Een digitale spion in elk mobieltje, voor uw eigen bestwil

Posted on 22 juni 2024 by Arnout Jaspers

Afgelopen donderdag zou de Europese ministerraad stemmen over een vérstrekkend voorstel om de online verspreiding van kinderporno tegen te gaan. Daarna zou het nog moeten worden voorgelegd aan het Europees Parlement. De ministerraad besloot het echter niet eens op een stemming aan te laten komen, omdat het voorstel nu waarschijnlijk geen meerderheid haalt. Maar 'Voorstel 12611/23' is nog niet definitief ingetrokken.

Als dit ooit nog wordt doorgevoerd, komt het er op neer dat elke Europeaan voortaan met een digitale spion van de overheid in zijn of haar mobieltje rondloopt. Voorstanders van dit soort *Big Brother*-surveillance zullen zeggen dat dit zwaar overdreven is, omdat er beperkingen aan zitten: die digitale spion in zijn huidige vorm controleert alleen of je geen kinderpornografische foto's of video's verstuurt via Whatsapp, Telegram of andere publieke communicatiekanalen. Zolang je dat niet doet, kijkt er niemand mee in je telefoon, wordt ons verzekerd. Maar als je dat wel doet, verklikt je eigen telefoon je volautomatisch aan de overheid.

Whatsapp, Telegram, en sinds kort ook Facebook Chat, maken gebruik van *end-to-end* encryptie. Dat wil zeggen: de tekst en beelden die jij verstuurt, worden in je telefoon omgezet in geheimschrift dat alleen je gesprekspartner kan ontcijferen, en vice versa (door middel van zogeheten *public key* encryptie, een ingenieus systeem waarmee twee partijen veilig kunnen communiceren zonder dat ze elkaar eerst een geheime sleutel hoeven toe te sturen. Zonder *public key* encryptie zouden online betalingen onmogelijk zijn).

Goed geïmplementeerde *end-to-end* encryptie is onkraakbaar. Noch de overheid, noch de internetprovider beschikt over de decryptiesleutels, en zonder die sleutels is ontcijferen onbegonnen werk. Het officiële EU-standpunt is dat zulke encryptie een groot goed is om de privacy van haar burgers te waarborgen. In het voorstel staat ook expliciet, dat men niet de bedoeling heeft om *end-to-end* encryptie te ondergraven.

Terrorisme als excuus

Dat is de theorie; in de praktijk gedragen overheden zich alsof ze zulke lekvrije encryptie een gruwel vinden. Eerder veroorzaakte de Amerikaanse FBI brede ophef, omdat ze Apple wilden dwingen een 'achterdeur' in hun besturingssoftware in te bouwen, waardoor de geheime dienst de wachtwoordbeveiliging van Apple-telefoons zou kunnen omzeilen. Echt alleen maar om in de telefoons van gearresteerde terroristen te kunnen kijken, uiteraard.

Voorstel 12611/23 houdt in, dat de EU telefoon- en internetproviders een 'detectiebevel' geeft voor kinderporno en online *grooming* van kinderen. Het voorstel zegt niet hoe die providers dat moeten doen, omdat de opstellers zich niet willen vastpinnen op de huidige stand van de techniek.

Onvermijdelijk is echter, dat tekst en beeld worden geanalyseerd voordat het met onkraakbare *end-to-end* encryptie verstuurd wordt. Dat moet dus gebeuren door software in de telefoon zelf.

Automatische alarmering

In 2021 kondigde Apple aan op eigen initiatief zulke spionagesoftware in het besturingssysteem van al zijn telefoons te gaan installeren. Hun systeem ging alle foto's en video's, die via een iPhone worden opgeslagen in de iCloud, vooraf

scannen op kinderporno. Ondanks geavanceerde waarborgen voor privacy, stak een storm van protest op onder cybersecurity-experts en privacyactivisten. Waarop Apple het plan schielijk in de ijskast zette.

Het AI-systeem van Apple maakte in de telefoon van elke foto of video die geback-upt werd naar de iCloud een soort digitale vingerafdruk (een *neural hash*, een getal van 96 cijfers). Die vingerafdruk werd vergeleken met de vele miljoenen vingerafdrukken van al bekende kinderporno in een centrale database, beheerd door de overheid. Na een minimum aantal matches (vijf of tien, om vals alarm zoveel mogelijk te voorkomen) gaat automatisch een alarmering naar de provider en naar opsporingsinstanties.

Omdat niet de foto's zelf worden gelekt of door een mens bekeken, scheen Apple te denken dat dit slechts een kleine, aanvaardbare inbreuk op de privacy van hun klanten was, vergeleken met het grotere goed van het betrappen van verspreiders van kinderporno.

Ook Voorstel 12611/23 voorziet in een 'EU Centre on Child Sexual Abuse' met een centrale databank van al bekende kinderporno. Daarnaast zou zo'n detectiebevel ook het signaleren van nieuwe kinderporno moeten omvatten. Hoe dat moet gebeuren wordt er niet bij gezegd; AI-systemen zijn momenteel niet in staat onschuldige vakantiekiekjes met blote kinderen bij een zwembadje in de achtertuin betrouwbaar te onderscheiden van kinderporno. Voorts is het ondoenlijk om de vele miljoenen foto's die dagelijks in de EU worden geüpload allemaal door mensen te laten beoordelen, nog los van de evidente privacybezwaren. Eigenlijk neemt het voorstel hier een voorschot op hypothetische, betere AI-systemen die dat wel voldoende betrouwbaar kunnen.

Alles of niets

Onder invloed van alle kritiek die eerder was losgebarsten, was het voorstel al iets afgezwakt: onder het fraaie eufemisme *moderated uploading* zou de gebruiker van de telefoon 'ja' of 'nee' mogen zeggen tegen het automatisch scannen van zijn beeldmateriaal. Maar uiteraard is dat een alles of niets keuze: 'nee' betekent dat hij of zij geen enkele foto of video meer kan back-uppen in de *cloud* of uploaden naar Whatsapp. Dat is geen keuze; dat is digitale afpersing.

Zelfs als je vindt dat kinderporno dermate afschuwelijk is dat dit forse inbreuken op

de privacy rechtvaardigt, is de vraag wat de bestrijding ermee opschiet. Je kunt beeld namelijk prima offline met *public key* encriptie onherkenbaar maken en daarna pas via je telefoon of computer uploaden.

De gehaaide producenten en grote verspreiders van kinderporno vang je er dus niet mee, hoogstens de domme viezeriken die zulk materiaal argeloos met elkaar delen. En daarnaast zullen er onvermijdelijk mensen onterecht door zulke AI-systemen worden gebrandmerkt als verspreiders van kinderporno. We hebben inmiddels ruime ervaring met wat er terecht komt van beloftes door de overheid, dat mensen nooit alleen maar door een AI-systeem of algoritme zullen worden aangemerkt als dader.

Nieuwe toepassingen

Nog gevaarlijker is *mission creep*, het stap voor stap uitbreiden van zo'n surveillancesysteem. Als zulke software eenmaal standaard in het besturingssysteem van telefoons zit, is het bijna een natuurwet dat politie en veiligheidsdiensten nieuwe toepassingen gaan bedenken.

Als er toch al een digitale vingerafdruk beschikbaar wordt gemaakt van elke verzonden foto of video, dan kun je die zonder veel extra moeite ook matchen met een database van beeldmateriaal van vermiste personen, of verdachten van terrorisme, of voorwerpen die aangemerkt worden als gerelateerd aan drugshandel. Vandaar is het nog maar een kleine stap naar die digitale vingerafdrukken matchen met een database van als desinformatie aangemerkt materiaal over, zeg, de oorlog in Oekraïne, of vaccinatie. Alles voor uw eigen bestwil en veiligheid, uiteraard.

Voorstel 12611/23 staat nu in de ijskast. Maar zulke *Big Brother*-surveillance is dermate aantrekkelijk voor overheden en veiligheidsdiensten, dat het in aangepaste vorm vast wel weer ergens opduikt. En de technische complexiteit zorgt ervoor, dat de gangbare media nauwelijks aandacht besteden aan zulke onderwerpen. Dat zouden ze aan de talkshowtafels beter wel kunnen doen.

*Van wetenschapsjournalist **Arnout Jaspers** verscheen onlangs **De Klimaatoptimist**, over energietransitie in Nederland. Het boek is **HIER** te bestellen. Informatie voor media en boekhandel: info@blauwburgwal.nl*

Wynia's Week** viert het vijfjarig bestaan. Wynia's Week wordt mogelijk gemaakt door de vrijwillig betaalde abonnementen van de lezers, kijkers en luisteraars. **Doet

u al mee?