Peter Olsthoorn

"Niet effectief en gevaar voor veilige communicatie"

Wetenschappers lopen te hoop tegen Child Sexual Abuse Regulation

Dossier

Kinderporno Privac

Gepubliceerd

2 mei 2024

Zo'n 270 wetenschappers uit 33 landen protesteren met een brief tegen een Europees voorstel met om de distributie van kinderporno in te dammen. De methoden schaden de beschermde communicatie van alle burgers, terwijl daders ze bovendien eenvoudig zullen weten te omzeilen.

De Raad van Europa maakte eind maart 2024 een aangepast voorstel voor het bestrijden van online kindermisbruik, met een tweetal veranderingen. Die schieten tekort, vindt een groot aantal wetenschappers. Hier staat de originele brief, hieronder vertaald.

De Raad wil met AI op telefoons van alle Europeanen kinderporno en ongepast contactleggen met minderjarigen ('grooming') bestrijden. Deze 'client-side scanning'is een veel te zwaar middel, vinden behalve wetenschappers Bits of Freedom, de Tweede Kamer, de meerderheid van het Europees Parlement en zelfs het Meldpunt Kinderporno.

Met de brief reageren de wetenschappers op een uitgelekt concept en ze hopen invloed uit te oefenen op het definitieve voorstel van de Raad van de Europese Unie, waarin de lidstaten hun gezamenlijke belangen opperen tegenover de Europese Commissie en Europees Parlement.

Van Nederlandse universiteiten tekenen 13 onderzoekers:

- Frederik Zuiderveen Borgesius, Radboud University
- Herbert Bos, Vrije Universiteit
- Andrea Continella, University of Twente
- Joan Daemen, Radboud University
- Jaap-Henk Hoepman, Radboud University/Groningen (zie zijn blog, en foto hiernaast)
- Chenglu Jin, CWI Amsterdam
- Karst Koymans, University of Amsterdam
- Tanja Lange, TU Eindhoven
- Kostas Papagiannopoulos, University of Amsterdam
- Roland van Rijswijk-Deij, University of Twente
- Simona Samardjiska, Radboud University
- Christian Schaffner, University of Amsterdam
- Jeroen van der Ham-de Vos University of Twente

Vertaalde delen van de brief:

1. De voorgestelde gerichte detectiemaatregelen zullen de risico's van massale surveillance niet verminderen

Het probleem is dat gebrekkige detectietechnologie niet betrouwbaar is voor het vaststellen van gevallen van belang, omdat ze gemakkelijk te omzeilen zijn en gevoelig voor fouten in de classificatie.

Dit laatste punt is zeer relevant voor het nieuwe voorstel, dat beoogt de impact te beperken door alleen "interessante gebruikers" te rapporteren, gedefinieerd als degenen die herhaaldelijk worden gemarkeerd (volgens het laatste ontwerp: twee keer voor bekend kinderporno-materiaal en drie keer voor nieuw kinderporno materiaal en grooming).

Dit is geen oplossing. Ten eerste werkt geautomatiseerde detectietechnologie voor nieuwe kinderporno en voor de detectie van kinderlokken slecht. Het aantal fout-positieven als gevolg van fouten zal hoogstwaarschijnlijk niet significant verminderen, tenzij het aantal herhalingen zo groot is dat de detectie niet meer effectief is. Gezien de miljarden berichten op grote platforms als WhatsApp kunnen we miljoenen valse alarmen verwachten

Ten tweede, de overtuiging dat het aantal fout-positieven aanzienlijk zal afnemen door het vereisen van een klein aantal herhalingen, berust op de misvatting dat voor onschuldige gebruikers twee positieve detectiegebeurtenissen onafhankelijk zijn en dat de overeenkomstige foutkansen kunnen worden vermenigvuldigd

In de praktijk bestaat communicatie in een specifieke context (bijv. foto's aan artsen, legitiem delen met familie en vrienden). In dergelijke gevallen is het waarschijnlijk dat ouders meer dan één foto naar artsen sturen, en families zullen meer dan één foto delen van hun vakanties aan het strand of zwembad, waardoor het aantal fout-positieven voor deze persoon toeneemt.

Bovendien zal client-side scanning moeilijk te controleren zijn op wat er wordt gedetecteerd en welke drempelwaarde wordt gebruikt op het apparaat wordt gebruikt om detecties als "interessant" te beschouwen.

Toepassingen met een hoog risico kunnen nog steeds zonder onderscheid een groot aantal mensen treffen. De tweede wijziging in het voorstel is om alleen detectie te vereisen van (delen van) diensten die geacht worden een hoog risico te hebben als het gaat om kinderporno-materiaal. Deze wijziging zal waarschijnlijk geen nuttig effect hebben.

Aangezien voor de uitwisseling van kinderporno-materiaal of grooming alleen standaardkenmerken vereist zijn die door veel dienstverleners worden ondersteund (zoals het uitwisselen van chatberichten en afbeeldingen), zal dit ongetwijfeld gevolgen hebben voor veel diensten.

Bovendien maken steeds meer diensten end-to-endencryptie, waardoor de privacy en veiligheid van de gebruiker sterk worden verbeterd, en de kans toeneemt dat deze diensten worden gecategoriseerd als diensten met een hoog risico.

Deze verandering zal waarschijnlijk evenmin gevolgen hebben voor misbruikers. Zodra misbruikers merken dat een dienstverlener client side scanning heeft geactiveerd, zullen ze overstappen naar een andere dienstverlener die op zijn beurt een hoog risico wordt. A l snel zullen alle diensten een hoog risico zijn.

Omdat open-source chatsystemen makkelijk te implementeren zijn, kunnen groepen overtreders makkelijk hun eigen dienst opzetten zonder enige detectiemogelijkheden.

2. Detectie in end-to-end versleutelde diensten ondermijnt per definitie bescherming

Het nieuwe voorstel heeft als een van zijn doelen om "cyberveiligheid en versleutelde gegevens te beschermen, terwijl diensten die end-to-end versleuteling gebruiken binnen het bereik van detectiebevelen blijven.

Dit is een oxymoron. De bescherming van end-to-end encryptie houdt in dat niemand anders dan de beoogde ontvanger van communicatie de inhoud ziet. Het inschakelen van detectie, zowel voor versleutelde gegevens als voor gegevens voordat ze versleuteld worden, schendt de definitie van vertrouwelijkheid die end-to-end encryptie biedt.

Bovendien staat in het voorstel: "Deze verordening schept geen verplichting die [een dienstverlener] ertoe verplicht om end-to-end versleutelde gegevens te ontsleutelen of toegang daartoe te creëren, of die de levering van end-to-end versleutelde diensten zou verhinderen."

Dit kan misleidend zijn, want of de verplichting om te decoderen bestaat of niet, het voorstel ondermijnt de bescherming die wordt geboden door end-to-end encryptie. Dit heeft rampzalige gevolgen. Het schept een precedent voor het filteren van het internet en en verhindert mensen om enkele van de weinige beschikbare middelen te gebruiken om hun digitale privacyrecht te beschermen.

Het zal een afschrikkend effect hebben, vooral op tieners die voor hun interacties sterk afhankelijk zijn van onlinediensten. En zal waarschijnlijk een negatief effect hebben op democratieën over de hele wereld.

3. De invoering van meer onvolwassen technologieën kan het risico vergroten

In het voorstel staat dat er maatregelen voor leeftijdsverificatie en leeftijdsbepaling zullen worden genomen, waardoor het nodig wordt om de leeftijd aan te tonen in diensten waar dat voorheen niet nodig was.

We willen erop wijzen dat er op dit moment geen goed bewezen technologische oplossing is met een gevestigd marktpotentieel die deze beoordelingen betrouwbaar kan uitvoeren. Het voorstel stelt ook dat een dergelijke verificatie en beoordeling de privacy moet beschermen. Hoewel er onderzoek wordt gedaan naar technologieën die zouden kunnen helpen bij het implementeren van privacy-beschermende leeftijdscontrole, is er momenteel geen enkele op de markt.

4. Gebrek aan transparantie

technologisch niet kan werken.

Het voorstel besteedt onvoldoende aandacht aan de technische risico's en legt - terwijl het beweert technologisch neutraal te zijn - eisen op waaraan geen enkel state-of-the-art systeem voldoet; laag percentage fout-positieve uitslagen, geheimhouding van de parameters en algoritmen bij gebruik in een groot aantal apparaten, bestaan van representatief gesimuleerd kinderpornomateriaal.

Voordat een dergelijk voorstel wordt ingediend, moeten de indieners serieuze gesprekken aangaan over wat wel en niet kan worden gedaan binnen de context van het garanderen van veilige communicatie voor de samenleving.

5. Betere wegen voor de bescherming van kinderen

Kinderen beschermen tegen onlinemisbruik en tegelijkertijd hun recht op veilige communicatie behouden is van cruciaal belang. Het uitroeien van kindermisbruik is afhankelijk van het uitroeien van misbruik, niet alleen van misbruikmateriaal .

Organisaties als de VN noemen methoden om misbruik te verminderen, zoals voorlichting over toestemming, over normen en waarden, over digitale geletterdheid en online veiligheid, en alomvattende seksuele voorlichting; 'traumasensitief' melden van seksueel misbruik; 'traumagevoelige' meldpunten; en interventies op basis van sleutelwoorden.

Educatieve inspanningen kunnen plaatsvinden in samenwerking met platforms, die hoge prioriteit kunnen geven aan educatieve resultaten van hoge kwaliteit bij het zoeken of samenwerken met hun contentmakers om boeiende bronnen te ontwikkelen.

We raden aan om aanzienlijk meer te investeren en inspanningen te leveren om bestaande bewezen benaderingen om misbruik uit te roeien te ondersteunen. Dergelijke benaderingen staan in tegenstelling tot het huidige techno-oplossingsgerichte voorstel, dat ten koste gaat van de veiligheid van de communicatie, met weinig potentiële invloed op misbruik van kinderen.

) Foto door Siddhant Soni on Unsplash