

AAN AANGETEKEND
Google Inc. en Google Netherlands B.V.

DATUM 23 maart 2011
ONS KENMERK z2010-01467
CONTACTPERSOON

UW BRIEF VAN
UW KENMERK

ONDERWERP - Last onder dwangsom
- Opdracht tot vernietiging payload data

Geachte directie,

Het College bescherming persoonsgegevens (CBP) heeft op grond van artikel 60 Wet bescherming persoonsgegevens (Wbp) een ambtshalve onderzoek ingesteld naar de verzameling van gegevens met betrekking tot wifi-netwerken in Nederland met Street View auto's door Google Inc. (hierna: Google). De verzameling van gegevens met betrekking tot wifi-netwerken door Google betreft enerzijds gegevens *over* wifi-netwerken en anderzijds gegevens *uit* wifi-netwerken (hierna: payload data). Naar aanleiding van dit onderzoek heeft het college besloten om Google Inc. en Google Netherlands B.V. ten aanzien van de verzamelde gegevens over wifi-netwerken een last onder dwangsom op te leggen. De last onder dwangsom en de overwegingen die tot de oplegging daarvan hebben geleid zijn beschreven in § 1 tot en met § 3 van deze beslissing. De opdracht tot vernietiging van de payload data en de achtergrond van deze opdracht zijn beschreven in § 4 en § 5 van deze beslissing.

Ten aanzien van de verzamelde gegevens over wifi-netwerken

1. *Het verloop van de procedure*

Uit het onderzoek van het CBP is onder meer naar voren gekomen dat Google van 4 maart 2008 tot en met 6 mei 2010¹ gegevens heeft verzameld over ongeveer 3.606.579 verschillende wifi-routers.² Van elk van deze routers heeft Google het unieke MAC-adres vastgelegd.³

¹ 6 mei 2010 is de laatst aangetroffen datum op de door het CBP onderzochte harde schijf met gegevens. Uit de schriftelijk ingewonnen inlichtingen blijkt dat Google "kort na 7 mei 2010 is gestopt met het verwerken van disks die zij heeft ontvangen van Street View auto's." Bron: Brief van Google van 8 juni 2010, bijlage, blz. 7.

² E-mail van Google van 12 juni 2010, bijlage gedateerd 9 juli 2010, blz. 1.

Google heeft dit unieke nummer vastgelegd van zowel beveiligde als onbeveiligde wifi-routers. Tevens heeft Google van elke wifi-router de RSSI (de signaalsterkte) vastgelegd en voor elke wifi-router zo nauwkeurig mogelijk een locatie berekend. Daarnaast heeft Google in veel gevallen de SSID (de netwerknaam) vastgelegd. Het CBP heeft vastgesteld dat Google op haar geolocatieserver (hierna: Google GLS) het MAC-adres opslaat, in combinatie met de berekende locatie van de wifi-router. Google biedt derde partijen kosteloos toegang tot de gegevens in de Google GLS via de zogenaamde Google Geo Location API. Een ieder kan van deze plaatsbepalingsdienst gebruik maken, door ofwel zelf de software te installeren die Google kosteloos ter beschikking stelt, dan wel door het intypen van een MAC-adres op de website van een derde partij die deze software op zijn server heeft geïnstalleerd. De Google GLS laat vervolgens als resultaat een berekende locatie van de wifi-router zien.

Bij brief van 21 september 2010 heeft het CBP het rapport van voorlopige bevindingen aan Google toegezonden.

Bij brief van 26 oktober 2010 heeft Google zijn zienswijze op het rapport van voorlopige bevindingen gegeven.

Naar aanleiding van de zienswijze heeft het CBP bij brief van 23 november 2010 het rapport van definitieve bevindingen (hierna: de bevindingen) aan Google toegezonden. De bevindingen worden als bijlage aangehecht en dienen hier als herhaald en ingelast te worden beschouwd.⁴

Samengevat is in de bevindingen geconcludeerd dat Google door het verzamelen van de SSID's in strijd handelt met artikel 7 Wbp, omdat er geen gerechtvaardigd doeleinde voor de verwerking is. Voorts is geconcludeerd dat Google, zowel ten aanzien van de SSID's als ten aanzien van de gegevens over wifi-routers, in strijd handelt met artikel 8 Wbp doordat er geen gerechtvaardigde grondslag voor deze verwerking is. Verder is geconcludeerd dat Google in strijd heeft gehandeld met artikel 34 Wbp doordat zij heeft nagelaten om betrokkenen in Nederland te informeren over het verzamelen en verwerken van gegevens over wifi-routers. Daarnaast is geconcludeerd dat Google in strijd heeft gehandeld met artikel 27 jo. artikel 28 Wbp doordat zij heeft nagelaten deze vorm van gegevensverwerking bij het CBP te melden.

Bij brief van 13 december 2010 heeft het CBP Google bericht dat het gelet op de conclusies van de bevindingen voornemens is om een last onder dwangsom op te leggen.

³ MAC-adressen zijn de unieke nummers die door de fabrikant zijn vastgelegd in de hardware van apparatuur, zoals op geheugenchips en/of netwerkkaarten in computers, telefoons, laptops of routers. MAC staat voor Medium Access Control.

⁴ Voor een uitgebreid overzicht van de loop van de procedure tot 23 november 2010 verwijst het CBP naar § 2.1 van de bevindingen.

Op 13 januari 2011 is Google in de gelegenheid gesteld om mondeling een zienswijze met betrekking tot het voornemen te geven. Van deze gelegenheid heeft Google gebruik gemaakt. Het verslag van de hoorzitting is als bijlage bij dit besluit gevoegd en maakt hier integraal deel van uit.

2. Overwegingen

2.1 Persoonsgegevens

Artikel 1, aanhef en onder a, van de Wbp luidt als volgt:

In de wet en de daarop berustende bepalingen wordt verstaan onder persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare persoon.

Om van persoonsgegevens te kunnen spreken dient allereerst vastgesteld te worden dat het gaat om gegevens die betrekking hebben op een persoon. In veel gevallen zal dit uit de aard van de gegevens voortvloeien. Indien dit niet het geval is, zal mede aandacht moeten worden besteed aan de context waarin de gegevens worden vastgelegd en gebruikt. Als gegevens medebepalend zijn voor de wijze waarop een persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, moeten die gegevens als persoonsgegevens worden aangemerkt. Het (maatschappelijk) gebruik dat van gegevens wordt gemaakt is dus medebepalend voor de beantwoording van de vraag of sprake is van een persoonsgegeven.⁵

Het tweede vereiste om van persoonsgegevens te kunnen spreken is het vereiste van identificeerbaarheid. Het uitgangspunt is dat een persoon identificeerbaar is, indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Er wordt onderscheid gemaakt tussen direct en indirect identificeerbare gegevens. Er is sprake van direct identificeerbare gegevens wanneer gegevens betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig vast te stellen is. Van indirect identificeerbare gegevens is sprake indien gegevens niet direct tot identificatie van een bepaald persoon leiden maar via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon.⁶

Om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enige andere persoon in te zetten zijn om genoemde persoon te identificeren. Er moet worden uitgegaan van een redelijk toegeruste verantwoordelijke. In concrete gevallen moet echter wel rekening worden gehouden met bijzondere expertise, technische faciliteiten, en dergelijke van de verantwoordelijke.⁷

⁵ TK 1997-1998, 25 892, nr. 3, blz. 46

⁶ TK 1997-1998, 25 892, nr. 3, blz. 47 - 48

⁷ TK 1997-1998, 25 892, nr. 3, blz. 48 - 49, richtlijn 95/46/EG overweging 26

Het CBP heeft in de bevindingen vastgesteld dat de door Google verzamelde MAC-adressen van wifi-routers in combinatie met de berekende locatie in de onderzochte context persoonsgegevens zijn in de zin van artikel 1 aanhef en onder a Wbp, aangezien het unieke, aan specifieke hardware toegekende nummers zijn waarmee individuele houders geïdentificeerd kunnen worden. Voorts heeft het CBP in de bevindingen vastgesteld dat SSID's (netwerknamen) in combinatie met het MAC-adres en de berekende locatie eveneens persoonsgegevens zijn. Beide categorieën worden hieronder in § 2.1.1 en § 2.1.2. ook wel aangeduid als 'wifi-gegevens'.

2.1.1 *Zienswijze*

Google heeft in haar op 26 oktober 2010 gegeven zienswijze en tijdens de hoorzitting gemotiveerd bestreden dat wifi-gegevens persoonsgegevens zijn. Google heeft daartoe de hieronder weergegeven argumenten naar voren gebracht.

Gegeven betreffende een persoon

Google heeft op de hoorzitting verklaard dat wifi-gegevens naar haar mening geen geïdentificeerde of identificeerbare personen betreffen. Naar de mening van Google gaat het daarentegen om gegevens over objecten. Google heeft in dit verband verwezen naar Opinie 4/2007 van de Artikel 29 Werkgroep en naar de memorie van toelichting bij de Wbp. Google heeft benadrukt dat noch Google noch de gebruiker van de GLS het doel heeft om de wifi-router te relateren aan een gebruiker of een eigenaar van de wifi-router.

Verder heeft Google gesteld dat het gebruik van wifi-gegevens door Google geen gevolgen zal hebben voor de betrokkene. De GLS van Google is er immers niet op gericht om gegevens over wifi-routers breder toegankelijk te maken dan die al zijn. Met uitzondering van hacking, kan het MAC-adres van een wifi-router slechts worden achterhaald als iemand zich in de nabijheid van de betreffende router bevindt. Hierdoor is de kans dat deze informatie oneigenlijk wordt gebruikt naar het oordeel van Google beperkt. Wat betreft het in de bevindingen beschreven experiment waarbij de onderzoekers een MAC-adres in de Google GLS hebben ingevoerd en de berekende locaties terugkregen, heeft Google gesteld dat dit een 'hack' door middel van een third party tool betreft. Als het al mogelijk is om op deze wijze de locatie van de wifi-router via de Google GLS te achterhalen, brengt dit gebruik van de GLS volgens Google geen (nadelige) gevolgen met zich mee voor de eigenaar van het apparaat.

Identificeerbaarheid

Google heeft in haar zienswijze gesteld dat SSID's en MAC-adressen van wifi-routers op zichzelf, en SSID's en MAC-adressen van wifi-routers in combinatie met berekende locatie naar haar oordeel niet redelijkerwijs zijn in te zetten om een persoon te identificeren. Google wijst daarbij op fysieke en wettelijke beperkingen waardoor identificatie naar het oordeel van Google juridisch onmogelijk, praktisch onuitvoerbaar en daarmee redelijkerwijs uitgesloten zou zijn. Verder heeft Google in dit verband naar voren gebracht dat MAC-adressen van

gebruikers in principe niet buiten het lokale draadloze netwerk worden doorgegeven. Iemand die met een draadloos MAC-adres de Google GLS-dienst doorzoekt, heeft dit adres derhalve waarschijnlijk verkregen door zich fysiek toegang te verschaffen tot het desbetreffende apparaat.

Guidance

Google heeft tijdens de hoorzitting als subsidiair argument naar voren gebracht dat zij er vanuit mocht gaan dat de verzameling van gegevens over wifi-netwerken niet onder de reikwijdte van de Wbp zou vallen. Handhaving zou naar de mening van Google dan ook in strijd zijn met het rechtzekerheidsbeginsel en het legaliteitsbeginsel. Naar de mening van Google zou eerst geconcretiseerd moeten worden, bijvoorbeeld in de vorm van beleidsregels (guidance), op welke wijze de Wbp van toepassing is op gegevens over wifi-netwerken. Daarbij zou volgens Google moeten worden meegewogen dat er verschillende andere aanbieders zijn die op precies dezelfde wijze als Google gegevens over wifi-netwerken verzamelen en inzetten. Het zou naar de mening van Google in strijd zijn met het gelijkheidsbeginsel om alleen ten aanzien van Google handhavend op te treden. Google heeft daarom gesteld dat, als maatregelen nodig worden geacht, gekozen zou moeten worden voor een branchebrede aanpak, bij voorkeur na consultatie van alle betrokkenen.

2.1.2 *Beoordeling*

Gegeven betreffende een persoon

Gegevens die geen directe relatie hebben met een persoon, kunnen toch informatie over een bepaalde persoon verschaffen en in dat geval als persoonsgegevens worden beschouwd. Zo kunnen telefoonnummers, kentekens van auto's en postcodes met huisnummers onder omstandigheden als persoonsgegevens worden aangemerkt.⁸

Voor de vaststelling dat gegevens die naar hun aard geen betrekking hebben op personen persoonsgegevens zijn is de maatschappelijke context waarin de gegevens worden verwerkt relevant. In dit verband is van belang dat MAC-adressen unieke hardware onderscheiden en dat deze hardware in de context van geolocatiediensten onverbrekkelijk verbonden is met de locatie van de houder van deze hardware. Door een MAC-adres in te voeren in de Google GLS kan de locatie achterhaald worden waar een wifi-router zich bevindt en kan het adres van de gebruiker van de wifi-router worden bepaald. Omgekeerd is het mogelijk, hoewel de Google GLS, zoals Google tijdens de hoorzitting heeft toegelicht, hier niet standaard op is ingesteld, een locatie in de Google GLS in te voeren en de MAC-adressen van de routers die zich in de buurt van die locatie bevinden terug te krijgen.

In reactie op de stelling van Google dat de Google GLS er niet op gericht is om gegevens over wifi-routers breder toegankelijk te maken dan ze al zijn, benadrukt het CBP dat dit juist wel het effect is van de Google GLS. De gegevens over wifi-routers worden immers, zodra deze in

⁸ TK vergaderjaar 1997-1998, 25 892, nr. 3, blz. 47.

de Google GLS zijn opgeslagen, voor een ieder die internettoegang heeft toegankelijk. Google heeft op de hoorzitting gesteld dat het nodig is om te 'hacken' teneinde via de GLS informatie over de locatie van wifi-routers te verkrijgen. Dit is onjuist. Door regulier gebruik te maken van de Google maps applicatie kan een ieder via de Google GLS de locatie van een bepaalde wifi-router opvragen. De uitleg voor het bevragen van de Google GLS, JSON, staat beschreven op de website van Google API.⁹

Wifi-gegevens kunnen medebepalend zijn voor de wijze waarop de houder van de wifi-router in het maatschappelijk verkeer wordt beoordeeld of behandeld. In de bevindingen is het voorbeeld gegeven van stalking en van een strafzaak waarbij het MAC-adres als hulpmiddel werd gebruikt bij de opsporing.

Daarnaast kunnen wifi-gegevens ook door Google zelf worden gebruikt op een wijze die de betrokkene in het maatschappelijk verkeer raakt. Wifi-gegevens verschaffen informatie over de woonomgeving van de houder van het betreffende wifi-netwerk. De wijk waarin een persoon woont kan een indicatie zijn voor bijvoorbeeld diens sociale achtergrond, inkomen of gezinssamenstelling. Dergelijke informatie kan gebruikt worden voor (geo)marketing doeleinden. Zo zou Google aan de hand van locatie wijzigingen van wifi-routers kunnen bepalen welke huishoudens recentelijk zijn verhuisd.

Google heeft tijdens de hoorzitting verklaard dat noch Google noch de gebruiker van de GLS het doel heeft om de wifi-router te relateren aan een gebruiker of eigenaar van de wifi-router. Het doel waarvoor Google de wifi-gegevens verzamelt is echter niet van belang voor de vaststelling dat het gaat om persoonsgegevens. Uit de memorie van toelichting blijkt dat het erom gaat dat de *mogelijkheid* bestaat om een gegeven te gebruiken op een wijze die een persoon in het maatschappelijk verkeer raakt.¹⁰ Het CBP is van oordeel dat die mogelijkheid reëel is.

Identificeerbaarheid

In de bevindingen is vastgesteld dat Google met behulp van de door haar verzamelde gegevens over signaalsterkte de locatie van de wifi-router kan bepalen. Uit onderzoek over RSSI locatiebepaling blijkt dat het met behulp van op signaalsterkte gebaseerde modellen

⁹ Voor de commando's voor het bevragen van de Google GLS middels JSON heeft het CBP aan de hand van de uitleg op de website van Google API, onderstaand voorbeeld uitgewerkt:

```
$ cat /tmp/post.5032
{"version":"1.1.0","host":"maps.google.com","request_address": true,"address_language":"en_GB","wifi_towers":
[{"mac_address":"<geanonimiseerd>","signal_strength": -72,"age": 0}]}
$ curl -X POST -d @/tmp/post.5032 http://www.google.com/loc/json
het antwoord van de Google server luidt:
{"location":{"latitude":51.9108478,"longitude":4.4977291,"address":{"country":"The
Netherlands","country_code":"NL","region":"South
Holland","county":"Rotterdam","city":"Rotterdam","street":"Halfgrond","street_number":"27"},"accuracy":36.0},"acces
s_token":"<geanonimiseerd>"}
```

¹⁰ TK 1997-1998, 25 892, nr. 3, blz. 47.

mogelijk is tot op enkele meters nauwkeurig te bepalen waar de wifi-router zich bevindt, zodat op deze wijze het adres van de betreffende woning kan worden achterhaald.¹¹ Via openbare bronnen zoals het Kadaster kan vervolgens tot identificatie van de eigenaar van de wifi-router worden gekomen. Zoals in de bevindingen vastgesteld, valt de inspanning die Google moet verrichten om tot de locatiebepaling van een wifi-router te komen niet onevenredig te noemen, aangezien Google een groot aantal terzake kundige technici in dienst heeft en over de benodigde technische faciliteiten beschikt. Daardoor is zij in staat de locatiebepaling vanuit haar kantoor, met behulp van gegevens die reeds in haar bezit zijn, te verrichten.

Guidance

Het CBP wijst de stelling van Google dat het CBP eerst tot handhaving zou mogen overgaan nadat vooraf nadere invulling is gegeven aan het wettelijke begrip persoonsgegevens van de hand. De constatering dat wifi-gegevens in de onderzochte context persoonsgegevens zijn vloeit direct voort uit artikel 1 van de Wbp en de relevante passages uit de memorie van toelichting. Alleen daarom al is er geen aanleiding de marktdeelnemers te raadplegen over de invulling van deze norm. Van strijd met het legaliteitsbeginsel en het rechtzekerheidsbeginsel is dan ook geen sprake. Wat betreft het argument van Google dat het in strijd is met het gelijkheidsbeginsel om alleen tegen Google op te treden en niet tegen de andere aanbieders van geolocatiediensten, wijst het CBP erop dat het naar aanleiding van een concreet vermoeden van overtreding van de Wbp bij Google onderzoek heeft gedaan naar de verzameling van wifi-gegevens. Van strijd met het gelijkheidsbeginsel kan dan ook geen sprake zijn.

Samenvattend concludeert het CBP dat de door Google tijdens de hoorzitting naar voren gebrachte argumenten geen aanleiding vormen om de in de bevindingen vastgelegde conclusie dat wifi-gegevens in de onderzochte context persoonsgegevens zijn, te wijzigen.

2.2 Welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden

Artikel 7 Wbp luidt als volgt:

Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld.

Persoonsgegevens mogen enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verkregen. «Welbepaald en uitdrukkelijk omschreven» betekent allereerst dat men geen gegevens mag verzamelen zonder een precieze

¹¹ Bijv. Lin Lau ea (2008), Enhanced RSSI-Based High Accuracy Real-Time User Location Tracking System for Indoor and Outdoor Environments, International Journal on Smart Sensing And Intelligend Systems, Vol. 1, No. 2, June 2008, te raadplegen via <http://www.s2is.org/Issues/v1/n2/papers/paper14.pdf> en Barsocchi, P. ea (2009) en A Novel Approach to Indoor RSSI Localization by Automatic Calibration of the Wireless Propagation Model, Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th, Barcelona, te raadplegen via http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5073315.

doelomschrijving. Het doel moet zijn bepaald alvorens men tot verzamelen overgaat. «Welbepaald» houdt in dat deze doelomschrijving duidelijk moet zijn, niet zo vaag of ruim bijvoorbeeld dat zij tijdens het verzamelproces geen kader kan bieden waaraan getoetst kan worden of de gegevens nodig zijn voor dat doel of niet. Het doel mag ook niet in de loop van het verzamelproces geformuleerd worden. «Uitdrukkelijk omschreven» houdt in dat de verantwoordelijke het doel waarvoor hij verwerkt, moet hebben omschreven bij de melding die hij op grond van artikel 27 verplicht is te doen.(...)¹²

Daarbij komt dat persoonsgegevens voor gerechtvaardigde doeleinden moeten worden verzameld. Artikel 8 bevat een limitatieve opsomming van gronden voor toelaatbare gegevensverwerking. Van «gerechtvaardigde doeleinden» kan alleen sprake zijn als deze met inachtneming van artikel 8 kunnen worden bereikt. Indien op grond van artikel 8 kan worden gesproken van een 'gerechtvaardigd doeleinde' is daarmee voldaan aan het vereiste van artikel 7 dat persoonsgegevens moeten zijn verkregen voor een gerechtvaardigd doeleinde.¹³

Het CBP heeft in de bevindingen vastgesteld dat SSID's in combinatie met het MAC-adres van de wifi-router en de berekende locatie persoonsgegevens zijn en dat Google geen welbepaald of uitdrukkelijk omschreven doel heeft voor de verwerking van de SSID's. Google handelt daarmee in strijd met artikel 7 Wbp.

2.2.1 *Zienswijze*

Google heeft tijdens de hoorzitting verklaard dat de SSID's ten behoeve van de Google GLS kunnen worden gebruikt, omdat deze de betrouwbaarheid van de GLS vergroten en omdat de SSID's kunnen helpen bij het achterhalen van de oorzaak van foutmeldingen. Google stelt zich dan ook op het standpunt dat zij gerechtigd is om de SSID's voor deze doeleinden te gebruiken.

2.2.2 *Beoordeling*

Gelet op het ontbreken, zoals hieronder uit § 2.3.2.2. blijkt, van een gerechtvaardigde grondslag voor de verwerking van SSID's, concludeert het CBP dat er evenmin een gerechtvaardigd doeleinde is. Verder stelt het CBP vast dat Google voor de verzameling van SSID's geen welbepaalde en uitdrukkelijke omschreven doelomschrijving heeft geformuleerd. Zoals in § 2.5.2. uiteengezet, heeft Google nagelaten het doel waarvoor zij verwerkt, te omschrijven bij de melding die zij op grond van artikel 27 Wbp verplicht is te doen. Er moet dan ook worden geconcludeerd dat de SSID's in strijd met artikel 7 Wbp worden verwerkt.

2.3 Gerechtvaardigde grondslag

Artikel 8, onder f, Wbp luidt als volgt:

¹² TK 1997-1998, 25 892, nr. 3, blz. 79.

¹³ TK 1997-1998, 25 892, nr. 3, blz. 79.

Persoonsgegevens mogen slechts worden verwerkt indien de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op de persoonlijke levenssfeer, prevaleert.

Artikel 8 bevat een limitatieve opsomming van de gronden die een gegevensverwerking rechtvaardigen. Het artikel behelst bovendien dat bij elke verwerking moet zijn voldaan aan de beginselen van proportionaliteit en subsidiariteit. Het proportionaliteitsbeginsel houdt in dat de inbreuk op de belangen van de bij de verwerking van persoonsgegevens betrokkene niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. Ingevolge het subsidiariteitsbeginsel mag het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene minder nadelige wijze kunnen worden verwerkelijkt.¹⁴

De bepaling schrijft in aanvulling op de eerste afweging (noodzakelijk voor een gerechtvaardigd belang van de verantwoordelijke), waarbij mogelijk de belangen van de betrokkene als onderdeel van een veelheid van belangen reeds onder ogen zijn gezien, nog een tweede toets voor. Deze tweede toets vergt een nadere afweging, waarbij de belangen van de betrokkene een zelfstandig gewicht in de schaal leggen tegenover het belang van de verantwoordelijke. Met deze tweede toets wordt nog eens extra de nadruk gelegd op het proportionaliteitsvereiste. Deze extra toets is aan het slot van het voorschrift opgenomen door middel van de zinsnede «tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert». Dit betekent niet dat op voorhand de belangen van de betrokkene zwaarder moeten wegen, doch slechts een hernieuwde aangescherpte toets, waarbij de belangen van de betrokkene afzonderlijk moeten worden gewogen. Indien de betrokkene geen belang heeft bij de door de verantwoordelijke voorgestane gegevensverwerking, behoeft dit geenszins te betekenen dat daarmee de gegevensverwerking ongeoorloofd is. Verantwoordelijke en betrokkene kunnen tegengestelde belangen hebben bij een gegevensverwerking. Alleen in het geval dat het belang van de betrokkene op bescherming van zijn persoonlijke levenssfeer doorslaggevend is, dient de verantwoordelijke af te zien van de gegevensverwerking. Bij de in onderdeel f voorgeschreven afweging speelt een rol de mate van gevoeligheid van de gegevens die de verantwoordelijke wil verwerken en de maatregelen die de verantwoordelijke heeft genomen ten einde rekening te houden met de belangen van de betrokkene. De belangen van de betrokkene zullen in mindere mate gewicht in de schaal leggen naarmate in zijn belang meer waarborgen voor een zorgvuldig gebruik van de gegevens zijn genomen.¹⁵

2.3.1 Ten aanzien van het Mac-adres en de berekende locatie

¹⁴ TK 1997-1998, 25 892, nr. 3, blz. 80

¹⁵ TK 1997-1998, 25 892, nr. 3, blz. 87-88

In de bevindingen is vastgesteld dat Google zich niet kan beroepen op de grondslag genoemd in artikel 8, onder f, van de Wbp (gerechtvaardigd belang), indien geen waarborgen zijn opgenomen voor een zorgvuldig gebruik van de gegevens.

2.3.1.1 *Zienswijze*

Google heeft tijdens de hoorzitting kenbaar gemaakt dat zij de bevindingen zo interpreteert, dat de schending van de artikelen 7 en 8 Wbp uitsluitend betrekking heeft op de verzameling van SSID's, en dat de verzameling van het MAC-adres in combinatie met de berekende locatie in overeenstemming is met de artikelen 7 en 8 Wbp. Google gaat er daarom vanuit dat het op 13 december 2010 aangekondigde voornemen geen betrekking heeft op de verzameling van MAC-adressen in combinatie met de berekende locatie.

Tijdens de hoorzitting is namens Google, in reactie op een daartoe strekkende vraag, verklaard dat het moeilijk is om een opt-out mogelijkheid voor de betrokkenen in te bouwen, omdat Google daarvoor over een register met MAC-adressen zou moeten beschikken met de daarbij behorende namen van de eigenaren van de wifi-routers en dat het aanleggen van een dergelijk register, met het oog op de privacy, ongewenst zou zijn.

2.3.1.2 *Beoordeling*

Anders dan Google veronderstelt, is in de bevindingen wel degelijk geconcludeerd dat Google ten aanzien van de verzameling van MAC-adressen in combinatie met de berekende locatiegegevens, in strijd met artikel 8 Wbp handelt, vanwege het ontbreken van een gerechtvaardigde grondslag. Hoewel Google een *gerechtvaardigd belang* kan hebben als bedoeld in artikel 8, onder f, Wbp voor het verzamelen van MAC-adressen in combinatie met de berekende locatie ten behoeve van haar geolocatiedienstverlening, is vastgesteld dat Google niet heeft voorzien in *waarborgen* voor een zorgvuldig gebruik van de gegevens. De belangenafweging die in het kader van artikel 8, onder f, Wbp dient te worden gemaakt, valt daarom uit in het voordeel van de betrokkene.

In dit verband is relevant dat het in casu gaat om een grootschalige gegevensverwerking waarbij er in de periode 2008-2010 gegevens zijn vastgelegd over ongeveer 3.606.579 verschillende wifi-routers. Doordat deze gegevens in de Google GLS zijn opgeslagen en via internet toegankelijk zijn, kan de verspreiding van deze gegevens in principe ongelimiteerd plaatsvinden, waardoor een aanzienlijk risico op schending van de persoonlijke levenssfeer ontstaat. Een betrokkene die niet wil dat de gegevens over zijn wifi-netwerk in de Google GLS worden opgenomen, staat geen algemene mogelijkheid ter beschikking om daartegen bezwaar te maken.

De belangenafweging die op grond van artikel 8, onder f, Wbp gemaakt dient te worden valt uit in het voordeel van Google, wanneer Google een belangrijke waarborg inbouwt door de betrokkenen de mogelijkheid te bieden via een online opt-out verzet aan te tekenen tegen de verwerking van hun MAC-adressen. Een vergelijkbare opt-out wordt door Google reeds aangeboden voor foto's van huizen in de dienst Street View. De online opt-out dient kosteloos te zijn en dient in alle gevallen te worden gehonoreerd. Vanzelfsprekend mogen daarbij geen bovenmatige gegevens worden verzameld. De opt-out dient bovendien effectief te zijn, hetgeen

betekent dat Google ervoor zorgdraagt dat informatie die op verzoek van de betrokkene is verwijderd, niet op andere wijze opnieuw in de Google GLS wordt opgenomen.

Het argument van Google dat zij de beschikking zou moeten hebben over een register met MAC-adressen en de daarbij behorende namen van betrokkenen om een opt-out mogelijkheid te kunnen bieden, gaat niet op. Er zijn immers verschillende mogelijkheden om een dergelijke opt-out mogelijkheid te realiseren, zonder dat een dergelijk register wordt aangelegd.¹⁶

2.3.2 Ten aanzien van de SSID's

In de bevindingen is vastgesteld dat Google geen grondslag op basis van artikel 8 Wbp heeft voor het verzamelen van SSID's en derhalve de SSID's niet mogen worden verwerkt.

2.3.2.1 *Zienswijze*

Google heeft tijdens de hoorzitting aangevoerd dat de verwerking van de SSID's de betrouwbaarheid van de GLS vergroot omdat SSID's kunnen helpen bij het achterhalen van de oorzaak van foutmeldingen. Verder is verklaard dat de SSID's nuttig kunnen zijn om misbruik van de GLS tegen te gaan. Google heeft in dit verband naar voren gebracht dat 'scraping' (het op grote schaal met geautomatiseerde middelen leegtrekken van een database door computers die willekeurige alfanumerieke combinaties opgeven) van de GLS-database kan worden tegengegaan door de combinatie met de juiste SSID te verlangen. Google is van mening dat zij gerechtigd is om de SSID's voor deze doeleinden te gebruiken.

2.3.2.2 *Beoordeling*

Tijdens de hoorzitting heeft het CBP Google de vraag gesteld of SSID's noodzakelijk zijn en of SSID's op dit moment gebruikt worden bij het bepalen van de geolocaties. Google heeft beide vragen ontkennend beantwoord.¹⁷ Google heeft tijdens de hoorzitting gesteld dat SSID's nuttig kunnen zijn voor de betrouwbaarheid en de beveiliging van de GLS. SSID's zijn echter, zoals door Google in reactie op een vraag van het CBP tijdens de hoorzitting aangegeven, niet

¹⁶ Bijvoorbeeld door middel van de volgende use case:

1. De betrokkene logt in op een webpagina van Google, waarop een MAC-adres kan worden ingevoerd. Het IP adres en datum, tijd zouden automatisch door Google kunnen worden gelogd.
2. Als het MAC adres in de GLS zit, zou Google de betrokkene kunnen doorsturen naar een verificatiepagina die scripting bevat waarmee de ARP tabel wordt opgevraagd. De WLAN MAC-adressen zijn theoretisch gezien op te vragen middels 'ARP -a'. Middels browsercode, bijv java, kan dit ARP lijstje worden opgevraagd op de achtergrond.
3. Als het opgegeven MAC adres in het ARP lijstje staat, is vastgesteld dat de gebruiker, die verbonden is met het WLAN, diegene is die toegang heeft tot het lokale WLAN MAC-adres, dat evenwel ook in de Google GLS is opgenomen. Het verzoek om verwijdering van de betrokkene is daarmee geverifieerd. De verificatie kan geautomatiseerd op de achtergrond plaatsvinden.

¹⁷ Google heeft er in haar commentaar op het verslag van de hoorzitting op gewezen dat de in het verslag gebruikte formulering van deze passage de indruk wekt dat gesproken zou zijn over noodzakelijkheid in de zin van artikel 8 Wbp, hetgeen in de herinnering van de namens Google aanwezigen niet het geval is geweest.

noodzakelijk voor de geolocatiedienstverlening. Google kan zich naar het oordeel van het CBP dan ook niet beroepen op artikel 8, onder f, Wbp (gerechtvaardigd belang) omdat de verwerking van SSID's niet noodzakelijk is voor het behartigen van de door Google gestelde belangen. De SSID's mogen dan ook niet worden verwerkt en dienen onomkeerbaar te worden gewist, door deze ten minste drie maal te overschrijven met verschillende patronen, bijvoorbeeld door het toepassen van DoD 5220.22-M (3 maal), NSA (7 maal) of Gutmann (35 maal). Tevens dient Google de SSID's te verwijderen uit de bestanden met ruwe data.

2.4 Informatieplicht

In artikel 33, eerste lid, Wbp is het volgende bepaald:

Indien persoonsgegevens worden verkregen bij de betrokkene, deelt de verantwoordelijke vóór het moment van de verkrijging de betrokkene de informatie mede, bedoeld in het tweede en derde lid, tenzij de betrokkene daarvan reeds op de hoogte is.

Artikel 34, eerste en vierde lid Wbp luiden als volgt:

1. *Indien persoonsgegevens worden verkregen op een andere wijze dan bedoeld in artikel 33, deelt de verantwoordelijke de betrokkene de informatie mede, bedoeld in het tweede en derde lid, tenzij deze reeds daarvan op de hoogte is:*
 - a. *op het moment van vastlegging van hem betreffende gegevens, of*
 - b. *wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van de eerste verstrekking.*
- (...)
4. *Het eerste lid is niet van toepassing indien mededeling van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In dat geval legt de verantwoordelijke de herkomst van de gegevens vast.*

Deze bepalingen vormen een uitwerking van het transparantiebeginsel en van het in artikel 6 neergelegde beginsel van «rechtmatige verwerking»: behoudens uitzonderingen is de gegevensverwerking slechts «behoorlijk» in de zin van artikel 6 Wbp, indien de betrokkene daarvan overeenkomstig de regels van de artikelen 33 of 34 Wbp op de hoogte wordt gebracht. De omstandigheid dat de onderhavige regeling een uitwerking vormt van het beginsel dat in artikel 6 is neergelegd heeft tot gevolg, dat overtredingen van de informatieplicht zullen leiden tot onrechtmatige verwerkingen.¹⁸

Worden de gegevens verkregen bij de betrokkene zelf, bijvoorbeeld wanneer hij aan de hand van een formulier gegevens over zichzelf moet invullen voor een bepaald doel, dan dient deze op de hoogte te worden gesteld op het moment van vergaring van gegevens. Deze vorm komt aan de orde in artikel 33. Artikel 34 regelt de situatie dat de gegevens op een andere wijze worden verkregen, dus buiten de betrokkene om.¹⁹

¹⁸ TK 1997-1998, 25 892, nr. 3, blz. 149.

¹⁹ TK 1997-1998, 25 892, nr. 3, blz. 149-150.

In de bevindingen is vastgesteld dat Google niet heeft voldaan aan de informatieplicht op basis van artikel 34 Wbp.

2.4.1 *Zienswijze*

Google heeft primair gesteld dat Google van oordeel is dat de uitzondering van artikel 34, vierde lid, Wbp van toepassing is, omdat het Google een onevenredige inspanning zou kosten om de betrokkenen te achterhalen. De identiteit van de betrokkenen zou bij Google niet bekend zijn. Om die identiteit alsnog te achterhalen zou volgens Google feitelijk van deur tot deur moeten worden gegaan in het gebied dat voor de betreffende SSID vermeld staat in de GLS. Google heeft gesteld dat dit niet alleen een onevenredige inspanning vergt, maar dat daardoor ook het identificerende karakter van de informatie zou toenemen.

Subsidiair heeft Google zich op het standpunt gesteld, dat voor zover er toch een - meer algemene - informatieplicht zou gelden, geconstateerd moet worden dat Google daaraan heeft voldaan door informatie ruimschoots beschikbaar te stellen via de publicaties op haar weblog en de nadere informatie waarnaar die publicaties linken.

2.4.2 *Beoordeling*

Het CBP heeft bij de bevindingen vastgesteld dat Google met zijn Street View auto's gegevens heeft verzameld over (het bestaan van) wifi-routers en dat Google de betrokkenen hierover niet heeft geïnformeerd. Vast staat dat Google uit eigen observatie de gegevens heeft verwerkt en dat derhalve artikel 34 Wbp van toepassing is.

Het standpunt van Google, dat het in het onderhavige geval een onevenredige inspanning kost om alle betrokkenen te informeren, gaat niet op. Het feit dat het in casu gaat om een groot aantal betrokkenen leidt niet zonder meer tot het gevolg dat geconcludeerd moet worden dat het een onevenredige inspanning vergt om de betrokkenen te informeren. Het is immers niet noodzakelijk dat Google de betrokkenen van deur tot deur benadert om aan de informatieverplichting te voldoen.

Zou het om één bepaalde betrokkene gaan, dan zal deze specifiek op de hoogte moeten worden gesteld. Gaat het daarentegen om meerdere betrokkenen, zoals in casu het geval is, dan kan de wijze van informeren algemener zijn. Wanneer de informatie aan een groep personen moet worden verstrekt, kan deze groep de informatie ter beschikking worden gesteld via een medium waarvan vaststaat dat deze groep daarmee wordt bereikt.²⁰

Bovendien ziet het CBP niet in waarom het thans voor Google een onevenredige inspanning zou vergen om de betrokkenen te informeren, nu deze inspanning niet wezenlijk verschilt van de wijze waarop Google bijvoorbeeld in Duitsland betrokkenen heeft geïnformeerd over het

²⁰ TK 1997-1998, 25 892, nr. 3, blz. 152 -153.

voornemen om op bepaalde tijden in bepaalde gebieden foto's van huizen te maken voor de Google dienst Street View. Zo zijn er ook in Nederland voldoende middelen beschikbaar om betrokkenen zowel online als offline te informeren over de verzameling van gegevens over wifi-routers.

Het door Google subsidiair naar voren gebrachte standpunt dat Google al aan de informatieplicht heeft voldaan doordat Google de informatie reeds ruimschoots beschikbaar heeft gesteld via de publicaties op haar weblog en de nadere informatie waarnaar die publicaties linken, kan het CBP niet volgen. Deze informatie wordt via de weblog van Google niet of nauwelijks gegeven. Bovendien is de weblog van Google niet op een breed publiek gericht en is de weblog bovendien Engelstalig. Deze wijze van informeren is derhalve niet in overeenstemming met de informatieplicht als beschreven in artikel 34 Wbp.

Doordat Google de betrokkenen niet (of in ieder geval onvoldoende) over de verzameling van gegevens over wifi-routers heeft geïnformeerd, heeft Google in strijd gehandeld met artikel 34 Wbp. Google dient de betrokkenen alsnog conform artikel 34, tweede lid, Wbp te informeren. Dit informeren dient zowel online als offline plaats te vinden. Het online informeren dient plaats te vinden op de bestbezochte nieuwssites op internet en via de Google website. De via de website van Google te geven informatie dient goed zichtbaar en eenvoudig te bereiken te zijn. Dit dient bij voorkeur te geschieden door deze informatie te plaatsen op de Street View pagina van Google (<http://maps.google.com/intl/nl/help/maps/streetview/privacy.html>) en met behulp van een hyperlink in het algemene Nederlandstalige privacy-centrum van Google (<http://www.google.nl/intl/nl/privacy/>) naar deze informatie te verwijzen. Het offline informeren dient plaats te vinden via landelijke dagbladen met een zo groot en divers mogelijk bereik of via regionale dagbladen, met een zo groot mogelijke landelijke spreiding.

Op grond van artikel 34, derde lid, Wbp dient Google tevens nadere informatie te verstrekken die nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen. In dit kader dient Google de betrokkenen te informeren over de mogelijkheid middels een opt-out verzet aan te tekenen tegen de verwerking van gegevens over de wifi-routers van de betrokkenen.

2.5 Meldingsplicht

Artikel 27 Wbp luidt als volgt:

1. *Een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens die voor de verwezenlijking van een doeleinde of van verscheidene samenhangende doeleinden bestemd is, wordt alvorens met de verwerking wordt aangevangen gemeld bij het College of de functionaris.*
2. *Een niet geautomatiseerde verwerking van persoonsgegevens die voor de verwezenlijking van een doeleinde of van verscheidene samenhangende doeleinden bestemd is, wordt gemeld indien deze is onderworpen aan voorafgaand onderzoek.*

In artikel 28 Wbp is beschreven wat de melding moet inhouden.

Het CBP heeft bij de bevindingen vastgesteld dat Google heeft nagelaten de verzameling van gegevens over wifi-routers te melden bij het CBP zoals bedoeld in artikel 27 jo. 28 Wbp.

2.5.1 *Zienswijze*

Google erkent dat zij geen gebruik heeft gemaakt van het voorgeschreven papieren of elektronische meldingsformulier, maar meent dat daartoe ook geen noodzaak meer bestaat. Zij meent dat het CBP reeds - vanwege het onderzoek - in kennis is gebracht van de informatie die de melding, zoals bedoeld in artikel 28 Wbp, dient te bevatten.

2.5.2 *Beoordeling*

Het CBP wijst erop dat de melding een wettelijke verplichting is. De verantwoordelijke is op grond van de Wbp verplicht een melding te doen van de (voorgenomen) gegevensverwerking. Ook in het geval het CBP op een andere manier dan door middel van een melding zoals bedoeld in artikel 27 Wbp in kennis is gebracht van de gegevens die bij melding moeten worden verstrekt, is de verantwoordelijke gehouden om de melding zoals bedoeld in de Wbp te doen. De melding in het voor iedereen toegankelijke meldingenregister heeft immers tot doel de transparantie van de gegevensverwerking te bevorderen. Het CBP is op grond van artikel 30 Wbp verplicht om een dergelijk register bij te houden.²¹

In dit verband wijst het CBP er verder op dat in het Meldingsbesluit Wbp is bepaald dat een melding dient plaats te vinden met behulp van het door de minister van Justitie vastgestelde meldingsformulier of het meldingsprogramma, zoals dat via de CBP website is te downloaden.

²¹ Dit register is te raadplegen via www.cbpweb.nl.

3. *Last onder dwangsom*

Vaststaat dat Google op grond van het bovenstaande in strijd handelt met de Wbp. Gelet op de bevindingen en naar aanleiding van hetgeen tijdens de hoorzitting naar voren is gebracht besluit het CBP tot het opleggen van een last onder dwangsom.

Het CBP is ingevolge artikel 65 Wbp bevoegd om een last onder bestuursdwang op te leggen ter handhaving van de bij of krachtens de Wbp gestelde verplichtingen. Op grond van artikel 5:32, eerste lid, Algemene wet bestuursrecht (Awb) kan een bestuursorgaan dat bevoegd is een last onder bestuursdwang op te leggen, in plaats daarvan de overtreder een last onder dwangsom opleggen.

Naar aanleiding van de hierboven genoemde overwegingen legt het CBP Google Inc. en Google Netherlands B.V. de volgende last onder dwangsom op en sommeert het de volgende maatregelen te treffen:

1. De verzamelde SSID's onomkeerbaar te wissen door deze ten minste drie maal te overschrijven met verschillende patronen.
2. Betrokkenen zowel offline als online conform artikel 34 Wbp te informeren over de verzameling van gegevens over wifi-routers met Street View auto's door Google ten behoeve van de Google GLS. In dat verband dient Google de betrokkenen tevens te informeren over de mogelijkheid middels een opt-out verzet aan te tekenen tegen het verwerken van gegevens over de wifi-routers van betrokkenen. Bovengenoemde informatie dient *online* te worden verstrekt door een advertentie te plaatsen op ten minste vier nieuwssites op internet, te kiezen uit de tien best bezochte Nederlandstalige nieuwswebsites én op een goed zichtbare en voor de betrokkenen goed bereikbare plaats op de Nederlandstalige website van Google. Bovengenoemde informatie dient *offline* te worden verstrekt op één van de volgende door Google te kiezen methoden:
 - a. een advertentie van minimaal een halve pagina in ten minste twee landelijke dagbladen met een zo groot en divers mogelijk bereik; of
 - b. een advertentie van minimaal een halve pagina in ten minste negen regionale dagbladen met een zo groot en divers mogelijk bereik.
3. Een online opt-out mogelijkheid aan te bieden waardoor alle betrokkenen te allen tijde kosteloos en effectief verzet kunnen aantekenen tegen de verwerking van gegevens over de wifi-routers van de betrokkenen.
4. De verwerking van gegevens over wifi-routers bij het CBP te melden conform artikel 27 en 28 Wbp en het Meldingsbesluit Wbp.

Indien u niet aan deze last voldoet, dan bent u vanaf de begunstigingstermijn per maatregel een dwangsom verschuldigd van € 5.000,- (zegge: vijf duizend euro) per dag dat niet aan de last is voldaan. Het bedrag waarboven geen dwangsom meer wordt verbeurd, is bepaald op € 250.000,- (zegge: twee honderd en vijftigduizend euro) per maatregel.

De hoogte van de dwangsom is gerelateerd aan de ernst van de overtreding en aan het maatschappelijk belang van de naleving van de regelgeving. Voor de vaststelling van de hoogte van de dwangsom is de grote schaal waarop Google persoonsgegevens heeft verzameld van belang. Google heeft immers gegevens verzameld over ongeveer 3.606.579 verschillende wifi-routers. Verder is rekening gehouden met de beoogde werking van de dwangsom. In dit verband is van belang dat de hoogte van de dwangsom voor Google voldoende financiële prikkel dient te vormen om aan de last te voldoen.

Ingevolge artikel 5:32a Awb dient het CBP een termijn te stellen gedurende welke de overtreder de last kan uitvoeren zonder dat een dwangsom wordt verbeurd. Voor de maatregel zoals geformuleerd onder 1 is deze termijn bepaald op zes weken. Voor de maatregelen zoals geformuleerd onder 2 en 3 is deze termijn bepaald op drie maanden. Tot slot is de termijn voor de maatregel zoals geformuleerd onder 4 bepaald op twee weken.

Ingevolge artikel 7:1 Awb kunt u tegen de last onder dwangsom bezwaar maken door het indienen van een gemotiveerd bezwaarschrift, gericht aan het CBP, Postbus 93374, 2509 AJ Den Haag, onder vermelding van "Awb-bezwaar" op de enveloppe. De termijn waarbinnen het bezwaarschrift kan worden ingediend bedraagt zes weken na de dag waarop dit besluit is verzonden.

Ten aanzien van de verzamelde payload data

4. *Het verloop van de procedure*

Naar aanleiding van het ambtshalve onderzoek op grond van artikel 60 Wbp, heeft het CBP bij brief van 23 november 2010 de definitieve bevindingen (hierna: de bevindingen) aan Google toegezonden.²² In de bevindingen is geconcludeerd dat Google onrechtmatig gegevens verwerkt door onder meer payload data te verzamelen in strijd met de artikelen 7 (gerechtvaardigd doel), 8 (grondslag), 16 (bijzondere persoonsgegevens) en 6 (zorgvuldige verwerking) van de Wbp. De bevindingen worden hier als herhaald en ingelast beschouwd.

Uit het onderzoek van het CBP is naar voren gekomen dat Google op grote schaal inhoudelijke communicatiegegevens heeft verzameld afkomstig uit onbeveiligde wifi-routers in Nederland. Google heeft in de periode maart 2008 tot mei 2010 ruim 8 miljoen packets aan gegevens opgeslagen. Deze payload data bevatten persoonsgegevens als bedoeld in de Wbp.

Bij brief van 13 december 2010 heeft het CBP Google bericht dat het, gelet op de conclusies van de bevindingen, voornemens is om een last onder dwangsom op te leggen.

Op 13 januari 2011 is Google tijdens de hoorzitting in de gelegenheid gesteld om mondeling een zienswijze met betrekking tot het voornemen van het CBP te geven. Google heeft van deze gelegenheid gebruik gemaakt en tijdens de hoorzitting verklaard dat zij er niet van op de hoogte was dat payload data werden verzameld en dat zij, zodra zij dit ontdekte, met medewerking en onder feitelijk toezicht van een extern forensisch onderzoeksbureau, Stroz Friedberg, de data in een aparte beveiligde server-omgeving heeft geplaatst. Hoewel Google haar standpunt handhaaft dat zij door het verzamelen van de payload data de wet niet heeft overtreden, heeft Google aangegeven bereid te zijn de payload data te vernietigen. De reden dat Google de gegevens thans nog bewaart is omdat het CBP hierom heeft verzocht. Google heeft toegelicht dat het overgrote deel van de Nederlandse payload data zich op een beveiligde server in de Verenigde Staten bevindt die buiten het netwerk van Google is geplaatst. Verder heeft Google tijdens de hoorzitting gemeld dat zich in een magazijn in België 7 harddisks met Nederlandse payload data bevinden en dat er 4 harddisks zijn waarop naast de Nederlandse payload data ook data uit andere landen zijn opgeslagen (de zogenaamde gemengde data).

²² Voor een overzicht van de loop van de procedure tot 23 november 2010 verwijst het CBP naar § 2.1 van de bevindingen.

Bij brief van 20 januari 2011 heeft het CBP, ter bevestiging van een vraag die zij tijdens de hoorzitting heeft gesteld, Google verzocht om een gedetailleerde beschrijving te geven van de harddisks waarop de gemengde payload data zijn opgeslagen.

Naar aanleiding van de brief van 20 januari 2011 heeft telefonisch contact plaatsgevonden tussen het CBP en Google. Naar aanleiding hiervan heeft het CBP in zijn e-mail van 21 januari 2011 bepaald welke informatie de reactie van Google op het verzoek van 20 januari 2011 in ieder geval dient bevatten, waaronder de hashwaarden van alle harddisks.

Bij faxbericht van 26 januari 2011 heeft Google gedeeltelijk aan het verzoek van het CBP voldaan. Uit deze fax blijkt dat, anders dan tijdens de hoorzitting was aangegeven, er 5 (in plaats van 7) harddisks zijn die alleen Nederlandse gegevens bevatten en er 2 (in plaats van 4) harddisks zijn met gemengde data. In het faxbericht wordt toegelicht dat één van deze twee harddisks met gemengde data, naast de Nederlandse payload data, payload data uit Duitsland bevat en dat de andere harddisk, naast de Nederlandse payload data, payload data uit België bevat. Daarnaast heeft Google gesteld dat, gelet op het feit dat de samenstelling van de harde schijf kan wijzigen en het grote tijdsbeslag dat gemoeid is met het creëren van de hashwaarden, zij niet aan het verzoek van het CBP kan voldoen om de hashwaarden van de harddisks te verstrekken.

Bij e-mail van 1 februari heeft het CBP Google verzocht de hashwaarden van de harddisks alsnog te verstrekken.

Per e-mail van 2 februari 2011 heeft Google toegelicht dat het voor Google bezwaarlijk zou zijn om de hashwaarden van de harddisks te verstrekken aangezien dit een grote extra inspanning zou vergen die naar het oordeel van Google niet opweegt tegen de meerwaarde die de hashwaarden zouden opleveren.

Per e-mail van 2 februari 2011 heeft het CBP hierop gereageerd.

Op 7 februari 2011 heeft het CBP Google telefonisch bericht dat Google kan volstaan met het verstrekken van de hashwaarden van de 2 harddisks met gemengde data en dat deze hashwaarden aan het CBP dienen te worden verstrekt op het moment dat de 5 harddisks met Nederlandse data uit het depot worden gehaald om deze op verzoek van het CBP te vernietigen. Dit is op 8 februari 2011 door het CBP per e-mail bevestigd.

Bij fax van 11 februari 2011 heeft Google - samengevat - op de mogelijkheid gewezen dat er na het genereren van de hashwaarden van de gemengde harddisks data-degeneratie als gevolg van fysieke veroudering zou kunnen optreden, waardoor het mogelijk is dat de opnieuw te genereren hashwaarden afwijken van de eerder gegenereerde hashwaarden, ook al heeft er geen datamanipulatie plaatsgevonden.

5. *Opdracht*

Het CBP draagt Google op om binnen 4 weken na dagtekening van deze brief:

1. De in Nederland verzamelde payload data, die zijn opgeslagen op de geïsoleerde beveiligde server in de Verenigde Staten, onomkeerbaar te wissen door deze ten minste drie maal te overschrijven met verschillende patronen, bijvoorbeeld middels DoD 5220.22-M.
2. De harddisks met Nederlandse payload data met serienummers 3QD16XS6, 5QD1NWKH, 5QD367NV, 5QD3T1NQ en PAHNG8UF onomkeerbaar te wissen. Het wissen dient te geschieden door de harde schijf ten minste drie maal te overschrijven met verschillende patronen, bijvoorbeeld middels DoD 5220.22-M. Vervolgens dient de schijf fysiek te worden vernietigd.
3. De harddisks met gemengde data met serienummers 5QD3V512 (Nederlandse en Duitse data) en PAGMZ6MF (Nederlandse en Belgische data) in depot te houden zolang de procedures in Duitsland respectievelijk België lopen, danwel, indien dit eerder is, tot het moment dat de betreffende toezichthouder opdracht tot vernietiging van de gegevens geeft of niet langer eist dat deze bewaard worden.
4. De hashwaarden (SHA1) van de onder punt 3 genoemde harddisks met gemengde data aan het CBP te verstrekken.
5. Een schriftelijke verklaring van een extern forensisch onderzoeksbureau over te leggen dat de payload data als bedoeld onder de punten 1 en 2 onomkeerbaar zijn gewist en zijn vernietigd en dat de harddisks met gemengde data zoals bedoeld onder punt 3 in depot zijn genomen.

Voorts draagt het CBP Google op om binnen 4 weken na het aflopen van de procedures in Duitsland dan wel in België, dan wel, indien dit eerder is, binnen 4 weken na het moment dat de opdracht tot vernietiging wordt gegeven:

6. Opnieuw een hashwaarde (SHA1) van de harddisk met gemengde data met serienummer 5QD3V512 (Nederlandse en Duitse data) dan wel met serienummer PAGMZ6MF (Nederlandse en Belgische data) aan het CBP te verstrekken.
7. De harddisk met gemengde data onomkeerbaar te wissen. Het wissen dient te geschieden door de harde schijf ten minste drie maal te overschrijven met verschillende patronen, bijvoorbeeld middels DoD 5220.22-M. Vervolgens dient de schijf fysiek te worden vernietigd.
8. Een schriftelijke verklaring van een extern forensisch onderzoeksbureau over te leggen dat de harddisk met gemengde data onomkeerbaar is gewist en fysiek is vernietigd.

Het CBP wijst erop dat indien Google niet of gedeeltelijk aan bovenstaande opdracht voldoet, het CBP alsnog zal overgaan tot het opleggen van een last onder dwangsom.

DATUM 23 maart 2011
ONS KENMERK z2010-01467

Hoogachtend,
Het College bescherming persoonsgegevens,

Mr. J. Kohnstamm
Voorzitter

Bijlage 1: rapport van definitieve bevindingen d.d. 23 november 2010
Bijlage 2: verslag van de hoorzitting d.d. 13 januari 2011 en pleitnotities