European Parliament

***To the European Commission***
*Margrethe Vestager, Executive Vice-President "A Europe Fit for the Digital Age"*
*Margaritis Schinas, Vice-President "Promoting our European Way of Life"*
*Věra Jourová, Vice-President "Values and Transparency"*
*Thierry Breton, Commissioner "Internal Market"*
*Didier Reynders, Commissioner "Justice"*
*Ylva Johansson, Commissioner "Home Affairs"*

Brussels, 27 January 2022

Dear Commissioners,

In March 2022 the Commission intends to propose unprecedented legislation requiring online service providers to **automatically and indiscriminately monitor** "relevant" services for potential child sexual exploitation material and to automatically report suspected users to the police. We are very concerned that this could make private communications via instant messaging, videoconferencing, chat and e-mail services subject to mass surveillance, and backdoors to end-to-end encrypted communications services could be required to enable general monitoring, while perpetrators would continue to use closed forums, self-hosted platforms and P2P networks.

In March[1] and October[2] 2021, Members of the European Parliament sent you letters underlining the need to do much more to protect children from sexual violence online and offline, including in terms of prevention, awareness-raising, support and law enforcement capacities. We stressed, however, that this **pressing need does not justify all means**. Indiscriminately and generally monitoring everybody's online activities "just in case" causes devastating collateral damage. It fails to respect the essence of the fundamental right to confidential communications (Article 7 of the Charter), and is therefore neither necessary nor proportionate, as clarified by the CJEU in the "Schrems I" judgment in 2015. It has a chilling effect on the exercise of fundamental rights online, including of children and victims, minorities, LGBTQI people, political dissidents, journalists etc. It sets a precedent for expanding it to other purposes. The outsourcing of law enforcement activities (crime detection) to private corporations and their machines removes the protection afforded by the independence and qualification of public investigators, as well as the institutional oversight over their activities. We are not aware of any other democratic state, including the United States, that imposes general monitoring on online intermediaries.

To this day we have **not received your response** to the October 2021 encryption day letter.

In the meantime we were alarmed to read media reports according to which investigators take down child sexual abuse platforms such as "Boystown" but **fail to report child sexual exploitation content** hyperlinked to by these platforms and hosted elsewhere, meaning that thousands of gigabytes of illegal images continued to be accessible. Investigators reportedly argue that they lack capacities to evaluate and report the material on child sexual exploitation websites.[3]

**Would you please explain:**

1. **Since Europol was involved in the "Boystown" investigation, is it correct to assume that Europol is not reporting known hyperlinks to child sexual exploitation content to the relevant hosting services?**
2. **How can ongoing child sexual abuse be detected and victims be rescued if investigators do not have sufficient capacities to screen known child sexual exploitation material such as was hyperlinked via the "Boystown" platform?**

1 https://www.patrick-breyer.de/wp-content/uploads/2021/03/20210318_COM_Letter_General_Monitoring.pdf.
2 https://www.patrick-breyer.de/wp-content/uploads/2021/11/20211020_Letter_General_Monitoring.pdf
3 Der Spiegel, Why Aren't Thousands of Gigabytes of Abusive Images Removed from the Web? (8 December 2021), https://www.spiegel.de/international/world/sexual-violence-against-children-why-aren-t-thousands-of-gigabytes-of-abusive-images-removed-from-the-web-a-99f36312-8054-479b-8d7c-ff86679daa45.

3. **Since perpetrators typically shared hyperlinks to encrypted file storages containing child sexual exploitation material, can the Commission confirm that indiscriminately monitoring private communications for known imagery would fail to detect such hyperlinks?**
4. **Have police standards or guidelines for sexual abuse investigations been developed?**
5. **Have Member States put centralized controlling of the number of investigations, their status and police capacities for investigating of child sexual abuse cases into place?**
6. **Have Member States centralized the processing and evaluation of seized image and video material or is this task assigned to local investigators?**
7. **Have police standards for carefully evaluating confiscated data with a view to identifying new material and victims been developed?**
8. **Does the Commission know whether national investigators can rely on sufficient hardware and software for data preparation and evaluation, technical tools for automated selection and reduction of data (AI), police hash databases and sufficient IT capacities to process seized data storage materials?**
9. **Are national child sexual abuse investigators trained specifically for this task and are they offered psychological support if needed?**

With criminal investigators lacking the capacities to evaluate the child sexual exploitation material already in their possession and identify victims of ongoing abuse, we are extremely concerned that **adding thousands and thousands of cases of circulation of well-known material via major communications services to their burden would fail victims whose safety depends on focusing all resources on preventing abuse** and the production of abuse imagery in the first place. To post new abuse imagery, perpetrators and producers do not typically use commercial messaging services, but closed channels. Once child sexual exploitation material has been produced and posted, it is technically impossible to effectively prevent its circulation, which is why all efforts need to focus on preventing abuse. We are alarmed therefore that the Commission's obsession with looking for recurrences of known material not only puts the privacy and security of all citizens at risk but also threatens to deprive victims of ongoing abuse of the capacities and protection they need. **While citizens are prepared to go a long way to keep children safe, your approach would do more harm than good when it comes to protecting children.**

The **effectiveness and efficiency** of the general algorithmic monitoring that you are pursuing has not been demonstrated. A German study confirmed years ago that "the solving of cases of sexual abuse on the occasion of investigations into child pornography is at best a random occurrence".[4] In line with this finding few cases of children rescued following NCMEC reports have been cited, and even fewer of those are demonstrably the result of indiscriminately monitoring private communications (rather than human reports and material detected on the web). Ever rising numbers of reports by US companies using indiscriminate content surveillance indicate that this method does not contain the circulation of illegal material. If it pushes such activities further underground (e.g. to dark net forums), it makes criminals even more difficult to prosecute. The only police force that has disclosed statistics, the Swiss Federal Police (Fedpol), says that 86% of the automatically generated US reports on allegedly illegal content do, in fact, not contain any criminally relevant material.[5] This means that every month thousands of innocent citizens are falsely reported to the police. Even true positive hits regularly result in the criminalization of children; for example in Germany 30% of all criminal investigations for child sexual exploitation material target minors.

The opposition to the Commission's plans to make mass surveillance of everybody's private communications mandatory is overwhelming. A representative survey in 10 EU Member States found that 72% of citizens oppose searching all private messages for allegedly illegal material, with only 18% supporting the idea.[6] The Commission's own public consultation on the proposal revealed that 51% of all respondents are opposed to indiscriminate monitoring by e-mail and messaging providers. Furthermore, 80% of respondents to the Commission's public consultation do not want indiscriminate monitoring to be applied to encrypted messages. A recent Special Eurobarometer on Digital Rights underlined that **91% of EU citizens consider the protection of the confidentiality of communications to be of the highest importance**.[7] Lately European IT professionals in the Council of European Professional Informatics Societies (CEPIS) have rejected the upcoming proposal as a

4 Abrecht et. al., Schutzlücken durch Wegfall der Vorratsdatenspeicherung? (2011), https://grundrechte.ch/2013/MPI_VDS_Studie.pdf, pp. 114 and 220.
5 Sonntagszeitung of 14 March 2021, p. 9.
6 https://nextcloud.pp-eu.eu/index.php/s/5bkdRGyxnAciNBz
7 Special Eurobarometer 518: Digital Rights and Principles (2021): https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=78937.

means of "total surveillance of digital communications in the EU".[8] Daniel Kretzschmar, spokesman for the Federal Board of the Association of German Criminal Investigators, warned that unsuspected persons could easily become the focus of investigations, and that privatizing detection means "making law enforcement dependent on these companies, which is actually a state and sovereign task."[9]

Having repeatedly postponed your proposal, you seem to be ignoring all this criticism and pushing ahead regardless.

Furthermore, you fail to explain how indiscriminate content surveillance could possibly meet the proportionality requirement under the Charter of Fundamental Rights. **According to the Court of Justice** "*the automated analysis of [communications] data can meet the requirement of proportionality only in situations in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and provided that the duration of that retention is limited to what is strictly necessary*" (case C-511/18, §§ 177-178). A **legal analysis on the matter by the German Bundestag**'s services[10] and the **legal expertise of Prof. Ninon Colneric,[11] a former judge at the Court of Justice**, confirm that "*EU legislation obliging providers of number-independent communications services (i.e. e-mail, messaging, chat) to generally and indiscriminately screen the content of all private correspondence for 'child pornography' and report hits to the police would not comply with the fundamental rights guaranteed by Articles 7, 8, 11 and 16 of the Charter*".

**Would you please explain:**

10. **In the Commission's view how can a requirement to indiscriminately, permanently and automatically analyze the content of all private communications possibly meet the requirement of proportionality under the Charter of Fundamental Rights and relevant case-law?**

Private companies generally and indiscriminately analysing the content of all private correspondence of citizens **compares to the post office opening and scanning all letters** in search of illegal content. A method as invasive as that is unacceptable with regard to the right of every citizen to respect for their communications. The confidentiality of communications is indispensable, including for counselling and victim support. Generally monitoring confidential communications can discourage victims from digitally seeking help and support. People relying on the confidentiality of communications also include citizens whose lives are in danger (e.g. witnesses, harassment victims). With search algorithms in place, self-recorded nude photos taken by minors (sexting) end up in the hands of company employees, organizations and authorities where they do not belong and are not safe. The citizens of Europe cannot accept having the confidentiality of their communications compromised, especially at times when digital correspondence has become the norm and indispensable for many in their private and professional lives.

The Commission's intention to also compel secure **end-to-end encrypted communications services** to search private correspondence would effectively turn every smartphone into a bug. Providers would need to implement a backdoor in their apps to enable such monitoring ("client-side scanning"). Such backdoors would not prevent the posting of CSAM via closed forums, self-hosted platforms or P2P networks. But implementing a routine for automatically searching and reporting suspected communications content in case of a match would break safe end-to-end encryption altogether and eliminate the security and trust that comes with it. Individuals, businesses and governments rely on end-to-end encryption to safeguard their personal, commercial and state secrets. The safety of individuals (e.g. witnesses, officials) depends on secure encryption protecting their confidential communications. Backdoors can and will be abused by criminals, foreign intelligence services and forces that seek to destabilise our society. The Commission keeps reiterating its commitment to not generally weaken encryption, but "client-side scanning" would do exactly this.

**We urge you to focus the upcoming legislative proposal on supporting and coordinating targeted investigations (including undercover investigations) and preventing child sexual abuse in the first place as well as providing assistance to victims, while refraining from creating or condoning a mass surveillance system of general and indiscriminate monitoring of electronic correspondence, relying on private**

8 Council of European Professional Informatics Societies (CEPIS): CEPIS against total surveillance of digital communications in the EU (7 December 2021), https://cepis.org/cepis-warns-against-new-regulation-to-oblige-monitoring-of-encrypted-content/.
9 Die Welt: Total surveillance (4 November 2021).
10 https://nextcloud.pp-eu.eu/index.php/s/rnGR3pXbZj7oQFn.
11 https://www.patrick-breyer.de/wp-content/uploads/2021/03/Legal-Opinion-Screening-for-child-pornography-2021-03-04_incl_Logos.pdf

**corporations and their error-prone algorithms to look for "suspicious" activities. Mass surveillance of digital correspondence specifically would cause widespread uncertainty, distrust and unrest among citizens and businesses for years before most likely being annulled by the CJEU in light of its case-law.**

Yours sincerely,

Patrick Breyer MEP

Rosa D'Amato MEP

Clare Daly MEP

Francesca Donato MEP

Gwendoline Delbos-Corfield MEP

Markéta Gregorová MEP

Francisco Guerreiro MEP

Irena Joveva MEP

Petra Kammerevert MEP

Marcel Kolaja MEP

Kateřina Konečná MEP

Sergey Lagodinsky MEP

Karen Melchior MEP

Mikuláš Peksa MEP

Ivan Vilibor Sinčić MEP

Mick Wallace MEP