Internet Society
Netherlands Chapter

Open Brief aan de Ministers van Justitie en Veiligheid, Economische Zaken, en de Staatssecretaris van Digitalisering

Datum **:** 17 September 2024

Onderwerp **:** Brede maatschappelijke zorgen over de impact van de EU CSA-regelgeving op encryptie, privacy en digitale veiligheid

Geachte ministers en staatssecretaris,

Met deze brief wendt Internet Society Nederland (ISOC NL) zich tot u om onze ernstige zorgen te uiten over het laatste voorgestelde Besluit inzake het tegengaan van seksueel misbruik van kinderen (CSA-regelgeving) van de Europese Unie en de implicaties hiervan voor eind-tot-eind versleutelde (E2EE) communicatie en de fundamentele rechten van burgers.

Wij worden in deze zorgen gesteund door meer dan 60 organisaties, waaronder Mozilla, Global Partners Digital, en de Center for Democracy & Technology, die gezamenlijk oproepen om scanningvoorstellen zoals client-side scanning af te wijzen vanwege de ernstige risico's voor privacy en veiligheid. Deze organisaties benadrukken dat het huidige compromisvoorstel van de EU niet effectief is en juist nieuwe gevaren introduceert.

Als onderdeel van een bredere wereldwijde coalitie van organisaties die pleiten voor sterke encryptie, waaronder het **Global Encryption Coalition**, willen wij uw aandacht vestigen op de ernstige veiligheids- en privacyrisico's die inherent zijn aan de voorgestelde maatregelen, zoals verwoord in onze eerdere verklaringen. Ons standpunt is gebaseerd op uitgebreide technische en juridische evaluaties van het gebruik van client-side scanning en andere vormen van monitoring binnen E2EE-diensten, zoals onder meer beschreven in het bijgevoegde rapport van de Internet Society over preëmptieve monitoring binnen E2EE-systemen.

De aanhoudende pogingen om intrusieve scantechnologieën in versleutelde omgevingen op te leggen, zullen de veiligheid van burgers en bedrijven in gevaar brengen en de digitale infrastructuren van Europese lidstaten kwetsbaar maken voor cyberaanvallen.

Problematiek en Gevolgen

Het recente compromisvoorstel van de Europese Raad, hoewel aangepast, blijft eisen stellen die detectie van illegale inhoud op versleutelde platforms verplichten. Dit voorstel ondermijnt de principes van sterke encryptie door scanning te verplichten van berichten voordat deze worden versleuteld, zoals ook benadrukt in het standpunt van de *European Data Protection Supervisor*. Het scannen van content direct op gebruikersapparaten, zonder hun medeweten en toestemming, schendt niet alleen hun recht op privacy maar verhoogt ook de kans op systeemkwetsbaarheden en cyberaanvallen.

Beperkte Effectiviteit van Verplichte Monitoring

Bovendien zal deze technologie, ondanks haar bedoelingen, slechts beperkt effectief zijn in het aanpakken van het complexe probleem van kindermisbruik. Het verplicht scannen creëert een breed scala aan foutpositieven, zoals aangetoond in technische evaluaties.

Daarnaast heeft een brede coalitie van meer dan 60 internationale organisaties zich uitgesproken tegen de implementatie van client-side scanning. In een gezamenlijke verklaring waarschuwen organisaties zoals Mozilla en de Internet Society dat deze technologie niet alleen ineffectief is, maar ook de veiligheid van burgers en bedrijven in gevaar brengt. Ze roepen de EU op om af te zien van maatregelen die massasurveillance mogelijk maken en om oplossingen te zoeken die de fundamentele rechten van burgers beschermen.

De voorgestelde maatregeen zorgen voor een zware belasting op wetshandhavingsinstanties, verhoogt de kans op fouten en compromitteert de privacy van onschuldige gebruikers. Uit onze analyse blijkt dat dergelijke maatregelen onevenredig zijn en niet voldoen aan de vereisten van noodzakelijkheid en proportionaliteit zoals gesteld door artikel 8 van het Europees Verdrag voor de Rechten van de Mens.

Hoewel het scannen van bekende kinderpornografische inhoud met cryptografische hashes doorgaans een lage foutmarge heeft, brengt het nog steeds aanzienlijke risico's met zich mee. De implementatie van client-side scanning op gebruikersapparaten opent vele nieuwe kwetsbaarheden die kunnen worden misbruikt door kwaadwillenden. Bovendien is deze technologie beperkt effectief tegen nieuwe vormen van misbruik, zoals grooming of gemanipuleerde beelden. Criminelen kunnen relatief eenvoudig detectiemechanismen omzeilen door kleine aanpassingen te maken, waardoor de doeltreffendheid van het systeem afneemt. Niet alleen criminelen, maar in feite iedereen kan relatief eenvoudig detectiemechanismen omzeilen, vooral in het geval van open source-technologieën. Dit gebeurt waarschijnlijk op grote schaal, waarbij ook bedrijven privacy- en beveiligingsredenen aanvoeren. Het omzeilen van monitoring lijkt legitiem zolang het EU Hof van Justitie dergelijke maatregelen niet disproportioneel en onwettig heeft verklaard.

Daarnaast ontbreken in de technische basis van het voorstel scenario’s voor peer-to-peer- en mesh-netwerkcommunicatie, waarbij het afdwingen van CSS praktisch onmogelijk is zonder fundamentele beperkingen op alle open communicatienetwerken. Zie hiervoor als voorbeeld oplossingen zoals Jami.net, waarbij peer-to-peer- en mesh-netwerkcommunicatie buiten het bereik van CSS zouden vallen.

Tot slot creëert deze technologie risico's voor bredere misbruikmogelijkheden, zoals surveillance door autoritaire regimes. Dit alles maakt dergelijke maatregelen onevenredig en in strijd met de vereisten van noodzakelijkheid en proportionaliteit, zoals vastgelegd in artikel 8 van het Europees Verdrag voor de Rechten van de Mens.

Risico van Massasurveillance en Dataretentie

Het produceren van digitale vingerafdrukken van elke afbeelding en deze vergelijken met een centrale database creëert een digitaal spoor van al het gedeelde materiaal. Dit kan worden gezien als een vorm van dataretentie, die door het Europese Hof in 2014 ongeldig is verklaard vanwege de inbreuk op fundamentele rechten. Het risico bestaat dat dergelijke vingerafdrukken, zelfs als ze tijdelijk worden opgeslagen, kunnen worden misbruikt om politieke tegenstanders of persoonlijke netwerken te traceren, wat neerkomt op massasurveillance.

Daarnaast lijken de voorgestelde maatregelen in strijd te zijn met de Nederlandse Nationale Cryptostrategie 2019 en de Nederlandse Cybersecuritystrategie 2022-2028. Beide strategieën benadrukken het belang van sterke cryptografie en veilige digitale producten. Het verplicht verzwakken van encryptie door client-side scanning zou deze principes ondermijnen en de Nederlandse positie op het gebied van cybersecurity verzwakken.

Het voorgestelde beleid creëert een valse tegenstelling tussen privacy en veiligheid, een benadering die al eerder kritiek heeft gekregen, zoals benadrukt in de gezamenlijke verklaring van ENISA en Europol in 2016.

Naast de risico's voor privacy en veiligheid, introduceert het gebruik van client-side scanning met centrale databases een aanzienlijke milieu-impact. De noodzaak om miljarden hashes per jaar te controleren en te beheren zou een grote ecologische voetafdruk met zich meebrengen, wat haaks staat op de duurzame ambities van de Europese Unie.

Aanbevelingen

1. Verwerping van Client-side Scanning (CSS): Wij roepen de Nederlandse regering op om de verplichting tot enige vorm van scannen binnen E2EE-diensten te verwerpen. CSS ondermijnt het vertrouwen in digitale infrastructuren en introduceert nieuwe kansen voor cyberaanvallen en manipulatie.

2. Versterking van Kindbescherming via Preventieve Maatregelen: In plaats van verregaande monitoring, pleiten wij voor meer investering in nationale programma's en hotlines voor de preventie van kindermisbruik. Dit omvat ook het opvoeren van educatieve campagnes en strafrechtelijke hervormingen die specifiek gericht zijn op kinderbescherming. Het Nederlands Jeugdinstituut (NJI) benadrukt dat preventie van kindermisbruik plaatsvindt op drie niveaus: universele, selectieve en geïndiceerde preventie. Deze strategieën richten zich zowel op algemene opvoedingsondersteuning als op specifieke risicogroepen. Interventies zoals oudertrainingsprogramma's en huisbezoeken zijn essentieel om opvoedvaardigheden te verbeteren en mishandeling te voorkomen. Dit sluit aan bij de oproep om meer te investeren in preventieve maatregelen in plaats van controversiële monitoringstechnologieën, zoals in de EU CSA-wetgeving wordt voorgesteld.

Het is belangrijk om te beseffen dat technologische oplossingen alleen vaak onvoldoende zijn om diepgewortelde maatschappelijke problemen zoals kindermisbruik op te lossen. Een preventieve aanpak,

gericht op educatie en ondersteuning van risicogroepen, kan meer effect sorteren dan alleen monitoring achteraf.

3. Bevordering van het Digitale Ecosysteem: Het bevorderen van veilige en betrouwbare digitale ecosystemen is essentieel voor zowel de bescherming van burgers als de ontwikkeling van een gezonde digitale economie. Het verplicht implementeren van kwetsbare technologieën zoals CSS en het als overheid omzeilen van cruciale technologieën zoals E2EE zal het vertrouwen in zowel deze systemen als in de overheid als beschermer van het publieke domein ondermijnen, en daarnaast bedrijven van alle groottes benadelen.

Wij verzoeken u met klem om bovenstaande punten mee te nemen in uw overwegingen bij de aankomende besluitvorming over het CSA-voorstel binnen de Raad van de Europese Unie. Tijdens het rondetafelgesprek van de Commissie Digitale Zaken op 11 oktober 2023 werd onder andere de position paper van Prof. Dr. Mr. Frederik J. Zuiderveen Borgesius besproken, waarin hij stelt dat CSS mogelijk in strijd is met fundamentele grondrechten. Wij verwijzen graag naar zijn analyse als verdere onderbouwing van onze zorgen.

Wij staan uiteraard open voor verdere dialoog om onze bevindingen en aanbevelingen nader toe te lichten.

Met vriendelijke groet,

Internet Society Nederland, mede namens de ISOC NL Werkgroepen Eerlijk Digitaal Onderwijs en Internet Transparancy en dr. J.H. Hoepman (Radboud Universiteit).

Internet Society
Netherlands Chapter

Bijlagen:

1. Preemptive Monitoring in End-to-end Encrypted Services (Internet Society, 2024)
2. Statement on the Future of the CSA Regulation (GEC, 2024)
3. Informatie over preventie van kindermishandeling (Nederlands Jeugdinstituut, NJI)
4. European Court of Justice Decision on Data Retention

 | e-mail: bureau@isoc.nl . Koninklijke Bibliotheek, Prins Willem-Alexanderhof 5 (kamer i4.301) . 2595 BE Den Haag . Nederland |