Vil EU forbyde kryptering?
(obligatoriske bagdøre)

Jesper Lund
IT-Politisk Forening
@je5perl

Cryptohagen
26. september 2021

To policy initiativer

- Traditionel ”exceptional access” for politi m.v.
  - Primært resolutioner i Rådet indtil videre
  - On/off siden ”forever” (i hvert fald siden 2016)
  - Måske EU-lovforslag i 2022
- Chatcontrol 2.0
  - Kommende EU-lovforslag om obligatorisk scanning af private beskeder for CSAM **vil måske omfatte E2EE** tjenester
  - Kommer 1. december 2021 (med/uden E2EE)
- Begge: **ingen ved** hvordan det skal gøres..

Security through encryption and security despite encryption

- Kryptering vigtig for cybersikkerhed
  - Efter Schrems II: persondata må overføres til USA, hvis data er krypterede (og nøglen bliver i EU)
- Men.. politiet kan ikke få adgang til data eller kommunikation selv med retskendelse
- Rådet vil have en ”bedre balance”
  - **Nævnes eksplicit: ingen bagdøre**, men..
  - Tjenester skal levere data/indhold i plaintext, hvis politiet kommer med en kendelse **(altså: bagdør)**

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!

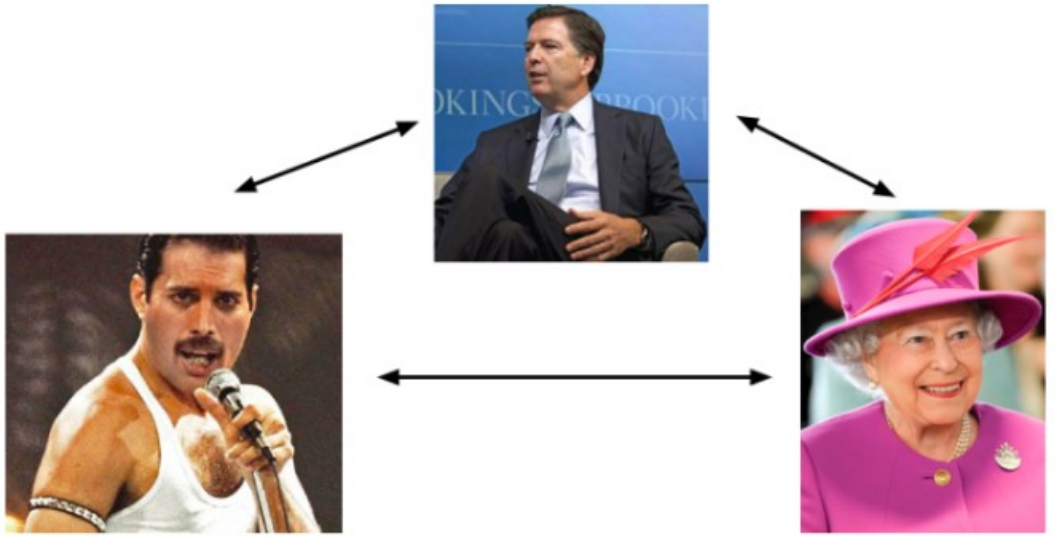
(See statewatch.org/news/2020/sept... by @StatewatchEU)

- 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.

GCHQ Ghost proposal

- Private, encrypted conversation (source)

- Intercepted “encrypted” conversation



Hvad med Pegasus..?

- Statstrojanere er ikke nok (7675/20)
  - The discussion highlighted that **most existing solutions to bypass encryption** (which do not work in all cases) are resource intensive, often extremely costly and **can only be used for some high value targets**, with some countries pointing to their limited forensic capabilities **and the fact that increasing investment in these capacities is met with ever decreasing results.** The discussion also stressed that the industry should play a stronger role in allowing lawful access for LEAs.

Alle kigger på de andre

- Kommissionens seneste ”plan”
  - Foreslå [2022] en tilgang til de retshåndhævende myndigheders **lovlige og målrettede adgang til krypterede oplysninger** i forbindelse med strafferetlig efterforskning. Denne tilgang bør være baseret på en **grundig kortlægning af medlems-staternes håndtering af kryptering** og en undersøgelse og vurdering af de konkrete lovlige muligheder i samarbejde med forskellige interessenter.
- KOM spørger EU-landene, der spørger KOM..

Chatcontrol 2.0

- Facebook Messenger, GMail m.fl. scanner billeder for CSAM vha. PhotoDNA **server-side**
- EU har **lovgivning om privatliv** for elektronisk kommunikation [eprivacy-direktivet]
- Undtagelse for **frivillig scanning** i juli 2021
- Kommende lovforslag [dec 2021] vil gøre det **obligatorisk** for kommunikationstjenester.
- Muligvis også tjenester med E2EE

Hvordan med E2EE?

- Spørg tjenesteudbyderne.. (fra 24.7.2020)
  - Kommissionen har via EU's internetforum **indledt en proces med eksperter fra erhvervslivet** for inden udgangen af 2020 at kortlægge og foretage en foreløbig vurdering af, hvilke **tekniske muligheder der er for at opspore og indberette seksuelt misbrug af børn i end-to-end-krypteret** elektronisk kommunikation [..]
- Ekspertrapport blev lækket i september 2020
- Client-side scanning (”PhotoDNA på device”)

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

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