Chat Control
Hvad sker der i Bruxelles?

Jesper Lund
IT-Politisk Forening
jesper@itpol.dk

Cryptohagen
26. marts 2023

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** [..]
- Overvågning NSA-style
  - Which people? The whole kingdom, Snow White (alle brugere)

Lidt længere version

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

Chat- og hostingtjenester

- Alle udbydere
  - Risikovurdering (”internettet er farligt for børn”)
  - Risikobegrænsning, fx alderskontrol
  - Risikorapportering til national myndighed
- Hvis **betydelig risiko** for anvendelse til misbrug af børn: påbud om opsporing i tre versioner
  - Kendt CSAM
  - Ukendt CSAM
  - Grooming (hvervning af børn)

Teknologier til opsporing

- Kendt materiale
  - Perceptual hashes (PhotoDNA, Neuralhash, m.v.)
  - Moden teknologi med høj præcision
- Ukendt materiale
  - AI classifiers til at genkende misbrug af børn
  - Stor usikkerhed
- Grooming
  - AI classifiers til at genkende grooming
  - Endnu større usikkerhed

Server-side scanning

Figure 1: detection of CSA in communications that are not end-to-end encrypted

Device: sends non E2EE message

ESP server: applies tools to detect CSA:
a) Detected ⇨ message forwarded for review/reporting
b) Not detected ⇨ message forwarded to recipient

Device: receives non E2EE message

Når AI tager fejl..

A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal.

Google has an automated tool to detect abusive images of children. But the system can get it wrong, and the consequences are serious.

Give this article 1.7K

By Kashmir Hill

Published Aug. 21, 2022 Updated Aug. 25, 2022

Hvad med kryptering?

- Også omfattet! (godt skjult i forslaget)
  - The proposed obligations on service providers as regards the detection of child sexual abuse material are **technologically neutral**, meaning they do not prescribe which technology should be used for detection. **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**.

Tjenesterne må finde ud af det..

Jesper Lund
@je5perl

The Commission has a clever political solution to solving the impossible problem of LEA access without mandating specific #encryption backdoors: put companies in charge of weakening the security of their own communications services!

(See statewatch.org/news/2020/sept... by @StatewatchEU)

- Given the broad spectrum of encryption solutions that may be concurrently deployed on devices or systems to provide multiple layers of protection, in the opinion of the Commission services there should be no single prescribed technical solution to provide access to the encrypted data (principle of technological neutrality). Companies providing the encryption for their products can contribute to identifying the best solutions.

Client-side scanning (CSS)

- Annex 9 i konsekvensanalysen
  - Identisk med udkast lækket i september 2020
  - Ingen svar på den omfattende kritik af CSS, fx ”Bugs in our Pockets” papiret fra oktober 2021
- Er det teknisk muligt?
  - Apple udspil i august 2021 om **kendt CSAM**, som blev trukket tilbage efter voldsom kritik
  - Større AI model på device? Næppe muligt.
- WhatsApp og Signal har offentligt afvist at kompromittere deres E2EE tjenester

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:

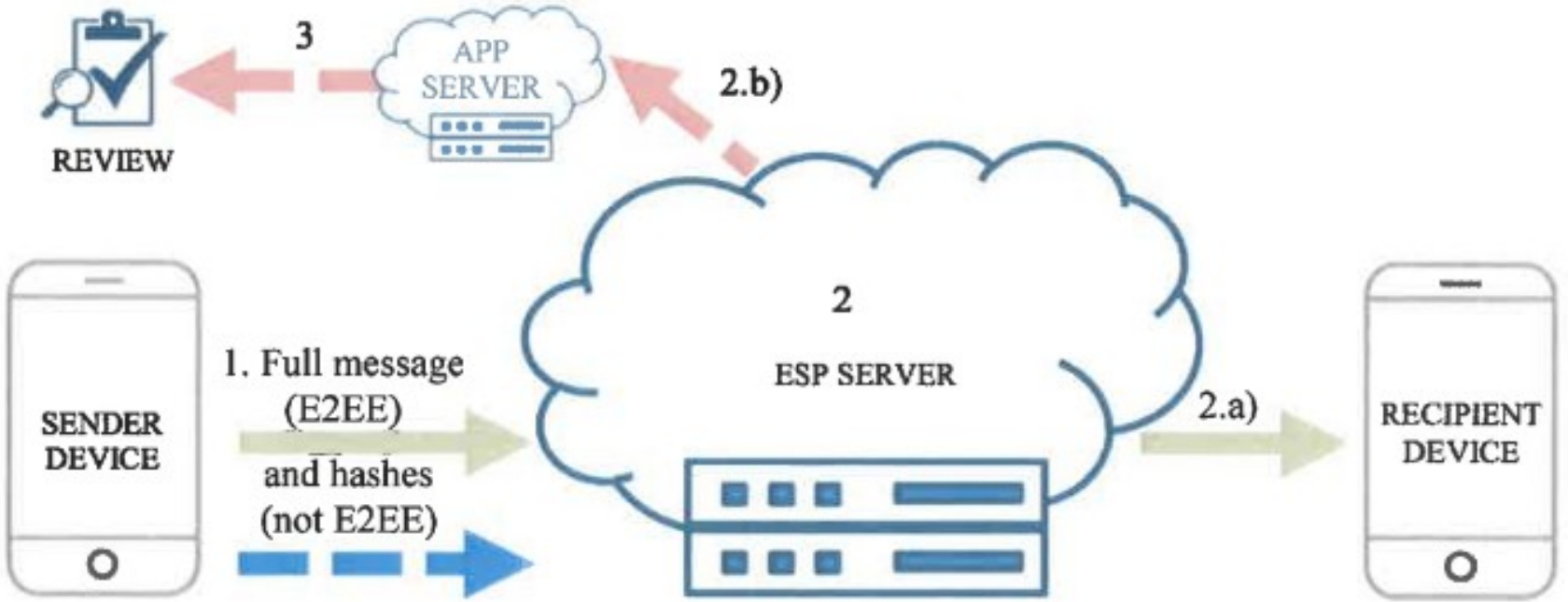
a) not detected ⇨ encrypts message end-to-end and sends to recipient
b) detected ⇨ sends message for review and/or reporting

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

Device: receives and decrypts message

Client-side scanning med match af hashes på server

Figure 5: on-device hashing with matching at server



Hvor udbredt bliver påbud om opsporing?

- TL;DR **uklart** (ikke alle tjenester)
  - Betydelig risiko bredt defineret
  - Krav om proportionalitet som kan begrænse
- **Flere end** der i dag laver **frivilling scanning**
  - Det er tydeligt, at den frivillige tilgang ikke fungerer. Én enkelt virksomhed [Meta] tegner sig for 95% af alle indberetninger [NCMEC] på verdensplan, og fem virksomheder tegner sig til sammen for 99% af alle indberetninger (KOM Q&A om forslaget).

Hvem rådgiver Kommissionen?

Ikke evidens-baseret forslag

- TU Delft forskere har lavet faktatjek af seks påstande fra Kommissionen
- Mindst tre påstande er falske!

Statement	Verdict
1 in 5 children is victim of sexual abuse online	*False*
85 million photo and videos of CSAM have been intercepted in 2021	*True*
90% of CSAM material is hosted in the E.U.	*False*
45% of CSAM material worldwide is hosted in the Netherlands	*Unclear, but it is likely substantial*
Report of CSAM in the E.U. member states have increased with 6,000% the last ten years	*False*
Distribution of CSAM is shifting from imagehosters to encrypted chatservices	*Not supported by the evidence*

- KOM har ikke overvejet andre tiltag end masseovervågning for at beskytte børn online

Fra EU forslag til vedtagelse...

- Kommissionen fremsætter forslag (maj 2022)
- Igangværende proces
  - Europarlamentet laver ændringsforslag
  - Rådet laver ændringsforslag
- Derefter: trilog-forhandlinger
- Ønske om at få processen afsluttet i 2023!
  - EP valg og ny EU-Kommission i 2024 (uden Ylva Johansson) spiller nok en rolle her

Europarlamentet

- LIBE udvalget
  - Udkast til rapport 14. april 2023
  - Ændringsforslag fra andre frem til 19. maj
  - Derefter forhandlinger og afstemning i LIBE
- Rådgivende udvalg: IMCO, FEMM og CULT
  - IMCO rapport udkast (Saliba) med mange gode ændringsforslag, bl.a. undtage E2EE tjenester, ingen alderskontrol og kun scanning for kendt CSAM
  - Andre i IMCO støtter eller vil udvide KOM forslaget
- Uklart hvad EP position bliver

Rådet (EU-landene)

- Arbejdsgruppe: Law Enforcement WP
  - Officielt **indre marked** forslag (TEUF Artikel 114)
  - Rådsdokumenter med ændringsforslag og analyser (hemmelige, offentlige og lækkede)
  - LEWP har mest arbejdet med andre dele af teksten end opsporing
- Tyskland og Østrig er de mest kritiske over for især indgreb mod kryptering og overvågning af private beskeder, ifølge netzpolitik.org

Danmarks holdning (Rådet)

- Positivt syn på forslaget i august (Altinget)
- Offentlig høring i december
- Ingen bemærkninger til Folketinget om høringssvarene (efter tre måneder)
- Fra lækkede rådsdokumenter
  - Dansk repræsentant i LEWP havde ingen instruks om kryptering (kan betyde flere ting)
  - Danmark vil forsætte nuværende praksis med (frivillige) DNS-blokeringer

Chat Control news updates

- EDRi (link)
- Stop scanning me! (link)
- Patrick Breyers Chat Control webside
- Dansk Chat Control webside
- Nyhedsmedier: netzpolitik.org (mest på tysk)
- Danske nyhedsmedier? Måske en dag..