Chat Control og ProtectEU
Stilhed før stormen?

Jesper Lund
IT-Politisk Forening
jesper@itpol.dk

Cryptohagen
29. juni 2025

To forskellige EU-initiativer

- **Chat Control** aka CSA-forordningen
  - EU-lovforslag fremsat i maj 2022
  - Stadig under behandling.. (del 1, del 2, del 3)
- **ProtectEU** – EU strategi for intern sikkerhed
  - Fortsættelse af arbejdet i Going Dark HLG
  - Ønske: målrettet aflytning af E2EE tjenester

Chat Control

Chat Control i én sætning..

- Artikel 10, stk. 1
  - Udbydere [..] der har fået et opsporingspåbud, **efterkommer påbuddet ved at installere og drive teknologier til opsporing** af udbredelsen af kendt eller nyt materiale, der viser seksuelt misbrug af børn, eller hvervning af børn [..] ved hjælp af de **tilsvarende indikatorer, der stilles til rådighed af EU-centret** [..]

Lidt længere version

- Forordning om regler til forebyggelse og bekæmpelse af seksuelt misbrug af børn
- Omfattede udbydere
  - Interpersonelle kommunikationstjenester (”chat”)
  - Hostingtjenester (private og offentlige)
  - App stores (risiko vurdering/begrænsning)
  - Internetudbydere (blokering på URL niveau)

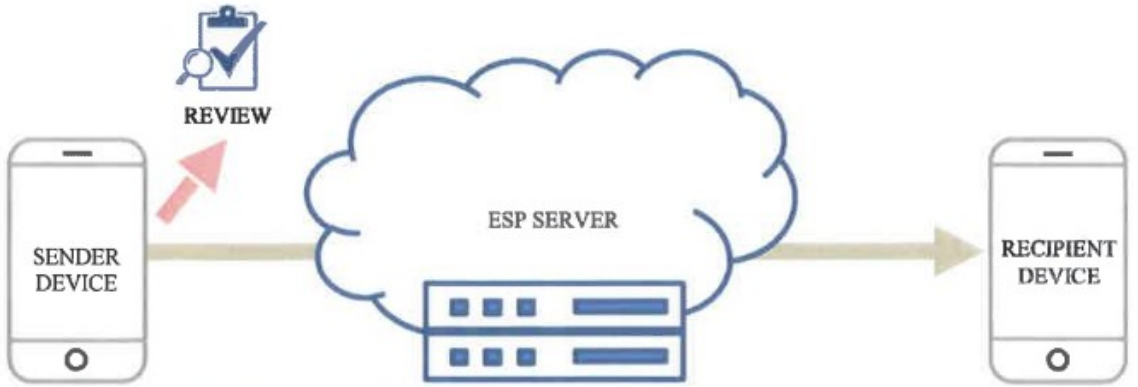
Også E2EE chat-tjenester

- Godt skjult i lovforslaget
  - The proposed obligations on service providers as regards the detection of child sexual abuse material are **technologically neutral** [..]. **It is an obligation of result not of means**, leaving to the provider the choice of technology to be operated [..].

    This **includes** the use of **encryption technology**.

Client-side scanning

Figure 4: all detection done on-device



Device: applies tools to detect CSA (e.g. hashing of images and matching with a database of known CSAM). If CSA is:

a) not detected ⇨ encrypts message end-to-end and sends to recipient
b) detected ⇨ sends message for review and/or reporting

ESP server: cannot apply existing tools to detect child sexual abuse on end-to-end encrypted messages

Device: receives and decrypts message

Fra EU forslag til vedtagelse

- Kommissionen fremsætter forslag (maj 2022)
- Igangværende proces
  - Europarlamentet har vedtaget rapport med ændringsforslag i november 2023
  - Rådet kan stadig ikke blive enig om en forhandlingsposition med EP
- Derefter trilogforhandlinger (fremtiden, måske)

Europaparlamentet

- Ændringsforslag
  - Kun **målrettede påbud** om opsporing – ingen masseovervågning
  - **E2EE-tjenester helt undtaget** fra CSA-forordningen
  - Ingen obligatorisk **alderskontrol** (undtagen porno)
  - Krav om ”zero knowledge” alderskontrol
  - Alle forslag om udvidelser af CSAR fra MEPs (frivillig scanning, søgemaskiner, m.v.) taget af bordet

Dansk nyhedsdækning :(

16. november 2023 kl. 05.00

EU-Parlamentet vil beskytte kryptering og undgå masseovervågning i CSAM-forslag: "Vi mangler svar på, hvordan man så vil løse problemet"

Red Barnet og Digitalt Ansvar er skuffede over de ændringer, som LIBE-udvalget i Europa-Parlamentet ønsker at lave til Kommissionens tiltag mod spredning af materiale med misbrug af børn online. It-Politisk Forening roser derimod udvalget for at have sagt "klart nej til masseovervågning".

Rådet (EU-landene)

- Flertal for masseovervågning, **inklusive E2EE**, som i Kommissionens forslag
- Blokerende mindretal efter **tre års diskussioner**
  - E2EE og cybersikkerhed
  - Usikre teknologier for andet end kendt CSAM
- Ignorerer Opinion fra Rådets Juridiske Tjeneste om at CSAR er **ulovlig masseovervågning**

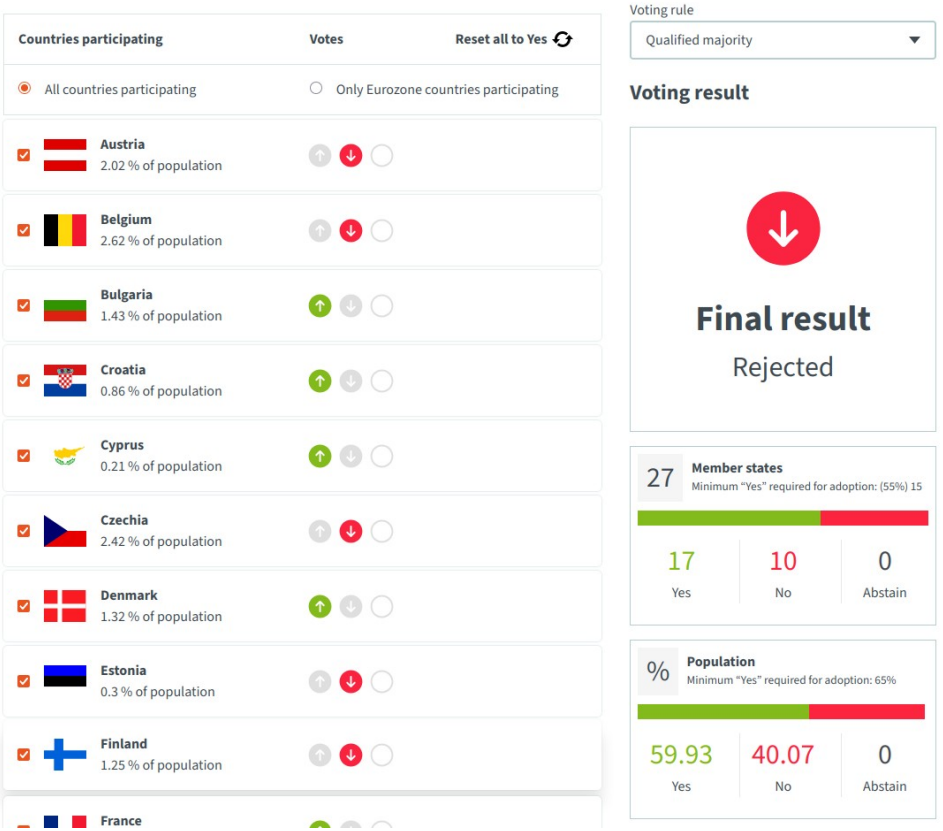
Forsøg på at skabe kompromis - 1

- Fjern/udskyd de mest problematiske dele
  - Løbende evaluering om udvidelse senere
- **Belgien** (1. halvår 2024)
  - Udelad grooming (kun kendt og ukendt CSAM)
  - Kun for high-risk tjenester (E2EE = high risk)
  - Samtykke til overvågning (hvis nej: ingen deling af video og billeder, be scanned – or get banned!)

Forsøg på at skabe kompromis - 2

- **Ungarn** (2. halvår 2024)
  - Kun scanning for kendt CSAM (rettet mod NL)
  - Stadig client-side scanning af E2EE
  - Trods pression: **blokerende mindretal holdt** på rådsmøde i dec'24 (AT, DE, SI, LU, NL, CZ, PL, EE, FI og BE)
- **Polen** (1. halvår 2025)
  - Nyt forslag: kun frivillig scanning som Chat Control 1.0
  - Klar afvisning fra de øvrige EU-lande

Council Voting Calculator



Next up: Danmark

- Danmark er stor tilhænger af Chat Control
  - Vil rulle polske ændringsforslag tilbage
  - Hummelgaard drømmer om at forbyde E2EE
- Men hvad kan DK realistisk gøre..
  - BE og PL har nærmest forsøgt alt med kosmetiske ændringer (bevarer masseovervågning af E2EE)
  - Mulig game changer: ny tysk regering?

ProtectEU
Going Dark HLG

Hvad er Going Dark HLG

- **Ikke konkret lovforlag** som Chat Control
- HLG er en arbejdsgruppe
  - Anbefalinger fra HLG maj 2024
  - Input til Kommissionen, ikke officiel politik p.t.
- Fokus på at fremme ”adgang til data” for politiet
  - Udfordringer skabt af kryptering
  - Manglende tilgængelighed for data (logning)

Vores protester virker!

- HLG ser den offentlige debat som et problem
  - Furthermore, the **current state of the public discourse** concerning privacy and security, which are at times erroneously contrasted, was proposed as a factor which **might have negatively affected the development of legislation to develop lawful pathways** for law enforcement authorities to access data.
- **Warning!!** HLG strategi om at omdefinere begreber, fx ”security by design” og hvad der (ikke) er en bagdør

Hvad lovede HLG..

- Bagdør med nyt navn (fra 8281/23)
  - The HLEG **will demonstrate** that security can be effectively strengthened whilst being in full compliance with the highest data protection and justice standards and safeguards. The concept of **‘security by design’ i.e., combining access by design and privacy by design** is important in this context and will be explored to the full.

..hvad leverede HLG

- Anbefaling nr. 26 (TL;DR nedsæt ny HLG..)
  - **Establishing a research group to assess the technical feasibility of built-in lawful access obligations** (including for accessing encrypted data) for digital devices, while maintaining and without compromising the security of devices and the privacy of information for all users as well as **without weakening or undermining the security of communications.**

EDRi: mission failure

ProtectEU strategi

- Meddelelse fra KOM i april 2025
  - Kommissionen **udarbejder i 2026 en køreplan** for kryptering med henblik på at kortlægge ”hvilke teknologiske løsninger der vil gøre det muligt [..] at tilgå krypterede oplysninger på en lovlig måde og **beskytte cybersikkerheden** og de grundlæggende rettigheder.”
- Plan om at udarbejde en plan.. (intet nyt)

Søges: den sikre bagdør

- Køreplan for adgang til data (24. juni 2025)
  - The HLG recommended taking a cautious approach to designing solutions for lawful access to systems, whereby industry **should not be asked to integrate systems that are likely to weaken encryption in a generalised or systemic way** for all users of a service.
  - Commission is tasking an expert group to provide **support in preparing a technology roadmap** on encryption.

Ny ekspertgruppe

- Opgaver ifølge terms of reference
  - Kortlæg nuværende tekniske løsninger for adgang til E2EE **uden at underminere** cybersikkerhed
  - Vurdering af disse løsninger (nemt – **der er ingen!**)
  - Hvis løsninger ikke eksisterer, skal ekspertgruppen komme med anbefalinger for udvikling
- Det har vi set før, ikke..?

Fremtiden for E2EE i EU

- Kommer der forslag med **krav om aflytning**?
  - **Ja:** Konsensus om at få denne mulighed
  - **Nej:** ingen aner hvordan det skal gøres uden at svække sikkerheden (og det vil man ikke, officielt)
  - Måske en ”Chat Control” model, hvor tjenesterne får ansvaret for at **gøre det umulige**? Måske..
- Laaang proces med mange udfordringer

EMD-dom om bagdøre i E2EE

- Podchasov v. Russia (33696/19)
  - E2EE er vigtig for retten til privatliv
  - Beskytter mod ulovlig overvågning
  - Lovgivning som kræver mulighed for aflytning af E2EE **svækker sikkerheden for alle brugere**
  - Udgør derfor et ikke-proportionalt indgreb i retten til privatliv (læs: **krav om bagdøre er ulovligt**)

Udbyderne afviser E2EE-bagdøre

- Case: UK Technical Capability Notices
  - Lovgivning om bagdøre fra IP Act 2016
  - Blev først anvendt i 2024 mod Apple
- Apple stopper E2EE-backup tjeneste i UK
- Tilsvarende udtalelser fra udbydere om Online Safety Act (UK), Chat Control (EU), etc.