

Rejo Zenger (\*)

30 mei 2022

## “Het onmogelijke doen”

Dat is natuurlijk niet letterlijk wat er in het [voorstel](#) staat dat de Europese Commissie op 11 mei lanceerde. Het voorstel zal bedrijven dwingen te controleren wat mensen met elkaar delen via chat-apps als WhatsApp en platforms als Instagram. Als dat nodig wordt geacht, zullen de platforms worden gedwongen om informatie te verwijderen of aan de autoriteiten te melden. Ook internetproviders kunnen worden verplicht het internetverkeer van hun klanten te controleren. Maar de Commissie laat heel slim achterwege te zeggen *hoe* ze dat precies moeten doen. In feite is haar boodschap voor bedrijven: “Doe het onmogelijke, je mag zelf bepalen hoe.” Het is technisch gewoon onmogelijk om iemands internetverbinding te filteren op de manier die de Europese Commissie wil.

## Door de overheid opgelegde spyware

Om een voorbeeld te geven: op basis van dit voorstel kan een instant messaging platform (FaceBook Messenger, WhatsApp, Skype, Telegram...) de taak krijgen om materiaal van seksuele uitbuiting van kinderen op te sporen. Dat kan bekend materiaal zijn, of ‘nieuw’ materiaal, of [grooming](#), dus tekst. Laten we er bij wijze van voorbeeld van uitgaan dat de opdracht aan Meta wordt gegeven met betrekking tot Whatsapp. Een platform dat, zoals men weet, beveiligd is met end-to-end encryptie. Dit type encryptie betekent dat Meta kan zien wie met wie communiceert, maar niet in staat is de inhoud van die communicatie te lezen. Maar hoe kan Meta iets ontdekken in een gesprek waartoe het geen toegang heeft? Gemakshalve laat de Commissie die beslissing (de “hoe het moet”) over aan het platform. Onze gok is dat de enige manier om het te doen, is door het installeren van een soort (nu, door de overheid opgelegde!) spyware op de telefoons van de mensen die een bepaalde dienst gebruiken. Dat is immers de enige plaats waar de inhoud van de chats leesbaar is.

## Wat fout kan gaan, zal fout gaan.

En ja, er zijn een paar waarborgen ingebouwd in het voorstel. Een bevel kan bijvoorbeeld alleen worden gegeven als “redelijke risicobeperkende maatregelen” ontoereikend zijn gebleken. En alleen als de redenen voor het uitvoeren van het bevel “zwaarder wegen dan de nadelige gevolgen voor de rechten en legitieme belangen van alle betrokkenen”. Op basis daarvan zou je kunnen stellen dat het installeren van spyware op *iedere* telefoon nooit een evenredige maatregel kan zijn als het gaat erom gaat *bepaalde* stukjes informatie van bepaalde apparaten op te sporen en te verwijderen. Maar in het

voorstel staat ook dat “de keuze van de technologie aan het bedrijf wordt overgelaten, zolang aan de eisen van deze wet wordt voldaan”. Jarenlange ervaring leidt er helaas toe dat wij voorgestelde wetgeving vanuit de meest pessimistische invalshoek interpreteren: wat fout kan gaan, zal vroeg of laat fout gaan!

We maken ons op voor een intens emotioneel politiek debat.

## **Technisch onmogelijk**

Er is weinig ruimte om het rooskleurig in te zien. Het voorstel biedt de autoriteiten bijvoorbeeld de mogelijkheid om de toegang tot bepaalde URL's (internetadressen) te laten blokkeren. Dat kunnen specifieke pagina's zijn, zoals 'https://www.bitsoffreedom.nl/doneren', of specifieke afbeeldingen op die pagina. Tegenwoordig zijn bijna alle websites alleen toegankelijk via een beveiligde TLS-verbinding (de "s" in "https://"). Zo ook de onze. Wanneer u de webpagina bezoekt waarop u zich op dat moment bevindt, wordt de verbinding tussen uw browser en de server waar de website is “opgeslagen”, versleuteld. Door die versleuteling kan uw provider alleen zien dat u onze website bezoekt, maar niet welke pagina of de inhoud daarvan. Uw provider kan de volledige URL niet zien. En dat betekent dat het technisch onmogelijk is om uw internet te filteren, zoals de Europese Commissie wil dat providers doen. Tenzij we de versleuteling gewoon afschaffen of van providers verwachten dat ze uw internetverkeer manipuleren.

## **Een intens emotioneel politiek debat**

We moeten ons schrap zetten voor een intens emotioneel politiek debat. De voorgestelde maatregelen zouden de vertrouwelijkheid van onze communicatie ernstig ondermijnen, en worden gepresenteerd in de context van een ongelooflijk gevoelig en belangrijk onderwerp, namelijk de bescherming van kinderen tegen seksueel misbruik. Dit wordt een debat waarin rationele argumenten, meer nog dan anders, het zwaar te verduren zullen krijgen.

## **Nu al rampzalig**

Ongeacht de precieze uitkomst is het voorstel nu al schadelijk omdat het bedrijven ontmoedigt hun diensten veiliger te maken door encryptie te ontwikkelen en toe te passen. Tegen de achtergrond van dit voorstel zou elke stap in die richting immers kunnen worden geïnterpreteerd als het doelbewust in een kwetsbaarder positie plaatsen van kinderen, als een besluit om de strijd tegen seksueel misbruik van kinderen te belemmeren. Geen enkel bedrijf zal dat willen. Als een bedrijf van plan was end-to-end-encryptie in te voeren voor een bestaande dienst, zijn die plannen nu ongetwijfeld op de lange baan geschoven. En daarmee, zelfs als het voorstel van de Europese Commissie uiteindelijk wordt verworpen, heeft het zijn schade al aangericht.

## Onmisbaar voor iedereen

Oh, en het spreekt voor zich dat iedereen, ook wij, de strijd tegen seksueel misbruik van kinderen ontzettend belangrijk vindt. Juist daarom is het van cruciaal belang om in te zetten op effectieve en duurzame maatregelen. Dit voorstel voldoet niet aan die normen. Vertrouwelijke communicatie is onontbeerlijk voor iedereen, ook voor kinderen en slachtoffers van seksueel misbruik. Je kunt alleen veilig communiceren met een vertrouwde vriend, raadsman, maatschappelijk werker of rechtshandavingsambtenaar als je er zeker van kunt zijn dat niemand over je schouder meekijkt. De Europese wetgever moet zich daarom richten op andere maatregelen. Bijvoorbeeld het stroomlijnen van grensoverschrijdende strafrechtelijke onderzoeken, het versterken van de samenwerking tussen verschillende diensten en het wegwerken van de enorme achterstand bij de zedenpolitie.

(\*) **Rejo Zenger** is beleidsadviseur voor [Bits of Freedom](#), een stichting opgericht in 1999 en gevestigd in Amsterdam. Ze telt nu 11 vaste medewerkers en meer dan 700 vrijwilligers. Bits of Freedom zet zich in voor een open en rechtvaardige informatiemaatschappij, en is medestichter van [EDRI](#) (European Digital Rights), een Europese koepel van organisaties ter verdediging van de digitale rechten van de burgers.

Dit artikel werd op 11 mei gepubliceerd met een Creative Commons licentie op de [site van Bits of Freedom](#) onder de titel "*European Commission wants to eliminate online confidentiality*". Nederlandse vertaling door Ander Europa. Het artikel verscheen ook op 25 mei op de [site van EDRI](#).

---

Dit delen:

[Facebook](#)

[Twitter](#)