I dette bilag kommenteres Hummelgaards udsagn i svar til Raabjerg og diverse presseklip. Vi refererer vi til Public version af "Interinstitutional File:2022/0155 (COD) 10131/25, når vi refererer til det danske kompromis (CSAR-DA).
https://data.consilium.europa.eu/doc/document/ST-10131-2025-INIT/en/pd

Kommentatorer (alfabetisk efter efternavn)
Diego Aranha (AU) – 2. Pressekontakt (dfaranha@cs.au.dk)
Aslan Askarov (AU)
Carsten Baum (DTU)
Ivan Damgaard (AU) – 3. Pressekontakt (ivan@cs.au.dk)
Kaj Grønbæk (AU) – 1. Pressekontakt (kgronbak@cs.au.dk)
Jacopo Mauro (SDU)
Claudio Orlandi (AU)
Jens Myrup Pedersen (AAU)
Carsten Schürmann (ITU)

Kommentarer til Hummelgaards svar til Dina Raabjergs spørgsmål.

A. Lad os først slå fast, hvad det er, end-to-end (E2E) kryptering sikrer: indholdet der sendes, er KUN tilgængeligt for afsender og modtager, dvs. den tjeneste der sender beskeden kan IKKE selv kigge i indholdet. CSAR forslaget fastholder at man har ret til at bruge E2E kryptering UDEN en "bagdør", hvor servicen selv eller en tredjepart kan dekryptere beskederne.

   CSAR-DA Punkt 26: "Providers should remain free to offer services using end-to-end encryption and should not be obliged by this Regulation to decrypt data or create access to end-to-end encrypted data."

B. **CSAR-DA** forslaget har været præsenteret som om det først og fremmest handler om at tvinge udbyderne til at rapportere om farligt indhold. Men de store beskedtjenester, Messenger, iMessage, Whatsapp osv bruger alle E2E kryptering. De kan derfor ikke rapportere noget som helst, for de har ikke adgang til indholdet. Hvis man alligevel insisterer på at scanne alt der sendes, er man derfor nødt til at scanne på klientsiden hos brugerne.

   CSAR-DA: Element C Detection Orders punkt 3:"Detection in interpersonal communications services using end-to-end encryption is enabled prior to the transmission of content requiring the users' consent;"

C. Det medfører, at *alle* brugere skal have installeret software, der scanner indholdet og rapporterer detekteret materiale til myndighederne (EU-Center). Det betyder for det første, at det **ikke** er en fordrejning af debatten, når modstanderne af CSAR-DA taler om overvågning - som tilhængerne ellers har påstået. Scanning betyder for det andet, at nu er indholdet ikke kun tilgængeligt for afsender og modtager. Det bryder fuldstændig med formålet med E2E kryptering. Derfor er det meningsløst når Hummelgaard i sit svar til Dina siger at man kan bevare E2E kryptering og samtidig

scanne på klientsiden. For man kræver at "postbuddet" checker og godkender brevet, før det puttes i den lukkede (krypterede) kuvert til afsendelse.

D. Hummelgaard har fremført at det jo er EU der detekterer (scanner) og ikke tech-giganterne, vel sagtens for at sige, at så kan det ikke være så farligt. Men det eneste der kan lade sig gøre i virkeligheden er, at det er tjenesteudbyderne, altså tech giganterne, der scanner på vegne af EU og under EU mandat. Detektion, skal aktiveres af den enkelte App - f.eks. WhatsApp -i forbindelse med at en besked er gjort klar til afsendelse. Så enten skal WhatsApp tvinges til at scanne og rapportere i egen App eller også skal den EU-udviklede detektor kaldes gennem et såkaldt API for hver eneste besked. Man må regne med at nogen af udbyderne vil gribe lejligheden til at indsamle mere data, det er noget vi har set mange gange tidligere.

E. Hummelgaard har også sagt, at scanning kun sker med brugerens samtykke, så man kan bare sige nej. Men gør man det, kan man ikke længere sende billeder og videoer. Beskedtjenesterne transporterer milliarder af billeder hver eneste dag, og derfor er det klart, at de fleste brugere vil opleve, at hvis de siger nej, kan de reelt ikke bruge tjenesten. Der er derfor **ikke** tale om et reelt valg.

   Samtidigt, må vi konstatere at at det visuelle indhold i CSAR-DA defineres meget bredt som “billeder og de visuelle komponenter af videoer, herunder diagrammer, infografikker, logoer, animationer, ikonografi, gifs, stickers eller de visuelle komponenter af livestreaming samt URL’er”, hvilket er meget vidtgående, og som vi siger nedenfor, så er URL’er tekst. Dette indebærer en voldsom detaljeret analyse af beskeder, for at afgøre hvilke indhold der falder ind under definitionen. Samtidigt er man nødt til at at stole på, at detektionen (dvs. en AI-model) også respekterer disse grænser.

F. Hvis man siger nej til samtykke, så, vil systemet stadig være nødt til at kontrollere det du sender, for du må jo ikke sende visuelt indhold. Det forudsætter at man kan skelne korrekt mellem tekst og billeder f.eks. Men det er ikke muligt i praksis. Det er nemt at omdanne et digitalt billede til en tekstfil, der kun indeholder bogstaver. Herfra kan man senere gendanne billedet. Man vil derfor kunne omgå kontrollen ved at omdanne billeder til tekstfiler, og sende dem i stedet.

   Der står også i CSAR-DA, at der skal detekteres for kendte CSAM webadresser (URLs) før besked sendes krypteret. Men en URL er jo en del af selve teksten, en sådan analyse kan derfor ikke foretages uden analyse af besked-teksten. Der er således en stor selvmodsigelse i disse dele af forordningen. Desuden er det nemt at undgå at skrive den præcise URL i teksten, og i stedet lave en beskrivelse af, hvordan den rigtige URL konstrueres. F.eks. **hvis jeg skriver https:\\www:url:com (udskift \\ med // og : med .) Man kan også lave synonymer/kodeord for adresser osv osv.** Der vil således være brug for en meget detaljeret AI analyse af teksten.

   CSAR-DA: Element C Detection Orders punkt 32”Detection is limited to visual content and URLs, while text and audio content are excluded;”

G. På den baggrund er der indirekte givet mulighed for at scanne tekst, og det er i høj grad muligt at mandatet til scanning kan udvides til også at omfatte andre dele end URL i teksten. Hvis det sker, er valget: enten scanner EU alt, eller også kan du ikke sende noget. Dette vil reelt være et forbud mod krypteret kommunikation - selvom det siges at E2E kryptering er bevaret.

H. Det vil være umuligt, at alle digitale kommunikationstjenester i verden vil tilslutte sig at udføre en sådan scanning, selv hvis det kræves ved EU lov. EU-borgere kan besøge ikke-EU-websteder og bruge de tjenester, de tilbyder, til at kommunikere. Kriminelle kan altid og vil ofte allerede vælge kommunikationstjenester, der ikke er placeret i EU og derfor ikke scanner. De kan også bruge teknologier som VPN eller TOR til at omgå netudbyderes eller myndigheders forsøg på blokering. Det er enkelt, selv for uerfarne brugere, at anvende sådanne teknologier, der giver adgang til udenlandske websteder, selv når de er blokeret. For at gennemtvinge scanning på alle tilgængelige kommunikationsplatforme ville EU derfor være nødt til at filtrere al kommunikation ind og ud af EU ved hjælp af teknologier, der kan blokere alle kendte anti-censurmetoder. At gøre dette svarer til den form for censur, der praktiseres i Kina. Samtidigt, så er var det jo præcis den form for NSA aflytning på kabel-niveau, som Snowdon afslørede, og som skabte stor opstandelse i Europa. Specielt da det kom frem, at Merkels telefon blev aflyttet.

I. Hummelgaard har udtalt til DR at det er en helt forkert opfattelse at borgerne skal have ret til at kommunikere via en krypteret app, så et forbud af den karakter er langt fra udelukket.

   Men I Danmark er brevhemmeligheden grundlovssikret (§72), og straffeloven (§263) gør det strafbart at ”bryde et brev eller anden lukket meddelelse”. Det er derfor rimeligt at antage at borgerne også i en digital verden har ret til at kommunikere privat. Men kryptering er den eneste teknologi, der kan sikre privat kommunikation på Internettet, så Hummelgaards synspunkt synes at være uforeneligt med danske retsprincipper.

   Straffeloven § 263 a. Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der uretmæssigt erhvervsmæssigt sælger eller i en videre kreds udbreder en kode eller andet adgangsmiddel til et ikke offentligt tilgængeligt informationssystem, hvortil adgangen er beskyttet med kode eller anden særlig adgangsbegrænsning.

J. Hummelgaard siger i sit svar at Red Barnet mfl. støtter forslaget, og at de er bange for at miste eksisterende effektivt redskab. Men der findes i dag ikke noget redskab af den type som CSAR-DA foreslår. Der findes til gengæld et Cloud baseret system PhotoDNA og en etableret amerikansk organisation NCMEC, modtrager rapporter fra Tech-platformenes scanninger.

   Dette system er evalueret i rapporten "The Strengths and Weaknesses of the Online Child Safety Ecosystem" fra Stanford University. Oranisationen NCMEC, (https://stacks.stanford.edu/file/druid%3Apr592kc5483/cybertipline-paper-2024-04-22.pdf), der analyseres, svarer lidt til det nævnte "EU-Center" der skal modtage indberetning om billeder i CSAR-DA forslaget. Rapporten sætter effektiviteten i

perspektiv og illustrerer også de store udfordringer, der vil være med at skalere server-side overvågning (som nogle platforme har lavet i flere år) til client-side-scanning af ALLE billeder for de store krypterede platforme iMessage, WhatsApp, Messenger, Signal mv. NCMEC behandlede sidste ÅR 20 Mio rapporter om 60 mio billeder. Scanner man Mia af billeder HVER DAG, så vil man få skabt et juridisk kaos med at behandle rapporter, og rense de mange, der har fået indrapporteret et falskt positivt billede eller ukorrekt data.

Ordentlig og effektiv manuel behandling af detekterede billeder/rapporterring tager meget længere tid end få sekunder eller minutter, som nogen ellers har budt ind med.

👉 Rapporten siger f.eks., at ud af de 20-30 Mio rapporter, som NCMEC CyberTipLine modtager på et ÅR, så er det meget få, der fører til en anholdelse: "Estimates of how many CyberTipline reports lead to arrests in the U.S. range from 5% to 7.6%."

👉Rapporteringen af et billede, er ikke tilstrækkeligt, der skal meget mere kontekst til for at politiet kan bruge det. Fra 36 tjenester var 90% af rapporterne ikke brugbare for politiet:

"... an overwhelming majority of their tips lacked sufficient location information for NCMEC to identify the appropriate law enforcement agency for referral. In 2022 NCMEC listed 36 platforms where at least 90% of the tips received were not actionable. We interviewed employees of several of the platforms on the list."

👉 Der overrapporteres for at være på den sikre side:
"Once a platform integrates with NCMEC's CyberTipline reporting API, they are incentivized to overreport. Consider an explicit image of a 22-year-old who looks like they could be 17: if a platform identified the content internally but did not file a report and it turned out to be a 17-year-old, they may have broken the law."

👉Det tager lang tid at behandle rapporterne, det anbefales:
"Extend the retention period for electronic service providers to safely preserve reported CSAM from 90 days to at least 180 days."

Argumenter for yderligere spørgsmål til Hummelgaard:

K. Relationen til GDPR: Det anbefales af datatilsynet at GDPR omfattet materiale kommunikeres krypteret med "sikker digital post" eller andet krypteret mail system, Der er bla. en kendt sag med amerikanske far der endte i fedtefadet for at sende billede af sønnens ædlere dele med udslæt, for at få en diagnose. I GDPR har man ligeledes retten til at blive "glemt" igen.

L. Ved at installere en scanning software på alle enheder introducerer man en risiko for at hackere kan udnytte en sådan softwarekomponent. Hackere kan f.eks. indsætte (injicere) ny kode og få adgang til alle de data fra brugerne, de ønsker. Ingen vil

opdage det, fordi det vil være normalt, at apps deler trafik med udbyderen.

M. SmitteApp sammenligning - App bliver alligevel dyr og skal alligevel benytte Apple og Google API:
https://www.version2.dk/artikel/politikere-undrer-sig-corona-appen-fra-netcompany-er-alligevel-ikke-gratis
https://www.computerworld.dk/art/251895/ny-kurs-for-netcompanys-smitteapp-apple-og-googles-loesning-skal-bruges-alligevel

N. PhotoDNA https://www.microsoft.com/en-us/photodna
Dette er en sever-side metode, der køres i Cloud. Der beregnes et unikt "fingeraftryk" - en såkaldt hash værdi, der blot er et matematisk beregnet tal - for alle registrerede CSAM billeder, der findes i en database med mere end 10 mio kendte CSAM billeder. Fejlraten er relativ lav på at detektere disse billeder, når man har adgang til fingeraftrykkene i skyen. Hovedudfordringen ved at benytte dette til klient-side scanning, idet databasen af fingeraftryk skal distribueres og være tilstede på den enkelte telefon, for at kunne lave analysen.
Selvom selve analysen af kendte billeder er ret præcis, så har NCMECs erfaringer været, at der skal meget mere kontekst information end blot billedet når der fremsendes til politiet, for at de kan bruge det som grundlag for en sag.

O. Former MEP Patrick Breyer: Danish Minister Uses "Blatant Lie" to Blackmail EU into "Chat Control" Mass Surveillance Deal https://www.patrick-breyer.de/en/former-mep-patrick-breyer-danish-minister-uses-blatant-lie-to-blackmail-eu-into-chat-control-mass-surveillance-deal/

"The Danish minister, chairing the rotating Council Presidency, claims the European Parliament will refuse to extend the current, expiring voluntary scanning regime unless the EU Council first agrees to the new mandate for mandatory, indiscriminate scanning of all private communications.

"This is a blatant lie designed to manufacture a crisis," states Dr. Breyer, a long-time digital freedom fighter. "There is no such decision by the European Parliament. There has not even been a discussion on this issue. The Commission has not yet proposed to extend the current legislation, and the European Parliament has not yet appointed Rapporteurs to discuss it.

P. Politiet er i forvejen langt bagud med hensyn til at opklare andre digitale kriminalitets sager.
https://www.version2.dk/artikel/det-gaar-den-forkerte-vej-politiet-dropper-rekordmange-sager-om-digital-svindel
Der skal jo tilføres mange flere ressourcer og kompetencer til politiet for at lave efterforskning, ellers vil en indsamling af CSAM billeder jo bare ende med en masse henlagte sager.

Q. Ministeren vælger at mødes med Tech-leverandører og Børneorganisationer , men ingen af de nationale eller internationale eksperter er inviteret.
https://www.justitsministeriet.dk/pressemeddelelse/justitsministeren-inviterer-tech-

virksomheder-til-moede-om-bekaempelse-af-materiale-med-seksuelle-overgreb-paa-boern/

R. Det amerikanske NCMEC med deres CyberTipline, har haft **en nedgang på 43% i** rapporter fra 2023 til 2024. Det kan tolkes på flere måder, men en tolkning kan være, at de kriminelle blot finder et mere sikkert sted i DarkWeb servere uden for EU at dele CSAM. Og hvis en generel overvågning af de E2E krypterede tjenester starter, så flytter de kriminelle helt til DarkWeb, og så vil det kun være almindelige borgere, der får scannet deres kommunikation.

   In 2024, the CyberTipline received 20.5 million reports of suspected child sexual exploitation. While this is a significant number, the overall number of reports declined from 36.2 million reports received in 2023.
   https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata?_gl=1*rauje4*_gcl_au*NDYwNjM3MjcwLjE3NTkxMzE2NjM.*_ga*NTE2OTM3NTA3LjE3NTkxMzE2NjM.*_ga_JGSFP8TSBM*czE3NTkxMzE2NjMkbzEkZzEkdDE3NTkxMzE3MTAkajEzJGwwJGgw

S. I mødeindkaldelsen
   https://www.justitsministeriet.dk/pressemeddelelse/justitsministeren-inviterer-tech-virksomheder-til-moede-om-bekaempelse-af-materiale-med-seksuelle-overgreb-paa-boern/

   …siger Justitsminister Peter Hummelgaard:
   "– Red Barnet har tidligere refereret, at der bliver delt mindst to billeder eller videoer af seksuelle overgreb mod børn i sekundet."

   Det er selvfølgelig alarmerende at der deles så mange. **Men** der deles 25 mia billeder pr. dag på de mest populære E2E krypterede tjenester, iMessage, WhatsApp, Messenger, Signal m.fl. Det svarer til at hver af godt 8 mia mobilabonnementer i verden deler godt 3 billeder hver dag. Omregnet til sekunder er det **ca 290.000 billeder pr. sekund**, der ultimativt skal scannes for at **finde de 2 CSAM billeder, som Red Barnet siger, der deles pr. sekund.**

   Dette er som at **lede efter en nål i en høstak**, for hvert eneste sekund i døgnet. Derfor er forslaget slet ikke proportionalt til den ønskede effekt.