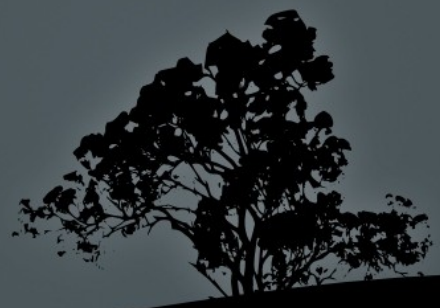
Fight Chat Control

Regulation to Prevent and Combat Child Sexual Abuse, aka "Chat Control"

Fight Chat Control

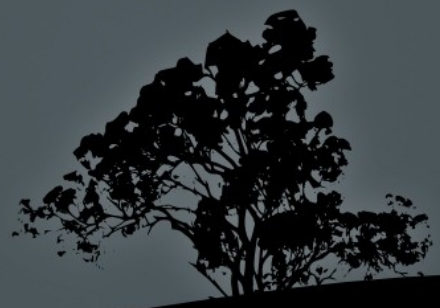
It is not the first time where children protection is used as a pretext to enforce authoritarian policies. Other similar pretexts:

- Terrorism
- Fighting Crime
- Copyright Infringement



Similar policies we faced in the past

- Online Safety Act, UK (2023)
- ~~TPP~~, Multilateral (2016~~)~~
- ~~PROTECT IP Act~~, USA (2011)
- ACTA, Multilateral (2011)
- ~~SOPA~~, USA (2011)
- Patriot Act, USA, (2001)



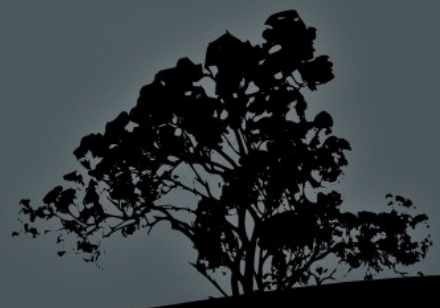
Impact

Mass Surveillance

- Every private message, file, picture will be intercepted
- No suspicion required
- No exceptions (unless you are a political figure!)
- Even encrypted communication → No end-to-end encryption will be allowed
- Or alternatively they will scan at the client side before the data will be encrypted

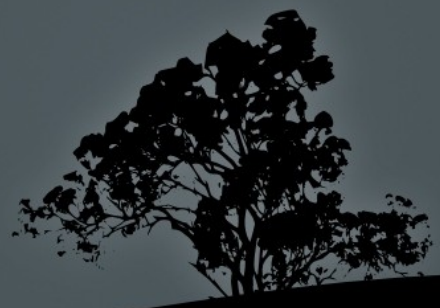
Breaking Encryption

- End-to-end encryption is vital for journalists, lawyers, refugees, political dissidents, whistleblowers, …
- Sensitive data like financial, medical, private will be intercepted
- Exposes citizens to cybercriminals, hostile actors, authoritarian regimes, ...



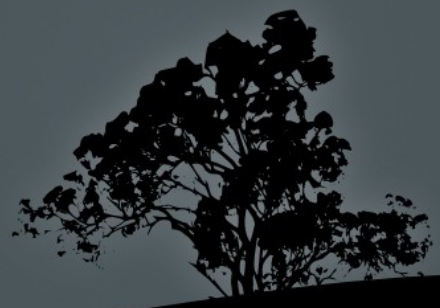
Fundamental Rights

- Violates our fundamental rights to privacy and data protection
- Articles 7 & 8 of the EU Charter
- Incompatible with the core European democratic values



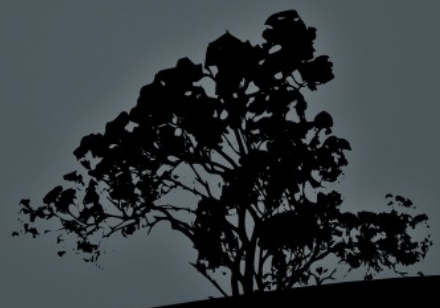
False Positives

- Automated systems often misinterpret content as harmful
- AI frequently outputs nonsense that can be hilarious but some times even dangerous
- This can result in false accusations and damaging investigations
- It can lead to abuses for personal or corporate profit



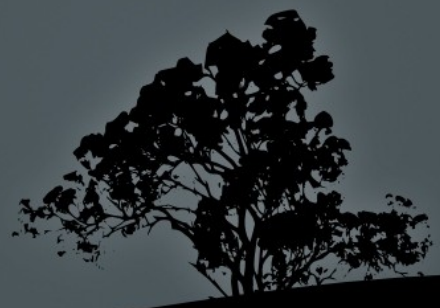
Ineffective Child Protections

- Child protections experts warn that these measures are ineffective or harmful even
- Weakening security for everyone especially the most vulnerable
- Diverts critical funds and resources from proven protective measures



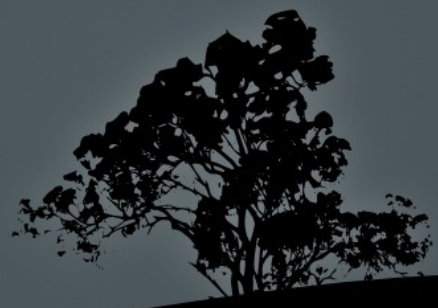
Global Precedent

- EU rules and regulations are an example to follow internationally (examples: GDPR, the right to repair)
- A harmful legislation can create a dangerous precedent that can empower dictators and authoritarian regimes
- This could undermine privacy and freedom of expression worldwide



Practical considerations

- Besides the mainstream communication platforms there are numerous self-hosted and peer to peer end-to-end encryption solutions and anomymization solutions
- Criminals will revert to these systems
- Unless the EU goes full Orwell (re: “1984”) and ban these alternatives systems, there is no way for this policy to serve the intended purpose



Alternative solutions

- Jami: E2E/distributed
- Tox: E2E/distributed
- Element/Matrix: E2E/decentralized
- VPNs: Anonymous browsing
- TOR: Anonymous browsing
- Hyphanet: Anonymous, censoship resistant network

What we expect from our representatives?

- Transparency for political figures
- Privacy for citizens
- Protect end-to-end encryption and anonymous networks
- Vote against “Chat Control”
- Promote Free and Open Source software for public administrations (“Public money, Public code”)

Important Dates

- 12 September 2025: EU Member States finalize positions in Council working groups.
- 14 October 2025: Earliest expected Council vote.

Who is behind this?

- It is proposed by the European Commissioner for Home Affairs **Ylva Johansson**
- She has connections with companies like Thorn and WeProtect who sell surveillance software
- She ordered targeted advertisements on Twitter paid by EU funds. This is illegal according to EU rules

Who fights against this?

- EDRi (European Digital Rights)
- FSFE (Free Software Foundation Europe)
- Cyprus FLOSS Community

What can we do?

- Contact our MEPs:
  https://fightchatcontrol.eu/
- Contact journalists, podcasters, influencers
- Contact political parties, unions, interest groups

Thank you!

License