

# Privacy en veiligheid in Europa

Axel Arnbak



**O**veral in de fysieke en digitale wereld woedt de slag om de sleutel tot onze privé-informatie. Apple en de FBI bevechten elkaar continu over de beveiliging van iPhones. Berichtenservice WhatsApp versleutelt sinds kort alle chats van ruim één miljard gebruikers.

Vorige week is de veelbesproken Europese Dataprotectie Verordening goedgekeurd. Gelijktijdig kondigde de Europese Commissie de grootschalige herziening aan van de EU-wet over de versleuteling van elektronische communicatie: de E-Privacy Richtlijn.

Versleuteling is hot omdat het monumentale economische- en (geo)politieke vraagstukken opwerpt. Het gaat om de vraag wie welke internetgebruikers kan tracken en bespioneren in de 21ste eeuw.

De huidige E-Privacy Richtlijn uit 2009 reguleert nu vooral aanbieders van internettoegang. Wie goed oplet, voor en achter de schermen, ziet grootse plannen van Europese politici: versleutelingsplichten voor alle aanbieders van communicatiediensten. Of je nu internettelefoon, Angry Birds, een dating-website of verzekeringsapp aanbiedt.

Het nieuws dat WhatsApp nu alle communicatie van alle gebruikers ver-

sleutelt, verraste vele gebruikers. 'Oh, was dat niet al zo?' Tot voor kort slingerden honderden miljoenen gebruikers volstrekt onveilig hun passwords, plaatjes en 'private parts' over de app.

Zodra jij en degene met wie je communiceert de laatste WhatsApp-update uitvoeren, is die gevoelige inhoud door 'end-to-end'-versleuteling alleen zichtbaar op de smartphone van zender en ontvanger. Niet voor WhatsApp, niet voor je internetprovider, en niet voor afluisterende overheden en cybercriminelen wereldwijd.

Versleuteling beschermt je metadata (zoals met wie je appt) meestal niet. Toch krijgt het analoge briefgeheim weer digitale betekenis. WhatsApp verdient een grote pluim dat het een miljard mensen beschermt en hen eraan herinnert dat het internet achter glimmende schermpjes vaak alarmerend onveilig is.

De inherente onveiligheid van het internet is geen technisch probleem, maar

**In feite beschermt versleuteling consument én nationale veiligheid tegen alle luistervinken**

een bewuste politieke keuze. Iedereen is vergeten dat het allereerste voorstel van de Europese Commissie voor een E-Privacy Richtlijn in 1990 een keiharde verplichting bevatte om communicatie end-to-end te versleutelen.

Voor mijn onlangs verdedigde proefschrift ondervroeg ik een aantal ambtenaren van de toenmalige Europese Commissie over de mysterieuze verdwijning van het voorstel. Voor westerse inlichtingendiensten bleek het volstrekt onacceptabel. Vooral voor de Fransen en Engelsen, die graag over de grens economisch spioneren. Sindsdien is end-to-end-versleuteling nooit meer in Brussel besproken.

Tot vandaag. Zal universele end-to-end-encryptie het halen in Brussel? Dat hangt in de eerste plaats af van politieke framing, net als in het Apple versus FBI-debat. Zien Europese politici versleuteling als kwestie van consumentenveiligheid of van nationale veiligheid? Over dat laatste heeft Europa niets te zeggen, over het eerste des te meer.

In feite beschermt versleuteling consument én nationale veiligheid tegen alle luistervinken. En zijn terroristen altijd via andere wegen op te sporen, zoals geldstromen, gerichte opsporing

en vooral door betere internationale samenwerking.

Een tweede factor, en een belangrijk verschil met de jaren negentig, is dat aanbieders als WhatsApp en Apple zich nu sterk maken om hun gebruikers end-to-end te beschermen. Zo sterk, dat zij zichzelf uit de communicatiewaardeketen snijden. Dat zal voor andere bedrijven niet gaan, zoals app- en gameontwikkelaars die hun businessmodel voeden met gebruikersdata.

Kiest de politiek voor universele encryptie, dan kiest zij niet voor economische spionage en geeft zij bepaalde businessmodellen voorrang. Robuuste encryptie betekent het één of het ander: volledige spionage, tracking én beveiliging gaat niet.

In dat immense krachtenveld moet de Europese Commissie haar versleutelingsvoorstel formuleren. Te midden van fundamentele debatten over terrorisme, innovatie en Europese integratie, wordt Brussel tot de mondiale politieke arena in de slag om encryptiesleutels.

**Axel Arnbak is advocaat bij De Brauw Blackstone & Westbroek en onderzoeker aan het Instituut voor Informatierecht (UvA). Reacties: @axelarnbak**