End-to-end encryptie en de risico's client-side scanning*

Jaap-Henk Hoepman

De Europese Commissie wil serieus werk maken van de bestrijding van online kindermisbruik. Vorig jaar diende de commissie hiervoor een wetsvoorstel in dat grote online dienstverleners *verplicht* noodzakelijke maatregelen te treffen. Middels dit position paper wil ik aandacht vragen voor een aantal fundamentele bezwaren die aan het voorstel van de Commissie kleven.

Gezien de ernst van kindermisbruik is de voortvarendheid van de Commissie volledig te begrijpen. Maar het voorstel leunt helaas zwaar op de inzet van zogenaamde client-side scanning technologie. Deze technologie is onbetrouwbaar en daarmee potentieel stigmatiserend. Ook is de noodzakelijkerwijs brede inzet van deze technologie buitenproportioneel, met grote risico's ten aanzien van de bescherming van de persoonlijke levenssfeer. Door de installatie van deze technologie op de telefoons van nagenoeg alle Nederlanders wordt daarnaast een onomkeerbare stap gezet naar een verregaande Europese infrastructuur voor massasurveillance.

De huidige (vrijwillige) maatregelen zijn gericht op het detecteren van *grooming* (digitaal kinderlokken) en kinderpornografie op de servers van webfora, sociale netwerken en cloudopslagdiensten. Straks worden ook aanbieders van *end-to-end* versleutelde communicatiediensten, zoals WhatsApp, iMessage, Signal, en Telegram, verplicht maatregelen te nemen. Het wetsvoorstel laat open *hoe* dergelijke aanbieders aan de wet moeten voldoen, maar als het kabinet en de Kamer bij het eerder ingenomen standpunt blijven dat aan de bescherming van end-to-end encryptie zelf niet getornd mag worden, blijft er maar één optie over. Dan zal het scannen van kinderpornografisch materiaal op de telefoons van de burgers zelf moeten plaatsvinden, gebruik makend van een (gecodeerde) database van bekend kinderpornografisch materiaal. Bij een positieve match wordt het materiaal en de eigenaar van de telefoon aan een nader onderzoek onderworpen. Dit heet '*client-side scanning*'. Het voorstel van de commissie laat in het midden welke specifieke technologie hiervoor gebruikt moet worden, maar functioneel zal het vergelijkbaar (moeten) werken als hierboven beschreven.

* (no version given)

Er zijn fundamentele technische, juridische én ethische bezwaren tegen deze maatregelen. Niet voor niets heeft de Kamer zich al tegen het verzwakken van encryptie en het verplicht stellen van client-side scanning uitgesproken, middels het aannemen van de motie Van Ginneken c.s. op 20 april van dit jaar. Laat mij deze bezwaren kort toelichten. (In een 'open letter' [1] van een groot aantal wetenschappers op het gebied van informatiebeveiliging en privacybescherming worden deze bezwaren in meer detail besproken.)

De technologie voor het detecteren van kinderpornografie (enkel op basis van een database van bekend beeldmateriaal) is inherent onbetrouwbaar. Kinderpornografisch beeldmateriaal is eenvoudig zo aan te passen dat ze niet als zodanig herkend wordt. Ook is het makkelijk om ogenschijnlijk onschuldige foto's zo te manipuleren dat ze als kinderpornografisch worden gezien, en de nietsvermoedende en onschuldige ontvanger op een lijst van verdachten voor verder onderzoek te plaatsen. Dit risico van onterechte verdenking kleeft ook aan het voorgestelde gebruik van kunstmatige intelligentie voor het herkennen van nog onbekende kinderpornografie, of het detecteren van 'grooming'.

Gezien de aard van het misdrijf kan een potentiële verdenking een grote impact hebben op de personen die daarmee geconfronteerd worden. Ook al blijkt bij nadere inspectie dat de afbeeldingen inderdaad onschuldig van aard zijn. Onder het motto 'waar rook is, is vuur' kan de directe omgeving van de verdachte, of de dienstaanbieder, of misschien de politie zelf, toch een interne aantekening van deze melding maken. Het is van hierbij van belang op te merken dat het voorstel van de commissie niet onder het strafrecht valt en daarmee ook niet met de daarbij behorende garanties is omkleed. De meest recente versie van het voorstel (van september dit jaar) geeft gebruikers waarover een melding wordt gedaan ook minder informatie over de aard en de reden van de melding dan eerdere versies.

Fundamenteler van aard is het bezwaar dat er een 'verklikker' op de telefoon van alle Europese burgers wordt geïnstalleerd die een melding naar de autoriteiten kan sturen bij iedere match met de database. Onze telefoon is zeer persoonlijk: we hebben hem altijd bij ons en zetten alles wat we doen, zien of denken in onze telefoon. Het wetsvoorstel komt er dus op neer dat instanties technisch de mogelijkheid krijgen mee te kijken in ons privéleven.

Weliswaar bepaalt het voorstel van de Commissie dat de inzet van deze verklikker enkel toegestaan is als dit strikt noodzakelijk is. Echter, onduidelijk

[1] https://edri.org/wp-content/uploads/2023/07/Open-Letter-CSA-Scientific-community.pdf

is wat precies onder strikte noodzaak wordt verstaan. Bovendien zijn deze beperkingen zijn slechts procedureel van aard, en worden enkel getoetst door de autoriteit die zelf juist verantwoordelijk is voor de bestrijding van kindermisbruik. Ook is onduidelijk hoe in de praktijk het gebruik van de verklikker daadwerkelijk gericht kan worden ingezet. Het is bijkans onvermijdelijk dat de verklikker standaard op de telefoons van alle gebruikers van de eerder genoemde communicatiediensten geïnstalleerd moet worden, en daarna (hopelijk) voldoende gericht geactiveerd wordt enkel op basis van een duidelijk gemotiveerde verdenking van kindermisbruik. In het voorstel van de commissie zijn daar echter geen enkele concrete bepalingen of beperkingen voor opgenomen, zodat de verwachting niet anders kan zijn dan dat het middel ongericht zal worden ingezet. Daarmee wordt een ongekende en onomkeerbare stap gezet naar een verregaande Europese infrastructuur voor massasurveillance. Het voorstel van de Commissie verhoudt zich dan ook slecht met het fundamentele recht op de bescherming van de persoonlijke levenssfeer, zoals vastgelegd in het handvest van de Europese Unie. Voor meer details verwijs ik hierbij graag naar een onlangs verschenen rapport van het Instituut voor Informatierecht (IViR). [2]

Het is hierbij ook belangrijk om op te merken dat in strikt technische zin het voorstel voor client-side scanning geen inbreuk doet op de techniek van end-to-end encryptie. Maar dat is wel een zeer enge interpretatie van wat end-to-end encryptie behelst: het is een technologie die bedoeld is om de *vertrouwelijkheid van communicatie* te beschermen. Het briefgeheim is ook weinig waard als de overheid wel mee mag lezen als de brief geschreven of gelezen wordt. Dat maakt duidelijk dat het dossier van het bestrijden van kindermisbruik een fundamentele discussie over de afweging van fundamentele rechten (die van het beschermen van de rechten van het kind en die van het beschermen van de persoonlijke levenssfeer) vereist. Waarbij ook opgemerkt moet worden dat de mogelijkheid tot vertrouwelijke communicatie juist ook in het belang van kinderen is.

Daarnaast bepaalt de inhoud van de database wat door de verklikker als verdacht materiaal wordt gezien. Daarmee is de scope van wat verdacht is dus eenvoudig uit te breiden: dat is een simpele update van de database. Op die manier kan het systeem ook gebruikt worden om ander ongewenst materiaal te detecteren, zoals terroristisch promotiemateriaal, of haatzaaiende afbeeldingen. Dat enkel een procedurele maatregel hierbij in de weg staat, is niet erg geruststellend gezien de vele voorbeelden van misbruik van een

[2] https://www.ivir.nl/publicaties/download/CSAMreport.pdf

dergelijke mogelijkheid tot '*function creep*', en de berichten dat Europol ook andere toepassingsgebieden van de technologie voor ogen heeft.[3]

Misschien helpt een vergelijking met bestaande technologie duidelijk te maken dat het voorstel van de commissie een gevaarlijk precedent schept. Client-side scanning is vergelijkbaar met het verplicht installeren van een beveiligingscamera in iedere woning, die *enkel* geactiveerd wordt zodra er sprake lijkt te zijn van huiselijk geweld. Hoe belangrijk we ook de bestrijding van huiselijk geweld vinden, een dergelijke maatregel zou (hoop ik) duidelijk veel te ver voeren. Toch is dat in essentie wat client-side scanning behelst: er gaat op ons 'digitale huis' automatisch een rood lampje branden als uitnodiging om een digitale huiszoeking te doen.

Ik hoop dat dit position paper duidelijk heeft gemaakt dat het voorstel van de Commissie een gevaarlijk precedent schept ten aanzien van de mogelijkheid tot verregaande inmenging van de (Europese) overheid in het privéleven van Europese burgers. Het bestrijden van kindermisbruik is ontegenzeggelijk van groot belang. Maar dit is niet de weg is die we daarvoor moeten gaan.

[3] https://www.groene.nl/artikel/wie-heeft-hier-baat-bij-niet-de-kinderen