

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

964

Vragen van het lid **Elissen** (PVV) aan de Staatssecretaris van Veiligheid en Justitie over *het registreren van routers* (ingezonden 25 november 2011).

Antwoord van staatssecretaris **Teeven** (Veiligheid en Justitie) (ontvangen 20 december 2011).

Vraag 1

Bent u bekend met het artikel: «5 misverstanden over Google's router opt-out»?¹

Antwoord 1

Ja.

Vraag 2

Deelt u de analyse van het College bescherming persoonsgegevens (Cbp) dat ten aanzien van het verzamelen van routerdata artikel 8 onder F, van de Wet bescherming persoonsgegevens (Wbp) van toepassing is en dat dus krachtens de Nederlandse wet een «opt-out» volstaat? Zo nee, welke andere interpretatie is er volgens u mogelijk en kan hieruit de verplichting voor een opt-in blijken? Bent u bereid hier nader onderzoek naar te doen, te meer het op grote schaal verzamelen en aggregeren van gegevens die in potentie de privacy kunnen schaden steeds vaker voor komt?

Antwoord 2

Ja. Artikel 8 onder f van de Wbp biedt een grondslag voor het verzamelen en verwerken van routerdata. De onderzochte verwerking betreft de combinatie van het MAC-adres (het unieke nummer van de wifi-router) in combinatie met de berekende locatie van de wifi-router. Deze verwerking is van andere aard dan bijvoorbeeld de verwerking van gegevens over surfgedrag met behulp van cookies of de locatiegegevens van smartphones. Deze verwerking brengt derhalve in tegenstelling tot gegevens die informatie verschaffen over het gedrag van de betrokkene geen grote inbreuk op de persoonlijke levenssfeer met zich mee.

Bij de belangenafweging tussen enerzijds de persoonlijke levenssfeer van betrokkenen en anderzijds het belang van de verantwoordelijken die gegevens willen verwerken speelt de mate van gevoeligheid van de gegevens

¹ «Misverstanden over Google's router opt-out» (<http://webwereld.nl/analyse/108652/5-misverstanden-over-google-s-router-opt-out.html>)

die de verantwoordelijke wil verwerken een rol, evenals de waarborgen die de verantwoordelijke heeft getroffen voor een zorgvuldig gebruik van de gegevens. Een belangrijke waarborg is transparantie, duidelijke informatie aan betrokkenen voor welk gerechtvaardigd doel hun persoonsgegevens worden verzameld en verwerkt. Een andere veelvoorkomende waarborg is de mogelijkheid van een opt-out.

Vraag 3

Kunt u één of meer scenario's schetsen waarbij het verzamelen en publiceren van Service Set Identifier (SSID)'s (in combinatie met samenhangende gegevens, zoals de locatie) resulteert in een aantasting van de privacy? Kunt u hierbij rekening houden met de mogelijkheid om deze gegevens met andere databestanden te combineren?

Antwoord 3

Het CBP heeft in zijn rapport van definitieve bevindingen als voorbeeld genoemd dat het MAC-adres van de wifi-router, eventueel samen met het SSID, in combinatie met de locatiegegevens gebruikt zou kunnen worden om een persoon te stalken. Het CBP heeft vastgesteld dat het verzamelen en verwerken van SSID's niet noodzakelijk is voor het kunnen aanbieden van de geolocatiedienst, en heeft Google een last opgelegd om alle in Nederland verzamelde SSID's te vernietigen.

Vraag 4

Deelt u de mening dat een «opt-in» (in tegenstelling tot een «opt-out») een veel kleinere inbreuk op de privacy inhoudt en dat een «opt-in», door bijvoorbeeld het SSID op «_yesmap» te laten eindigen, vanuit privacyperspectief een betere optie is dan de door Google voorgestelde «_nomap»? Zo nee, waarom niet? Denkt u dat huidige regelgeving volstaat?

Antwoord 4

Vanuit het perspectief van betrokkenen is een opt-in (toestemming) vaak te verkiezen boven een opt-out (verzet). Echter, zoals uiteengezet in mijn antwoord op vraag 2 biedt de Wbp naast het toestemmingsvereiste ook de mogelijkheid om te volstaan met een opt-out constructie. Het gaat dan om diensten, waarbij het bedrijfsbelang van de verantwoordelijke in het algemeen opweegt tegen het recht op bescherming van persoonsgegevens en de persoonlijke levenssfeer. Aangezien ik met het CBP van mening ben dat met het verzamelen van routergegevens geen aanzienlijke inbreuk op de privacy wordt gemaakt deel ik de in uw vraag verwoorde mening niet. In de reeds toegezegde brief aan uw Kamer naar aanleiding van de Motie Van Toorenburg e.a. (Kamerstukken II 2011/12 32 761, nr. 12) zal ik hier nader op ingaan.

Vraag 5

Deelt u de stelling uit het artikel dat bedrijven als Microsoft, Apple, Blackberry en Skyhook in overtreding zijn? Bent u bereid het Cbp te vragen dit te onderzoeken? Zo nee, bent u dan bereid een strafrechtelijk onderzoek in te stellen? Zo nee, waarom niet? Welke bedrijven zijn er nog meer in overtreding wanneer het gaat om het verzamelen van gegevens van routers? Wat bent u van plan hieraan te gaan doen?

Antwoord 5

Het oordeel of de in het artikel genoemde bedrijven in overtreding zijn is aan het CBP. Het CBP is een onafhankelijke toezichthouder die zelf kiest bij welke bedrijven en instellingen het onderzoek doet en die bovendien exclusief bevoegd is ten aanzien van de handhaving de Wbp. Er is geen aanknopingspunt voor strafrechtelijk optreden. Ik beschik niet over gegevens welke bedrijven gegevens van routers verzamelen.