



VICE PRESIDENT VĚRA JOUROVÁ

[REDACTED]
[REDACTED] META PLATFORMS

LOCATION: BERL 11/154

DATE AND TIME: 19 MAY 2022 AT 11H00 – 12H00

MEMBER RESPONSIBLE: DANIEL BRAUN

Contents

Steering brief	3
Background and defensives	10
Support to Ukrainian and independent Russian media	10
Code of practice	15
Privacy shield 2	17
International Data Flows	20
Better internet for kids	23
Media freedom act	27
CV	32

STEERING BRIEF

Scene setter

You are meeting [REDACTED] Meta Platforms. The proposed topics of discussion are:

- Work of Meta to support/give visibility to Ukrainian media and independent Russian media.
- Code of Practice on disinformation. (You can expect [REDACTED] to signal difficulties endorsing the commitments through Facebook lawyers and a call for the Code to be flexible.)
- Privacy shield 2 and international data flows.
- Better internet for kids. Meta floated the idea of a code for children in a previous meeting with Renate and Daniel.
- The proposal for a European Media Freedom Act: Meta contributed to the public consultation.

To be noted: [REDACTED]
[REDACTED]).

Key messages

Fight against propaganda and support to media freedom

- In the context of the war, we have stepped up efforts to fight Russian war propaganda and support trustworthy information.
- So we push for less space for disinformation and more space for information.
- This goes hand and hand.

i. On support to Ukrainian and independent Russian media

- When it comes to media, our first priority is the safety of journalists in Ukraine. This is why the EU has already dedicated more than 6 million euros for emergency support for journalists in Ukraine, including protective equipment, training, and also relocation when necessary.

- We are working with various partners, including Deutsche Welle, Reporters without Borders, the European Endowment for Democracy (EED).
- We also welcome that the European Broadcasting Union is supporting their Ukrainian member, organises a lot of solidarity initiatives and content in Ukrainian for refugees.
- EEAS provides support to Ukraine with shaping and promoting narratives and communication content. The Ukrainian Centre for Strategic Communication receives EUR 1 million over 18 months via the Foreign Policy Instrument. EEAS (East Stratcom Task Force) assists with project design and management as well as needs assessment.
- EEAS contributes to the design of several media development projects run by the Support Group for Ukraine and EUDEL in Kyiv (notably Media4Democracy). These projects are currently re-purposed to meet emergency needs.
- We also need trustworthy information in Russian. I had the opportunity to meet independent, investigative Russian journalists in Riga last week.
- They need to be able to continue their investigative work. I am in contact with colleagues in charge when it comes to visa and work permits. They also need channels to reach Russian people. [REDACTED]
[REDACTED]
[REDACTED]
- Anything you can do to **support the visibility and distribution of trustworthy information, in particular in Ukrainian and Russian**, is welcome. [REDACTED]

ii. On Russian state propaganda

- Around the world, Russia (and China) are driving a damaging disinformation campaign blaming the Western sanctions for the deteriorating global food security situation, rising energy prices and increasing inflation.
- In the EU, we are more aware now when it comes to disinformation, we have sanctions in place and new sanctions will come. But we see now Russia clearly targeting other continents, in particular Africa.
- We must make it crystal-clear together in international fora and with like-minded multilateral and bilateral partners that the sole responsibility lays with Putin's regime and its unprovoked decision to invade Ukraine.
- The EU is further working on the support of collection and storage of evidence of war crimes, and determined to prevent any manipulation of information to hide/discredit the investigation of war crimes, like the atrocities in the town of Bucha. Russia must be held accountable for these blatant violations and war crimes.
- I appreciate your efforts, the good initial implementation of the sanctions on RT and Sputnik, the labelling of or the increased cooperation with fact-checkers.
- It is important to diligently enforce your terms and conditions, as well as the sanctions and their possible circumvention by Russian-state affiliated accounts. Do you see **gaps in implementing rules or in the effectiveness of your policies in this regard?** We are seeing more and more worrying signals that the engagement with the **content of RT and Sputnik** is almost back to normal.

On the revision of the Code of Practice

- The war in Ukraine shows the importance that platforms deliver a strong revised Code of Practice on Disinformation as soon as possible.
- I appreciate Meta's engagement in strengthening the Code.
- The Commission counts on Meta's strong commitment to **deliver a strong Code on time, and to sign up, as Meta, to all commitments and measures for all of its services** (with Whatsapp and Messenger – their coverage is important and appreciated!).
- So far, the provisional chapters look promising, though we still need to see some improvements and clearer language.
- I have high expectations from Facebook in particular regarding coverage and capacities across **all languages**, the commitment on enabling the use of trustworthiness indicators, and **access to data**.
- The commitments should also include one on political advertising on messaging services (Guidance: "*when sponsored political content is shared between users, it should continue to be labelled as paid-for content*").
- And we expect the Code to come with strong key performance indicators, allowing the Commission and the public to monitor whether the signatories have lived up to their commitments.

On Privacy shield 2

- On 25 March 2022, President von der Leyen and President Biden announced an agreement in principle for a new transatlantic data transfer framework to replace the Privacy Shield.

- We are now working on the details to translate the agreement in principle into legal texts.
- To adopt the final decision, we will need to go through a multi-step process that involves an opinion from the European Data Protection Board (EDPB), a vote of our Member States and scrutiny by the European Parliament.
- Because of the work that remains to be done and the different procedural steps we need to go through, it is difficult to give a precise timeline at this stage.

On international data flows

- International data flows are indispensable for the growth of the European and global data economy. That is why the EU will remain open to all actors that comply with European rules and values. Ultimately, this raises trust and contributes to making Europe the most attractive place in the world to store and process data.
- Our legislative proposals (the data governance act, and the data act) are fully in line with EU's international commitments and obligations (WTO, FTA). We want that protection afforded to data held in the EU actually travels with the data when it is transferred outside the EU.
- But we also have to make sure that companies offering digital products and services to European citizens respect EU laws. EU is doing some things as the first in the world (DSA, DMA, AI act). We do it to address the risks stemming from the digitalisation. Simply, digital rules have to respect EU democratic values. I would hope that by now Facebook will be a constructive player.




On Better internet for kids (BIK) - age verification

- The new strategy for a better internet for kids (BIK+) reflects the recently proposed digital principle that ‘Children and young people should be protected and empowered online’.
- The updated BIK+ Strategy addresses age-verification mechanisms, in particular a European technical standard, to support methods and technologies to prove age in a privacy-preserving and secure manner, to be recognised EU-wide;
- We welcome Meta’s efforts to make age verification mandatory in your apps and your work with the EU funded euCONSENT Consortium to help develop an EU-wide infrastructure for effective online age verification and parental consent, going beyond self-declaration.
- We look forward to working with Meta on our code.

On legislation to detect, report and remove child sexual abuse online

- The Commission welcomes the fact that Meta has traditionally been a global leader when it comes to identifying and removing child sexual abuse on its services.
- The proposal for a Regulation on preventing and combating child sexual abuse will bring the needed legal clarity for Meta and other internet service providers to continue and enhance the fight against child sexual abuse online.
- The proposed rules will put all the service providers under its scope under the same obligations to detect, report and remove child sexual abuse material on their services.

On the European media freedom act (EMFA)

- At the start of this mandate, we decided to look at the situation of media freedom and pluralism in all Member States as part of our annual rule of law report.
- This helped us design our European Democracy Action Plan. It includes a series of measures to strengthen media freedom and pluralism, along with the protection of elections and the fight against disinformation.
- The next step is a proposal for a European media freedom act. It is of course a matter of protecting our values, but also our single market, as **we see that threats to media freedom and pluralism are also threats to the single market.** The single market is affected by the fragmentation of national rules related to media, decisions targeting actors based in other Member  and so on.
- We are looking at a common series of principles, such as the editorial independence of the media and the transparency of ownership. This would apply to all media, not only audiovisual media.
- Our internal work is well underway. I thank you for your contribution to the public consultation where you describe your approach regarding news content 
.
- We ask platforms to pay specific attention to media freedom and pluralism, this is in the DSA. We are analysing how we can build on this in the EMFA, but there is no final decision. One area we are looking at for example is the transparency of audience measurement. This is important for the media sector to get reliable data on the audience they reach online, especially when it comes to advertising. But let me be clear there is no intention to come up with a “media exemption”.

CODE OF PRACTICE

- The strengthened Code of practice aim is, to be fit for becoming part of the co-regulatory instrument foreseen in the Digital Services Act (DSA) to address disinformation on online platforms in the EU. In particular:
 - **Coverage of messaging apps.** The revised Code needs to feature strong commitments on messaging apps. We are pleased that Meta – as the only signatory so far – took this issue forward. We believe that the latest text goes in the right direction and look forward to finalising the work with your representatives.
 - **Access to data.** One of the critical aims of the strengthening of the Code is to guarantee access to data for purposes of the research on disinformation. Effective access requires close cooperation between the platforms, the research community and the civil society. We urge Meta to ensure rapid implementation of the framework being developed by the European Digital Media Observatory in cooperation with the platforms, including Meta.
 - **Trustworthiness indicators:** We are pleased to see that the draft of the revised Code’s user empowerment chapter features both a comprehensive commitment and measure on the use of trustworthiness indicators in signatories’ services. We strongly encourage Meta to sign up to these provisions and offer users access to such indicators, supporting their informed navigation of your services.
 - **Political ads:** We appreciate the constructive and quick manner in which the political ads chapter has been developed. We count on Meta’s continued commitment in finalising the work on this core aspect of the Code.
 - **Strong key performance indicators for monitoring the Code:** We expect the Code to come with strong key performance indicators, allowing the Commission and the public to monitor whether the signatories have lived up to their commitments. A difficult discussion herein lies in the disclosure of human and financial resources committed by platforms to fight disinformation. We strongly encourage Meta to explore ways how such data could be collected and disclosed.

Defensives

What is the Commission’s role in the drafting process?

- The drafting of the Code of Practice belongs to the signatories. The Commission’s role in the ongoing revision process is to ensure a robust instrument, in line with the Guidance.
- In short, the Commission’s role is to make sure that the Guidance is respected but it is for signatories to discuss and agree on operational commitments that are relevant for their services.

What does the Commission expect from Meta following the adoption of the Code?

- The revised Code will set out the actions to take in a range of areas, from demonetising misinformation, to stepping up efforts against manipulative behaviour, to improving the ability of users to understand and report misinformation, as well as to increasing cooperation with the community of fact checkers, researchers and civil society organisations.
- Following its adoption, the reinforced Code will have to be implemented quickly, in a uniform way in all Member States and in all languages.
- The final text will set forth a timeline for implementation. We encourage Meta to develop key elements of the Code, in particular related to the access to data and the disclosure of service level indicators as soon as possible, ideally even before the end of the implementation period.

What will be the role for European regulators?

- We intend to continue to rely on the expertise of European media regulators in this regard. The European Regulators Group for Audiovisual Media Services (ERGA) published recommendations (October 2021) following its own assessment of the implementation of the current Code and the COVID-19 monitoring programme.
- These recommendations touch on issues that are at the heart of the Commission's expectations and of the ongoing work to strengthen the code.
- The Commission will also rely on expert advice and support from ERGA as we assess progress in implementing the new Code. ERGA will also be part of a permanent task force aimed at developing and adapting the Code according to technological, societal and legislative developments.

PRIVACY SHIELD 2

Meta has been very vocal about the ongoing investigation of the Irish data protection authority, including by claiming that it will no longer be able to offer its services in Europe if the Irish Data Protection Authority (DPA) prohibits data transfers to the US which by some commentators and media has been interpreted as "threatening" to leave the European market. For example, in a recent annual report (that Meta is required to publish under US law), Meta mentioned that "If a new transatlantic data transfer framework is not adopted and we are unable to continue to rely on Standard Contractual Clauses (SCCs) or rely upon other alternative means of data transfers from Europe to the United States, we will likely be unable to offer a number of our most significant products and services, including Facebook and Instagram, in Europe, which would materially and adversely affect our business, financial condition, and results of operations". While Meta subsequently indicated in public statements (and a letter addressed to the Commission) that it has no plans to withdraw from Europe and includes such standard language in previous annual reports, [REDACTED]

*On 25 March 2022, the EU and US announced an **agreement in principle on a new Trans-Atlantic Data Privacy Framework**. Like the Privacy Shield, this new framework will take the form of a Commission adequacy decision, on the basis of which personal data could flow freely from the EU to participating companies in the US. While there is an agreement in principle, the two sides will now need to translate it into legal texts. In particular, the US commitments will be included in an Executive Order that will form the basis of the Commission's assessment in its future adequacy decision.*

Background

Negotiations on a Privacy Shield successor

The **agreement in principle with the US for a new Trans-Atlantic Data Privacy Framework** to replace the EU-US Privacy Shield (that was invalidated by the Court of Justice in July 2020 in its *Schrems II* judgment, C-311/18). Like the Privacy Shield, this **new framework will take the form of a Commission adequacy decision**, on the basis of which personal data could flow freely from the EU to participating companies in the US.

The future arrangement will provide for:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The details of this agreement in principle need now to be translated into legal texts. In particular, the **US commitments will need to be reflected in a new Executive Order** to be adopted by the US President, [REDACTED].

Once this new Executive Order and other relevant acts will be in place, the **Commission will be able to propose a draft adequacy decision and launch the adoption procedure** for the final adequacy decision. The first formal step of the decision-making process is obtaining an **opinion of the EDPB**. Second, the Commission will need to obtain the green light from the **Member States** in the comitology procedure. Finally, the **European Parliament** has a right of scrutiny over adequacy decisions. [REDACTED]

Ongoing procedures in Ireland following the Schrems II judgment

The **Schrems II case** was based on a complaint of Austrian privacy activist Max Schrems before the Irish DPA (Data Protection Commission, or DPC) about **data transfers by Facebook Ireland to its headquarters in the US on the basis of SCCs**. Now that the Court of Justice has issued its judgment, it is **for the DPC to apply the clarifications provided by the Court** in this specific case. This means that the DPC will have to decide whether Facebook can continue to transfer data to the US on the basis of SCCs.

Facebook initiated legal proceedings against the DPC before the Irish High Court on procedural grounds, after the DPC issued a preliminary order to Facebook in fall 2020 to suspend its data transfers to the US. While this was only an intermediary step as part of the ongoing investigation, Facebook claimed, in particular, that it did not receive sufficient time to present its views. In May 2021, the Irish High Court dismissed Facebook's claim.

Post-Schrems II actions of other data protection authorities

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, cases before the Belgian and French Councils of State (insisting on the importance of specific protections, such as encryption).

These cases were triggered by complaints from None of Your Business, the non-profit organisation headed by . the **Austrian DPA issued the first enforcement decision** in January, concluding that the transfers to the US operated in the context of the use of Google Analytics are unlawful. This decision was **followed by a similar one from the French DPA** in February and it is expected that others will follow in the coming weeks/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.

INTERNATIONAL DATA FLOWS

*Launched in February 2020, the **European Data Strategy** describes the vision to create a genuine internal market for data, where data flows freely across sectors and countries, in line with European rules and values, and data-driven innovation is embraced by society.*

*The proposal for a **data act**, adopted on 23 February 2022, is the second horizontal legislative initiative implementing the European strategy for data. It will set horizontal rules for access to and use of data to boost a fair data economy.*

*Following the Council's approval on 16 May of the European Parliament's position, **the data governance act** was adopted. The ceremonial signature by the co-legislators in Strasbourg will possibly take place in June. The legislative act will then be published in the Official Journal and enter into force 20 days after publication. The new rules will apply 15 months thereafter.*

Meta has not explained its position on either the data act or the data governance act at any stage of the legislative adoption process (feedback to the inception impact assessment or online public consultation).

In their position paper on the 2020 EU Data Strategy, Meta highlighted that the data centre and cloud computing industry's self-regulation ensured sufficient security, availability and resilience. Meta was positive on data portability but noted that there were unresolved data protection challenges.

The Commission will maintain its open, yet assertive approach regarding international data flows, as announced in the European data strategy of February 2020.

This is not just about increasing data flows, but also about doing it in a responsible and sustainable way. Ethical collection, processing and use of data is critical to ensuring trust in the data ecosystem. This is at the heart of the "European way of handling data".

Defensives

Is there an inherent contradiction between "data sovereignty" and data localisation and the "push for the free flow of data in the digital world", both of which are simultaneously promoted by the EU in various contexts?

- No. Sovereignty in strategic areas means that the EU must be able to define its own rules, make autonomous technological choices, and develop and deploy strategic digital infrastructures. However, the EU will remain open to all businesses that comply with European rules and standards.
- Specifically for data, the data strategy presents data governance "in the European way", which will guarantee that individuals and companies keep control over their data, thus guaranteeing an increased level of data sovereignty in Europe.
- Thanks to the European data strategy of February 2020, more data will be available for the EU economy and society, while individuals and businesses will retain full control over the data they generate.

Is the EU creating data localisation measures?

- No. We have repeatedly confirmed the Commission's commitment to facilitate data flows. The Commission understands the economic importance of international data flows and firmly believes that ensuring a high level of data protection should go hand in hand with a policy of facilitating such data flows.
- To allow secure and trusted international flows of personal data, there is a sound legal framework under the General Data Protection Regulation (GDPR), working on the basis of adequacy decisions, standard contractual clauses and binding corporate rules. Its implementation is assessed on a case-by-case basis.
- In line with this, the measures dealing with international access and transfer in the data governance act and the data act add a layer of legal certainty, insofar they take a uniform approach to the protection of non-personal data held in Europe against unlawful access by non-EU governmental authorities, in complement to the measures that the GDPR imposes for personal data.
- There is no imposition of any data localisation requirements whatsoever, nor limitations on companies to transfer non-personal data internationally.

Are the international provisions of the data act similar to a Schrems II for industrial data?

- Yes, we have already proposed such provisions in the data governance act for which we have a political agreement by the co-legislator. The data act would extend these provisions to cloud and edge services.
- These rules are **similar to Schrems II** in the sense that their aim is to shield non-personal, industrial data held in Europe from unlawful access and transfer requests coming from third countries.
- These rules are **different from Schrems II** in the sense that they also impose requirements on cloud service providers active in Europe and apply mainly to governmental access requests.
- When a cloud customer voluntarily transfers the data outside the EU, the international provisions of the data act would not apply.
- The provisions are thus not impacting on economically important international flows of non-personal data.
- With this, we complement the rules for **personal data with rules for non-personal data**, which have a different intensity and scope of application. These provisions will make cloud services in Europe more secure and trustworthy, while not affecting who can offer those services on the EU market.

Background

Overview of the data act

The data act encompasses the following issues:

- Better access to Internet of Things (**IoT**) data:
 - manufacturer of IoT objects needs to allow access and can continue to use the data;

- users of IoT objects can access and port data;
- 3rd parties can use the data to offer services (Small and medium sized enterprises (SMEs) get special conditions).
- **horizontal rules** for IoT data also frame data access and use in other sectors to converge the patchwork of existing legislation ;
- tackle **contractual unfairness** in business to business data sharing agreements, where unilaterally imposed on SMEs;
- **business-to-government data sharing**: Companies must make data available to public sector bodies in case of emergencies and other exceptional needs
- **easier switching** between cloud services;
- facilitate **interoperability**: COM may adopt technical specifications if necessary to reduce transaction costs related to the use of data even across sectors;
- protection of cloud data held in Europe from unlawful non-EU governmental access.

Overview of the data governance act

The proposal for a data governance act was adopted on 25 November 2020. It will increase trust in data sharing by regulating organisations that bring the supply and demand of data together. It is a key building block for the creation of “common European data spaces” by regulating the orchestrators of these data spaces.

The data governance act builds entirely on existing legislation on who can use what data, in particular GDPR. It thus aims to support voluntary sharing.

It has four intervention areas:

- **Re-use of public sector information that is sensitive** because it contains personal data or commercially confidential information.
- Fostering the emergence of **new data sharing intermediaries**. Such intermediaries would be services that companies and individuals can use in order to “monetise” data about them.
- **Data altruism**. The proposal makes it possible for not-for-profit organisations to registers as data altruism organisations. This should bring trust in such novel players and make it possible to establish data pools based on voluntary contributions by individuals and companies at scale.
- **Governance on standardisation**. The data governance act proposes to set in place a European Data Innovation Board in order to better steer standardisation and ensure interoperability between different data spaces.

BETTER INTERNET FOR KIDS

*Meta has traditionally been a global leader when it comes to identifying and removing child sexual abuse on its services. 95% of global reports originate from Meta, with more than two-thirds of that stemming from Facebook Messenger. Meta intermittently stopped detecting child sexual abuse in Facebook Messenger in 2021 because of concerns about the legal situation brought about by the EU electronic communications code, which led to a drop of **more than half** of global reports. They have since resumed scanning.*

Meta wishes to reinforce efforts towards the common goal of protecting and promoting children's rights online. In July 2021, they announced their plans to make age verification mandatory. Meta uses artificial intelligence (AI) backed systems to detect the accurate age of its users, like through birthday wishes, or age used in apps linked to Facebook.

Instagram made it mandatory for all users to share date of birth to use the app. In case someone tries to provide false date of birth details, Instagram's AI algorithms will scan for the data on the account and verify whether it is correct or wrong.

Defensives

How will the BIK+ address age verification?

- EU laws - in particular the AVMSD and the GDPR - are in place and technical solutions to check age exist. Nevertheless, in practice age-verification mechanisms are mostly ineffective, and users often only need to enter a birth date to register.
- Under BIK+, the Commission will work towards a European standard on age verification. This type of standard will clarify what is expected from industry when age verification is required on any online tools and services. Such recognised methods would be used by pornography websites, for example, to ensure their users are aged 18 or over.
- In parallel, the Commission will explore how to use the planned European Digital Identity Wallet for age verification. The Commission will work with Member States and encourage them to issue electronic IDs to the under-18s to strengthen effective age verification methods.
- This would lead to an EU-wide recognised proof of age based on date of birth in a privacy-preserving and secure manner.

Who will the new rules on detecting, reporting and removing child sexual abuse material online apply to?

- The proposed rules will apply to online service providers offering services in the EU, namely hosting services and interpersonal communication services (such as messaging services), app stores and internet access providers.

What material is covered under the proposal?

- The detection obligations cover known material (re-uploaded photos and videos that have been previously identified as child sexual abuse material), new material (photos and videos not previously identified), and grooming. The identification of grooming only concerns interpersonal communications where it is known that one of the users is a child.

What about the use of encryption technology when detecting child sexual abuse material?

- As indicated, the proposal is technologically neutral and is an obligation of results. This includes the use of encryption technology. A large portion of reports of child sexual abuse, which are instrumental to starting investigations and rescuing children, come from services that are already encrypted or may become encrypted in the future. If such services were to be exempt from requirements to protect children and to take action against the circulation of child sexual abuse images and videos via their services, the consequences would be severe for children.

Background

The Better Internet for Kids (BIK+) Strategy

The new European strategy for a better internet for kids (BIK+) is an update of the previous BIK strategy from 2012. The update replies to the challenges and opportunities of the vastly changed digital environment and digital transformation of the society, further accelerated by the COVID-19 pandemic. The Commission's first comprehensive Strategy on the Rights of the Child from 2021 also called for an update of the strategy.

The strategy, one of the flagship actions of the European Year of Youth 2022, is built on three pillars:

- **safe digital experiences** to protect children from harmful and illegal online content, conduct, contact and consumer risks and to improve their well-being online through a safe, age-appropriate digital environment, created in a way that respects children's best interests;
- **digital empowerment** so children acquire the necessary skills and competences to make sound choices and express themselves in the online environment safely and responsibly;
- **active participation**, respecting children by giving them a say in the digital environment, with more child-led activities to foster innovative and creative safe digital experiences.

Legislation to detect, report and remove child sexual abuse online

The proposal, announced in the EU Strategy for a more effective fight against child sexual abuse has been adopted on 11 May 2022.

The initiative builds on and complement existing policy instruments in the fight against child sexual abuse, addressing gaps in the current legislative framework. Horizontal instruments such as the eCommerce Directive or the DSA address some of the problems and challenges of keeping children safe online but provide only limited and partial solutions and do not offer the possibility to put in place comprehensive and targeted measures. Sectoral instruments (such as the CSA Directive, the Europol Regulation, the interim Regulation or the ePrivacy Directive) are not able to provide a comprehensive EU-level solution to combat online child sexual abuse and sexual exploitation as they focus on particular aspects of the problem, such as harmonisation of criminal laws, improving police investigations, exchanging or processing of personal data and the protection of privacy. None of these instruments define the role of the service providers specifically enough to provide them with legal certainty on their powers and do not foresee effective obligations for the providers relevant in the fight against child sexual abuse.

The new proposal includes obligations for companies to detect and report known child sexual abuse material to public authorities. This step is necessary, as voluntary action has proven insufficient: willingness to engage in the fight against child sexual abuse and the effectiveness of such efforts varies greatly from company to company, and current action lacks harmonised safeguards, including transparency. This may interfere with users' rights, including those of privacy and data protection.

European Centre to prevent and counter child sexual abuse

The new proposal also defines the role of the EU Centre to prevent and combat child sexual abuse. The need of an EU Centre, established in the EU and operating according to EU rules, featured prominently in negotiations of the interim derogation from the ePrivacy Directive as agreed in April 2021.

The centre as currently envisaged could have three major roles: support efforts on prevention, improve assistance to victims, support detection, reporting and removal of CSA online.

The detection and reporting role is key given the international cooperation dimension. In this regard an EU Centre could:

- eliminate the need for international transfers of personal data of EU citizens;
- support detection by, for example, maintaining a database of child sexual abuse hashes to reliably enable detection of child sexual abuse as defined by EU rules, rather than rely on what is criminalised under US law as is currently the case.

It will also function as an important safeguard, as a source of information on what is defined as child sexual abuse according to EU rules, ensure visibility on the effectiveness of detection measures, and transparency and accountability of the process.

The centre would serve as an expert hub for all aspects of prevention and victim support, and engage with counterparts such as NCMEC in the US, the Australian Centre to Counter Child Exploitation, and the Canadian Centre for Child Protection.

Data on grooming

Reports concerning grooming increased from 37 872 in 2020 to 44 155 in 2021, and the age of children falling victim to sexual abuse continues to decrease. On average, the first exposure to sexually-explicit content online happens at 12 years. The Internet Watch Foundation (IWF) noted a three-fold increase in imagery showing 7-10 year olds who have been targeted and groomed by predators online.

According to the WPGA-Global Threat Assessment 2021, veiled or hidden use of typical grooming or child sexual abuse material (CSAM) terms in gaming has grown over 13% 2019-2020. This resulted in the further discovery of 50% additional harmful content.

Europol's 2021 Internet Organised Threat Assessment (IOACT) shows that there has been a steep increase in online grooming activities on social media and online gaming platforms.

In May 2021, Save the Children Finland published a report which provides new data on online grooming. According to the report, 62% of children - respondents had been contacted online by a person they knew or suspected to be an adult or at least five years older than them.

Background

META position on EMFA

META didn't fill in the public consultation on the EMFA, but they sent a response to the EMFA Call for Evidence (below):

Meta's mission is to give people the power to build community and bring the world closer together. People use Facebook and Instagram to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them. At Meta, we recognise we have a role to play in ensuring that our users connect with official sources in reducing misinformation and in building community and connection between people in difficult times. We look forward to engaging with the European Commission as it evaluates the best possible way for the EMFA proposal.

META's approach to news content

META's core mission is to connect users with friends and family and to help them find quality content. A user's Feed primarily contains relevant posts from family and friends as well as posts that reflect user interests.

News is only a small part of the content on Facebook- around 4% of the content on Feed. We're also one part of a much larger supply chain when it comes to news. We are just one part of a very big supply chain when it comes to news. Social media is just one small element of a much larger ecosystem.

The digitisation of news has led to increased choice, diversity, access and engagement. There are many new opportunities for new entrants and established operators to innovate and reach audiences that were previously inaccessible or hard to reach. These developments offer to our users:

Choice and Diversity

- *increased access to a wider range of news sources, domestic and international;*
- *emergence of new digital publications tailored to the needs of underserved communities;*
- *facilitation of access to news from multiple publishers.*

Access

- *new opportunities to access news "on demand" rather than just at the evening news broadcasts;*
- *new opportunities to engage with news on a variety of devices including laptops, tablets, desktops, and mobile phones.*

Engagement

- *new opportunities to engage with news publishers and journalists themselves, and share and discuss news content on social media;*

- *new opportunities to create a personalised and/or curated stream of news content.*

At Meta we are determined to help build a more informed community. We have invested in products, programs and partnerships that drive value for news providers to ensure that the people who are using Facebook to discover what is going on in the world find news sources that further educate and engage them.

Facebook allows all publishers of all sizes to reach and engage with new audiences while providing analytical tools to better understand their audiences and how they engage with news links. We also provide various monetisation tools that allow publishers to build their businesses. Many established media operators use Facebook as a free means to reach an existing audience or an audience that they may previously not have had access to, and to monetise their content in new and innovative ways. Reduced cost of distribution enables more journalists and publishers to create and distribute content to more people—and do it faster and more easily.

Monetisation and distribution

The Facebook platform allows news publishers to publish, distribute, monetise and interact with viewers of their content at no cost to publishers and consistent with their publishing preferences, via Facebook’s business tools. Notably, publishers typically do not place entire articles on Facebook, but rather preview text to attract readers and a link back to the publisher’s site. This enables publishers to direct users to their websites where publishers can serve their own ad experience directly to those users and monetise the traffic provided by Facebook. It also enables publishers to generate reader revenue through subscriptions and other engagements with their customers, on their terms. Referral traffic totals from Facebook to news publishers vary with the news cycle.

As an opt-in platform, publishers choose to place their content directly on Facebook via their Facebook Pages. This opportunity exists for all businesses that wish to publish their content on Facebook, and is subject to complying with the Facebook terms of service.

Facebook has built its services to respect the decisions of publishers on monetisation and data flow of their own content. Facebook doesn’t require publishers to change their applicable paywall policies, or dictate to them what happens once a user clicks on a link and is taken to the publisher’s website to read the article. For publishers who do not operate paywalls, they are able to monetise their content on Facebook through advertising and other methods outlined in the next section below. Publishers can remove any content that they previously posted on the Facebook platform at any time. If publishers no longer want to enable other features such as the Like or Share plugins on their websites and apps, or to use Instant Articles, they are free to disable their participation. To protect publisher content, we have tools such as the Rights Manager and Facebook’s reporting tools which enable publishers to flag IP violations and any infringing content anywhere on our platform can be removed. For non-infringing news content, Facebook honours publishers’ choices about whether to allow third parties to render news content, as expressed by the publisher’s use of generally established coding tools, such as meta tags.

Facebook’s customised commercialisation products and innovations incorporate feedback from the news industry. Our custom-built publisher tools are designed to help news organisations build and understand their audiences, as well as drive additional revenue to them, which we think is the best way we can help them build sustainable business models for the future.

These are different and separate from our advertising tools. The types of tools we provide are:

Tools like CrowdTangle give publishers data and insights into audiences in markets where newsrooms are still developing skills and tools to understand digital audiences.

Publishers can use Instream Video, Instant Articles, and subscription offerings to monetise their content -- turning readers on Facebook into payers subscribers, where they can then keep that new revenue.

Products like Live, Groups, and the breaking news tag can create new audience engagement and communities based on feedback directly from the industry

The tools and data we provide to help gather insights on the performance of posts and advertising campaigns are also particularly valuable in helping small and emerging publishers who are in greatest need of support and who benefit most from being able to reach new audiences.

Facebook News

In Germany and France, we have also entered into commercial deals with publishers for new content. By launching Facebook News, we created a dedicated news surfaces. In doing so, Meta has entered into commercial deals for net new content links with a wide range of diverse publishers, including international, national, and local publishers, to feature on this unique new surface. The product - which was shaped by publishers and people who requested a specific destination inside Facebook for news - is a multi-year investment that puts original journalism in front of new audiences as well as providing publishers with more advertising and subscription opportunities to help build a sustainable business for the future. Facebook News does not contain any advertising and Meta does not have any direct revenues from this surface.

Users may also discover video news content on Facebook Watch, a dedicated surface for video content. Facebook Watch provides another surface on which publishers can freely distribute content as the news content on Facebook Watch is drawn from content already posted by news publishers on their Page. Facebook has entered into commercial deals with some publishers to produce high-quality video content specifically for Facebook Watch.

Meta's approach to misinformation

We use a three-part strategy with regards to combating misinformation: we remove misinformation likely to contribute to the risk of imminent harm or interference with political processes, we reduce the distribution of content which independent fact checking organisations determine to be false or altered, and we inform people so they can decide what to read, trust and share. We have recently published additional transparency on our approach to combating misinformation in our Community Standards.

We remove misinformation where it is likely to directly contribute to the risk of imminent physical harm. We also remove content that is likely to directly contribute to interference with the functioning of political processes and certain highly deceptive manipulated media. In determining what constitutes misinformation in these categories, we partner with independent experts who possess knowledge and expertise to assess the truth of the content and whether it is likely to directly contribute to the risk of imminent harm. This includes, for instance, partnering with human rights organisations with a presence on the ground in a country to determine the

truth of a rumour about civil conflict, and partnering with health organisations during the global COVID-19 pandemic.

For all other misinformation, we focus on reducing its prevalence or creating an environment that fosters a productive dialogue. As part of that effort, we partner with third-party fact-checking organisations to review and rate the accuracy of the most viral content on our platforms. We currently work with our growing network of independent third party fact-checking partners. We partner with over 80 fact-checking organisations around the world, covering over 60 languages. In the EU and greater Europe, we partner with 37 fact-checking organisations, covering 33 languages. We also provide resources to increase media and digital literacy so people can decide what to read, trust and share themselves.

State media labelling

We are currently restricting access to RT and Sputnik across the EU given the exceptional circumstances of the war in Ukraine. But already in July 2020 we have begun implementing our policy on state controlled media to help people better understand who's behind the news they see on Facebook and label media outlets that are wholly or partially under the editorial control of their government. Through this step we're providing greater transparency into these publishers because they combine the influence of a media organisation with the strategic backing of a state, and we believe people should know if the news they read is coming from a publication that may be under the influence of a government. We're equally transparent when it comes to paid content from these publishers, we are labelling ads from these publishers later this year. To inform our policy criteria, we consulted more than 65 experts around the world specialising in media, governance, and human rights and development. The input we received from these organisations was crucial to understanding the different ways and degrees to which governments exert editorial control over media entities. We know that governments continue to use funding mechanisms to control the media, but this alone doesn't tell the full story. That's why our definition of state-controlled media extends beyond just assessing financial control or ownership and includes an assessment of editorial control exerted by a government.