

Gevecht om de macht woedt in digitale wereld

Het juridisch gevecht over de beveiliging van iPhones kan uitgroeien tot dé techcase van het decennium. De vete gaat om één simpele vraag: wie is de baas in de digitale wereld, de overheid of Silicon Valley? De FBI eist dat Apple de iPhone hackbaar maakt. Apple weigert. De iPhone is zo versleuteld dat niet Apple, maar de consument bepaalt wie bij alle data op het toestel kan.

Apple stelt terecht dat het hackbaar maken voor de FBI inhoudt dat de iPhone ook hackbaar wordt voor cybercriminelen, dictators, iedereen. De rechter moet nu, voor het eerst, bepalen of Apple met een softwareupdate een achterdeurtje in de iPhone moet bouwen.

Digitale veiligheid en nationale veiligheid lijken te botsen, maar in feite staat de FBI juridisch en technisch zwak. De kwestie gaat niet alleen om de feiten, maar om iets groters: macht. En naast politieke invloed en juridisch gelijk, treden productontwerp en cybersecurity op de voorgrond als cruciale machtsfactoren in de informatiesamenleving.

Juist vanwege de gevoeligheid van de aanleiding — de dramatische aanslag door Isis in San Bernardino — is helder inzicht in de feiten, de technologie en juridische argumenten essentieel. Dader Farook had twee smartphones en de FBI weet, blijkt ook uit de processtukken, dat zijn iPhone (een werktelefoon) weinig gebruikt werd. Apple heeft reeds alle beschikbare gegevens aan de FBI geleverd. Het is onzeker of de FBI al langs andere communicatiebedrijven is gegaan voor data en vrij onwaarschijnlijk dat de FBI

iets aan de gedwongen hack zal hebben. Apple kan bij alle data op de iCloud, maar niet bij de iPhone zelf. Apple dwingt zo technologisch af dat gebruikers controleren met wie zij welke data delen. Apple beschermt zo ook de gebruiker tegen misbruik van gevoelige foto's, creditcard- en identiteitsfraude nadat een iPhone is gestolen of verloren. De techniek van exclusieve toegang voor gebruikers, niet voor Apple, is pas sinds kort betaalbaar, schaalbaar en wordt steeds belangrijker: Apple hoopt van de relatief veilige iPhone het platform voor het internet der dingen, fintech en connected cars te maken. Met een lekke iPhone gaat dat niet.

De praktijk wijst verder uit dat exclusieve achterdeurtjes niet bestaan: vreemde overheden en cybercriminelen wereldwijd zullen met man, macht en geld jagen op de kwetsbaarheid die Apple zou moeten bouwen voor de FBI. Of het nu om de iPhone van Mark Rutte, activisten in dictaturen of gewone consumenten gaat, iedereen loopt gevaar als lekke software circuleert. China, Rusland en Assad zullen nu ook een lek eisen. Gezien de feiten, technologie en geopolitiek, zullen achterdeurtjes nationale veiligheid niet dienen, eerder ondergraven.

De FBI baseert zich bovendien op een wankele juridische grondslag, te weten een algemene wet uit 1789 (!) over medewerking van particulieren aan overheidsverzoeken. De FBI probeert al jaren

Post, telegraaf, telefoon en satellieten zijn ontwikkeld door de overheid, die altijd kon meekijken waar nodig

specifiekere wetgeving voor achterdeurtjes door het Amerikaanse Congres te loodsen, zonder succes. Met Silicon Valley, wetenschappers en privacyactivisten voor een keertje zij aan zij, waagt de politiek zich er niet aan. Sluwe vos FBI stapt dan maar, met een gevoelige casus, naar een conservatieve rechter in California.

Het geschil gaat dus niet zozeer om opsporing of juridisch gelijk, maar om iets groters. Sinds de Romeinen en vooral Napoleon weten wij dat macht in een natie staat is gebaseerd op de uitlesbaarheid en controle van burgers, bedrijven, vreemde mogendheden en hun communicatie. Post, telegraaf, telefoon en satellieten zijn ontwikkeld door de overheid, die altijd meekijkt waar nodig of gewenst. In de digitale wereld is de rol van de staat beperkt. Bij de iPhone staan cybersecurity en productontwerp overheidscontrole zelfs technologisch in de weg. En techniek als machtsfactor is een doorn in het oog van autoriteiten.

In de trias politica ligt het gecontroleerde machtsmonopolie bij de overheid. Productontwerp is een nieuwe machtsfactor. Ook al lijken de feiten, techniek en het recht aan Apple's zijde, en nog los van het wantrouwen in de VS-overheid na Snowden, FBI vs Apple gaat over de complexe en fundamentele vraag wie mag bepalen hoe veiligheid en productontwerp in de digitale wereld vorm krijgen. Wij staan dus aan de vooravond van 'design wars' tussen autoriteiten, techbedrijven, politiek en de rechter.

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



Axel Arnbak