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, 20 October 2021

Dear Commissioner,

On 1 December 2021, the Commission intends to propose unprecedented legislation requiring providers to **automatically and indiscriminately monitor "**relevant" online services in search of possible child sexual exploitation material and to report users to police. We are very concerned that private communications could be made subject to mass surveillance, and backdoors to end-to-end encrypted communications services could be made mandatory to enable general monitoring.

In March, several of us sent you a letter[1] 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, but stressing 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 is a method so far only used in authoritarian states such as China and sets a precedent for expanding it to other purposes in Europe as well. 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.

In the meantime a "temporary derogation from certain provisions of Directive 2002/58/EC" has been adopted (Regulation (EU) 2021/1232), but even supporters agree that it is "legally flawed"[2]. **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). It follows that such indiscriminate and general analysis of private communications may not be performed permanently and for everybody.

We have already shared with you the **legal expertise of Prof. Ninon Colneric, a former judge at the Court of Justice**, concluding that "*having regard to the relevant case-law, 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*

1 https://www.patrick-breyer.de/wp-content/uploads/2021/03/20210318_COM_Letter_General_Monitoring.pdf.
2 Sophia in 't Veld, on behalf of the Renew Group (5 July 2021), https://www.europarl.europa.eu/doceo/document/CRE-9-2021-07-05-ITM-017_EN.html

hits to the police would not comply with the fundamental rights guaranteed by Articles 7, 8, 11 and 16 of the Charter". "*If the providers were allowed instead of obliged to practice such screening, the result would be the same [...]*".[3]

We would now like to provide you with a **new legal analysis on the matter by the German Bundestag**'s services (attached). According to their legal assessment, the CJEU only deems automated analysis of communications content justifiable under EU law in exceptional circumstances. "*The permanent latent risk that a crime (even of a serious nature) may be committed should not suffice to justify continuous and comprehensive automated analysis.*" It follows that the legislation you are envisioning, providing for permanently analysing the content of private correspondence in order to search for possible crimes, would be legally flawed and doomed to be annulled by the CJEU.

At the same time the **effectiveness and efficiency** of general algorithmic monitoring has not been demonstrated. Ever rising numbers of reports by US companies using this method indicate that it does not contain the circulation of illegal material on the surface web. If it pushes such activities further underground (e.g. to dark net forums), it makes criminals even more difficult to prosecute. Any obligation in EU law would be easy to circumvent by using providers that do not have a subsidiary in Europe, or by using self-hosted communications services. 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.[4] This means that every month thousands of innocent citizens are falsely reported to the police. False accusations of possessing illegal material of minors may result in house searches, questioning etc. - the public visibility of which may have devastating effects on the lives of innocent citizens even if investigations are eventually closed. Even true positive hits regularly result in the criminalization of children; for example in Germany 30% of all criminal investigations for child pornography target minors.

We are particularly concerned about the practise of generally and indiscriminately analysing the **content of all private correspondence** of unsuspected citizens by private companies. This 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 (Article 7 CFR). 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 life is 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.

In her reply to our earlier letter, Commissioner Johansson announced stakeholder meetings but there seems to be no transparency whatsoever in this regard. The Commissioner wrote that the content of the proposed legislation would depend on the outcome of the impact assessment, and pointed out the **public consultation** on the matter. This public consultation has in the meantime revealed that **51% of all respondents are opposed to indiscriminate monitoring by e-mail and messaging providers.** Indeed 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.[5]

Furthermore 80% of respondents to the Commission's public consultation do not want indiscriminate monitoring to be applied to encrypted messages. Indeed there has been a **public outcry when Apple in August announced plans to indiscriminately search personal photos** for suspicious content on end user devices. More than 90 organisations urged Apple to scrap its plans: "*Once this capability is built into Apple products, the company and its competitors will face enormous pressure -- and potentially*

3 https://www.patrick-breyer.de/legal-opinion-screening-for-child-pornography-2021-03-04/
4 Sonntagszeitung of 14 March 2021, p. 9.
5 https://nextcloud.pp-eu.eu/index.php/s/5bkdRGyxnAciNBz

legal requirements -- from governments around the world to scan photos not just for CSAM, but also for other images a government finds objectionable."[6] More recently security experts warned: "*The proposal to pre-emptively scan all user devices for targeted content is* ***far more insidious than earlier proposals for key escrow and exceptional access****. Instead of having targeted capabilities such as to wiretap communications with a warrant and to perform forensics on seized devices, the agencies' direction of travel is the bulk scanning of everyone's private data, all the time, without warrant or suspicion.*"[7] Apple eventually put its plans on hold.

If the Commission now proposed to compel securely **end-to-end encrypted services** to search private correspondence, it would trigger a similar storm of protests. Providers would need to implement a backdoor in their software ("client-side scanning") to enable such monitoring. Implementing a routine for automatically 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.[8] Individuals, businesses and government 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 your efforts and capacities on supporting and coordinating targeted investigations and preventing child sexual abuse in the first place as well as providing assistance to victims, and to refrain from creating or condoning a mass surveillance system of generally and indiscriminately monitoring online activities and relying on private corporations and their error-prone algorithms for detecting alleged criminal activities. If the scope of your announced legislation extended to private correspondence it 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

Alviina Alametsä MEP
Rosa D'Amato MEP
Pernando Barrena MEP
Saskia Bricmont MEP
Antoni Comín MEP
Gwendoline Delbos-Corfield MEP
Francesca Donato MEP
Cornelia Ernst MEP
Claudia Gamon MEP
Markéta Gregorová MEP
Francisco Guerreiro MEP
Svenja Hahn MEP
Irena Joveva MEP
Petra Kammerevert MEP
Marcel Kolaja MEP
Moritz Körner MEP
Karen Melchior MEP
Clara Ponsatí MEP
Mikuláš Peksa MEP

6 https://cdt.org/wp-content/uploads/2021/08/CDT-Coalition-ltr-to-Apple-19-August-2021.pdf
7 Ableson et al.: "Bugs in our Pockets: The Risks of Client-Side Scanning", https://www.cs.columbia.edu/~smb/papers/bugs21.pdf
8 Internet Society: "Client-Side Scanning: What it is and why it threatens trustworthy, private communications", https://www.internetsociety.org/wp-content/uploads/2020/04/Client-side-Scanning-Fact-Sheet-EN.pdf