Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2010–2011 **Aanhangsel van de Handelingen**

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

1220

Vragen van het lid **Gesthuizen** (SP) aan de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Veiligheid en Justitie over *device fingerprinting (i.e. «instrumentgebruik vingerafdrukken»)* (ingezonden 10 december 2010).

Antwoord van staatssecretaris **Teeven** (Veiligheid en Justitie), mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 27 januari 2011) Zie ook Aanhangsel Handelingen, vergaderjaar 2010–2011, nr. 987.

Vraag 1 en 2
Bent u bekend met het fenomeen «device fingerprinting»?[1]
Bent u op de hoogte van de extreme wens van internetbedrijven om het internetgedrag van internetgebruikers te bestuderen, ondermeer door ook de karakteristieken van de door hen gebruikte apparatuur te analyseren teneinde gericht advertenties op hen los te kunnen laten?[2]
Acht u dit wenselijk?

Antwoord 1 en 2
Ik ben bekend met de fenomenen «device fingerprinting» en «behavioural advertising». Internetten kan tot gevolg hebben dat bedrijven dit internetgebruik waarnemen, gegevens verzamelen, daar conclusies aan verbinden en vervolgens gebruik maken van die informatie. Zo lang bedrijven hierbij handelen in overeenstemming met de wet, acht ik dit niet onwenselijk. Ik verwijs verder naar het antwoord op vraag 3.

Vraag 3
Is de Nederlandse burger wettelijk gezien voldoende beschermd tegen dit soort praktijken? Wordt er door het Goverment Computer Emergency Respons Team (GOVCERT) van de Nederlandse overheid en het College Bescherming Persoonsgegevens onderzoek gedaan naar dit soort praktijken en de gevolgen ervan voor de privacy? Zo nee, bent u bereid dit te initiëren?

[1] http://online.wsj.com/article/SB10001424052748704679204575646704100959546.html
[2] http://www.google.com/hostednews/ap/article/ALeqM5jxLgr3rZl37RqHsoLM9eaAk7OHJg?docId=ddf0d983e55041d7be79df05048a6c08

ah-tk-20102011-1220
ISSN 0921 - 7398
's-Gravenhage 2011

Antwoord 3
Ik ben van mening dat de Nederlandse burger wettelijk gezien voldoende beschermd is tegen bedrijven die gericht adverteren tijdens internetgebruik. Daarbij is het volgende van belang.
Bij device fingerprinting is sprake van het waarnemen en verzamelen van gegevens van de hardware en software van het soort apparatuur, zoals een computer of mobiele telefoon, waarmee gebruik wordt gemaakt van internet. Een bedrijf kan de door middel van device fingerprinting verzamelde gegevens gebruiken om op het moment dat het betreffende apparaat verbonden is met internet en bepaalde websites bezoekt, gerichte advertenties op het scherm te laten verschijnen.
Als hierbij sprake is van het verwerken van persoonsgegevens, is de Wet bescherming persoonsgegevens (Wbp) in beginsel van toepassing en heeft de Nederlandse burger de rechten die uit deze wet voortvloeien. In artikel 4, tweede lid, Wbp is vastgelegd dat deze wet ook van toepassing is op partijen die geen vestiging hebben in de Europese Unie, voor zover zij gebruik maken van infrastructuur die zich in Nederland bevindt, tenzij die infrastructuur slechts worden gebruikt voor de doorvoer van persoonsgegevens. Voor relevante ontwikkelingen in Europees verband verwijs ik naar de brief aan uw Kamer van de Staatssecretaris van Buitenlandse Zaken van 21 december 2010 (Kamerstukken II, 2010–2011, 22 112, nr. 1116).
Aangezien device fingerprinting geengevolgen heeft voor de veiligheid van het internetgebruik of de internetgebruiker, bestaat er voor GOVCERT.NL vanuit zijn taakopdracht geen aanleiding onderzoek te verrichten naar dit verschijnsel.
Het College bescherming persoonsgegevens (CBP) is een onafhankelijke toezichthouder en doet in beginsel geen uitspraken over lopende of toekomstige onderzoeken. Wel heeft het CBP mij meegedeeld dat het onderwerp «profiling» (het maken van profielen) hoog op zijn agenda staat.

Vraag 4
Kan de Nederlandse burger ergens terecht met klachten wanneer dit soort praktijken vanuit het buitenland in Nederland worden verricht? Zijn of worden hier internationale afspraken over gemaakt c.q. beperkingen aan gesteld?

Antwoord 4
Ja, als sprake is van gegevensverwerking en de verantwoordelijke voor de gegevensverwerking in Nederland gevestigd is, kan een betrokkene zich wenden tot het CBP. Als de verantwoordelijke in een andere lidstaat van de Europese Unie is gevestigd, is de wetgeving van die andere lidstaat van toepassing. De betrokkene kan zich tot het CBP wenden met het verzoek om zijn klacht door te geleiden naar de relevante toezichthouder in de andere lidstaat.
Op dit moment bestaan op internationaal vlak richtsnoeren van de samenwerkende Europese toezichthouders op privacywetgeving. Deze toezichthouders hebben een opinie over behavioural advertising vastgesteld op 22 juni 2010 (Opinie 2/2010 van de Artikel 29-Werkgroep, www.ec.europa.eu). Deze gaat over de toepasselijkheid van de EU privacyrichtlijn (95/46/EG) en de wijze waarop de toezichthouders deze zullen toepassen. Verder heeft de verantwoordelijke Eurocommissaris aangegeven bij de herziening van de EU privacyrichtlijn aandacht te willen besteden aan profiling en behavioural advertising.

Vraag 5
Denkt u na over online «do not track me» (i.e. volg mij niet) voorzieningen, gelijk aan de «ik wil niet gebeld worden» initiatieven, in het kader van direct marketing campagnes of webtoepassingen die veel verder gaan dan het gebruik van cookies? Bent u bereid de Kamer hierover te informeren?

Antwoord 5
Nee, gezien mijn toelichting op het fenomeen device fingerprinting in het antwoord op vraag 3 en gezien het feit dat het hierbij gaat om een activiteit die alle landsgrenzen overschrijdt, acht ik een met het «ik wil niet gebeld worden»-initiatief vergelijkbaar register van «opt out»-verklaringen onwerkbaar.

Vraag 6
Vindt u dat bedrijven die het gedrag van internetgebruikers monitoren en hun apparatuur fingerprinten, die gebruikers daarvan op de hoogte dienen te brengen? Zo ja, hoe gaat u dit regelen? Zo nee, waarom niet?

Antwoord 6
Als sprake is van het verwerken van persoonsgegevens en de Wbp van toepassing is, geldt dat in die wet is geregeld dat de betrokkene (vooraf) geïnformeerd dient te worden over (het doel van) de gegevensverwerking (artikel 33 en 34). Ik verwijs verder naar het antwoord op vraag 4 en de eerdergenoemde brief van de Staatssecretaris van Buitenlandse Zaken.

Vraag 7
Bent u bereid een analyse te maken van de risico's en kansen van deze technologie, en deze aan de Kamer te doen toekomen?

Antwoord 7
Nee, gezien de voorgaande antwoorden zie ik daar geen aanleiding toe.