PATRICK BREYER
Digitaler Freiheitskämpfer und Europaabgeordneter

Chat Control

The End of the Privacy of Digital Correspondence

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

Other consequences of the proposal are ineffective network blocking, screening of person cloud storage including private photos, mandatory age verification leading to the end of anonymous communication, censorship in Appstores and the paternalism and exclusion of minors in the digital world.

Chat control 2.0 on every Smartphone

A majority of the Members of the European Parliament adopted the voluntary chatcontrol regulation on 6 July 2021 allowing providers to scan communications voluntarily. So far only a few unencrypted US services such as GMail, Meta/Facebook Messenger and X-Box scan private communications voluntarily.

The European Commission went a step further on the 11 May 2022 by presenting a proposal which would make chat control *mandatory* for all e-mail, chat and messenger providers and would even apply to so far securely end-to-end encrypted communication services. However, a public consultation by the Commission demonstrated **that the majority of respondents, both citizens and stakeholders, were opposed to an obligation to use chat control.** Over 80% of respondents opposed its application to end-to-end encrypted communications.

This is what the proposal actually entails:

EU Chat Control Proposal	Consequences

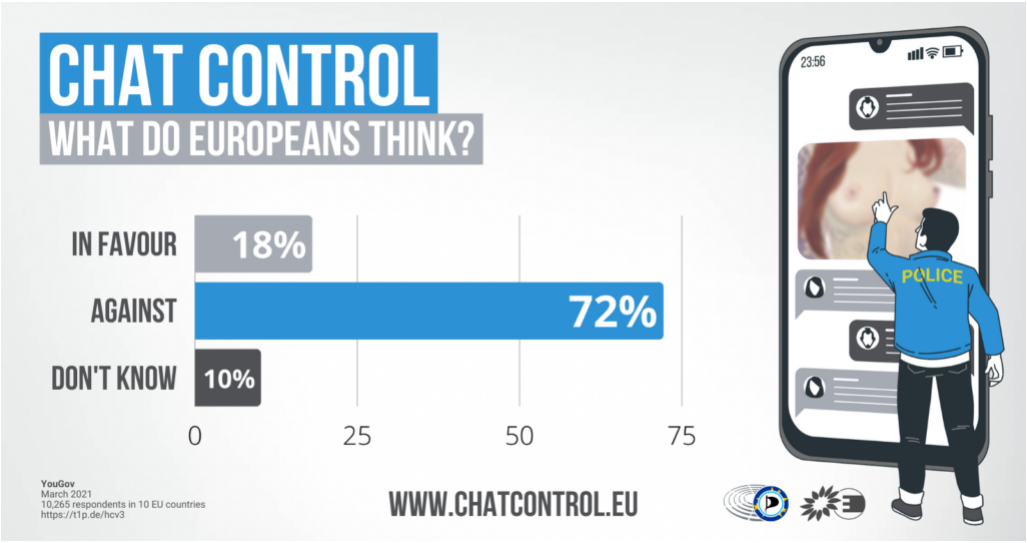
Envisaged are chat control, network blocking, mandatory age verification for communication and storage apps, age verification for app stores and exclusion of minors from installing many apps	
The communication services affected include telephony, e-mail, messenger, chats (also as part of games, on part of games, on dating portals, etc.), videoconferencing	Texts, images, videos and speech could be scanned
End-to-end encrypted messenger services are not excluded from the scope	Providers will of end-to-end encrypted communications services have to scan messages on every smartphone (client-side scanning) and, in case of a hit, report the message to the police
Hosting services affected include web hosting, social media, video streaming services, file hosting and cloud services	Even personal storage that is not being shared, such as Apple's iCloud, will be subject to chat control
Services that are likely to be used for illegal material or for child grooming are obliged to search the content of personal communication and stored data (chat control) without suspicion and across the board	Since presumably every service is also used for illegal purposes, all services will be obliged to deploy chat control
The authority in the provider's country of establishment is obliged to order the deployment of chat control	There is no discretion in when and in what extent chat control is ordered
Chat control involves automated searches for known CSEM images and videos, suspicious messages/files will be reported to the police	According to the Swiss Federal Police, 87% of the reports they receive (usually based on the method of hashing) are criminally irrelevant
Chat control also involves automated searches for unknown CSEM pictures and videos, suspicious messages/files will be reported to the police	Machine searching for unknown abuse representations is an experimental procedure using machine learning ("artificial intelligence"). The algorithms are not accessible to the public and the scientific community, nor does the draft contain any disclosure requirement. The error rate is unknown and is not limited by the draft regulation. Presumably, these technologies result in massive amounts of false reports. The draft legislation allows providers to pass on automated hit reports to the police without humans checking them.
Chat control involves machine	Machine searching for potential child grooming is an experimental procedure using machine

searches for possible child grooming, suspicious messages will be reported to the police	learning (“artificial intelligence”). The algorithms are not available to the public and the scientific community, nor does the draft contain a disclosure requirement. The error rate is unknown and is not limited by the draft regulation, presumably these technologies result in massive amounts of false reports.
Communication services that can be misused for child grooming (thus all) must verify the age of their users	In practice, age verification involves full user identification, meaning that anonymous communication via email, messenger, etc. will effectively be banned. Whistleblowers, humai rights defenders and marginalised groups rely on the protection of anonymity.
App stores must verify the age of their users and block children/young people from installing apps that can be misused for solicitation purposes	All communication services such as messenger apps, dating apps or games can be misused for child grooming and would be blocked for children/young people to use.
Internet access providers can be obliged to block access to prohibited and non-removable images and videos hosted outside the EU by means of network blocking (URL blocking)	Network blocking is technically ineffective and easy to circumvent, and it results in the construction of a technical censorship infrastructure

Protest

Protest now by contacting your national government, who decides in the Council about the proposal! Politely tell them your concerns about chat control (**arguments below**). Experience shows that a phone call is more effective than e-mails or letters. The official name of the planned mandatory chat control law is “Proposal for a Regulation laying down rules to prevent and combat child sexual abuse”.

How did we get here?



In 2020 the European Commission **initiated "temporary" legislation** which allows the searching of all private chats, messages, and emails for illegal depictions of minors and attempted initiation of contacts with minors. This allows 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, in part using error-prone "artificial intelligence". If an algorithm considers a message suspicious, its content and meta-data are disclosed (usually 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. However, a

representative survey conducted in March 2021 clearly shows that a majority of Europeans oppose the use of chat control (Detailed poll results here).

More videos on Chatcontrol are available in this playlist

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 algorithms 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, 86% 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.

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?

Click here for further arguments against messaging and chat control

Click here to find out what you can do to stop messaging and chat control

Timeline

The European Parliament adopted the legislation allowing for chat control on 6 July 2021.

On 11 May 2022 the EU Commission made 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. The European Parliament and the Council of the EU will discuss amendments. The deliberations could be completed by the end of 2022.

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). Former judge of the European Court of Justice Prof. Dr. Ninon Colneric has extensively analysed the plans and **concludes in a legal assessment that the EU legislative plans on chat control are not in line with the case law of the European Court of Justice and violate the fundamental rights of all EU citizens** to respect for privacy, to data protection and to freedom of expression. For this reason, Member of the European Parliament Patrick Breyer has **filed a lawsuit** against U.S. company Meta.

Upcoming dates

11 May 2022: Commission proposal on mandatory messaging and chat control

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**

Protest now by contacting the responsible EU Commissioners! Politely tell them your concerns about chat control (**arguments here**). Experience shows that a phone call is more effective than e-mails or letters. Officially, the planned obligation for messaging and chat control is called “legislation to effectively tackle child sexual abuse online”. Contact details on top of this page.

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

Mass surveillance is the wrong approach to fighting “child pornography” and sexual exploitation

Scanning private messages and chats does not contain the spread of CSEM. Facebook, for example, has been practicing chat control for years, and the number of automated reports has been increasing every year, most recently reaching 22 million in 2021.

Mandatory chat control will not detect the perpetrators who record and share child sexual exploitation material. Abusers do not share their material via commercial email, messenger, or chat services, but organize themselves through self-run secret forums without control algorithms. Abusers also typically upload images and videos as encrypted archives and share only the links and passwords. Chat control algorithms do not recognize encrypted archives or links.

The right approach would be to delete stored CSEM where it is hosted online. However, **Europol does not report** known CSEM material.

Chat control harms the prosecution of child abuse by flooding investigators will millions of automated reports, most of which are criminally irrelevant.

Message and chat control harms everybody

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.

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. A Google engineer has been **reported** to stalk minors.

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.

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.

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.

Indiscriminate messaging and chat control creates a precedent and opens the floodgates to more intrusive technologies and legislation. 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.

Messaging and chat control harms children and abuse victims

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. This can discourage victims from seeking help and support.
2. **Self-recorded nude photos of minors (sexting) end up in the hands of company employees** and police where they do not belong and are not safe.
3. **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.

4. **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.

Alternatives

Strengthening the capacity of law enforcement

Currently, the capacity of law enforcement is so inadequate it often takes months and years to follow up on leads and analyse collected data. Known material is often neither analysed nor removed. Those behind the abuse do not share their material via Facebook or similar channels, but on the darknet. To track down perpetrators and producers, undercover police work must take place instead of wasting scarce capacities on checking often irrelevant machine reports. It is also essential to strengthen the responsible investigative units in terms of personnel and funding and financial resources, to ensure long-term, thorough and sustained investigations. Reliable standards/guidelines for the police handling of sexual abuse investgations need to be developed and adhered to.

Addressing not only symptoms, but the root cause

Instead of ineffective technical attempts to contain the spread of exploitation material that has been released, all efforts must focus on preventing such recordings in the first place. Prevention concepts and training play a key role because the vast majority of abuse cases never even become known. Victim protection organisations often suffer from unstable funding.

Fast and easily available support for (potential) victims

1. **Mandatory reporting mechanisms at online services:** In order to achieve effective prevention of online abuse and especially grooming, online services should be required to prominently place reporting functions on the platforms. If the service is aimed at and/or used by young people or children, providers should also be required to inform them about the risks of online grooming.

2. **Hotlines and counseling centers:** Many national hotlines dealing with cases of reported abuse are struggling with financial problems. It is essential to ensure there is sufficient capacity to follow up on reported cases.

Improving media literacy

Teaching digital literacy at an early age is an essential part of protecting children and young people online. The children themselves must have the knowledge and tools to navigate the Internet safely. They must be informed that dangers also lurk online and learn to recognise and question patterns of grooming. This could be achieved, for example, through targeted programs in schools and training centers, in which trained staff convey knowledge and lead discussions. Children need to learn to speak up, respond and report abuse, even if the abuse comes from within their sphere of trust (i.e., by people close to them or other people they know and trust), which is often the case. They also need to have access to safe, accessible, and age-appropriate channels to report abuse without fear.

Document pool

Technical solutions to screen end to end encrypted communications (September 2020)

Answers given by the Commission to questions of the Members of Parliament (28 September 2020)

Answers given by the Commission to questions of the Members of Parliament (27 October 2020)

Impact Assessment by the European Parliamentary Research Service (5 February 2021)

Legal Opinion on the Compatibility of Chatcontrol with the case law of the ECJ (March 2021)

Answers by Europol on statistics regarding the prosecution of child sexual abuse material online (28 April 2021)

Voluntary chat control Regulation

Answer by the Commission in reply to a **cross-party letter** against mandatory chat control (9 March 2022)

Leaked opinion of the Commission sets off alarm bells for mass surveillance of private communications (23 March 2022)

Draft regulation on mandatory chat control (11 May 2022)

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 October 2020)

Civil Society Organisations and Trade Unions: "**European Commission: uphold privacy, security and free expression by withdrawing new law**" (8 June 2022)

> *"we suggest that the Commission prioritise this non-technical work, and more rapid take-down of offending websites, over client-side filtering […]"*

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)

> *"Due to the absence of an impact assessment accompanying the Proposal, the Commission has yet to demonstrate that the measures envisaged by the Proposal are strictly necessary, effective and proportionate for achieving their intended objective."*

Alexander Hanff (victim of child abuse and privacy professional): "**Why I don't support privacy invasive measures to tackle child abuse.**" (11 November 2020)

> *"As an abuse survivor, I (and millions of other survivors across the world) rely on confidential communications to both find support and report the crimes against us – to remove our rights to privacy and confidentiality is to subject us to further injury and frankly, we have suffered enough. […] it doesn't matter what steps we take to find abusers, it doesn't matter how many freedoms or constitutional rights we destroy in order to meet that agenda – it WILL NOT stop children from being abused, it will simply push the abuse further underground, make it more and more difficult to detect and ultimately lead to more children being abused as the end result."*

AccessNow: "**The fundamental rights concerns at the heart of new EU online content rules**" (19 November 2020)

> *"In practice this means that they would put private companies in charge of a matter that public authorities should handle"*

Federal Bar Association (BRAK) (in German): "**Stellungnahme zur Übergangsverordnung gegen Kindesmissbrauch im Internet**" (24 November 2020)

> *„the assessment of child abuse-related facts is part of the legal profession's area of responsibility. Accordingly, the communication exchanged between lawyers and clients will often contain relevant keywords. […] According to the Commission's proposals, it is to be feared that in all of the aforementioned constellations there will regularly be a breach of confidentiality due to the unavoidable use of relevant terms."*

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)

> *"I didn't have confidential communications tools when I was raped; all my communications were monitored by my abusers – there was nothing I could do, there was no confidence. […] I can't help but wonder how much different my life would have been had I had access to these modern technologies. [The planned vote on the e-Privacy Derogation] will drive abuse underground making it far more difficult to detect; it will inhibit support groups from being able to help abuse victims – IT WILL DESTROY LIVES."*

German Data Protection Supervisor (in German): „**BfDI kritisiert versäumte Umsetzung von EU Richtlinie**" (17 Dezember 2020)

> *"A blanket and unprovoked monitoring of digital communication channels is neither proportionate nor necessary to detect online child abuse. The fight against sexualised violence against children must be tackled with targeted and specific measures. The investigative work is the task of the law enforcement authorities and must not be outsourced to private operators of messenger services."*

European Digital Rights (EDRi): Wiretapping children's private communications: Four sets of fundamental rights problems for children (and everyone else) (10 February 2021)

> *"As with other types of content scanning (whether on platforms like YouTube or in private communications) scanning everything from everyone all the time creates huge risks of leading to mass surveillance by failing the necessity and proportionality test. Furthermore, it creates a slippery slope where we start scanning for less harmful cases (copyright) and then we move on to harder issues (child sexual abuse, terrorism) and before you realise what happened scanning everything all the time becomes the new normal."*

German Bar Association (DAV): "Indiscriminate communications scanning is disproportionate" (9 March 2021)

> *"The DAV is explicitly in favour of combating the preparation and commission of child sexual abuse and its dissemination via the internet through effective measures at EU-level. However, the Interim Regulation proposed by the Commission would allow blatantly disproportionate infringements on the fundamental rights of users of internet-based communication services. Furthermore, the proposed Interim Regulation lacks sufficient procedural safeguards for those affected. This is why the legislative proposal should be rejected as a whole."*

Letter from the President of the German Bar Association (DAV) and the President of the Federal Bar Association (BRAK) (in German) (8 March 2021)

> *"Positive hits with subsequent disclosure to governmental and non-governmental agencies would be feared not only by accused persons but above all by victims of child sexual abuse. In this context, the absolute confidentiality of legal counselling is indispensable in the interest of the victims, especially in these matters which are often fraught with shame. In these cases in particular, the client must retain the authority to decide which contents of the mandate may be disclosed to whom. Otherwise, it is to be feared that victims of child sexual abuse will not seek legal advice."*

Strategic autonomy in danger: European Tech companies warn of lowering data protection levels in the EU (15 April 2021)

> *"In the course of the initiative "Fighting child sexual abuse: detection, removal, and reporting of illegal content", the European Union plans to abolish the digital privacy of correspondence. In order to automatically detect illegal content, all private chat messages are to be screened in the future. This should also apply to content that has so far been protected with strong end-to-end encryption. If this initiative is implemented according to the current plan it would enormously damage our European ideals and the indisputable foundations of our democracy, namely freedom of expression and the protection of privacy […]. The initiative would also severely harm Europe's strategic autonomy and thus EU-based companies.*

Article in "Welt.de: Crime scanners on every smartphone – EU plans major surveillance attack" (in German) (4 November 2021)

> *Experts from the police and academia are rather critical of the EU's plan: on the one hand, they fear many false reports by the scanners, and on the other hand, an alibi function of the law. Daniel Kretzschmar, spokesman for the Federal Board of the Association of German*

> *Criminal Investigators, says that the fight against child abuse depictions is "enormously important" to his association. Nevertheless, he is skeptical: unsuspected persons could easily become the focus of investigations. At the same time, he says, privatizing these initiative investigations means "making law enforcement dependent on these companies, which is actually a state and sovereign task. "*
>
> *Thomas-Gabriel Rüdiger, head of the Institute for Cybercriminology at the Brandenburg Police University, is also rather critical of the EU project. "In the end, it will probably mainly hit minors again," he told WELT. Rüdiger refers to figures from the crime statistics, according to which 43 percent of the recorded crimes in the area of child pornographic content would be traced back to children and adolescents themselves. This is the case, for example, with so-called "sexting" and "schoolyard pornography ", when 13- and 14-year-olds send each other lewd pictures.*
>
> *Real perpetrators, who you actually want to catch, would probably rather not be caught. "They are aware of what they have done and use alternatives. Presumably, USB sticks and other data carriers will then be increasingly used again," Rüdiger continues.*

European Digital Rights (EDRi): **Chat control: 10 principles to defend children in the digital age** (9 February 2022)

> *"In accordance with EU fundamental rights law, the surveillance or interception of private communications or their metadata for detecting, investigating or prosecuting online CSAM must be limited to genuine suspects against whom there is reasonable suspicion, must be duly justified and specifically warranted, and must follow national and EU rules on policing, due process, good administration, non-discrimination and fundamental rights safeguards."*

European Digital Rights (EDRi): **Leaked opinion of the Commission sets off alarm bells for mass surveillance of private communications** (23 March 2022)

> *In the run-up to the official proposal later this year, we urge all European Commissioners to remember their responsibilities to human rights, and to ensure that a proposal which threatens the very core of people's right to privacy, and the cornerstone of democratic society, is not put forward.*

Council of European Professional Informatics Societies (CEPIS): Europe has a right to secure communication and effective encryption (March 2022)