



MESSAGING CONTROL: BRIEFING ON THE EPRIVACY DEROGATION

MESSAGING AND CHAT CONTROL:

The End of the Secrecy of Digital Correspondence.

The EU wants to have all private chats, messages, and emails automatically searched for suspicious content, generally and indiscriminately. The stated aim: To prosecute child pornography. The result: Mass surveillance through fully automated real-time messaging and chat control and the end of secrecy of digital correspondence.

In 2020 the European Commission proposed “temporary” legislation aimed at allowing the search of all private chats, messages, and emails for illegal depictions of minors and attempted initiation of contacts with minors. This is to allow the providers of Facebook Messenger, Gmail, et al, to scan every message for suspicious text and images. This takes place in a fully automated process and using error-prone “artificial intelligence”. If an algorithm considers a message suspicious, its content and meta-data are disclosed automatically and without human verification to a private US-based organization and from there to national police authorities worldwide. The reported users are not notified.

Some U.S. providers of services such as Gmail and Outlook.com are already performing such automated messaging and chat controls. Through a second piece of legislation, the EU Commission intends to oblige all providers of chat, messaging and e-mail services to deploy this mass surveillance technology.

Contents

How Does This Affect You?	2
The Timeline	4
What You Can Do	6
Argumente gegen die Chatkontrolle	7
Additional Information and Arguments	7
Why Messaging and Chatcontrol Harms Children	9
Documents on the Legislative Procedure	10
Critical Commentary and Further Reading	11
Press Releases	12



EUROPEAN PIRATES
in the European Parliament

HOW DOES THIS AFFECT YOU ?

- > **All of your chat conversations and emails will be automatically searched for suspicious content.** Nothing remains confidential or secret. There is no requirement of a court order or an initial suspicion for searching your messages. It occurs always and automatically.
- > If an algorithm classifies the content of a message as suspicious, **your private or intimate photos may be viewed** by staff and contractors of international corporations and police authorities. Also your private nude photos may be looked at by people not known to you, in whose hands your photos are not safe.
- > **Flirts and sexting may be read** by staff and contractors of international corporations and police authorities, because text recognition filters looking for “child grooming” frequently falsely flag intimate chats.
- > **You can falsely be reported and investigated** for allegedly disseminating child sexual exploitation material. Messaging and chat control algorithms are known to flag completely legal vacation photos of children on a beach, for example. According to Swiss federal police authorities, 90% of all machine-generated reports turn out to be without merit. 40% of all criminal investigation procedures initiated in Germany for “child pornography” target minors.



EUROPEAN PIRATES
in the European Parliament

PATRICK BREYER

- > **On your next trip overseas, you can expect big problems.** Machine-generated reports on your communications may have been passed on to other countries, such as the USA, where there is no data privacy – with incalculable results.
- > **Intelligence services and hackers may be able to spy on your private chats and emails.** The door will be open for anyone with the technical means to read your messages if secure encryption is removed in order to be able to screen messages.
- > **This is only the beginning.** Once the technology for messaging and chat control has been established, it becomes very easy to use them for other purposes. And who guarantees that these incrimination machines will not be used in the future on our smart phones and laptops?



EUROPEAN PIRATES
in the European Parliament

TIMELINE

What's next?

Trilogue negotiations are underway between representatives of the European Parliament and EU governments with participation of the EU Commission regarding the [legislative proposal](#). [The different positions of the three institutions are listed here in detail](#). Child protection organizations are exerting massive pressure. All parliamentary groups are in favor of indiscriminate messaging and chat control, with the exception of Greens/EFA and the Left. The adoption of the legislation could take place in March.

In April the EU Commission intends to make a second legislative proposal, which is to force all providers of email, messaging and chat services to comprehensively search all private messages in the absence of any suspicion.

According to the [case-law of the European Court of Justice](#) the permanent and comprehensive automated analysis of private communications **violates fundamental rights and is prohibited** (paragraph 177). For this reason, Member of the European Parliament Patrick Breyer has filed a complaint against U.S. companies Facebook and Google with the data protection authorities for violating the General Data Protection Regulation.

Timeline including dates on the following page.

Upcoming dates

- > **22 February 2021:**
Shadow rapporteurs' meeting
- > **23 February 2021:**
Second Political Trilogue negotiations between Council, Commission and Parliament
- > **26 February 2021:**
Internal technical negotiations of the European Parliament
- > **2 March 2021:**
Internal technical negotiations of the European Parliament
- > **Expected for early March:**
Third Political Trilogue
- > **Expected for April 2021:**
Third Political Trilogue
- > **Expected for May 2021:**
Commission proposal on mandatory messaging and chat controls



EUROPEAN PIRATES
in the European Parliament

WHAT YOU CAN DO

- > **Talk about it!** Inform others about the dangers of chat control. [Here, you can find tweet templates, share pics and videos](#). Of course, you can also create your own images and videos.
- > **Generate attention on social media!** Use the hashtags #chatcontrol and #secrecyofcorrespondence
- > **Reach out to your representatives in Parliament!** With one click on the name of the competent representative, you can send a [pre-worded message](#) to the negotiators [Birgit SIPPEL \(GER, Social Democrats\)](#), [Sophia IN 'T VELD \(ENG, Renew Liberals\)](#), [Annalisa TARDINO \(ENG, ID\)](#), [Patrick BREYER \(GER Greens/EFA\)](#), [Jadwiga WIŚNIEWSKA \(ENG, ECR\)](#) und [Cornelia ERNST \(GER, GUE/NGL The Left\)](#). However, experience has shown that individually worded messages are more effective.
- > **Contact your government's permanent representation.** EU governments are negotiating with the European Parliament.
- > **Generate media attention!** So far very few media have covered the messaging and chat control plans of the EU. Get in touch with newspapers and ask them to cover the subject – online and offline.
- > **Ask your e-mail, messaging and chat service providers!** Avoid Gmail, Facebook Messenger, outlook.com and the chat function of X-Box, where indiscriminate chat control is already taking place. Ask your email, messaging and chat providers if they generally monitor private messages for suspicious content, or if they plan to do so.

ADDITIONAL INFORMATION AND ARGUMENTS

1. **All citizens are placed under suspicion, without cause, of possibly having committed a crime.** Text and photo filters monitor all messages, without exception. No judge is required to order to such monitoring – contrary to the analog world which guarantees the privacy of correspondence and the confidentiality of written communications. According to a judgment by the European Court of Justice, the permanent and general automatic analysis of private communications violates fundamental rights (case C-511/18, Paragraph 192). Nevertheless, the EU now intends to adopt such legislation. For the court to annul it can take years. Therefore we need to prevent the adoption of the legislation in the first place.
2. **The confidentiality of private electronic correspondence is being sacrificed.** Users of messenger, chat and e-mail services risk having their private messages read and analyzed. Sensitive photos and text content could be forwarded to unknown entities worldwide and can fall into the wrong hands. NSA staff have reportedly circulated nude photos of female and male citizens in the past.
3. **Indiscriminate messaging and chat control wrongfully incriminates hundreds of users every day.** According the Swiss Federal Police, 90% of machine-reported content is not illegal, for example harmless holiday photos showing nude children playing at a beach.
4. **Securely encrypted communication is at risk.** Up to now, encrypted messages cannot be searched by the algorithms. To change that back doors would need to be built in to messaging software. As soon as that happens, this security loophole can be exploited by anyone with the technical means needed, for example by foreign intelligence services and criminals. Private communications, business secrets and sensitive government information would be exposed. Secure encryption is needed to protect minorities, LGBTQI people, democratic activists, journalists, etc.



EUROPEAN PIRATES
in the European Parliament

PATRICK BREYER

5. **Criminal justice is being privatized.** In the future the algorithms of corporations such as Facebook, Google, and Microsoft will decide which user is a suspect and which is not. The proposed legislation contains no transparency requirements for the algorithms used. Under the rule of law the investigation of criminal offences belongs in the hands of independent judges and civil servants under court supervision.
6. **Indiscriminate messaging and chat control creates a precedent and opens the floodgates.** Deploying technology for automatically monitoring all online communications is dangerous: It can very easily be used for other purposes in the future, for example copyright violations, drug abuse, or “harmful content”. In authoritarian states such technology is to identify and arrest government opponents and democracy activists. Once the technology is deployed comprehensively, there is no going back.
7. **The temporary legislation on the table is ineffective.** Contrary to its intent, it will not allow Facebook et al to continue the mass monitoring of private correspondence. It does limit the ePrivacy directive. The chat control, however, will continue to violate the General Data Protection Regulation (DSGVO) because it lacks a legal basis and violates the principle of proportionality. A complaint filed by Patrick Breyer is being examined by the Irish Data Protection Agency.

WHY MESSAGING AND CHAT CONTROL HARMS CHILDREN

Messaging and chat control is useless

Proponents claim indiscriminate messaging and chat control facilitates the prosecution of child sexual exploitation. However, this argument is controversial, even among victims of child sexual abuse. In fact, messaging and chat control can hurt victims and potential victims of sexual exploitation:

1. Safe spaces are destroyed.

Victims of sexual violence are especially in need of the ability to communicate safely and confidentially to seek counseling and support, for example to safely exchange among each other, with their therapists or attorneys. The introduction of real-time monitoring takes these safe rooms away from them.

2. Minors are being criminalized.

Especially young people often share intimate recordings with each other (sexting). With messaging and chat control in place, their photos and videos may end up in the hands of criminal investigators. German crime statistics demonstrate that 40% of all investigations for child pornography target minors.

3. It makes it more difficult to prosecute child sexual exploitation

Indiscriminate messaging and chat control does not contain the circulation of illegal material but actually makes it more difficult to prosecute child sexual exploitation. It encourages offenders to go underground and use private encrypted servers which can be impossible to detect and intercept. Even on open channels, indiscriminate messaging and chat control does not contain the volume of material circulated, as evidenced by the constantly rising number of machine reports.

Documents on the Legislative Procedure

- > [Legislative Proposal by the Commission](#) (10 September 2020)
- > [Report of the Committee for Civil Liberties, Justice and Home Affairs](#) (11 December 2020)
- > [Answers by the Commission to questions of the Members of Parliament](#) (28 September 2020)
- > [Answers by the Commission to questions of the Members of Parliament](#) (27 October 2020)
- > [Impact Assessment by the European Parliamentary Research Service](#) (05 February 2021)

Critical commentary and further reading

- > Prostasia Foundation: "[How the War against Child Abuse Material was lost](#)" (19. August 2020)
- > European Digital Rights (EDRi): "[Is surveilling children really protecting them? Our concerns on the interim CSAM regulation](#)" (24. September 2020)
- > Civil Society Organisations: "[Open Letter: Civil society views on defending privacy while preventing criminal acts](#)" (27. Oktober 2020)
- > European Data Protection Supervisor: "[Opinion on the proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online](#)" (10. November 2020)
- > Alexander Hanff (Victim of Child Abuse and Privacy Activist): "[Why I don't support privacy invasive measures to tackle child abuse.](#)" (11. November 2020)
- > AccessNow: "[The fundamental rights concerns at the heart of new EU online content rules](#)" (19. November 2020)
- > Global Encryption Coalition: "[Breaking Encryption Myths: What the European Commission's Leaked Report Got Wrong About Online Security](#)" (19. November 2020)
- > German Lawyer's Association (in German): "[Stellungnahme zur Übergangsverordnung gegen Kindesmissbrauch im Internet](#)" (24. November 2020)
- > Alexander Hanff (Victim of Child Abuse and Privacy Activist): "[EU Parliament are about to pass a derogation which will result in the total surveillance of over 500M Europeans](#)" (4. Dezember 2020)
- > German Data Protection Supervisor (in German): "[BfDI kritisiert versäumte Umsetzung von EU Richtlinie](#)" (17. Dezember 2020)

Press Releases

04-01-2021

[European Parliament Research Service: EU plans for blanket message and chat control violate fundamental rights](#)

Press Release by MEP Patrick Breyer

27-01-2021

[Act now: Unprecedented EU plans to indiscriminately screen private correspondence online'](#)

Press Release by MEP Patrick Breyer

04-01-2021

[Mass screening of electronic mail: Facebook suspends controversial 'incrimination machine'](#)

Press Release by MEP Patrick Breyer

07-12-2020

["Denunciation machine": EU Parliament supports mass surveillance of e-mail, messengers and chats](#)

Press Release by MEP Patrick Breyer

25-11-2020

[Mass surveillance to protect children? Opposition to new EU private messaging upload filter plans](#)

Press Release by MEP Patrick Breyer

28-10-2020

[Data protection supervisor to assess legality of blanket analysis of private communications in search for illegal content](#)

Press Release by MEP Patrick Breyer

17-09-2020

[Child protection through scanning of private messages? Investigation instead of monitoring!](#)

Press Release by MEP Patrick Breyer

10-09-2020

[Protect children without spying on citizens! Patrick Breyer warns against EU proposal on filtering of all private online communications](#)

Press Release by MEP Patrick Breyer

08-09-2020

[Effective child protection instead of indiscriminate interception: Patrick Breyer warns about the EU Commission's communications censorship plans](#)

Press Release by MEP Patrick Breyer