

“Privacy zal in de toekomst enkel voor de rijken zijn”: twee Vlaamse experts waarschuwen voor onze afkalvende privacy

18-10-2023 *Het Laatste Nieuws* - Jay Stout

Als het van de federale regering afhangt, heeft ons land binnenkort 10.000 ANPR-camera's voor automatische nummerplaatherkenning. Nieuwe identiteitskaarten moeten nu al vingerafdrukken bevatten en Europa denkt na over achterpoortjes in chatapps. Privacyactivist en -jurist Matthias Dobbelaere-Welvaert en cryptograaf Bart Preneel over de huidige staat van online privacy en de zin en onzin van sommige maatregelen. “Koop geen cryptotelefoon. Daarmee trek je gegarandeerd de aandacht van de overheid.”

PREMIUM

Bestaat privacy nog, volgens jullie?

Matthias Dobbelaere-Welvaert : “Ik word haast moedeloos van sommige nieuwsberichten. Maar ja, er bestaat volgens mij nog steeds privacy in België. In ons land is het bijvoorbeeld nog mogelijk om je mening te uiten en dat is in sommige andere landen - zoals China - toch anders. We hebben dus nog privacy, maar daar wordt aan geknabbeld.”

Op welke manier?

“Als we even terugspoelen, zien we dat we steeds meer privacy moeten inleveren. Eind 2016 besloot de Belgische overheid bijvoorbeeld dat we geen prepaid simkaart meer mogen kopen zonder eerst onze identiteitskaart te laten registreren. In 2019 besliste de overheid dan weer dat vingerafdrukken voortaan aan onze identiteitskaart gekoppeld moeten zijn. Enige tijd geleden zagen we dat er een derde Belgische dataretentiewet werd gestemd en die zorgt ervoor dat we allemaal gecontroleerd kunnen worden. Het begint te wringen. Niet enkel bij mij, overigens. Bij heel wat mensen.”

Bart Preneel : “In 1999 zei Scott McNealy, de toenmalige grote baas van het Amerikaanse Sun Microsystems: ‘

You have no privacy, get over it .’ Je hebt geen privacy, leg je erbij neer. Het klopt dat we vandaag in een hoogtechnologische wereld leven waarin het schenden van privacy door de overheid heel wat eenvoudiger is geworden. Vroeger hadden de ordediensten ook de mogelijkheid om telefoonlijnen af te tappen, of om mensen te schaduwen, maar dat kostte heel wat geld en mankracht. De technologische middelen om dit voor elkaar te krijgen zijn vandaag de dag veel toegankelijker en veel intrusiever. Niet enkel de overheid is overigens in staat om jouw privacy te schenden: ook bedrijven beschikken over deze technologie. En andere burgers ook.”

Maar misschien moet je niets te verbergen hebben?

Dobbelaere-Welvaert : “Die uitspraak is eenvoudig te weerleggen. Vraag maar eens aan de man in de straat of die zijn adres, financiële toestand of medische gegevens zomaar met iedereen wil delen. Dan stuit je al snel op verzet. Dat je niets te verbergen hebt, is overigens relatief. In ons land heb je met een andere seksuele geartheid inderdaad niets te verbergen. In Polen of Hongarije ligt dat toch anders en dat zijn ook Europese landen.”

Preneel: “Niet alles wat je verbergt, hoeft ook negatief te zijn. Soms wil je een geschenk voor je partner nog even achter de hand houden of wil je in staat zijn om iemand te verrassen. Privacy is een essentieel onderdeel van menselijke relaties en van onze samenleving. Het is één van de basiselementen van menselijke interactie. Binnenkort zullen er AI-systemen bestaan die gevoelens van mensen via gelaatsuitdrukkingen kunnen registreren. Dat zal weer tot nieuwe vragen over privacy leiden.”

Politici zouden moeten beseffen dat zij het meeste risico lopen om bespioneerd te worden.

Bart Preneel, KULeuven

Wat zal die toekomst brengen, meer of minder privacy?

Dobbelaere-Welvaert: “Ik denk dat privacy in de toekomst enkel voor de rijken zal zijn. Je ziet de eerste sporen daar nu al van. Je kan in de supermarkt een klantenkaart aanvragen om extra korting te ontvangen, maar daarvoor geef je wel je persoonsgegevens op. Zo’n klantenkaart is aantrekkelijk voor mensen die moeite hebben om de eindjes aan elkaar te knopen, maar veel minder voor mensen met een aardige loonbrief. Privacy wordt dus als het ware een betaalmiddel ...”

“Politici lijken dit niet te beseffen. Meer zelfs, ze hangen onze straten vol met slimme camera’s om vervolgens te kunnen zeggen dat de veiligheidsgraad in het dorp omhoog gaat. Wat ze niet zeggen is dat we met z’n allen een flinke prijs aan het betalen zijn: onze privacy.”

Preneel : “De politici zouden ook moeten beseffen dat zij het meeste risico lopen om bespioneerd te worden. Neem het voorbeeld van Israëlische oud-premier Netanyahu. Zijn vertrouwenskring werd met behulp van de Pegasus-spyware afgeluisterd en dat door eigen politiediensten. Machthebbers zijn de eersten die in het vizier komen als privacy komt te vervallen en hebben er dus alle baat bij dat die beschermd wordt.”

Niet elke persoon met cryptografische software op zijn telefoon heeft slechte bedoelingen. Soms is het tegendeel net waar.

Matthias Dobbelaere-Welvaert, privacyactivist en -jurist

Nochtans lijkt de politiek van mening dat privacy in sommige gevallen moet wijken. Versleutelde chatplatforms zijn een doorn in het oog van ordediensten en de jacht op cryptografische telefoons wordt opgevoerd. Dit zouden middelen zijn van criminelen?

Dobbelaere-Welvaert : “Cryptografische telefoons waarvan alles dichtgetimmerd is, zijn inderdaad niet bestemd voor consumenten. Toch wil dat niet zeggen dat Jan Modaal geen voordeel kan halen uit een beveiligde telefoon. Kijk maar naar bepaalde landen waar mensen onderdrukt worden wegens een afwijkende mening. Klokkeluiders en journalisten hebben overigens ook baat bij deze tech. Niet elke

persoon met cryptografische software op zijn telefoon heeft dus slechte bedoelingen. Soms is het tegendeel net waar.”

Preneel : “De criminelen met cryptografische telefoons, zoals we die kennen vanuit het

Sky ECC-dossier , hebben overigens een grote vergissing gemaakt. Ze trokken de aandacht van de autoriteiten door hun telefoons dicht te spijkeren en hebben daardoor eigenlijk een groot kruis op hun voorhoofd geplaatst. De fabrikanten van deze dure telefoons kwamen ook in het vizier van de overheid terecht, want ze trekken een bepaald crimineel publiek aan. Wil je dus een privacyvriendelijke telefoon? Koop dan zeker niet zo’n toestel.”

Wat kunnen mensen dan wel doen om hun digitale privacy te waarborgen?

Dobbelaere-Welvaert : “Wat online privacy betreft, kan je apps gebruiken waarmee je data veilig zijn. Signal is een privacyvriendelijk alternatief voor WhatsApp, bijvoorbeeld. Brave is een privacyvriendelijke webbrowsen en er bestaat ook privacyvriendelijke videobelsoftware. Maar blijf vooral kritisch en blijf de maatregelen van de overheid aan de kaak stellen. Alleen kan je bitter weinig doen, helaas. Daarom zijn activistische organisaties zoals NOYB, Bits of Freedom of Ministry of Privacy volgens mij zeer belangrijk.”

Preneel : “Er zijn heel wat oplossingen om je online privacy beter te beschermen. Signal is inderdaad een goed voorbeeld. Je moet je enkel je vrienden overtuigen om over te stappen. Voor sommige andere oplossingen heb je heel wat technische kennis nodig en dat ontbreekt bij de bevolking. Een firewall installeren om na te gaan welke data je slimme wasmachine verstuurt, is bijvoorbeeld een pak lastiger. Het Tor-netwerk gebruiken is ook niet eenvoudig. VPN’s zijn populair, maar bevatten ook een groot risico: ze leiden je internetverkeer om naar een centrale server en hierdoor komt ook al deze informatie op één plaats terecht. Dat is makkelijk om bij te houden. Wist je trouwens dat de Chinese overheid meerdere VPN-bedrijven heeft opgekocht? Dat is niet zonder reden. Er bestaan heel wat manieren om je digitale privacy te beschermen, maar er is tegelijkertijd te weinig

knowhow bij de gewone man in de straat.”

De Europese Commissie denkt erover om onze telefoons te scannen op foto’s van kindermisbruik. Kunnen we ons daartegen beschermen?

Preneel : “Ik denk niet dat deze maatregel er komt. Het zou in ieder geval een grote vergissing zijn. De onderliggende technologie is in de eerste plaats niet in staat om 100 procent feilloos te werken. Daardoor kunnen miljoenen mensen foutief de stempel van kindermisbruiker krijgen, en daar raak je niet zomaar van verlost. Bovendien kan deze technologie ook voor andere politieke doeleinden dienen en dat lijkt me een zeer slecht idee. Apple heeft al zulke scansoftware ter beschikking, maar heeft besloten om die toch niet uit te rollen.”

Dobbelaere-Welvaert : “Ik denk dat die software er wél aankomt. Politici bereiden dit rustig voor door af en toe een ballonnetje op te laten en na te gaan hoe de bevolking reageert. Men laat ons momenteel wennen aan het idee en op een bepaald moment is zo’n ingreep het nieuwe normaal. De vraag is inderdaad, wat als deze technologie in foute handen terechtkomt? De slotsom is deze: technologie op zich is altijd neutraal. Maar

hoe gaan wij ermee om? Dat is de ultieme vraag.