Commissioner Ylva Johansson

VISIT TO SILICON VALLEY
CHILD SEXUAL ABUSE & CHILD EXPLOITATION

27-28 January 2022

Table of contents

ITINERARY

DAY 1 – 27 January

Meetings with:

- [redacted]
- Meeting with **TikTok**
- Meeting/ discussion panel with **academia (possible)**

DAY 2 – 28 January

- Meetings with [redacted]

High-level officials confirmed

- [redacted]
- **TikTok:** Erich Andersen, Head of Corporate Affairs and General Counsel for Bytedance/TikTok and Suzy Loftus, Global head of risk and response operations TikTok
- [redacted]

SCENE SETTER

Purpose of the visit

You will travel to the USA to discuss how to more effectively prevent and combat child sexual abuse online in individual meetings with Microsoft, Twitter, Facebook, Google and Apple. A joint meeting with Roblox, Twitch, Discord, Dropbox and Snap is also being planned.

The visit takes place a few weeks before the expected adoption on 2 March of the new proposal for a regulation on preventing and combatting child sexual abuse. The aim is to discuss collaboration with the companies in view of the forthcoming proposal, how they envisage interaction with the future EU Centre, and elicit commitments from the companies to step up their efforts to prevent and combat child sexual abuse.

Key messages

- Highlight the importance of protecting children on the internet.
- Convey an overview of the European Commission’s efforts to fight CSA, namely the new proposal that is expected to be presented in the beginning of March this year and the creation of a new EU Centre to prevent and combat child sexual abuse;
- Note that the legislative proposal is an opportunity to make a significant, long-lasting positive change in the fight against CSA in the EU (and globally, given the cross-border nature of the crime).
- Outline the main elements planned:
    - enabling companies to do their part by **mandating them to detect, report and remove** child sexual abuse online, and
    - establishing an **EU centre to prevent and combat child sexual abuse**: This EU Centre will provide reliable information on what is illegal in the EU and on available tools to detect CSA online, to facilitate the work of companies in detection, reporting and removal of CSA online. It will also receive the reports from companies, analyse them and provide them to the competent national law enforcement authorities and Europol.
    - In addition, the Centre will also act as a **hub of expertise** for all aspects of **prevention and victim support**, supporting Member States, and cooperate with similar Centres around the globe.
- Reiterate the importance of companies’ role in preventing and combating child sexual abuse,
- Acknowledge the good work they are already doing, also through the Tech Coalition, and call for their continued commitment and increased efforts to fight these crimes.
- **Safety by design** is key: there should be a regular check what more could be done to incorporate features in products that safeguard children in the online space and prevent risky situations. The well-being of children should be a key concern from the initial design stage of any product.
- Looking ahead, **encryption** remains a key issue [redacted] [redacted] We need to make sure that detection, removal and reporting of child sexual abuse is possible in an effective manner even if end-to-end encryption is put in place.

Pages 4-6 redacted - out of scope

15.15 – 16.15 **tbc**	**Meeting with TikTok** **Erich Andersen, Head of Corporate Affairs and General Counsel of Bytedance/TikTok, Suzy Loftus, Global Head of Risk & Response Operations, TikTok** Venue: [redacted] Contact: [redacted] EU based but only contact)

Scene Setter

TikTok makes efforts to prioritise safety-by-design elements in their application and appears committed to making sure that children's safety and well-being is priorities on the app.

[radicalization] Institute for Strategic Dialogue research recently showed how TikTok content sharing algorithms have been spreading extremist and borderline content among young users, providing examples of hate speech and right wing extremist material. The New York Times also recently reported about a leaked TikTok internal document confirming TikTok algorithm can lead youngsters into dangerous rabbit holes by recommending content based on visualization time.

You last spoke to Eric Andersen (General Council and head Corporate Affairs) on 26 October 2021 to discuss TikTok's measures and actions to prevent and counter the dissemination of CSAM and violent extremism and terrorist content online. TikTok gave an overview of the safety-by-design features the company deploys to keep children safe on their platform.

On 4 November TikTok organised a virtual tour of their Transparency Centre in Dublin where they informed about measures they take to ensure digital well-being. TikTok became a member of the EU Internet Forum in November 2021 and also intervened at the meeting.

Main objective

Encourage TikTok to continue and to provide inspiration on safety by design.

Specific points to raise

- Note TikTok's efforts to priorities safety-by-design elements in their application and their commitment from an early stage to making sure that children's safety and well-being is priorities on the app.
- Discuss with TikTok their current technical efforts and any upcoming measures they are looking to introduce.
- Highlight the value of collaborating with TikTok, including in the context of the EUIF which the company has just joined.
- Discuss with TikTok any current and future challenges relating to combating child sexual abuse.
- Ask TikTok about the types of technologies they deploy to detect known, and new content and whether they utilise tools to detect text-based grooming attempts.
- Ask TikTok what new trends and challenges they see, particularly in the area of self-generated child sexual abuse content.

Pages 8-14 redacted - out of scope

Further general speaking points on specific issues:

1. On encryption in the context of criminal investigations and prosecution

- Encryption is an important tool for protecting cybersecurity and fundamental rights, however its widespread use also causes challenges to law enforcement and prosecutors to gain lawful access to electronic evidence needed to carry out investigations and safeguard citizens' security.
- Welcome companies' efforts to set out structured support to law enforcement including to facilitate the access to electronic evidence and note the Commission's commitment to continue fostering such collaboration.
- Remind of the adoption of the Council Resolution on encryption adopted in December 2020 which called for an active discussion with technology industry to identify solutions that would allow national authorities to carry out their operational tasks effectively while protecting security of communications and fundamental rights; and inform of the Commission's commitment set out in the EU Strategy to tackle organized crime to support the implementation of this resolution.
- A mapping of EU Member States' current legal and technical measures to tackle the challenges that maybe posed by encryption has been completed. As a next step the Commission will organize dialogues with relevant stakeholders including service providers, with an aim to inform on a possible way forward during 2022.

2. Trafficking in Human Beings

- Raise the highly disconcerting fact that each human trafficking offence bears an online element. According to the 2020 US federal human trafficking report, **41% of defendants in active sex trafficking cases met their victims on social media and 59% of online victim recruitment occurred on Facebook**. **The report also states that 65% of identified child sex trafficking victims recruited on social media were recruited through Facebook.**
- Encourage the companies to actively engage in the fight against trafficking in human beings in different ways, e.g. the deployment of technical tools capable of detecting explicit human trafficking offences; deletion of fake accounts used to profile and lure victims; awareness raising campaigns; active monitoring of adverts targeting minors.

- Refer to the newly appointed Anti-trafficking Coordinator, who will actively engage in a dialogue with the companies in the first semester 2022.

3. Radicalisation

- Refer to imminent application of the TCO regulation (June 2022) which will impose obligations on hosting services providers offering services in the EU and the work of the EU Internet Forum to increase collaborative efforts to prevent the use of online platforms to radicalise and recruit people into violent extremism and terrorism.

- The EU Internet Forum is delivering on enhancing public-private partnership, with concrete tools as the EU Crisis Protocol and the Knowledge Package on Violent right-wing extremists groups, symbols and manifestoes to support companies in their moderation efforts. Looking forward to step up our collaboration in this framework.

    - ▪ Underline the importance of focussing on violent right wing extremism and terrorism. More needs to be done to moderate neo-Nazi and white supremacist content and make sure terms of services clearly cover this type of material. Borderline content that can lead users towards violent forms of radicalisation should also be addressed.
    - ▪ The EUIF Knowledge Package on violent right wing extremist groups, symbols and manifestos is aimed at supporting more effective content moderation actions. We look forward to you input on the Knowledge Package to further improve it.

BACKGROUND

1. Further recent interactions with the companies

At Cabinet/Commissioner level:

- **EU Internet Forum Ministerial Meeting on 8 December 2021.** This meeting focused on "Ensuring security online, shared responsibilities" with a debate on the fight against CSAM as well as on preventing radicalisation online. [redacted] TikTok's VP Public Policy Theo Bertram also intervened in the meeting.

At service/technical level:

- **Workshop on Safety-By-Design to prevent and combat CSA online organised by DG HOME on 21 October 2021.** Participation by the following companies: TikTok, [redacted]

- **EU Internet Forum Senior Officials Meeting on 16 November 2021.** Four companies, [redacted] TikTok, presented their activities and were welcomed as new members to the EUIF.

  The EUIF Knowledge Package of violent extremist groups, symbols and manifestoes was presented and approved by the Forum for the voluntary use of companies to support their content moderation efforts. Feedback will be obtained from companies in Q1 2022 on how they were able to use the information in the knowledge package and to advise on future approach. An updated version of the knowledge package will be presented in the Fall 2022 and will be based on feedback by companies and contributions by Europol, Member States and external experts.

  A EU Internet Forum workshop on algorithmic amplification took place on 17th September 2021 to reach a better understanding of the possible impact of the misuse of recommender systems on the process of radicalisation online. [redacted] presented their assessment of the risks related to the misuse of recommended systems and introduced the measures they have been taking to tackle harmful content on their platforms. TikTok, [redacted] and other platforms were present at the meeting.

- **EU Internet Forum Technical Meeting on the misuse of video-gaming and adjacent platforms on 4 October 2021.** [redacted] gave presentations on their activities to prevent misuse by violent extremist.

- **Europol Table Top Exercise,** on 5 November 2021, to test the implementation of the EU Crisis Protocol, and build synergies to other protocols, including that of the industry, coordinated by the Global Internet Forum on Counter-Terrorism (GIFCT), as well as that of the Christchurch Call's shared Crisis Response Protocol.

2. Facts about child sexual abuse

The number of reports received by law enforcement in the EU in Jan-October 2021 has decreased by 2/3 compared to the same period last year, driven by Facebook's decision to turn off the detection of CSA online in the EU on December 2020.

- 1 January – 30 October 2020: 972,581 reports, vs 341,326 reports in 1 January – 30 October 2021.
- As most of the reports come from Facebook Messenger, this confirms the previous estimate on the decrease in the number of reports that would occur if Facebook implements end-to-end encryption, as the consequences would be practically the same as turning off the detection of CSA.
- This means a loss of 2100 reports per day, reports that could have led to rescue of children from ongoing abuse and the prevention of further abuses by arresting offenders.

In November 2021, the ECPAT network on ending the sexual exploitation of children, with 122 mostly NGO members in 104 countries, conducted a survey on public attitudes towards privacy and child protection online in 8 Member States (DE, FR, IT, NL, PL, SE, ES, HU). The majority of respondents indicated that:

  - Detection (of CSA online) is perceived to be **as or more important than people's personal privacy** online (76% of respondents)
  - There is a **strong support** for the upcoming legislative proposal on CSA (mandatory detection by companies), even when people hear about the possible downsides (68%)
  - People believe that **kids are not safe online (73%)**
  - People believe that online privacy has gone (68%)

WeProtect Global Alliance-Global Threat Assessment, 2021: main findings

- Offenders continually seek new tools.

Over 56.8% of all discussion observed on known offender dark web forums was related to new tools to evade detection and make offending more secure—with the only other two categories being Social Media Platforms (32.8%) and Direct Messaging (10.4%).

- Masked language hides harmful content in gaming.

Veiled or hidden use of typical grooming or child sexual abuse material (CSAM) terms in Gaming has grown over 13% in 2019-2020. This resulted in an increase of 50% additional harmful content detected.

- Cloud sharing

Fuels interactions with harmful content. From 2020 Q1 to 2021 Q1, instances of user engagement or interactions with harmful content relating to CSEA exploded to nearly 20 million in Q1 2021—up significantly from more than 5.5 million in Q1 2020.

- Offenders re-traumatize survivors using fake profiles.

Many offender groups reference known CSAM survivors to indicate online preferences and to find and network with like-minded individuals. In Q1 2021, Crisp identified 3,324 unique pieces of posted content, each resulting in as many as 2,000 interactions. This "network effect" illustrates the malignancy of this sharing, with each interaction perpetuating the exploitation of the survivor referenced in the account.

US and NCMEC statistics: In 2020, there were over 21.7 million reports of suspected child sexual exploitation made to the National Center for Missing & Exploited Children's

CyberTipline. Online enticement reports — which detail when someone is communicating with a child via the internet with the intent to exploit them — increased by more than 97% from the year before.

Half of offenders arrested for CSAM possession were or had been physically abusing children; detection of CSAM frequently leads to stopping hands on/physical abuse happening in parallel.

A high proportion of cases involved material depicting extreme abuse and/or large quantities of material; viewing CSAM increases demand for more and more extreme abuse - 52.2% of offenses included images or videos of infants or toddlers.

3. Safety by design to safeguard children online

Safety by design is an important preventative and proactive approach that ensures user safety is embedded into the design, development and deployment of online digital products and services. This approach involves consideration of age-appropriate design and access to services that take into consideration the child users' maturity and capacities when interacting with technical platforms and online services.

Companies are well-placed to invest in safety by design elements in existing and new services to make it difficult for bad users to identify and make contact with children. This approach may also be used to ensure that online environments in which children are interacting are supportive and limit the possibility of risky situations.

On the 21 October, the EU Internet Forum held a workshop with companies to discuss safety by design in the prevention and combating of child sexual abuse. The meeting provided opportunities to better understand the initiatives that companies are implementing in their services to keep children safe from online child sexual abuse, and gain insight into the legal and operational challenges hindering implementation of these design efforts.

Tech companies asked for more support to find solutions to allow access to data required to effectively train new technologies and more robust and futureproof legislation that provides legal certainty and clarity to support the developments of new technologies whilst safeguarding fundamental rights.

As part of its work to develop a proposal for a regulation to prevent and combat child sexual abuse the Commission will take into consideration the inclusion of safety by design principles to continue supporting aspects on prevention.

4. Online dimension of trafficking in human beings

The use the online environment, in particular social media and online market places significantly contributed to the expansion of human trafficking offences world-wide, which makes human trafficking one of the most lucrative crimes in global scale as Europol estimates the annual global profit for traffickers EUR 29.4 billion. The online environment decreased the barriers to engage in such activities; the use of social media facilitated the recruitment of victims while the exploitation in encrypted chatrooms makes the detection and the protection of victims much more difficult while it ensures anonymity for the traffickers. At least one or several elements of each and every human trafficking offence takes place online, from luring or exploiting victims, organising their transport and accommodation, advertising the exploited services online and reaching out to potential clients, controlling victims, communicating between perpetrators and hiding the criminal proceeds. Children are at particular risk of falling victim to traffickers online.

In the recent years, social media platforms has become a major market place for human trafficking. A 2020 US federal human trafficking report showed that 41% of defendants in active sex trafficking cases met their victims on social media and 59% of online victim recruitment occurred on Facebook. The report also states that 65% of identified child sex trafficking victims recruited on social media were recruited through Facebook. Instagram and Snapchat were the most frequently cited platforms after Facebook for recruiting child victims in 2020. For adult victims, the next-most cited were WeChat and Instagram. Moreover, TikTok is increasingly used by traffickers to lure or recruit victims with false promises as cases occurred in Africa and Asia. Despite all these in 2020, Facebook deactivated a software tool to automatically detect content violating their slavery ("domestic servitude") policy. As of the last update on the Facebook transparency page in July 2021, internal reviewers label violating content using three categories: hate speech, violence or nudity but not human exploitation.

The **EU Strategy on combatting trafficking in human beings (2021-2025)**[4] introduces as a new action a dialogue with relevant internet and technology companies to reduce the use of online platforms for the recruitment and exploitation of victims. The Commission will also encourage similar dialogues to be conducted by Member States at national level. Such dialogue has already started prior to the adoption of the Strategy , when on 16 February 2020, Unit D5 and other DG HOME staff met some representatives of the online platforms [redacted] to discuss challenges and opportunities to addressing trafficking in human beings. The platform representatives pointed out existing company policies in place and tools to address criminal activities, including via tracking systems, the removal of content and extracting evidence; forms of partnerships with civil society are already in place. As regards trafficking in human beings, limited information is available on referral and removal of content; companies highlighted that cooperation with law enforcement is crucial. Participants agreed that while some form of cooperation exists between the technology industry, law enforcement and civil society, more could be done to strengthen cooperation between internet and social media companies with law enforcement, establish communication and cooperation channels to improve prevention and combatting the crime of trafficking in human beings. This dialogue should continue in 2022

5. Lawful access to encrypted information

Encryption is an important tool for protecting cybersecurity and fundamental rights, however its widespread use also causes challenges to law enforcement and prosecutors to gain lawful access to electronic evidence needed to carry out investigations and safeguard citizens' security.

Following the adoption of the EU Council resolution on encryption, the Commission confirmed in the EU Strategy to tackle organised crime that it will work 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.

The Commission is steering the process to analyse with the relevant stakeholders the existing capabilities and approaches for lawful and targeted access to encrypted information in the context of criminal investigations and prosecutions. EU Member States answered a detailed 2-part questionnaire and participated in follow-up discussions and rounds of questions where necessary to assist with the mapping and analysis. Broader stakeholder consultations will follow to support identification of solutions.

[4] COM(2021) 171 final

Approaches should not result in a general weakening of encryption or in indiscriminate surveillance. This analysis will not only focus on addressing the current obstacles but will also anticipate the likely evolution of encryption and decryption technologies, and the necessary cooperation with academia and the private sector to this end. As indicated in the EU Strategy to tackle organised crime, the Commission will present a way forward in 2022.

6. Data retention

Access to electronic communications metadata is important for police and public prosecutors to ensure investigation of crimes and safeguarding of public security.

The Strategy to tackle Organised Crime presented in April 2021 announces that the Commission will analyse and outline possible approaches and solutions, in line with the Court's judgements, which respond to law enforcement and judiciary needs in a way that is operationally useful, technically possible and legally sound, including by fully respecting fundamental rights.

Accordingly, the Commission consulted Member States in June 2021 with a view to devising the way forward, as it is paramount to work together to find options that can deliver for security and that respect the framework set by the Court of Justice at the same time. Although most Member States indicated to be in favour of EU legislation, they are opposed to targeted retention, which is the 'model' that the Court advocates. Before taking a decision or devising any way forward, the Commission will wait for the outcome of the pending court cases in relation to national data retention regimes of Ireland and Germany and other cases related to data retention e.g. from France. The Advocate General of the Court issued his opinions in these cases on 18 November 2021. He essentially confirmed the Court's current case law, reiterating that the general and indiscriminate retention of traffic and location data relating to electronic communications is permitted only in the event of a serious threat to national security. It is therefore likely that the Court will also stick to its current reasoning.

7. E-evidence/Budapest convention/International negotiations

Electronic evidence is nowadays needed in 85% of criminal investigations. In more than half of criminal investigations, a cross-border request needs to be made to obtain electronic evidence for a criminal investigation.

The Commission's April 2018 e-evidence proposals aim to improve cross-border access to electronic evidence by introducing European Production and Preservation Orders that would allow EU Member State authorities to obtain e-evidence from service providers that are offering services in the Union, irrespective of the location of their headquarters or the location of the storage of the data. The proposes include strong safeguards to ensure a high level of protection of the persons whose data is sought by means of the orders.

The proposals are currently being discussed by the European Parliament and the Council as part of the EU legislative procedure. The first trilogue meeting took place on 20 February 2021, and four trilogue meetings have taken place until now (the last one on 9 July 2021). Although progress has been made in recent months, the discussions will continue under the French Presidency in the first half of 2022.

We should also work towards compatible rules at international level for cross-border access to electronic evidence to avoid conflicts of law.

The Commission has been participating, on behalf of the Union, in the negotiations for a Second Additional Protocol to the Council of Europe 'Budapest' Convention on Cybercrime since 2019. The Protocol aims to enhance cooperation on cybercrime and electronic evidence amongst the 66 State Parties to the Budapest Convention (including e.g. all EU Member States except Ireland, the United States, Canada and Japan). On 17 November 2021, the Committee of Ministers of the Council of Europe adopted the text of the Second Additional Protocol, which formally concludes the negotiation process. On 25 November

2021, the Commission adopted proposals for Council Decisions to authorise EU Member States to sign and ratify the Second Additional Protocol.

The Commission is also engaged, on behalf of the Union, in a negotiation for a bilateral EU-US agreement on cross-border access to electronic evidence. Four rounds of negotiations have taken place on 25 September, 6 November, 10 December 2019 and 3 March 2020. Although both sides are committed to the negotiations, it is difficult to make progress without more clarity on the internal EU rules on e-evidence. It is hoped that it will be possible to intensify the EU-US negotiations once trilogues on the EU internal rules on e-evidence move forward.

8. Artificial intelligence

Emerging technologies are becoming increasingly available to criminals. We can see a disconcerting trend of spreading deepfakes for deception, using drones for the transportation of explosives, communicating of highly secured encrypted devices.

The proposed AI regulation is a step to create trust in the technology by setting strict rules for high-risk AI tools. Law enforcement also needs to work with AI tools to be able to investigate crimes, while ensuring that there are string safeguards for privacy and fundamental rights.

9. Other relevant legislative initiatives – e-privacy and DSA

The December 2020 Commission proposal for the Digital Services Act (DSA) aims to ensure that providers of innovative digital services can fully benefit from the internal market, to contribute to online safety and the protection of fundamental rights in that context, and to set a robust and effective governance structure for the effective supervision of providers of intermediary services online. The proposal defines clear responsibilities for providers of intermediary services, and in particular online platforms, such as social media and online marketplaces. Amongst other things, this includes an obligation for providers to inform competent authorities about the follow-up given to orders to act against illegal content or to provide information about their users. Providers of hosting services would also need to report the suspicion of certain criminal offences to law enforcement and judicial authorities.

In the Council, the Slovenian Presidency obtained a General Approach at the COMPET Council on 25 November 2021. The European Parliament voted on its report on 20 January 2022. It is now expected that the co-legislators express their commitment to find an agreement swiftly, as both institutions consider the file a priority, with the French Presidency indicating the aim to reach an agreement during their term.

The Commission’s 2017 proposal for a Regulation on e-privacy aims to update and bring the current Directive in line with the General Data Protection Regulation and technological developments. In the second political trilogue held in November 2021 the co-legislators discussed some horizontal issues, endorsed several provisions on which there was provisional agreement at technical level, discussed provisions on which there was not yet such agreement and decided on the next steps.

The proposed e-privacy regulation (Article 11), like the current e-privacy directive (Article 15), provides Member States with the possibility to develop national data retention laws and to restrict the right to confidentially of communications for public interest purposes, such as criminal law enforcement, public security and national security. In its various data retention judgments, most recently on 6 October 2020, the Court confirmed that the exception in Article 15 of the Directive is precisely that: an exception that cannot become the rule. In imposing general and indiscriminate retention of data for law enforcement and national security purposes, the Court found that Member States were essentially turning the exception into the rule. Moreover, the Court was clear in stating that processing activities by private entities fall under the scope of e-privacy, read in light of the Charter of Fundamental Rights, irrespective of whether that processing was for national security, law enforcement or public security purposes. In light of the jurisprudence, the Council's General Approach proposes to carve out from the scope of the draft regulation not only the activities of state authorities (already excluded in the Commission proposal and in the current ePrivacy Directive) but also of providers when they process data for national security and defence purposes. The co-legislators have not yet discussed these data retention-related provisions. It is likely that they will be left to a later stage and are expected to be very difficult. With the entry into application of the European Electronic Communications Code ("EECC") on 21 December 2020, which changes the definition of electronic communications services, non-traditional communication services, such as webmail messaging services and internet telephony, will be covered by the ePrivacy Directive. They could thus in principle become subject to data retention requirements if legislators chose to include them.

Pages 24-27 redacted - out of scope