

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

1811

Vragen van het lid **Oosenbrug** (PvdA) aan de Ministers van Veiligheid en Justitie en van Economische Zaken over *wifi- en bluetooth tracking* (ingezonden 17 maart 2014).

Antwoord van Staatssecretaris **Teeven** (Veiligheid en Justitie) mede namens de Minister van Economische Zaken (ontvangen 25 april 2014). Zie ook Aanhangsel Handelingen, vergaderjaar 2013–2014, nr. 1696.

Vraag 1

Kent u het bericht «Waarom zet Apple steeds ongevraagd Bluetooth aan»?¹ Herinnert u zich voorts uw eerdere antwoorden op vragen over wifitracking?²

Antwoord 1

Ja.

Vraag 2

Hoe wordt uitgemaakt of op grond van artikel 8, sub f, Wet bescherming persoonsgegevens (Wbp) het verzamelen van gegevens als een gerechtvaardigd eigen belang van degene die die informatie verzamelt (bijvoorbeeld een winkelier) kan worden gezien dat opweegt tegen het belang van de bescherming van de persoonlijke levenssfeer? Wie kan die afweging maken en wie bepaalt wanneer het verzamelen van die gegevens gerechtvaardigd is?

Antwoord 2

Artikel 8, onder f, van de Wet bescherming persoonsgegevens (Wbp) geeft aan dat degene die daarop een beroep doet twee aspecten moet toetsen. In de eerste plaats moet worden vastgesteld of er een gerechtvaardigd belang van de verantwoordelijke of van een derde bestaat aan wie de gegevens worden verstrekt. Ook moet de verwerking noodzakelijk zijn voor het nagestreefde belang. Aan dit noodzakelijkheidsvereiste wordt uitsluitend voldaan als het nagestreefde belang niet anderszins of met minder ingrijpende middelen kan worden gediend. Bij een gerechtvaardigd belang kan worden gedacht aan de noodzaak voor de verantwoordelijke om de gegevens te verwerken om zijn reguliere bedrijfsactiviteiten te kunnen verrichten. In de

¹ <http://www.parool.nl/parool/nl/224/BINNENLAND/article/detail/3612609/2014/03/13/Waarom-zet-Apple-steeds-ongevraagd-Bluetooth-aan.dhtml>

² Aanhangsel Handelingen, vergaderjaar 2013–2014, nr. 1264

tweede plaats moet het gerechtvaardigde belang van de verantwoordelijke of de derde worden afgewogen tegen het belang van de betrokkene en diens fundamentele rechten en vrijheden, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer. Verantwoordelijke en betrokkene kunnen immers een onderling tegengesteld belang bij de verwerking van gegevens hebben. Maar ook de aard van de gegevens en van de verwerking, de verwachtingen die betrokkenen redelijkerwijs kunnen hebben, de waarborgen die zijn getroffen bij de verwerking van deze gegevens, en andere relevante omstandigheden behoren bij de afweging te worden betrokken. Een voorbeeld van een dergelijke waarborg is het onmiddellijk en onomkeerbaar anonimiseren en aggregeren van de gegevens die met wifitracking worden verzameld (bijvoorbeeld door de identificerende kenmerken van de telefoons of andere apparaten van de betrokkenen direct te verwijderen), op zodanige wijze dat individuele gebruikers niet door de tijd heen kunnen worden herkend of onderscheiden. Hoewel artikel 8, onder f, van de Wbp een objectief geformuleerde norm is, is het in de praktijk de verantwoordelijke die de geschetste afwegingen als eerste verricht. De toezichthouder en de rechter kunnen het proces en het resultaat van die afwegingen toetsen.

Vraag 3

Deelt u de mening dat niet ieder commercieel belang achter het verzamelen van gegevens een gerechtvaardigd belang is als men het afweegt tegenover de bescherming van de persoonlijke levenssfeer? Zo ja, hoe en door wie worden uiteindelijk de grenzen bepaald? Zo nee, waarom deelt u die mening niet?

Antwoord 3

Het resultaat van de afweging zoals geschetst in antwoord op vraag 2 kan zijn dat een commercieel belang niet rechtvaardigt dat gegevens worden verzameld, of dat de afweging tussen de belangen van de verantwoordelijke of de derde enerzijds, en de belangen van de betrokkene anderzijds in het voordeel van de laatste uitvalt. Het is niet mogelijk in abstracto aan te geven hoe die belangenafweging moet worden verricht. Zoals bij het antwoord op vraag 2 is aangegeven, is een en ander primair de taak van de verantwoordelijke.

Vraag 4

Wordt er in geval van wifitracking ingevolge de artikelen 33 en 34 van de Wbp kenbaar gemaakt dat er sprake is van verwerking van persoonsgegevens? Zo ja, waar blijkt dat uit? Zo nee, wat zijn de gevolgen voor degene die die persoonsgegevens verzamelt zonder dat kenbaar te maken?

Antwoord 4

Indien door middel van wifitracking persoonsgegevens worden verzameld, gelden voor de verantwoordelijke de verplichtingen van de artikelen 33 en 34 van de Wbp. De verantwoordelijke kan op tal van manieren aan deze verplichtingen voldoen. Uitgangspunt is dat de informatie zodanig moet worden verstrekt dat de betrokkene daarover daadwerkelijk beschikt. Denkbaar is een aankondiging op het pand of object waar de wifitracker is geïnstalleerd. In aanvulling daarop zouden een voldoende duidelijke privacyverklaring op een website of een vastgestelde gedragscode ook denkbaar zijn. Wat de meest in aanmerking komende methode is, is afhankelijk van de omstandigheden in een concreet geval. Wie nalaat aan de verplichtingen van de Wbp te voldoen, stelt zich bloot aan een sanctie door het College bescherming persoonsgegevens (CBP).

Vraag 5

Heeft u inmiddels overleg gehad met het College bescherming persoonsgegevens (Cbp) over wifitracking van passanten op de openbare weg? Zo ja, wat was de uitkomst van dit overleg? Zo nee, wanneer gaat dit overleg plaatsvinden en wilt u de uitkomst daarvan met de Kamer delen?

Antwoord 5

Ik heb overlegd met het CBP. Het College geeft aan dat in het geval van wifi-tracking op de openbare weg, artikel 8 van de Wet bescherming persoonsgegevens van toepassing is, in het bijzonder onderdeel a en f. Dat

betekent dat persoonsgegevens slechts mogen worden verwerkt indien de betrokkene voor de verwerking ondubbelzinnig zijn toestemming heeft verleend of als een beroep op onderdeel f mogelijk is, zoals in mijn antwoord op vraag 2 is aangegeven. Het ligt in de rede dat de voornoemde belangenafweging anders uitpakt bij gegevens die op de openbare weg zijn verzameld dan bij gegevens die zijn verzameld in de winkel, omdat betrokkenen op de openbare weg in algemene zin vaak niet adequaat zullen kunnen worden geïnformeerd over de gegevensverwerking. Het belang van de betrokkene zou dan zwaarder kunnen wegen dan dat van de winkelier, waarbij ook meespeelt dat passanten er niet op verdacht hoeven te zijn dat zij mogelijk worden gevolgd. Door het ontbreken van de benodigde informatie kunnen deze personen ook geen maatregelen nemen om het verzamelen van de gegevens te voorkomen, zoals het uitschakelen van Bluetooth en WiFi.

Vraag 6

Gelden voor het volgen van klanten via een bluetoothverbinding dezelfde regels als voor wifitracking? Is er verschil in de aard en de omvang van persoonsgegevens die verwerkt worden?

Antwoord 6

Kern van de zaak is dat wanneer door middel van het opvangen van signalen van mobiele telefoons persoonsgegevens worden verzameld en verwerkt, de relevante bepalingen uit de Wbp moeten worden nageleefd. Of er technisch gezien bij het volgen van klanten via een ingeschakelde bluetoothverbinding op dezelfde technische manier gegevens kunnen worden opgevangen als bij wifitracking is mij niet bekend.

Vraag 7

Moeten gebruikers van mobiel besturingssysteem iOS die bluetooth standaard hebben uitgeschakeld bij een update van dat systeem op de hoogte worden gesteld dat bluetooth weer ingeschakeld is? Zo ja, gebeurt dat ook en op welke wijze? Zo nee, waarom niet?

Antwoord 7

Er is geen wettelijke regel die verplicht om de gebruikers van iOS software op de hoogte te stellen van het herstel van sommige fabrieksinstellingen in hun apparatuur.

Vraag 8

Deelt u de mening dat het gewenst is dat gebruikers van iOS die bluetooth standaard hebben uitgeschakeld bij een update van iOS op de hoogte worden gesteld dat bluetooth weer ingeschakeld wordt? Zo ja, waarom? Zo nee, waarom niet?

Antwoord 8

Ik acht het primair de verantwoordelijkheid van gebruikers van alle apparaten, ook de apparaten die werken met het iOS besturingssysteem, zelf regelmatig de privacy instellingen te controleren. Bij vernieuwing of vervanging van de besturingssoftware is dat zeer aan te bevelen.

Vraag 9

Heeft iBeacon de aandacht van het Cbp? Zo ja, wat zijn de bevindingen van het Cbp? Zo nee, waarom niet?

Antwoord 9

Daar kan ik geen uitspraken over doen. Uit de door het CBP gepubliceerde jaarlijkse onderzoeksprioriteiten blijkt dat het volgen van gebruikers op internet of via draadloze verbindingen hoog op de agenda staat van het CBP. Het CBP is een onafhankelijke toezichthouder die als regel geen mededelingen doet over lopende of mogelijke onderzoeken of andere werkzaamheden.