European Parliament

To the European Commission
Margrethe Vestager, Executive Vice-President „A Europe Fit for the Digital Age“
Věra Jourová, Vice-President „Values and Transparency“
Thierry Breton, Commissioner „Internal Market“
Didier Reynders, Commissioner „Justice“
Ylva Johansson, Commissioner „Home Affairs“

Brussels, 18 March 2021

Dear Sir/Madam,

the Commission has announced unprecedented plans to propose permanent 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. An online consultation is underway, including on whether private communications should be covered and on whether backdoors to end-to-end encrypted communications services should be required to enable this monitoring.

While we underline 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, this **pressing need does not justify all means**. Indiscriminately and generally monitoring everybody‘s online activities „just in case“ causes devastating collateral damage. 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.

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 darknet 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 decentralised communications services. The only police force that has disclosed statistics, the Swiss Federal Police (Fedpol), says that 90% of the automatically generated US reports on allegedly illegal content do, in fact, not contain any criminally relevant material. This means that every month thousands of innocent citizens could be 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 40% 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 electronically 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 being compromised, especially at times when digital correspondence has become the norm and indispensable for many in their private and professional lives.

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 for other purposes (e.g. detecting crime) or permanently.

We have commissioned Prof. Ninon Colneric, a former judge at the Court of Justice, with writing a **legal expertise** on this issue, which we attach to this letter. She concludes 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 hits to the police would not comply with the fundamental rights guaranteed by Articles 7, 8, 11 and 16 of the Charter".

If even securely **end-to-end encrypted services** were compelled to search private correspondence, they would need to implement a backdoor ("client-side scanning") to enable such monitoring. Disclosing a unique identifier ("hash value") of attachments to the provider for the purpose of matching, and implementing a routine for reporting the entire content unencrypted in case of a match, would break safe end-to-end encryption altogether and eliminate the security that comes with it.[1] 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. In a letter to concerned MEPs your Commission only recently committed to not generally weaken encryption, which "client-side scanning" would.

1 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

If providers were allowed rather than obliged to indiscriminately analyse the content of private communications, the interference in the fundamental rights to privacy, data protection and freedom of expression would still be disproportionate, according to Prof. Colneric's expertise. From the point of view of the individuals whose communications are placed under general monitoring it makes no difference whether data processing by a service provider takes place on the basis of a legal obligation or not. The collateral damage and chilling effect on citizens resulting from indiscriminately monitoring the content of private correspondence is the same.

We urge you to focus your efforts on supporting and coordinating targeted investigations and prevention efforts as well as assistance to victims, and refrain from creating or condoning a 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 such legislation extended to private correspondence it would very likely be annulled by the CJEU in light of its case-law, as confirmed by former CJEU judge Prof. Colneric.

Yours sincerely,

Patrick BREYER MEP

Saskia BRICMONT MEP

Damien CAREME MEP

Gwendoline DELBOS-CORFIELD MEP

Tineke STRIK MEP