Meeting with Apple [redacted]

7 September – 19:00

In-Person Dinner with Apple [redacted]

Scene setter

- This high-level dinner will be an opportunity to explore the challenges posed by cybersecurity threats and how the EU's existing regulatory frameworks and latest proposals have tried to address them. [redacted] will share how Apple has tried to keep bad actors away from its customers' data and the challenges it has faced in doing so. This dinner will also include a moderate discussion with participants as leading policymakers, industry, and civil society representatives.
- ***Participants:*** they expect around 20 high-level guests in total (e.g. the Permanent Representative of Romania to the EU, the former Security Union Commissioner Sir Julian King, Mr. Cristian-Silviu Busoio MEP, along with others from European think tanks focusing on digital policy). They are also speaking to the US Mission to the EU about Charge Adams-Smith's attendance, and expect senior representatives from the Cabinets of Vice-Presidents Jourová and Schinas to attend as well.
- ***Format:*** This event will be an ***entirely off-the-record roundtable.*** This dinner will begin at 19:00 hrs CEST and will end by 21:30 hrs at the latest. [redacted] will open with a few brief remarks about Apple's position on cybersecurity and the tech sector's understanding of the EU's digital regulation or proposals. Following her remarks, [redacted] will lead a moderated discussion with all participants. They intend to make these roundtables as interactive as possible to create an open dialogue on concrete ideas to move the US-EU relationship forward.

Transatlantic Data flows/Schrems II – Key messages

- In response to the Schrems II judgment, we have been working on different work streams.
- We recently adopted modernised Standard Contractual Clauses for international data transfers. These have been fully aligned with the 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.
- The new clauses provide companies with a practical toolbox to assist them in their compliance efforts.
- The standard contractual clauses are the most used tool for international data transfers from the EU and finalising the new clauses was therefore a priority for us.
- We will now work together with stakeholders to develop a user-friendly practical guide, on the basis of questions and answers, to further facilitate the use of these new Clauses. In that context, we would welcome any feedback on your practical experience with the clauses.
- Of course, also the new Clauses have to be used in accordance with the Schrems II judgment and the guidance of the EDPB.
- That is why we worked closely with the Board to ensure consistency between our respective instruments. This is reflected in the final guidance of the EDPB that was adopted in June, which is certainly more aligned with the approach of the standard contractual clauses than the original EDPB draft.
- When it comes to transatlantic data transfers, the most comprehensive solution remains a new

adequacy decision, which is what we are currently discussing with the US.

- Developing a successor arrangement to the Privacy Shield is a priority for both sides. Our teams are negotiating intensively and have continued to do so throughout the summer.
- At the same time, it should be clear that there are no shortcuts and there will be no quick fix. We will only accept a solution that is fully in line with the requirements of Union law, as interpreted by the Court of Justice in the Schrems II judgment.
- Developing an arrangement that complies with the Schrems II judgment is also the only way to provide stakeholders on both sides of the Atlantic with the stability and legal certainty they expect.

Encryption in the context of criminal investigations – Key messages

- Encryption is essential to the digital world, securing digital systems and transactions and protecting a series of fundamental rights, including freedom of expression, privacy and protection.
- We also understand the challenges posed by encryption to law enforcement authorities. In this context, the Commission is working to identify technical, operational, and legal solutions to ensure lawful and targeted access to encrypted information, while maintaining the effectiveness of encryption in protecting privacy and security of communications.
- Such solutions **must not result in a general weakening of encryption or in indiscriminate surveillance**.
- To this end, the Commission is currently mapping Member States' legal frameworks and practical approaches to the challenge of encryption in criminal investigations. Subject to the results of this exercise, the Commission will reflect on a way forward to address the issue of lawful and targeted access to encrypted information in the context of criminal investigations and prosecutions.
- It is important to define a **horizontal approach to encryption**, across sectors.

Cybercrime and child sexual abuse – Key messages

- Refer to the adoption of the interim derogation from the ePrivacy Directive. This should allow companies to continue or resume their voluntary activities to detect online child sexual abuse in so far as they are **lawful**. They should in particular comply with data protection rules. It will apply for a maximum of three years, allowing sufficient time for the adoption of more comprehensive, **long-term legislation**.
- Welcome the engagement of private companies in finding an appropriate solution, both from a legal and technical point of view.
- Refrain from commenting specifically on Apple's decision to deploy new tool to detect child sexual abuse material in end-to-end encrypted environments using on-device hashing and matching.

  If comment is required: stress that Apple's efforts are commendable, and that their solution is an example of technology that shall be further assessed as to its usefulness and appropriateness to address child-sexual abuse as well as its impact on fundamental rights, including data protection and privacy**.**

Meeting with Apple [redacted]

7 September – 19:00

[redacted]

Meeting with Apple [redacted]

7 September – 19:00

[redacted]