European Union launches full scale war against internet privacy with #ChatControl (ePrivacy Derogation)

On July 6, 2021, the European Union voted on the new “ChatControl” proposal. With a shocking number of 537 Members of the European Parliament voting in favor, 133 voting against and 20 abstentions, it was approved. The proposal was put forward under the banner of “emergency measures” and it allows internet companies to scan users’ private messages for material containing child sex abuse. This controversial decision is supposed to fix problems with the European Electronics Communications Code, which came into force last December.

The so called “e-Privacy Interim Regulation” (2020/0259(COD)) requires online messenger and email service providers to automatically scan private message content in real time for suspicious text and image content using error-prone artificial intelligence. All cases identified by AI would be automatically disclosed to investigative authorities in the EU, without the individuals concerned knowing about it. This is intended to counter the spread of child pornography on the

internet, at least that is the story behind it.

But the EU's plans for ChatControl have been confirmed to violate fundamental rights by a former judge of the European Court of Justice.

The delegation of the European Pirate Party inserted in the Greens / EFA group has strongly condemned what it considers automated mass surveillance, which as they say means the end of privacy in digital correspondence. German Pirate Party Member of the European Parliament Patrick Breyer plans to take legal action against the regulation and is looking for victims of abuse who would file such a complainant. *„Abuse victims are particularly harmed by this mass surveillance*", says Breyer. *„To be able to speak freely about the abuse they have suffered and seek help in a safe space is critical to victims of sexualised violence. depend on the possibility to communicate safely and confidentially. These safe spaces are now being taken away from them, which will prevent victims from seeking help and support."*

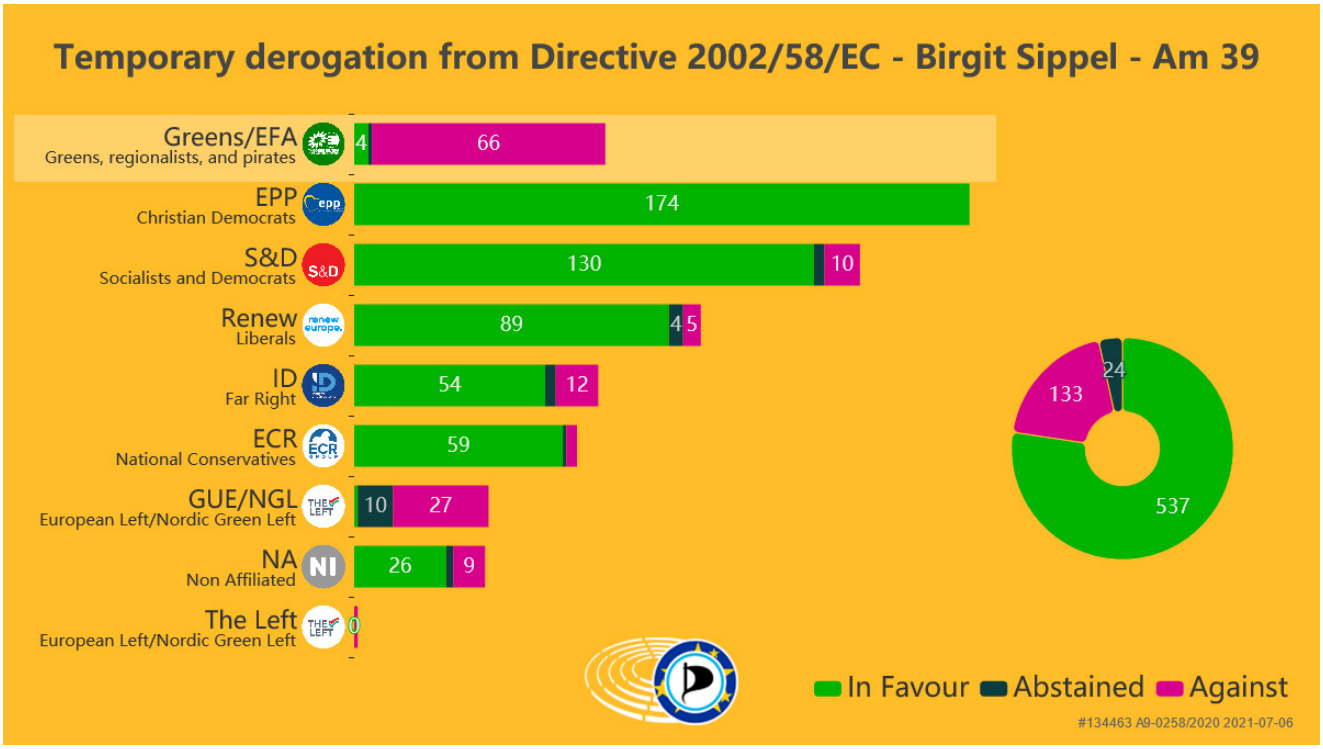
Digital Human Rights Blog states the following:

"The ePrivacy Derogation planned in the EU is an unprecedented attack on our electronic privacy of correspondence. And it is completely unsuitable for the supposed good purpose, combating child abuse. Sometimes you have the impression of being a little crazy. You read about something and think: that just can't be true, the whole world would be upset about that. But it is true. And nobody seems to be upset. That is what happened to me when I learned about the ePrivacy Derogation, a massive attack on our electronic privacy of correspondence, right from the heart of our liberal democracy.

One could just as well open all letters, scan all trash cans and equip all apartments, cellars, allotments and forests with cameras and microphones in the hope of finding evidence of child abuse. How is it that the argument "this may help

against child abuse" is capable of short-circuiting the voting behavior of most EU parliamentarians? It should be obvious, I thought, what immense damage this is doing to our fundamental rights. To our democratic processes, to the attitude to life of every single person, if we knew that our entire communication was under general suspicion."

Here are the results of the vote on the 6th of July:



So now the European Commission wants to make Chat Control mandatory for all email and messaging providers. And to check whether the content flagged by the algorithm is actually prohibited, a manual review would need to take place. This requires a technical feature allowing third parties to check the content of normally encrypted communications, a backdoor. So called secure end-to-end encrypted messenger services such as Signal, Whatsapp and Wire would be forced to install this backdoor. Arguably, this might be the biggest attack against internet privacy ever.

There is a considerable backlash against these plans: A public consultation carried out by the EU Commission revealed that 51% of all respondents oppose Chat Control for e-mail and

messaging providers. And over 80% of the European respondents do not want Chat Control to be applied to encrypted messages. Due to this resistance, EU Commissioner for Home Affairs Ylva Johannson has delayed the proposal until September 2021. Backdoors fundamentally jeopardise the security of end-to-end encryption, due to external adversaries such as intelligence services or criminal hackers being able to find and abuse these vulnerabilities. Nor is private correspondence, especially nude images, safe in the hands of the provider or the authorities, as reports of misuse of intimate data by US agencies as well as big tech companies have demonstrated.

Victims of a crime as terrible as child sexual abuse deserve steps that prevent the abuse in the first place. The correct approach would be, for example, to intensify covert investigations of child pornography networks and reduce delays in processing and evaluating seized data.

Is this even compatible with the GDPR?

The GDPR (General Data Protection Regulation) which governs the scope of personal data protection and the protection of rights of individuals with regard to the processing of their data. In article 22 of the GDPR, the European legislator has provided for particular guarantees for people who are subjected to automated decision making processes that may have legal (or similar) consequences.

The automated scanning of private conversations in search of child pornography can certainly lead to legal consequences for people (even serious ones), and for this I believe that the aforementioned article applies. Article 22 makes sure that the law authorizing this treatment must provide for adequate measures to protect the rights, freedoms and legitimate interests of individuals. Among the measures to protect people’s rights there are some particularly important:

- specific information to the interested party

- the right to obtain human intervention
- the right to obtain an explanation of the decision
- the right to challenge the decision

The legislator then specifies in recital 71 of the GDPR that these automated decisions should not concern a minor . Starting precisely from this point, it seems clear that the mass surveillance to which the European Commission wants to subject us cannot technically discriminate between minors and adults, thus violating the rights of the same people it intends to protect.

And regarding the rights provided for by article 22, at the moment there is nothing found in the regulation that shows of any way to obtain human intervention and challenge the decision. There is also no record of how people will be specifically informed that all their chats and emails will be subject to surveillance and eavesdropping.

What can we do to stop this?

Perhaps start out with learning more about ChatControl: www.chatcontrol.eu

I will write an update about this situation soon.

Do you like the things I do or the articles I write? You can follow me on Twitter @CensoredLubbers to stay in touch. I never ask for donations or money, but I do spend hours a day on writing things. So if you want to buy me a coffee to stay awake, you can do that here: Buy Me A Coffee. Thanks!