

- the identity of the sponsor and its contact details;
- the period during which the political advertisement is intended to be published and disseminated;
- information on the aggregated amounts spent or other benefits received in part or full exchange for the preparation, placement, promotion, publication and dissemination of the relevant advertisement, and of the political advertising campaign where relevant, and their sources;
- where applicable, an indication of elections or referendums with which the advertisement is linked;
- where applicable, links to online repositories of advertisements;
- information on how to use the mechanism established by the Regulation to allow citizens to indicate political advertising which may not comply with the Regulation
- where applicable, information about how the advertising is targeted and amplified

Do the rules apply for online actors as well as offline ones?

- Yes, these new measures on transparency and on targeting are designed to apply regardless of the medium used for political advertising. The rules are formulated in such a way as to be technology neutral, hence adaptable to any existing medium but also future ones.
- The rules further apply to 'offline' actors in the sense that, beyond the online (and offline) publishers of political advertising, actors providing political advertising services (such as ad agencies, PR firms, designers) are also in scope.

How do we move forward to close the gap between offline and online campaigning?

- The gap is caused by legislation and enforcement, which is not adapted to the online environment, and did not anticipate the cross-border element that this also creates. It can result in legal uncertainty and problems for political actors, but it can also represent loopholes which open the ground to political ads being misused, causing distortion to the democratic debate.
- We have therefore proposed measures that pursue the following aims:
    - support the creation of a single market for services in the EU by providing for high transparency standards and defined requirements for the use of personal data in the context of political advertising for relevant service providers, EU political parties and other political actors;
    - help improve the resilience of our democracies; and
    - reduce the opportunity for interference in elections in the EU.
- Elections are a national lead, but in electoral advertising, especially in the context of the digital transformation, we can already see that there is a great deal of applicable EU law.
- The European Democracy Action Plan recognises the need for more transparency in political advertising, and the commercial activities surrounding it, in order for citizens, civil society and responsible authorities to be able to see clearly the source and purpose of such advertising.

- The current proposal on the transparency and targeting of political advertising represents a significant step forward in this respect.

Who is covered by the new rules? Ad companies, like Google Ads, but what about bloggers and newspapers? Does this regulation also cover private persons or only political parties and foundations?

- The requirements concerning the transparency of political advertising established by the new rules will apply to the providers of political advertising services.
- This includes all services consisting of the preparation, placement, promotion, publication or dissemination, by any means, of a message by, for or on behalf of a political actor, unless it is of a purely private or a purely commercial nature; or which is liable to influence the outcome of an election or referendum, a legislative or regulatory process or voting behaviour.
- This would include newspapers and other traditional media such as radio and television when they are publishing political advertising, but also bloggers and influencers when they are paid to present political messages. It would also cover, for instance, new websites which provide paid-for content which meets the new definition.
- This could also include, for instance, Google when it provides political ads through its search services, or Facebook when it displays political ads to its users.
- However, the rules about the transparency of advertising will not be engaged in the context of online intermediary services which are provided without consideration for the placement, publication or dissemination of a specific message, unless the user has been remunerated by a third party for the political advertisement.
- This means that individual's personal social media posts will not fall under the definition of political advertising, unless they have been paid to make political posts.
- The requirements concerning the targeting and amplification of political advertising apply to anyone who uses personal data to target or amplify political advertising using personal data. This would cover in many instances service providers, but also other actors like European political parties.

What about if individuals endorse a piece of info (on TT or FB) that is a political ad – will they then be responsible too?

- The new rules should not apply to messages shared by individuals in their purely personal capacity.
- However, individuals should not be considered as acting in their personal capacity if they are publishing messages the dissemination or publication of which is paid for by another.
- Obligations could be engaged, including those concerning targeting and amplification, if someone were to pay for the individual's endorsement to be targeted or boosted.

Why is non-paid-for, partisan material that citizens see organically excluded?

- The new regulation is based on a broad common definition of political advertising, which could include partisan material, but the rules that it introduces only impose obligations regarding transparency in connection with a political advertising service, or regarding targeting and amplification when personal data is processed in connection with political advertising.

- The new rules should not apply to messages shared by individuals in their purely personal capacity. This is not the case when individuals are publishing messages the dissemination or publication of which is paid for by another.
- Transparency requirements apply when a political advertising service are involved in the political ad. This excludes situations where an online intermediary service is used without payment, such as a person posting partisan content on an online blog. Where that person is paid or where other paid services are provided, such as boosting or targeting, would the transparency obligations be involved.
- Also, once an advertisement is indicated as being political advertising, this should be clearly indicated to subsequent other service providers involved and, its further dissemination should still comply with transparency requirements. Therefore, if sponsored content is shared organically, the advertising should still be labelled as political advertising.
- The rules governing targeting and amplification of political messages apply when the use of such techniques involve the processing of personal data.

What will people be able to find about political ads on the ad libraries of very large platforms like Facebook?

- Very large online platforms will be required to manage and update a repository with all the political ads that they publish, which will be publicly available
- Citizens will be able to see in the repository the following information linked to each political advertisement:
    - the content of the advertisement;
    - the person on whose behalf the advertisement is displayed;
    - the period during which the advertisement was displayed;
    - whether the advertisement was intended to be displayed specifically to one or more particular groups of recipients of the service and if so, the main parameters used for that purpose;
    - the total number of recipients of the advertisement
    - information on the money spent on the advertisement,
    - an indication of the elections to which the advertisement is linked to
    - information on the mechanism for citizens to indicate political advertising which may not comply with the Regulation;

How is this proposal articulated with the recent DSA proposal and why is it necessary to have additional rules in the field of political advertising?

- This initiative will complement the proposal for a DSA, which the Commission announced in December 2020.
- The DSA proposes horizontal obligations on online intermediaries, especially for very large online platforms, to provide certain information about all online advertising. This includes ad libraries and the provision of information about targeting.

- The political ads initiative proposes general transparency obligations for all actors involved in the preparation, publication, placement, promotion and dissemination of political advertising, offline and online.
- Compared to the DSA, it expands the categories of information to be disclosed in the context of political advertising, as well as the scope of the relevant service providers concerned.
- While the DSA imposes transparency requirements on online platforms, the political advertising initiative covers the entire spectrum of political advertising publishers, as well as other relevant service providers involved in the preparation, placement, publication and dissemination of political advertising.

How will this legislation address attempts from outside the EU to interfere in elections?

- This initiative applies to all to political advertising prepared, placed, published or disseminated in the Union, or directed to individuals in one or several Member States, irrespective of the place of establishment of the advertising services provider, and irrespective of the means used. Moreover, organisations which provide political advertising services in the European Union which do not have a physical presence here will have to designate a legal representative in one of the Member States where the services are offered. This will ensure more transparency and accountability of services providers acting from outside the Union.

How is this legislation going to mitigate the risk that stems from Facebook and other platforms taking on such an important role in political campaigns? Will the Commission's political ads initiative solve the Facebook policies issue?

- This initiative provides harmonised rules on transparency of political advertising, which will increase legal certainty and mitigate the risk and costs resulting from the fragmentation of the relevant framework at Member States level.
- It will also provide harmonised rules on the use of targeting and amplification techniques in the context of the publication, dissemination or promotion of political advertising that involve the use of personal data, further clarifying the obligations of online platforms such as Facebook.
- Legal certainty will support the provision of political advertising services in the internal market, including when campaigns are organised at the European level. It should remove the need for policies which create obstacles to cross-border campaigning.

Will this legislation restrict free speech or ban certain content?

- Beyond the requirements for transparency and targeting, the initiative does not interfere with the substantive content of political messages.
- Since advertisements by, for or on behalf of a political actor cannot be detached from their activity in their role as political actor, they can be presumed to be liable to influence the political debate, except for messages of purely private or purely commercial nature.

- Also, in full respect of freedom of expression as protected by Article 11 of the Charter of Fundamental Rights, this Regulation should not apply to messages shared by individuals in their purely personal capacity.
- The obligations under the regulation connected to political advertising are only engaged in connection to the processing of personal data, or if political advertising services are involved.
- In particular, the transparency rules should only apply to political advertising services, i.e. political advertising that is normally provided against remuneration, which may include a benefit in kind. The transparency requirements should not apply to content uploaded by a user of an online intermediary service, such as an online platform, and disseminated by the online intermediary service without consideration for the placement, publication or dissemination for the specific message, unless the user has been remunerated by a third party for the political advertisement.

Will targeting be banned?

- Political targeting and amplification techniques using special categories of personal data will be banned – unless a person explicitly consents to it. Special categories of personal data may also be used in the context of political advertising in the course of the legitimate activities of organisations with a political, philosophical, religious or trade union aim in a very limited number of situations, such as when it is about their own members.
- Anyone making use of political targeting and amplification involving the processing of personal data will also need:
  - o to adopt and implement an policy on the use of such techniques
  - o to keep records of the techniques used and sources of personal information
  - o provide the person being targeted additional information concerning the targeting or amplification, including:
    - the specific groups of recipients targeted,
    - the parameters used to determine the recipients to whom the advertising is disseminated (with the same level of detail as used for the targeting),
    - the categories of personal data used for the targeting and amplification,
    - the targeting and amplification goals, mechanisms and logic including the inclusion and exclusion parameters and the reasons for choosing these parameters
    - the period of dissemination, the number of individuals to whom the advertisement is disseminated and indications of the size of the targeted audience within the relevant electorate.
    - the source of the personal data use, including, where applicable, information that the personal data was derived, inferred, or obtained from a third party and its identity as well as a link to the data protection notice of that third party for the processing at stake;
    - a link to effective means to support individuals' exercise of their rights under EU data protection rules.
- Publishers of political ads will need to ensure that this additional information about the targeting of political advertising they publish is included in the transparency notices they make available with the political advertising

Why is micro-targeting not prohibited altogether in the context of political advertising?

- With the new proposal, targeting or amplification techniques in the context of political advertising based on sensitive personal data if prohibited. This means that the targeting and amplification of political advertising on the basis of sensitive data including ethnic origin, political opinions, sexual orientation or religion will be prohibited. There are two exceptions to this where explicitly consented to by the data subject, or for certain bodies such as political parties for their members or persons they are in regular contact with.
- When using targeting or amplification techniques that do not process sensitive personal data, controllers will still need to comply with enhanced safeguards, which include providing information together with the ad being targeted or amplified on the size of the population being targeted. This will increase the transparency and accountability of the use of targeting and amplification and will allow citizens to discern when they are being the subject of such techniques.

What is the scale of the issue? How prevalent is disinformation in European elections? Have there been any cases like Cambridge Analytica recently?

- Disinformation is an issue which came dramatically to the public eye following the Cambridge Analytica revelations, and which has continued to present challenges to EU citizens and our democracies, including though the infodemic which accompanied the coronavirus pandemic.
- The Commission has adopted a number of initiatives since 2018 to tackle disinformation, including the Action Plan against Disinformation and the electoral package for the 2019 European elections.
- The Commission assessed the implementation of the electoral package in its report on the 2019 elections, including from the perspective of efforts to combat disinformation. This evaluation, and experience with coronavirus related disinformation, contributed to the European Democracy Action Plan, which included concrete measures to promote free and fair elections and strong democratic participation; support free and independent media; and counter disinformation.
- The proposed regulation delivers on the priority to promote free, fair and resilient electoral processes. It does the not seek to regulate the substantive content of political advertising, beyond ensuring a high standard of transparency in the provision of political advertising services in the internal market, and the requirements as regards targeting and amplification.
- The transparency and targeting and amplification requirements will nevertheless target some of the methods used to disseminate disinformation, as well as supporting better monitoring and accountability.
- This is particularly important in the context of the growing political advertising market, especially online.

How do we moderate the content of political advertising to avoid manipulation and disinformation whilst preserving freedom of expression, freedom of the press and media pluralism?

- The current proposal does not concern the moderation of the content of political advertising.

- Nothing in the proposed regulation should be understood as imposing a general monitoring obligation on intermediary service providers for political content shared by natural or legal persons, nor should they be understood as imposing a general obligation on intermediary service providers to take proactive measures in relation to illegal content or activities which those providers transmit or store
- The results of the democracy section in our 2021 Eurobarometer show that 51% of its respondents report that they have been exposed to disinformation online. This can have negative effects on democratic discourse and trust in our institutions.
- However, when fighting disinformation, the EU's work remains firmly rooted in European values and principles, including upholding freedom of expression and people's right to access legal content.
- This initiative does not regulate the content of political advertising beyond providing for high transparency standards so that citizens can recognise political ads as such, and understand their aims and context.

How is the regulation to be supervised and enforced?

- National data protection authorities designated to supervise and enforce EU data protection rules will also take the targeting and amplification requirements of the current proposal into account.
- Member States will designate competent authorities to supervise and enforce the other provisions of the proposal, and will also provide for proportionate and effective sanctions.
- Member States will ensure that competent authorities coordinate their tasks nationally, and cooperation will be supported at the European level to ensure cross-border enforcement via single national contact points.
- Contact points shall meet periodically at Union level in the framework of the European Cooperation Network on Elections to facilitate the swift and secured exchange of information on issues connected to the exercise of their supervisory and enforcements tasks pursuant to this Regulation

Are you going to introduce any measures affecting directly the national electoral process/national political parties?

- Member States are responsible for organising national elections and for establishing the rules applicable to national political parties, in accordance with their constitutions and relevant international commitments and standards, such as those provided by the Council of Europe and the Organization for Security and Cooperation in Europe.
- There can be EU law applicable to national elections and political parties, such as data protection rules – including the requirements on targeting and amplification in the current proposal – and the rights extended to mobile EU citizens when participating in municipal or European elections in their country of residence.
- Moreover, the current proposals, while not addressed to national political actors (except when they process personal data to target political advertising), will support Member State authorities in the monitoring and enforcement of national electoral processes.

GPSR

Meeting with [redacted], Google

1 December 2021- 15:00

How does the GPSR cover software? Does the product definition cover software?

- The GPSR establishes new provisions to **regulate the relations between software and physical product,** in particular the case of software updates and substantial modifications.
- **The definition of product remains open enough to cover software**. This is also ensuring that the GPSR is future proof.

Does the manufacturer remain responsible for the safety of the product if its product has been modified by a software update?

- Yes, unless the software update entails a substantial modification fulfilling the criteria established in the GPSR:
    - A change in the functionality of the product.
    - A modification of the level of risk or hazard.
    - A new placing on the market.
- For example, if an app aimed to improve the efficiency of a battery is downloaded into a device and consequently the hazards of the device increase, the software developer would become the responsible actor. That would ensure that actors in charge of substantial modifications take into account the impact of their changes in a specific product. In any case, this would not apply for most software updates, such as the download of games that do not interfere with the safety of a device.

Meeting with [redacted], Google

1 December 2021- 15:00

BACKGROUND

Standard Contractual Clauses

The standard contractual clauses (SCCs) are model data protection clauses that an EU-based exporter of data and a data importer in a third country can decide to incorporate into their contractual arrangements (e.g. a service contract requiring the transfer of personal data) and that set out the requirements related to appropriate safeguards. These SCCs can be used as a tool for transfer of personal data to countries outside the EU that are not subject to a Commission adequacy decision.

SCCs represent by far the most widely used data transfer mechanism for EU companies that rely on them to provide a wide range of services to their clients, suppliers, partners and employees. Their broad use indicates that, through their standardisation and pre-approval, SCCs are an easy-to-implement tool for businesses to meet data protection requirements in a transfer context and are of particular benefit to companies, especially the SMEs that do not have the resources to negotiate individual contracts with each of their commercial partners. The SCCs are of general nature and are not country specific.

The SCCs that had been adopted under the previous data protection regime (the data protection Directive) had to be modernised and on 4 June 2021, the Commission adopted new SCCs. Compared to the previous ones, the modernised SCCs:

- have been updated in line with new GDPR requirements;
- provide one single entry-point covering a broad range of transfer scenarios, instead of separate sets of clauses;
- provide more flexibility for complex processing chains, through a 'modular approach' and by offering the possibility for more than two parties to join and use the clauses;
- contain a practical toolbox to comply with the Schrems II judgment.

For controllers and processors that are currently using previous sets of standard contractual clauses, a transition period of 18 months is provided.

Negotiations on a successor to the privacy shield

Immediately after the invalidation of the Privacy Shield by the Schrems II judgment, the EU and US expressed strong willingness to work on a new, strengthened framework[2]. In a joint press statement, Commissioner Reynders and Secretary of Commerce Raimondo announced that the EU and US are intensifying their negotiations[3].

While we are seeing a willingness across the Biden administration to engage [redacted], the issues that have to be addressed are very complex and concern the delicate balance between privacy and national security. At the same time, the only way to ensure stability of data flows and deliver the legal certainty stakeholders are expecting is to develop a new arrangement that is fully compliant with the Schrems II judgment, which may take some time.

[2] https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en.
[3] https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1443.

The Commission and US Administration are currently discussing possible solutions to address the issues raised by the Court (in particular on the limitations to intelligence surveillance (necessity/proportionality) and individual redress). Progress has been made, but it is still too early to say whether they will allow us to come to an arrangement that would satisfy the Court's requirements (and thus withstand likely court challenges).

EDPB Recommendations on supplementary measures

On 18 June 2021, the EDPB adopted the final version of its 'recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data', which provide an overview of the steps companies have to take following the Schrems II ruling when using tools such as standard contractual clauses. This is the version after the public consultation, which ended in December 2020.

The main change in the recommendations (compared to the version that was published in the fall) concerns the approach of the EDPB to the factors that companies can take into account when assessing whether sufficient protections are in place for their transfers. According to the first version of the recommendations, this assessment would only have to take into account the scope of relevant laws in the third country of destination, i.e. whether the data importer would be subject to those laws.

This would have meant that data importers that fall within the scope of third country legislation but in practice never receive government access requests would still need to put in place supplementary measures, or would no longer be able to receive data from the EU. This was heavily criticised by stakeholders, who expressed a preference for the approach of the draft SCCs (as they were published in November), which included the relevant practical experience of companies with prior requests (or the absence thereof) as one of the factors to be taken into account in this assessment. The final version of the recommendations contains more nuanced wording, allowing companies to take into account their practical experience with government access requests. The language is overall aligned with the final SCCs.

The language of the recommendations has also been nuanced on several other aspects, e.g. on some of the so-called 'use cases', i.e. examples of situations for which the EDPB has identified/has not managed to identify possible supplementary measures. For example, the revised recommendations no longer contain an example that requires companies transferring data to countries benefiting from an adequacy decision to put in place supplementary measures if their data would be 'routed' via a another third country where it may be subject to disproportionate government access.

At the same time, the two 'negative' use cases, i.e. examples of situations where the EDPB was not able to identify any solution that would allow companies to continue transferring personal data to a third country where it would be subject to disproportionate government access, have been maintained. These examples were heavily criticised by stakeholders, as they concern two scenarios that are very common in the commercial sector. First, the scenario where EU companies use cloud providers (or other service providers) in a third country that need to have access to 'clear', unencrypted data. Second, the scenario where an EU company shares clear, unencrypted data with a commercial partner outside the EU for common business purposes (e.g. within a corporate group). However, given that the final recommendations allow companies to take into account their practical experience, companies in those scenarios will now be provided with more flexibility and could still transfer data if they conclude that the data importer/the transferred data will in practice not be subject to government access requests (whereas under the first version, such data transfers could never take place as long as the non-EU company fell within the scope of disproportionate surveillance laws, regardless of whether or not access requests are received in practice).

Political ads initiative

- **Google's policy on political advertising**

	Proposal	Google	Delta
Definitions	'political advertising' means the preparation, placement, promotion, publication or dissemination, by any means, of a message: (a) by, for or on behalf of a political actor, unless it is of a purely private or a purely commercial nature; or (b) which is liable to influence the outcome of an election or referendum, a legislative or regulatory process or voting behaviour.	In the EU, election ads include ads that feature: a political party, a current elected officeholder, or candidate for the EU Parliament a political party, a current officeholder, or candidate for an elected national office within an EU member state. Examples include members of a national parliament and presidents that are directly elected a referendum question up for vote, a referendum campaign group, or a call to vote related to a national referendum or a state or provincial referendum on sovereignty Note that election ads don't include ads for products or services, including promotional political merchandise like t-shirts, or ads run by news organizations to promote their coverage of referendums, political parties, candidates, or current elected officeholders.	The Google definition is roughly aligned to the political actor point (a) limb of the COM proposal. To the extent that it also covers content raising election/referendum questions, it also partly corresponds to the second, but there are differences, and Google will need to make changes to implement the COM approach.
Obligations	**Publish in each ad:** - Statement that it is political - Identity of the sponsor	**All ads:** Labelling obligation + "About this Ad", which gives people additional	The google policy includes some but not all elements included in the transparency requirements, notably

	- Transparency notice or link to it, which includes: o the identity of the sponsor and contact details; o the period during which the political advertisement is intended to be published and disseminated; o information on the aggregated amounts spent or other benefits received in part or full exchange for the preparation, placement, promotion, publication and dissemination of the relevant advertisement, and of the political advertising campaign where relevant, and their sources; o where applicable, an indication of elections or referendums with which the advertisement is linked; o where applicable, links to online repositories of advertisements; o information on the mechanism for citizens to indicate political advertising which may not comply with the Regulation; o where applicable, information about how the advertising is targeted and amplified	transparency into why they are seeing an ad, shows them the verified name of the advertiser behind each ad, and provides options to immediately "block" or "repo" the ad. **Political content ads :** Election ads in the EU may run only if the advertiser is verified by Google. For regions where election ad verification is required, all election ads must show a disclosure that identifies who paid for the ad. For most ad formats, Google will automatically generate a "Paid for by" disclosure, using the information provided during the verification process. Please note that this disclosure is not a replacement for any other disclosures you may be required to include in your ad by law.	regarding the amounts spent and the targeting information. Also as regards scope, it is not clear that Google includes all of its "Google Ads" business into the repositories, or whether only ads directly placed via Google ads (and not placed via an intermediary service) are included. These obligations would be clarified under the transparency regulation.

Restrictions	The proposed Regulation will **prohibit** the targeting and amplification of political advertising using sensitive personal data, **except in two specific conditions** (the explicit consent of the data subject, or for certain bodies such as political parties for their members or persons they are in regular contact with	Election ads in the EU may run only if the advertiser is verified by Google. Only the following criteria may be used to target election ads in regions where election ad verification is required: - Geographic location (except radius around a location) - Age, gender - Contextual targeting options such as: ad placements, topics, keywords against sites, apps, pages and videos All other types of targeting are not allowed for use in election ads.	The COM proposal includes an obligation to take reasonable steps to ascertain the political nature of political ads and to obtain the information required by publishers. Regarding targeting – contextual targeting can still fall under the category of inferred personal data and should be subject to the provisions – this will be a contentious point with Google.

- **Democracy package**

During the elections to the European Parliament of 2019, European political parties encountered difficulties when trying to campaign across borders and the European Parliament has called for reform. The swift move of the political debate to the online environment also stimulated the growth of the market for online political advertising, on which European political actors in Europe spent EUR 23 million in relation to the elections to the European Parliament of 2019.

These challenges call for a new effort to strengthen the trust in our democratic systems. Protecting free and fair elections is a political priority of this Commission. The European Democracy Action Plan ('EDAP') set out steps the Commission plans to take to strengthen democracy , building on experience from the 2019 European Parliament elections and drawing on the work of the European Cooperation Network on Elections ('EU Network on elections') , as well as on the EU Citizenship Report 2020 .

The democracy package includes a proposal for a Regulation on transparency of political advertising, two proposals recasting the Directives on the electoral rights, a proposal to recast the Regulation on the statute and funding of the European political parties and European political foundations, and announces a joint mechanism for electoral resilience.

The package is composed of following main elements:

1. **Proposal for a regulation on transparency and targeting of political advertising**. It aims to contribute to the proper functioning of the internal market for political advertising by laying down harmonised rules for a high level of transparency of political advertising and related services. These rules will apply to providers of political advertising services. It also aims to protect natural persons with regard to the processing of personal data by laying down rules on the use of targeting and

amplification techniques in the context of political advertising. These rules will apply to all controllers -i.e., beyond providers of political advertising services, making use of such targeting and amplification techniques. It also provides supporting measures to ensure that supervision and enforcement of these rules is effective and coordinated among Member States.

2. **Proposal to recast Regulation 1141/2014 on the statute and funding of European political parties and foundations**, to provide clearer rules on the funding of European political parties. It seeks to increase the financial viability of European political parties and foundations, facilitate their interactions with their national member parties, close the remaining loopholes regarding transparency, in particular in relation to donations, cut excessive administrative burden and increase legal certainty. It also aims at clarifying that nothing should prevent European political parties from campaigning cross-border within the EU, which is central to their role. This proposal will also include the amendments aimed at establishing specific transparency requirements for European political parties when making use of political ads.
3. **Proposal to recast Directives 93/109/EC and 94/80/EC** on the right of mobile EU citizens to vote and stand in European parliamentary and municipal elections, respectively in their Member State of residence. The existing legal framework will be updated with measures which will improve how mobile EU citizens access these democratic rights, the information they receive about participating in relevant elections, and how Member States work together, including to combat dual voting.
4. The Commission is also taking action to **strengthen cooperation on electoral resilience**, including through its European Cooperation Network on Elections, which will be strengthened and will offer to the Member States a 'joint mechanism for electoral resilience' as of 2022 to support deployment of joint expert teams and expert exchanges with the aim of building resilient electoral processes, in particular in the area of online forensics, disinformation and cybersecurity of elections.

Hate speech

The Code is signed by Facebook, Instagram, Twitter, YouTube, Dailymotion, Snapchat, jeuxvideo.com, and recently TikTok (September 2020) and LinkedIn (June 2021). The results of the evaluation have shown a continuous improvement until 2020. In 2016, only 28% of content was removed, while it was over 70% in 2020; today 81% of the notices are reviewed within 24h versus 40% when the Code was signed. The most recent evaluation of October 2021 shows slight decrease in the average removal rates (62.5%). Similarly, the YouTube's removal rates have been lower. Some differences among the platforms persist (Twitter removes less content than Instagram, Facebook and YouTube for example). In relation to the cooperation with civil society organisations, the IT Companies since 2016 have built larger networks of "trusted flagger" NGOs and have engaged with them also on counter narrative and awareness raising campaigns.

General Product Safety Regulation and Google's position on the proposal:

On 30 June 2021, the Commission adopted a proposal for a new General Product Safety Regulation (GPSR) aiming at updating and modernising the general framework for the safety

of non-food consumer products to preserve its role as a safety net for consumers and ensure a level-playing field for businesses.

Google sent a separate feedback to the Commission during the draft Inception Impact Assessment state (September 2020). In their submission:

- Google advocated to limit the focus on physical injury risks (rather than covering also mental health), especially when it comes to connected or new technology products.
- Google was against covering also substantial modifications in the GPSR as they considered it as additional burden on manufacturers.
- Google advocated that the main responsibility for product safety should remain with the manufacturer, and consumers should always turn to the manufacturer in case of issues.

Moreover, they are a member of the following business association that gave feedback to the Commission proposal for the GPSR: the Developers Alliance (USA, hereafter DA) and the Information Technology Industry Council (BE, hereafter ITI).

The associations overlaps on the following points in their feedback:

- The DA welcomes the choice for a regulation.
- The DA and ITI stress alignment with harmonised product safety legislation amd with the DSA, AI Act, cybersecurity act, and the EU Omnibus Directive
- The DA regards the term ‘misuse’, in the definition of a ‘safe product’ (Article 3) to be unclear and suggest ‘reasonably foreseeable misuse’.
- DA and ITI have reservations regarding including cybersecurity and AI in the GPSR.
- ITI finds the timeframe of 6 months for the implementation of the GPSR to be too short

[redacted]

Meeting with [redacted], Google

1 December 2021- 15:00

[redacted]