COLLEGE BESCHERMING PERSOONSGEGEVENS

DEFINITIEVE BEVINDINGEN

Onderzoek CBP naar de verzameling van Wifi-gegevens met Street View auto's door Google

z2010-00582

7 december 2010

OPENBARE VERSIE

INHOUDSOPGAVE

1. Inleiding

Het College bescherming persoonsgegevens (CBP) heeft op grond van artikel 60 Wet bescherming persoonsgegevens (Wbp) ambtshalve onderzoek ingesteld naar de verzameling van gegevens met betrekking tot wifi-netwerken in Nederland (hierna: Wifi-gegevens) met Street View auto's door Google Inc. (hierna: Google).

Het bedrijf heeft de Wifi-gegevens verzameld tijdens het maken van foto's ten behoeve van zijn dienst *Street View*. Met deze dienst publiceert Google foto's van huizen, straten en pleinen op internet. De gegevens zijn verzameld met behulp van Street View auto's. De auto's zijn uitgerust met camera's om de panoramische foto's te kunnen maken. De auto's waren van maart 2008 tot mei 2010 in Nederland tevens uitgerust met een antenne en bijbehorende apparatuur en programmatuur om signalen op te vangen van draadloos internetverkeer.

Google maakte op 27 april 2010 bekend dat met de Street View auto's wereldwijd gegevens over draadloze netwerken werden verzameld.[1] Het bedrijf stelde toen alleen gegevens *over* (het bestaan van) wifi-routers te verzamelen. Het bedrijf stelde géén gegevens te verzamelen afkomstig *uit* draadloze internet netwerken.

Op 14 mei 2010 maakte Google via zijn 'Official Google Blog' bekend dat het bedrijf bij het verzamelen van gegevens over wifi-netwerken ook de inhoud van communicatie over onbeveiligde wifi-netwerken had opgenomen en bewaard.[2]

Het CBP heeft vanuit zijn toezichthoudende rol naar aanleiding van het bovenstaande onderzoek ingesteld. Het onderzoek is geconcentreerd op de volgende vijf vragen:

- Wat voor Wifi-gegevens heeft Google precies verzameld, zowel *over* als *afkomstig uit* wifi-netwerken? Zijn dit persoonsgegevens zoals gedefinieerd in artikel 1, aanhef en onder a, Wbp?

- Zitten bij de verzamelde Wifi-gegevens ook *bijzondere* persoonsgegevens, zoals gedefinieerd in artikel 16 Wbp?

- Voor welke doeleinden heeft Google de Wifi-gegevens verzameld? Zijn deze doeleinden gerechtvaardigd, zoals bedoeld in artikel 7 Wbp?

- Heeft Google betrokkenen geïnformeerd over de verschillende doeleinden waarvoor persoonsgegevens zijn verzameld en verwerkt, zoals voorgeschreven in artikel 33 en 34 Wbp?

- Heeft Google de verwerking van Wifi-gegevens gemeld bij het CBP, zoals bedoeld in artikel 27, jo. 28 Wbp?

Het onderzoek richt zich op toetsing aan de artikelen 7 (gerechtvaardigd doeleinde), 8 (grondslag van de verwerking: toestemming of noodzaak), 16 jo. 23 (verbod op het verwerken van *bijzondere*

[1] Bron: Google, 'Data collected by Google cars', 27 april 2010, URL: http://googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html.
[2] Bron: Google, 'WiFi data collection: An update', 14 mei 2010, met updates van 17 mei en 9 juni 2010, URL: http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html

persoonsgegevens, tenzij met *uitdrukkelijke* toestemming), 27 jo. 28 (melding bij het CBP), 33, 34 (informatieplicht) en 6 Wbp (behoorlijke en zorgvuldige gegevensverwerking).

2. Procedure

2.1 Verloop

Bij brief van 21 mei 2010 heeft het CBP schriftelijke inlichtingen ingewonnen bij Google. Google is verzocht antwoord te geven binnen tien kalenderdagen. Bij e-mail van 27 mei 2010 heeft Google om uitstel van beantwoording verzocht. Bij brief van 27 mei 2010 heeft het CBP uitstel van beantwoording verleend tot uiterlijk dinsdag 8 juni 2010. Het CBP heeft een deel van de gevraagde inlichtingen ontvangen bij brief van 8 juni 2010.[3]

Bij brief van 17 juni 2010 heeft het CBP een onderzoek ter plaatse aangekondigd op maandag 28 juni 2010. Het CBP heeft Google om medewerking verzocht tijdens genoemd onderzoek bij het verlenen van inzage in en het maken van twee leesbare forensische kopieën, namelijk van gegevens op een representatieve harde schijf met Wifi-gegevens opgenomen in Nederland en van het bestand met alle inhoudelijke communicatiegegevens afkomstig uit draadloze netwerken in Nederland, hierna: *payload data*. Google heeft een schriftelijk gemotiveerd verzoek verstuurd om het onderzoek één dag uit te stellen, naar dinsdag 29 juni 2010. Dit verzoek is gehonoreerd.

Bij brief van 24 juni 2010 heeft Google aangegeven geen medewerking te zullen verlenen aan het maken van de gevraagde forensische kopieën. Bij brief van 28 juni 2010 heeft het CBP medewerking gevorderd.

Op 29 juni 2010 heeft het CBP onderzoek ter plaatse ingesteld. Tijdens genoemd onderzoek heeft Google geen medewerking verleend aan het maken van de gevraagde, leesbare, forensische kopieën. Naderhand heeft Google alsnog de gevraagde kopie van alle in Nederland verzamelde *payload data* verstrekt, zie hierna. Het CBP heeft genoemd onderzoek die dag besteed aan onderzoek naar de gegevens op de harde schijf, middels *remote access* naar een computer in België met een kopie van deze harde schijf.

Tijdens genoemd onderzoek heeft het CBP mondeling inlichtingen ingewonnen bij twee relevante technische medewerkers en de namens de directeur gemachtigde bedrijfsjurist van Google. Het CBP heeft een aantal (kopieën van) stukken meegenomen, in de vorm van drie print-outs van 1 A4. Van de tijdens het onderzoek opgestelde en gekopieerde stukken is een kopie verstrekt aan Google.

Tijdens genoemd onderzoek heeft het CBP verzocht de twee ontbrekende antwoorden op de brief van 21 mei 2010 alsnog uiterlijk 2 juli 2010 te verstrekken. Google heeft deze inlichtingen niet tijdig verstrekt. Naar aanleiding van feitelijke vragen die rezen tijdens genoemd onderzoek heeft het CBP een aanvullend verzoek om inlichtingen verzonden. Google heeft op 6 juli 2010 een deel van de gevraagde (aanvullende) inlichtingen verstrekt, maar niet de gevraagde inlichtingen van 21 mei 2010.

Bij brief van 8 juli 2010 heeft het CBP medewerking gevorderd om uiterlijk 12 juli 2010, 17.00 uur, een volledig antwoord te geven op de gestelde vragen. Tevens heeft het CBP bij brief van 8 juli

[3] Van de 11 vragen waren er 2 niet beantwoord.

2010 nieuwe inlichtingen verzocht en inzage in zakelijke gegevens en bescheiden met betrekking tot de in Nederland vastgelegde *payload data*, met het verzoek deze informatie uiterlijk 15 juli 2010, 17.00 uur, te verstrekken. Bij twee e-mails van 12 juli 2010 heeft Google de ontbrekende twee antwoorden op de vragen van 21 mei 2010 verstrekt en aangegeven meer tijd nodig te hebben om een andere inlichting te kunnen verstrekken. Bij e-mail van 15 juli 2010, 16:48 uur, heeft Google een deel van de gevraagde inlichtingen verstrekt. Google heeft niet de gevraagde print-outs verstrekt met betrekking tot de *payload data*. In plaats daarvan heeft Google een leesbaar gemaakte kopie aangeboden van het bestand met alle in Nederland verzamelde *payload data*.

Bij brief van 16 juli 2010 heeft het CBP een rappel verstuurd van de vordering bij brief van 8 juli 2010. Bij deze brief is Google gevorderd uiterlijk maandag 19 juli 2010 een leesbaar gemaakte kopie te verstrekken van het bestand met alle in Nederland verzamelde *payload data*. Het CBP heeft tevens aanvullende inlichtingen gevorderd om onduidelijkheden op te helderen in eerder verstrekte inlichtingen, met de opdracht deze inlichtingen uiterlijk 21 juli 2010 te verstrekken. Bij e-mail van 19 juli 2010 heeft Google gemotiveerd om uitstel gevraagd bij het leveren van de gevraagde kopie van het bestand met alle in Nederland verzamelde *payload data*. Bij brief van 20 juli 2010 heeft het CBP uitstel verleend tot uiterlijk 22 juli 2010. Het CBP heeft de harde schijf met de *payload data* ontvangen op 21 juli 2010 en proces-verbaal opgesteld van de overdracht. Google heeft hiervan een kopie ontvangen. Bij fax van 21 juli 2010 heeft de firma Stroz Friedberg in opdracht van Google het wachtwoord verstrekt om de gegevens op de harde schijf te ontsluiten. Bij e-mail van 22 juli 2010 heeft Google de aanvullende inlichtingen verstrekt die gevorderd waren bij brief van 16 juli 2010.

Bij brief van 21 september 2010 heeft het CBP zijn rapport van voorlopige bevindingen aan Google toegestuurd, met het verzoek binnen 2 weken te reageren, op 5 oktober 2010. Bij brief van 22 september 2010 heeft Google gemotiveerd om 2 weken uitstel verzocht, tot 2 november 2010. Bij brief van 8 oktober 2010 heeft Google verzocht om zijn zienswijze op het rapport van voorlopige bevindingen in het Engels te mogen indienen. Bij brief van 11 oktober 2010 heeft het CBP aangegeven dat de zienswijze in het Nederlands dient te worden gegeven. Bij brief van 12 oktober heeft Google 1 week uitstel gevraagd om de zienswijze in het Nederlands te kunnen aanleveren. Bij brief van 12 oktober 2010 heeft het CBP nog één week uitstel verleend, tot 26 oktober 2010. Bij brief van 26 oktober 2010 heeft Google zijn zienswijze aan het CBP gestuurd.

Bij brief van 9 november 2010 (nader gespecificeerd per brief van 11 november 2010) heeft het CBP Google gevraagd binnen tien kalenderdagen aan te geven welke verstrekte gegevens het bedrijf als bedrijfsvertrouwelijk beschouwt. Bij brief van 19 november 2010 heeft Google geantwoord. Bij brief van 23 november 2010 heeft het CBP de definitieve Bevindingen toegestuurd aan Google. Hierbij was tevens een concept openbare versie van de Bevindingen gevoegd, met het verzoek binnen vijf kalenderdagen aan te geven of in de openbare versie naar het oordeel van Google toch nog bedrijfsvertrouwelijke gegevens waren opgenomen. Google heeft hierop tot tweemaal toe om uitstel van beantwoording gevraagd. Beide verzoeken zijn afgewezen. Google heeft per e-mail van vrijdagavond 26 november 2010 inhoudelijk gereageerd op het verzoek om (nogmaals) de bedrijfsvertrouwelijkheid te toetsen.

3. Feiten

3.1 Algemene werkwijze Google mbt Wifi-gegevens

Google Inc., opgericht op 4 september 1998, met hoofdkantoor in Mountain View, Californië in de Verenigde Staten, heeft als doel "o*m alle informatie wereldwijd toegankelijk en bruikbaar te maken*".[4] Daartoe biedt Google niet alleen een internet zoekmachine, maar biedt het bedrijf een heel palet aan online diensten, variërend van webmail tot de verkoop van online advertenties, en van online plattegronden (Maps) tot een browser (Chrome). Google Inc. heeft in Nederland het kantoor Google Netherlands B.V., gevestigd te Amsterdam en ingeschreven bij de Kamer van Koophandel sinds 27 november 2003 onder nummer 34198589. De bedrijfsomschrijving van Google Netherlands B.V. is: "*Het drijven van een onderneming op het gebied van een internet zoekmachine en het verlenen van diensten en geven van informatie en advies op het gebied van het zoeken en ophalen van informatie van internet, intranet en andere (elektronische) communicatie.*"

Google heeft Wifi-gegevens verzameld tijdens het maken van foto's ten behoeve van door haar aangeboden dienst *Street View*. Met deze dienst publiceert Google wereldwijd foto's van huizen, straten en pleinen op internet.[5] De gegevens zijn wereldwijd verzameld in 30 landen met behulp van Street view auto's.[6] De auto's zijn uitgerust met camera's om de panoramische foto's te kunnen maken. De auto's waren van maart 2008 tot mei 2010 in Nederland tevens uitgerust met een antenne en bijbehorende apparatuur en programmatuur om signalen op te vangen en te bewaren van draadloze internet netwerken.

Google heeft de Wifi-gegevens opgevangen met behulp van een algemeen in de handel verkrijgbare antenne.[7] De opgenomen gegevens zijn met behulp van eveneens algemeen verkrijgbare open source software (Kismet) opgevangen. De met Kismet verkregen data zijn vervolgens in een door Google zelf ontwikkelde applicatie (gstumbler en gslite als executable) verwerkt ten behoeve van de opslag van de data. De software was ingesteld om vijf keer per seconde van kanaal te wisselen, om opnames te maken van 0,2 seconde per kanaal.

De auto's waren uitgerust met [VERTROUWELIJK: beschrijving technische toerusting auto's en technische werkwijze locatiebepaling].

De Wifi-signalen werden opgeslagen op een harde schijf in de Street View auto. Google heeft deze harde schijven wekelijks per koerier afgeleverd bij een magazijn in België. Vanuit dit magazijn werd de inhoud van de harde schijf via internet verstuurd naar een Google data center in België, en van daaruit via internet verstuurd naar servers van Google in de Verenigde Staten. Google heeft verklaard geen archief of kopie te hebben gemaakt van de harde schijven, omdat het

[4] Bron: Google bedrijfsinformatie, URL: http://www.google.nl/intl/nl/corporate/facts.html
[5] De foto's zijn toegankelijk via http://maps.google.com. Dit is een website met plattegronden en satellietbeelden. Gebruikers van deze online dienst kunnen inzoomen op straatniveau om de foto's van Street View te bekijken.
[6] Bron: Google, 'Where is Street View available?', URL: http://maps.google.com/intl/en_us/help/maps/streetview/where-is-street-view.html
[7] Maxrad BMMG24005 omnidirectionele antenne. Bron: Google, 'Data collected by Google cars', 27 april 2010, URL: http://googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html.

verlies van een enkele harde schijf minder kost dan het optuigen van een archiveringssysteem of het maken van back-ups.[8]

Google heeft met de rondrijdende Street View auto's twee verschillende soorten gegevens vastgelegd: inhoudelijke communicatiegegevens (*payload data*) afkomstig uit onbeveiligde draadloze wifi-netwerken in Nederland en gegevens over (het bestaan en de locatie van) wifi-routers en andere communicatie-apparatuur.

3.2 Payload data

Op 9 juni 2010 publiceerde Google een rapport van het Amerikaanse forensisch onderzoeksbureau Stroz Friedberg LLC.[9] Het bureau heeft in opdracht van Google de (broncode van de) software bestudeerd waarmee Google de Wifi-gegevens heeft verzameld. Het rapport bevestigt dat de software was ingesteld om inhoudelijke communicatiegegevens (*payload data*) van onbeveiligde wifi-netwerken op te vangen en op te slaan.

Uit de analyse door Stroz Friedberg van de broncode blijkt dat de software de mogelijkheid bood om wel of niet de inhoudelijke communicatiegegevens op te slaan van onbeveiligde wifi-routers en andere wifi-geschikte apparaten.[10] De programmeur kon kiezen tussen *true* (aan) of *false* (uit) om de gegevens van onbeveiligde netwerken op te slaan, en heeft gekozen voor *true*. Door die keuze heeft Google wel de *payload data* van onbeveiligde netwerken opgeslagen, maar niet van beveiligde netwerken.[11]

Tijdens het onderzoek ter plaatse heeft het CBP een harde schijf onderzocht met Wifi-gegevens met betrekking tot routers in een gebied ten zuiden van Rotterdam, uit de periode van 28 april tot en met 6 mei 2010. Zie **bijlage I** voor een plattegrond waar deze Wifi-gegevens zijn verzameld. Het CBP had verzocht om een schijf met gegevens uit een gebied dat zowel qua bevolkingsdichtheid als internetgebruik representatief zou zijn voor Nederland.

Google heeft aangegeven dat er nog twee harde schijven aanwezig waren in het magazijn in België, en dat de getoonde harde schijf de meest representatieve beschikbare harde schijf was. Het gebied bleek naderhand een relatief dun bevolkt gebied, ten zuiden van Rotterdam.[12]

De gegevens op de harde schijven uit de Street View auto's zijn in *binair* formaat opgeslagen. Google heeft tijdens het onderzoek ter plaatse ten behoeve van het CBP de alfanumerieke

---

[8] Verklaring van Google tijdens het onderzoek ter plaatse op 29 juni 2010.
[9] Bron: Google, 'WiFi data collection: An update', 14 mei 2010, hyperlink in de update 9 juni 2010 naar: Stroz Friedberg, 'Source Code Analysis of gstumbler, 3 juni 2010, URL: http://www.google.com/googleblogs/pdfs/friedberg_sourcecode_analysis_060910.pdf
[10] Bij vrijwel elk *packet* wordt een WEP-bit meegezonden, zowel in een aantal management frames, als in de control frames en de data frames. Alleen in de dataframe (waar de *payload data* zijn opgeslagen) geeft dit bit een betrouwbare indicatie of de *payload* versleuteld is of niet.
[11] Met betrekking tot het wegschrijven van data naar de harde schijf waren er in totaal vier opties voor standaardinstellingen. Bron: Stroz Friedberg rapport, blz. 11, paragraaf 56.
[12] Bij brief van 2 juli 2010 ontving het CBP van Google een kaart van het gebied ten zuiden van Rotterdam waar de opnames waren gemaakt op de door het CBP onderzochte harde schijf.

gegevens met behulp van eigen software vertaald in (leesbaar) *ascii* formaat. De niet-alfanumerieke tekens zijn daarbij omgezet in *octaal* formaat.[13]

De aard van de door Google aan het CBP verleende toegang tot de gegevens (middels *remote access* met een *command line*) stelde in technisch opzicht aanzienlijke beperkingen aan de mogelijke vragen die gesteld konden worden.

Het CBP heeft tijdens het onderzoek de door Google gebruikte broncode vergeleken met de in het Stroz Friedberg rapport beschreven broncode. Op twee afwijkingen na staat vast dat de door Google gebruikte software overeenstemde met de beschreven broncode.[14]

Gegeven de bovenbedoelde technische beperkingen heeft het CBP geen sluitend beeld kunnen krijgen van de gegevens die Google heeft verzameld *over* de wifi-routers en evenmin een sluitend beeld van de inhoudelijke *payload data*. Daarom heeft het CBP alsnog medewerking gevorderd bij het maken van een forensische kopie van het (in de Verenigde Staten opgeslagen) bestand met alle in Nederland verzamelde, leesbaar gemaakte, *payload data*.

Het verkregen bestand bestaat uit *packets*, dat wil zeggen, informatie die ingedeeld is om zo slim mogelijk vervoerd te worden over een (*packet-switched*) internet. Een *packet* bestaat uit twee soorten informatie. Controle-informatie en inhoud, vergelijkbaar met een brief (*payload)* in een envelop (informatie zoals afzender en bestemming*)*.

In het bestand met alle in Nederland verzamelde *payload data* dateert het eerste *packet* van 7 maart 2008. Het laatste *packet* dateert van 29 april 2010. In totaal heeft Google gedurende 451 dagen gegevens verzameld in Nederland.

Vast staat dat Google in die tijd in Nederland bijna 30 gigabyte aan (in leesbare vorm vertaalde) *payload data* heeft verzameld afkomstig *uit* wifi-netwerken, vastgelegd op 714 harde schijven met in totaal 4.774 gstumbler logfiles.[15]

De kwantitatieve analyse voor het berekenen van diverse percentages is gebaseerd op deze 4.774 logfiles.[16]

De vastgelegde data zijn geen betekenisloze fragmenten. Het is feitelijk mogelijk om van een individuele gebruiker 1 tot ruim 2.500 *packets* op te vangen in 0,2 seconden. Bovendien kan de

---

[13] De software die Google heeft toegepast om het protocol buffer formaat leesbaar te maken heet codex. De protocol buffer is beschreven door Google in een Developers Guide op http://code.google.com/intl/nl-NL/apis/protocolbuffers/docs/overview.html. In afwijking van deze beschrijving heeft Google een eigen *proprietary* volgorde gehanteerd bij het wegschrijven van de wifi-gegevens naar de harde schijf.

[14] De broncode van de door Google gebruikte software bevatte twee extra velden die niet in appendix C van het Stroz Friedberg rapport zijn beschreven. Het CBP heeft vastgesteld dat deze twee velden in ieder geval geen *payload data* bevatten.

[15] In zijn zienswijze op de voorlopige bevindingen van 26 oktober 2010 heeft Google aangevuld dat het oorspronkelijke bestand in binaire vorm slechts 6,75 gigabyte bevatte. Het bestand dat het CBP van Google ontving bevatte 29,8 gigabyte aan leesbaar gemaakte *payload data*. Het onderzoek van het CBP heeft zich gericht op de in dit bestand aanwezige 'RAW' velden.

[16] In zijn zienswijze stelt Google dat de payload data maar een heel klein onderdeel vormden van het materiaal op de harde schijven, waaronder foto's voor de Street View dienst. Het CBP heeft de inhoud onderzocht van de door Google verzamelde en aan het CBP verstrekte kopie van de *payload data*.

auto meerdere keren een signaal hebben opgevangen van dezelfde wifi-router, bijvoorbeeld als de auto stilstond voor een rood stoplicht, of als de auto om een gebouw heenreed.

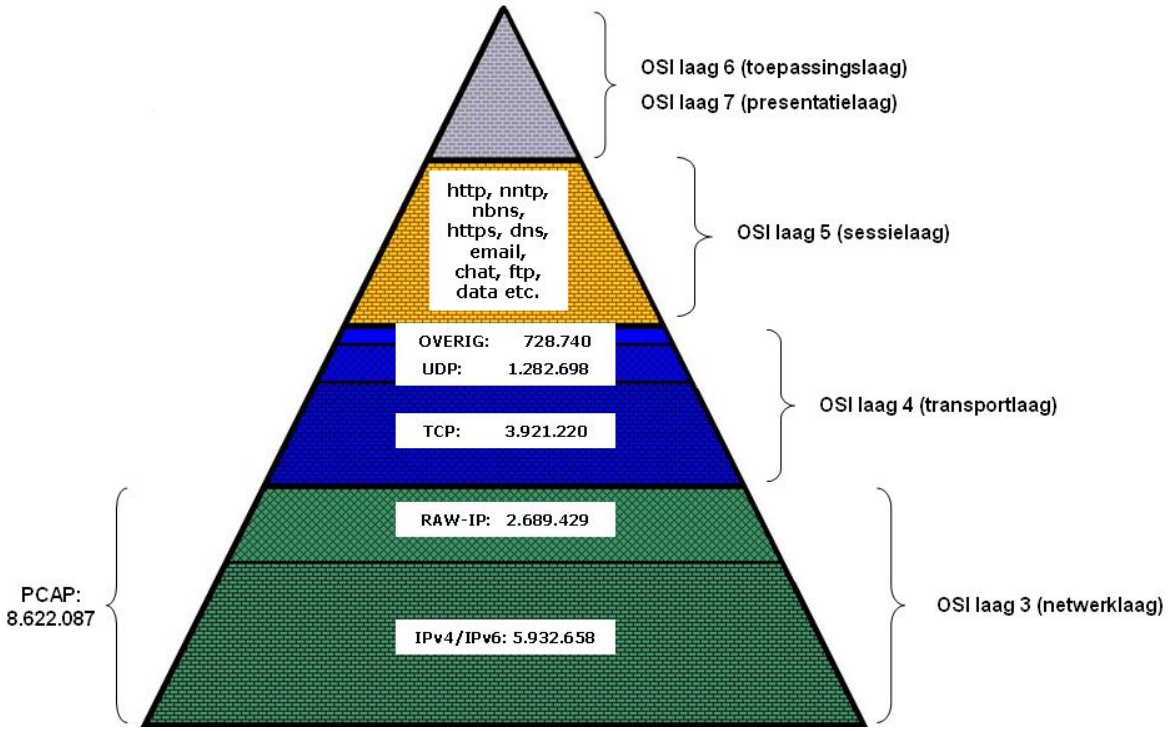
Omdat elk *packet* adresseringsgegevens bevat zoals (interne) IP-adressen en/of e-mailadressen, is het mogelijk om meerdere *packets* van 1 internetgebruiker aan elkaar te koppelen en daarmee een uitgebreid beeld op te bouwen van de communicatie van een veelal identificeerbare gebruiker.

Uit het onderzoek is gebleken dat Google niet alleen gegevens uit het veld '*raw data*' heeft opgeslagen in het bestand met alle *payload data*, maar ook 12 aanvullende velden, waaronder de latlon van de auto op het moment dat het *packet* werd opgevangen. Van elk *packet* is dus, waar GPS-ontvangst mogelijk was, nauwkeurig bekend wat de positie van de auto was op het moment dat het *packet* werd opgevangen en opgeslagen..

Het CBP heeft de *payload data* (zoals door Google ten behoeve van het CBP van proprietair binair formaat vertaald in octaal formaat en ascii) terug omgezet naar binair formaat, teneinde de gegevens systematisch te kunnen onderzoeken. In het aldus verkregen binaire pcap-bestand van 4,7 gigabyte zijn ruim 8,8 miljoen wifi-*packets* aangetroffen.[17]

De *payload data* kunnen worden beschreven aan de hand van de verschillende lagen van het OSI-model. Dit model is een gestandaardiseerde indeling van netwerkverkeer in 7 lagen. De lagen zijn, van laag naar hoog: fysiek, datalink (LLC), netwerk (routering van de *packets* via IPv4 en IPv6), transport (TCP en UDP), sessie (onderhouden en beëindigen van een sessie tussen twee communicerende hosts), presentatie en toepassing (e-mail, webverkeer, IRC etcetera).

GRAFIEK I: opbouw *packets* volgens OSI-model



[17] In dit rapport wordt consequent over *packets* gesproken, ook als het gaat om andere lagen uit het OSI-model. De officiële terminologie is bijvoorbeeld 'frame' voor *packets* in de datalink-laag en 'data' voor *packets* in de buitenste applicatielaag.

Het CBP heeft het LLC-deel van de *packets* uit laag twee van het OSI-model verwijderd teneinde standaard op internet beschikbare tools te kunnen gebruiken voor verdere analyse in laag drie en verder. In pcap-formaat zijn dan nog ruim 8,6 miljoen *packets* in beginsel leesbaar. Een deel van deze *packets* is niet nader onderzoekbaar, omdat het slechts een fragment betreft.

Uit dergelijke fragmenten kan niet worden afgeleid om wat voor type internetverkeer het gaat. Van de 8,6 miljoen *packet*s zijn 2,7 miljoen van dergelijke fragmenten *raw IP* (31,2%).

Het verdere onderzoek van het CBP is beperkt tot 68,8 procent van de leesbare data, in totaal 5.932.658 *packets* die in laag drie van het OSI-model herkenbaar zijn als IPv4 en IPv6.

Deze *packets* bestaan voor 66% uit TCP-verkeer, voor 22% uit UDP-verkeer (gebruikt voor bijvoorbeeld DNS queries) en voor 12% uit overig verkeer.[18]

Al deze *packets* bevatten ten minste twee IP-adressen: van de verzender en van de ontvanger. Met de ontvanger wordt hier een apparaat bedoeld dat verbonden is met een wifi-router. Van deze ontvangers zijn niet de publieke IP-adressen opgeslagen, maar de interne, niet-unieke adressen, in de reeksen 10.0.0.1 tot 10.255.255.254, 172.16.0.1 tot 172.31.255.254 en 192.168.0.1 tot 192.168.255.254. In geval van websitebezoek bevat een *packet* ook een publiek IP-adres (van de website).

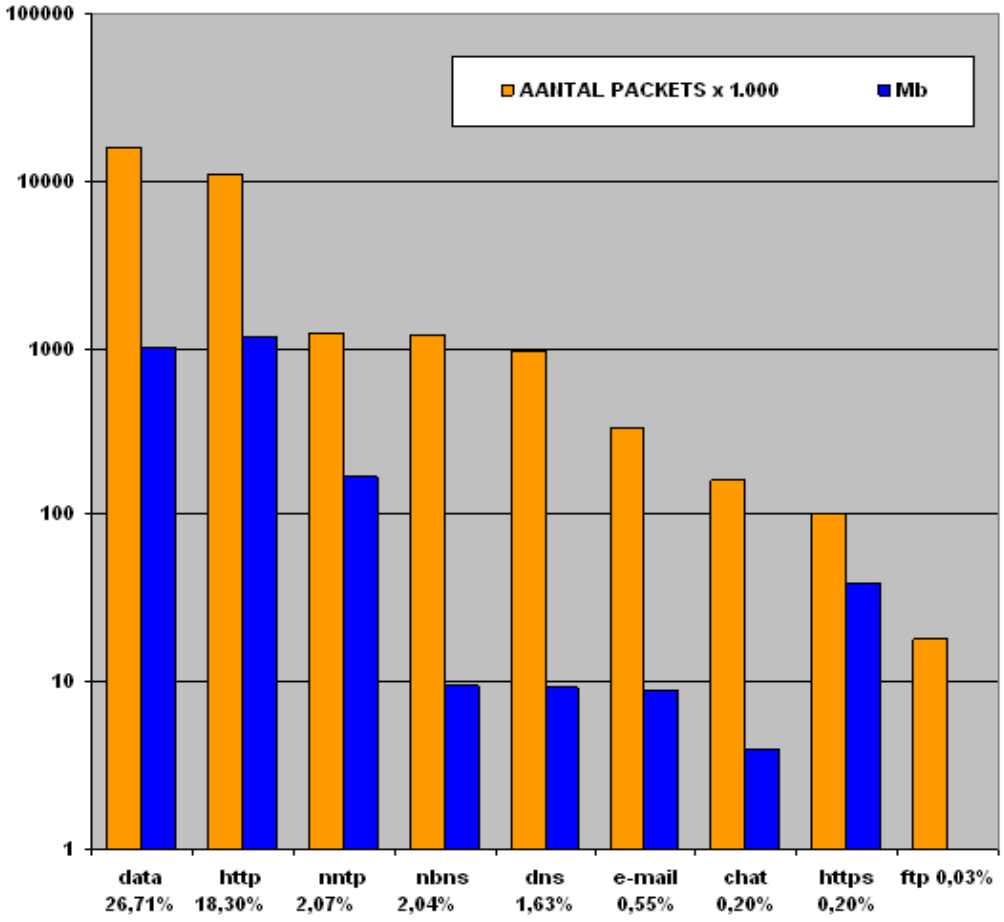
De *packets* zijn verder geanalyseerd met behulp van programma's als Wireshark, capinfos, tshark, ngrep, perl scripts en foremost om een kwantitatieve analyse te kunnen doen van de soorten internetverkeer (zoals e-mail, webverkeer, etcetera) in de TCP- en IP-laag van het verkeer. Zie **bijlage II** voor een stroomdiagram van de onderzoeksmethode.

De gemiddelde omvang van elk opgevangen *packet* is 564.58 bytes (dwz ruim 500 cijfers, letters of tekens, inclusief spaties). Hoeveel *packets* Google heeft kunnen opvangen in 0.2 seconde is afhankelijk van de doorvoersnelheid van het wifi-netwerk. De maximum snelheid in de 802.11g standaard is 54 Mbit per seconde. Daarmee kunnen maximaal 2.507 *packets* worden verzonden (in alle lagen van het OSI-model), en dus opgevangen. Bij een snelheid van 5,5 Mbit per seconde kunnen in 0,2 seconde maximaal 255 *packets* worden verzonden en bij een snelheid van 1 Mbit per seconde is het aantal *packets* maximaal 46.

Vaak zijn *packets* meer dan een keer uitgezonden en door Google opgeslagen, bijvoorbeeld omdat een ontvanger om herhaling vraagt als een *packet* niet compleet is ontvangen of als een verzendende computer geen ontvangstbevestiging heeft gekregen. Dit is inherent aan de werking van internet.

[18] Overig verkeer bestaat bijvoorbeeld uit ICMP (gebruikt voor bijvoorbeeld *ping*), IGMP (gebruikt bij *multicasting* van games en videostreaming) en L2TP (gebruikt voor bijvoorbeeld *Virtual Private Lan)*.

GRAFIEK II: Aantallen *packet*s per verkeersstroom en megabytes, in logaritmische schaal



Data kan allerlei soorten internetverkeer bevatten. Doordat er fragmenten ontbreken, valt niet automatisch te analyseren welk protocol is gebruikt. Deze gegevens zijn wel leesbaar en daarmee bruikbaar voor verdere analyse.

DNS staat voor *domain name system*. DNS-servers maken op internet de vertaalslag van domeinnamen naar IP-adressen.

NNTP is het protocol dat gebruikt wordt om te lezen en bijdrages te posten in Usenet nieuwsgroepen.

NBNS staat voor netBIOS Name Service. Dit verkeer is afkomstig van computers met Windows als besturingssysteem waarop het netBIOS protocol draait in een TCP-IP netwerk.

E-mail bevat POP-verkeer, SMTP en IMAP.

Chat bevat IRC, Microsoft Messenger, Yahoo Messenger en Yabber.

3.2.1 E-Mail

In het leesbare e-mailverkeer zijn 98 unieke wachtwoorden aangetroffen. In het opgevangen e-mailverkeer is 56 keer een combinatie aangetroffen van loginnaam, wachtwoord en het IP-adres van de mailserver. Het gaat om mailservers van bekende providers in Nederland, zoals Caiway, Chello, KPN, Solcon, Tiscali, Versatel, Wanadoo, XS4ALL en Ziggo. Daarnaast zijn inloggegevens aangetroffen van mailservers die door meerdere domeinen kunnen worden gebruikt, waarmee dus alleen na uitzoekwerk ingelogd kan worden.

In het inkomende e-mailverkeer is inhoudelijke correspondentie aangetroffen. De aard van deze correspondentie is zeer divers. Dat e-mail in leesbare vorm kan worden opgevangen door derden komt omdat weinig providers de beveiligde versie aanbieden van de internetprotocollen om e-mail van de server op te halen (secure POP) of te verzenden (secure SMTP).

Het CBP heeft bijvoorbeeld twee opeenvolgende inkomende mails van een bank aangetroffen. De bank bevestigt een effectentransactie van een klant. De mails bevatten de voorletters, achternaam, het e-mailadres en het bankrekeningnummer van de betreffende persoon, met het te betalen bedrag.

De *payload data* bevat 32.862 *packets* met e-mailverkeer.[19] Omdat veel *packets* zowel het e-mailadres van een verzender en/of ontvanger bevatten als het (niet-publieke) IP-adres van de ontvanger, kunnen meerdere *packets* van 1 persoon aan elkaar worden gekoppeld, en kan op basis van meerdere *packets* van eenzelfde persoon een beeld worden opgebouwd met wie hij of zij correspondeert, op welke tijdstippen en over welke onderwerpen.

Een ander voorbeeld uit de *payload data* betreft de inbox van een klant van een webmail provider. Op basis van de timing van de e-mails, de adressen van de verzenders en vooral de onderwerpsregel valt een nauwkeurig beeld te reconstrueren van momenten uit het leven van deze betrokkene, zijn interesses en zijn loopbaanontwikkeling.

E-mailadressen

In totaal bevat de payload data 16.640 e-mailadressen waarvan een deel gefragmenteerd is opgevangen.[20] Het aantal volledig opgevangen e-mailadressen is 10.195 stuks. Het grootste deel hiervan, 5.890 (57,8%) eindigt op het toplevel domein .com.

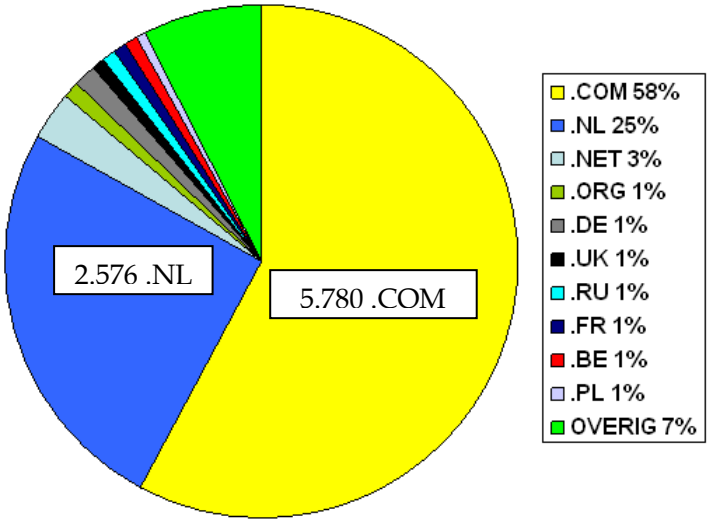
---

[19] Het CBP heeft het aantal e-mail *packets* als volgt geteld:
tshark -r tt-BIG-chunks_00000_20100810114607.pcap -R "pop || imap || tcp.port == 25 || tcp.port == 110" -w smtp_pop_imap_000.pcap && \
tshark -r tt-BIG-chunks_00001_20100810121956.pcap -R "pop || imap || tcp.port == 25 || tcp.port == 110" -w smtp_pop_imap_001.pcap && \
tshark -r tt-BIG-chunks_00002_20100810125505.pcap -R "pop || imap || tcp.port == 25 || tcp.port == 110" -w smtp_pop_imap_002.pcap && \
tshark -r tt-BIG-chunks_00003_20100810135058.pcap -R "pop || imap || tcp.port == 25 || tcp.port == 110" -w smtp_pop_imap_003.pcap && \
mergecap -w smtp_pop_imap.pcap smtp_pop_imap_000.pcap smtp_pop_imap_001.pcap smtp_pop_imap_002.pcap smtp_pop_imap_003.pcap && \
capinfos smtp_pop_imap.pcap.

[20] De gebruikte zoekopdracht is: "ngrep -I tt-fileset-1to20.pcap -q "[a-zA-Z0-9]+@[a-zA-Z0-9]+\....." | grep -Eirho '[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,4}' | sort | uniq"

Van de op .com eindigende e-mailadressen is ruim 55% uitgegeven door hotmail.com (Microsoft), 9% door gmail.com (Google), 5% door yahoo.com en 3% door msn.com (Microsoft). Van de .nl adressen is 25% uitgegeven door hyves.nl, 19% door Live.nl (Microsoft) en 3% door chat.spelpunt.nl.

GRAFIEK III Aantallen e-mailadressen per domein



3.2.2 Webverkeer

In de *payload data* zijn ook allerlei soorten webverkeer aangetroffen. Het webverkeer bevat bijvoorbeeld 137 herkenbare zoekopdrachten bij de Google zoekmachine.[21] Een aantal zoekopdrachten heeft betrekking op gevoelige gegevens.

"groene+poep+baby"
"hoeveel+weken+zwanger"
"thuiszorg+winkel+TWELLO"
"tinto+brass+posta+kutusu+18+porno"
"bruidsjurk+te+huur+in+amsterdam"
"<voornaam>+<achternaam>+<achternaam>"

Van elk van de personen die deze zoekopdrachten hebben gegeven, zijn meerdere *packets* opgevangen. Van de persoon die zocht naar de combinatie van postbusadres en een pornofilm van regisseur Tinto Brass zijn 944 *packets* vastgelegd. Uit dat verkeer blijkt dat deze persoon een aantal specifieke filmsites en weblogs heeft bezocht en via die sites een aantal erotische films heeft bekeken.

De laatst genoemde zoekopdracht betreft een unieke combinatie van voornaam, meisjesnaam en achternaam.[22] Deze combinatie leidt naar 1 persoon. Het is mogelijk dat deze persoon naar zichzelf heeft gezocht op internet, een zogenaamde *vanity search*.

[21] In de dataset is gericht gezocht op de term "www.google.nl/search?" Gekeken is naar de resultaten vanaf "?q=". De resultaten zijn vervolgens ontdubbeld.
[22] Door het CBP geanonimiseerde namen. Het origineel is beschikbaar in het onderzoeksdossier van het CBP.

Referrers
In het webverkeer zijn ook veel zogenaamde 'referrers' aangetroffen, de URL van de laatste webpagina die een persoon heeft bezocht. In totaal zijn er 3.354 verschillende adressen aangetroffen[23]. De referrers bevatten een groot aantal pagina's met titels die duiden op pornografie, dating en/of seksuele geaardheid. Daarnaast zijn ook enige pagina's aangetroffen met medische gegevens en pagina's gericht op bezoekers met een bepaald geloof en/of levensovertuiging. Er zijn ook twee pagina's aangetroffen waarop personen online konden solliciteren, my.monsterboard.nl en solliciteren.werkenbijdelandmacht.nl

Uit het onderzoek blijkt dat in het webverkeer 983 URL's voorkomen van profielpagina's bij de sociale netwerksite Hyves. Leden van Hyves hebben de mogelijkheid om hun profielpagina af te schermen tot alleen zelfgekozen vrienden. Leden kunnen daarmee verhinderen dat derden het bestaan van hun pagina achterhalen via externe of interne zoekmachines. Aangezien de gebruikers hun instellingen in de loop der tijd gewijzigd kunnen hebben, valt niet vast te stellen welk deel van deze URL's afgeschermd was toen Google het inhoudelijke internetverkeer opving.

Webverkeer overig
In het webverkeer zijn dertien mobiele telefoonnummers aangetroffen.

In het webverkeer zijn tevens twee met *malware* besmette computers aangetroffen, die openlijk hun SSID en de PSK key uitzonden. Met de combinatie van de SSID en de PSK key kan een kwaadwillende derde de beveiligingssleutel van een up-to-date beveiligde wifi-router (beveiligd met WPA2) invoeren en vervolgens al het verkeer meelezen. Dat er malware is geïnstalleerd blijkt ook uit de gebruikte poort voor het verzenden van verkeer: 34444.

3.2.3 NBNS

In de *payload data* zijn Word-documenten aangetroffen, in de categorie 'NBNS'. Onderdeel van het netBIOS verkeer is SMB-verkeer (*Server Message Block*), het netwerkprotocol dat gebruikt wordt in Microsoft Windows om bestandsuitwisseling tussen meerdere computers mogelijk te maken. Als deze bestandstuitwisseling via een (onbeveiligde) wifi-router verloopt, kunnen de bestanden in leesbare vorm door derden worden opgevangen.

In het NBNS verkeer is twee keer hetzelfde Word-document aangetroffen. Dit document is een uitgebreid psychologisch rapport over een minderjarige jongen met een ernstige leesachterstand. Het rapport bevat zijn voornaam, achternaam, adres en geboortedatum. Het rapport is gemarkeerd als 'vertrouwelijke gegevens'.[24]

3.2.4 Chat / MSN

In de *payload data* is ook chatverkeer aangetroffen. In het chatverkeer zijn zes mobiele nummers en één VOIP-nummer aangetroffen. Er zijn 187 *private messages* aangetroffen, tussen mensen onderling, in plaats van berichten die voor alle deelnemers aan de chat leesbaar zijn. 112 *private messages* zijn verzonden door deelnemers aan de website Spelpunt.nl.

In één chatbericht meldt een persoon "ik werk nu niet meer afgeke[u]rd". Een ander bericht meldt: "vinger zwaar gekneusd". Er zijn berichten waarin over (kop)pijn wordt gesproken.

[23] Het totale, niet ontdubbelde aantal *packets* is 18.606. De gebruikte zoekopdracht is: "ngrep -I tt-merged-1to20.pcap -q 'erer' | grep -Ehrio '...erer.+' | grep -Ehrio '\/\/.+\/' ".
[24] Het CBP heeft in het NBNS-verkeer gericht gezocht met trefwoorden als 'vertrouwelijk' en 'ziek'.

"jawel je weet hoe die shit werkt heh:P", gevolgd (van dezelfde persoon) door: "jawel maar ik werd vanochtend wakker met ontzettende koppijn". Drie andere personen schreven: "tis zo lekker maar je krijgt er zo'n koppijn van :P"; "pijn! dus sssssst." en "hoofdpijn,enzoo".

3.2.5 Overige bestanden

In de *payload data* zijn 16.456 beeld- en geluidsbestanden aangetroffen, zoals plaatjes of foto's in gif (8.534) en jpeg formaat (5.883), maar ook webbestanden (1.956 htm), 6 geluidsopnames (wav) en 3 filmpjes (avi en wmv). Uit nader onderzoek blijkt dat slechts weinig bestanden integraal zijn vastgelegd. Het grootste deel betreft fragmenten, zoals de onderste helft van een foto.

In het DNS-verkeer (*Domain Name System*) zijn veel zelfgekozen namen aangetroffen van apparatuur zoals PC's, laptops en iPhones. Dat kan een voornaam zijn (PC van Sanne), maar ook een combinatie van voornaam met achternaam, al dan niet in combinatie met het MAC-adres van het apparaat. In totaal heeft het CBP 12.554 unieke DNS-opdrachten aangetroffen.[25] Deze set bevat 2.205 keer (18%) een (unieke) voornaam of de combinatie van voornaam en achternaam, of een MAC-adres, al dan niet in combinatie, zoals PC_VAN_FAM<achternaam>, IPhone-van-<Voornaam>-<Achternaam>, MacBook van <voornaam> <achternaam>, iPod-van-<Voornaam>-<Achternaam,> iMac van <Voornaam> <Achternaam>, laptop van <voornaam> <achternaam> [MAC-adres], Computer van <Voornaam> <Achternaam> of iPhone-<MAC-adres>.[26]

In het FTP-verkeer zijn 7 login-namen aangetroffen, 2 unieke wachtwoorden en 1 keer de combinatie van loginnaam, wachtwoord en betreffende server.

Ten slotte zijn er 31 telefonie-conversaties aangetroffen via internet telefonie (sip, session initation protocol), bestaande uit 199 *packets*. De *packets* bevatten verkeersgegevens over het telefoonverkeer, wanneer en met wie (publiek IP adres) heeft getelefoneerd. De inhoud van de gesprekken is in alle gevallen versleuteld (middels sip-tls).

3.3 Gegevens over wifi-routers

Uit de schriftelijk ingewonnen inlichtingen blijkt dat Google van 4 maart 2008 tot 6 mei 2010[27] gegevens heeft verzameld over **3.606.579 verschillende wifi-routers**.[28] Van elk van deze routers heeft Google het unieke MAC-adres vastgelegd.

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*.

---

[25] Dit zijn de unieke, ontdubbelde queries. Het totale aantal niet-ontdubbelde DNS in de pcap bedraagt 97.220. Middels een zoekvraag is uit deze *packets* alleen de zogenaamde 'dns query' gehaald. Dat levert 96.436 *packets* op. Door te sorteren en te ontdubbelen is de dataset gereduceerd tot 14.816 *packets*. Ten slotte zijn de *packets* weggefilterd waarin het woord 'malformed' voorkomt en de uitdrukking 'standard query response unknown'. Er blijven dan 12.554 *packets* over.

[26] Door het CBP geanonimiseerde versies van de voornamen, achternamen en MAC-adressen. De originelen zijn beschikbaar in het onderzoeksdossier van het CBP.

[27] 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.

[28] E-mail van Google van 12 juli 2010, bijlage gedateerd 9 juli 2010, blz. 1.

Een voorbeeld van een MAC-adres is: <mac-adres>. Het MAC-adres van een wifi-router (een internet access point) wordt BSSID genoemd.[29]

Google heeft dit unieke nummer vastgelegd van zowel beveiligde als onbeveiligde wifi-routers. Tevens heeft Google van elke wifi-router de signaalsterkte vastgelegd, in veel gevallen de netwerknaam, en heeft hij voor elke wifi-router een locatie berekend.

Per 1 januari 2009 telde Nederland 16.485.787 inwoners, woonachtig in 7.312.579 huishoudens. Daarnaast telde Nederland op dat moment ruim 900.000 bedrijven. Op 1 januari 2009 waren er in Nederland 5,73 miljoen breedband aansluitingen, ofwel bijna 35 aansluitingen per 100 inwoners.[30]

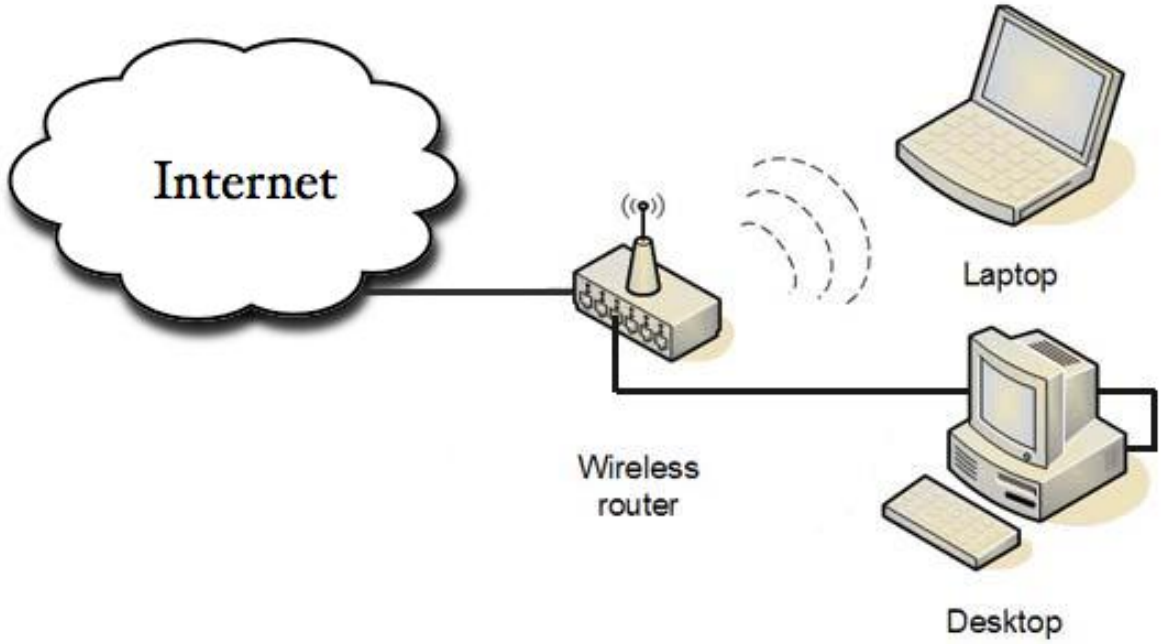
Zelfs als gemakshalve wordt aangenomen dat alle huishoudens en bedrijven met een breedbandaansluiting over een wifi-router beschikken,[31] dan nog heeft Google over bijna 63% van de huishoudens en bedrijven met breedbandinternet in Nederland gegevens verzameld.[32]

[VERTROUWELIJK: aantallen door Google verzamelde MAC-adressen van wifi-routers per provincie]

Google stelt niet te hebben bijgehouden wanneer (in welke maand, jaar) de Wifi-gegevens precies zijn verzameld en of er meer dan 1 keer per provincie door de Street View auto's is gereden.[33]

Het zeer grote aantal wifi-routers dat Google heeft kunnen registreren kan verklaard worden uit de wijze waarop wifi-routers hun bestaan bekend maken. De meeste breedbandrouters hebben standaard ook een wifi-antenne. De standaardinstelling van de meest gebruikte routers in Nederland is dat deze wifi-verbinding 'aan' staat, ook als de gebruiker zijn computer(s) alleen via vaste kabels met de router heeft verbonden en ook als de gebruiker de inhoudelijke draadloze communicatie beveiligd heeft met WEP, WPA of WPA2. Vergelijkbaar met een radio zendt de wifi-router voortdurend zijn eigen netwerknaam en zijn MAC-adres uit, ook als er niemand van de verbinding gebruikt maakt.

[29] Uit het Stroz Friedberg rapport blijkt dat er meerdere adresvelden zijn om MAC-adressen op te slaan. Welk MAC-adres het unieke hardware adres is van de router (en dus niet van een ander wifi-geschikt communicatie-apparaat zoals een iPhone, desktop computer of laptop), is per *packet* afhankelijk van de instelling van het FromDS en het ToDS veld.
[30] Bron: OPTA marktmonitor 2009, URL: http://www.opta.nl/nl/download/bijlage/?id=545 en Telecompaper, 'Dutch broadband market to reach six million in 2009', 11 juni 2009, URL: http://www.telecompaper.com/news/article.aspx?cid=675788
[31] Er zijn bij het CBP geen cijfers of onderzoeken bekend over de aantallen wifi-routers in relatie tot het aantal breedbandaansluitingen in Nederland per 1 januari 2009. De aanname van 100% bezit van wifi-router is ongetwijfeld te hoog ingeschat, maar compenseert voor het feit dat er ook huishoudens en bedrijven zijn met meer dan 1 router en dat sommige routers misschien vervangen zijn in de periode van twee jaar dat Google deze gegevens heeft verzameld met zijn Street View auto's.
[32] Over 62,9% van alle huishoudens en bedrijven per 1 januari 2009.
[33] E-mail van Google van 12 juli 2010, bijlage, blz. 2.



Een gebruiker moet een bewuste keuze maken om de netwerknaam van de router te verbergen, dat wil zeggen, om de zogenaamde *beacon frame* uit te zetten. De beacon frame stuurt voortdurend korte signalen in de ether met de naam van het netwerk en het MAC-adres van de router, het BSSID. Gebruikers die hun SSID verbergen door de *beacon frame* uit te zetten, doen dat vaak uit veiligheidsoverwegingen, om te voorkomen dat buren of passanten toegang krijgen tot het netwerk. Een gebruiker kan daarmee evenwel niet voorkomen dat de netwerknaam, het MAC-adres en de signaalsterkte van de router toch worden opgevangen door derden en/of vastgelegd door derde partijen als Google. De netwerknaam en het BSSID zijn namelijk niet alleen opgenomen in de *beacon frame* maar ook in een aantal andere management frames.[34]

Google stelt: "*Zoals dat wordt uitgelegd in het Stroz Friedberg rapport: "[t]he gslite program parses and stores the SSID information for all wireless networks, whether the SSID is broadcast or not." (P. 12, para. 52.b.). Dit is gedaan omdat ook in het geval dat een netwerk is ingesteld om geen SSID uit te zenden als onderdeel van de beacon frames, de 802.11 standaard nog steeds kan vereisen dat de SSID wordt inbegrepen in andere draadloze data frames (die publiekelijk worden uitgezonden en daardoor worden ontvangen en opgeslagen door de gslite programmatuur), niettegenstaande de netwerkinstelling om de SSID te "verbergen"*.[35]

Een gebruiker die wil voorkomen dat het SSID van zijn wifi-router wordt opgevangen door derden, kan dus niet volstaan met het uitzetten van de *beacon frame*. Immers, zodra er communicatie plaatsvindt via de antenne van de wifi-router, kan een derde partij uit alle frames de naam opvangen van de wifi-router en de signaalsterkte.

[34] SSID zit in het management frame, dat diverse subtypen kent. Een van die subtypen is Beacon. Andere zijn: Association Request, Association Response, Reassociation Request, Reassociation Response, Probe Response en Probe Request. In deze laatste zes typen is het SSID altijd zichtbaar.
[35] Brief van Google van 8 juni 2010, bijlage, blz. 3.

Uit de schriftelijk ingewonnen inlichtingen blijkt dat Google bij elk ontvangen wifi-signaal op de harde schijf in de auto 18 eigenschappen *over* de wifi-routers heeft opgeslagen.[36] Van deze gegevens worden er 8 verder verwerkt door het bedrijf.[37] Dit zijn:

- Latlon gegevens
- MAC-adres
- SSID
- tijd per seconde
- tijd per micro-seconde
- signaalsterkte
- error flags
- kanaal

Latlon gegevens zijn plaatsbepalingsgegevens afkomstig van GPS-satellieten (Global Positioning System), uitgedrukt in lengte- en breedtegraad. Google heeft de GPS lengte en breedtegraden in 32bits getallen opgeslagen, het equivalent van 7 cijfers achter de komma. De latlon gegevens betreffen de positie van de auto op de momenten dat een wifi-signaal wordt opgevangen.

SSID staat voor *Service Set Identifier* en duidt op de leesbare netwerknaam van de wifi-router. Die naam kan standaard ingesteld zijn door de fabrikant of routerverkoper (zoals 'Linksys' of 'SpeedtouchBFCB8F'), maar gebruikers kunnen ook zelf een naam geven aan hun draadloze netwerk, zoals 'netwerk van Piet Smit' of 'Jansenstraat 10 2 hoog'.

Signaalsterkte is de reikwijdte van de signalen die wifi-routers uitzenden. Hoe sterker het signaal, hoe verder het kan worden opgevangen. Voor de meeste verkochte wifi-routers in Nederland (volgens de IEEE 802.11b en 802.11g standaard) wordt een bereik aangehouden van circa 30-40 meter binnenshuis en 90-95 meter buitenshuis.[38]

Kanaal is de frequentie in Megaherz waarop de wifi-router signalen zendt. Normaal gesproken beschikken wifi-routers over 14 verschillende kanalen.[39] Een gebruiker kan ervoor kiezen om een ander kanaal in te stellen dan standaardkanaal nr. 6 als er bijvoorbeeld interferentie optreedt met andere apparaten in de buurt die op dezelfde frequentie uitzenden, zoals andere routers, magnetrons of draadloze telefoons.

Van elk BSSID kunnen meerdere *latlon* gegevens zijn opgeslagen, afhankelijk van de sterkte van het uitgezonden signaal en de afstand van de Street View auto tot de betreffende router. [VERTROUWELIJK: technische werkwijze locatiebepaling wifi-routers]

[36] E-mail van Google van 22 juli 2010, bijlage, blz. 9-10. Zie ook: Stroz Friedberg, blz 21, overzicht van de Kismet metadata.
[37] Google stelt de volgende eigenschappen niet te gebruiken: carrier encoding, data rate, adapter ID, signal quality, noise level, header length, drone version, data length en capture length.
[38] Bronnen: About.com, 'What Is the Typical Range of a Wi-Fi LAN?, URL: http://compnetworking.about.com/cs/wirelessproducts/f/wifirange.htm, Fon Wikibeta, Range/nl, URL: http://wiki.fon.com/wiki/Range/nl (laatst bezocht 27 augustus 2010).
[39] De wifi-standaard is gedefinieerd in IEEE 802.11. In Nederland zullen de meeste routers gebruik maken van de 802.11b en 802.11g standaard, in het 2.4 Ghz bereik. Deze standaarden verdelen het spectrum in 14 kanalen. In Europa zijn de kanalen 1 tot 13 toegestaan.

Google heeft de gegevens over de wifi-routers die met de Street View auto's zijn verzameld opgeslagen op servers in de Verenigde Staten. Deze servers bevatten de BSSIDs (MAC-adressen van routers), in veel gevallen de SSID (netwerknaam) van de router, RSSI (de signaalsterkte) en het kanaal waarover de router heeft uitgezonden. In de Google geolocatieserver (hierna: Google GLS) is het MAC-adres opgeslagen in combinatie met de zo nauwkeurig mogelijk berekende locatie van de wifi-router. [VERTROUWELIJK: gegevens die Google gebruikt voor de locatiebepaling van wifi-routers]

Google heeft op de harde schijven in de Street View auto's niet alleen de MAC-adressen vastgelegd van de wifi-routers (de BSSID's), maar ook alle andere MAC-adressen van apparatuur die met de wifi-router communiceerde op het moment dat de auto langsreed, zoals desktop computers, laptops en andere wifi-geschikte communicatieapparaten zoals iPhones. Uit het onderzoek blijkt dat Google al deze andere MAC-adressen heeft bewaard. Dat blijkt uit een door Google verstrekte berekening van het aantal MAC-adressen die BSSID's zijn van wifi-routers, rekening houdend met de aard van het MAC-adres, ofwel ontvanger ofwel verzender (zie voetnoot 33). De verzameling en verwerking van deze 'andere' MAC-adressen valt buiten de scope van dit onderzoek.

Hoewel Google kort na 7 mei 2010 gestopt is met het verzamelen van Wifi-gegevens via de Street View auto's, verzamelt Google dagelijks doorlopend nieuwe BSSID's via de talloze internetgebruikers die met een mobiel wifi-geschikt apparaat een beroep doen op de Google GLS. Gebruikers van moderne smartphones geven daarbij vaak de exacte GPS-gegevens mee van hun eigen locatie. Dit blijkt uit specifieke privacy-verklaringen van Google, gericht op gebruikers van zijn geolocatiediensten. Zie paragraaf 3.4 van dit rapport. Dit doorlopend verzamelen van MAC-adressen van wifi-routers en verfijnen van de plaatsbepaling van de wifi-routers valt buiten de scope van dit onderzoek.

Google biedt derde partijen kosteloos toegang tot de gegevens in de Google GLS via de zogenaamde *Google Geo Location API.* Een derde partij als Twitter maakt hier volgens Google gebruik van. Gebruikers van Twitter kunnen met behulp van de Google GLS automatisch een precieze plaats toevoegen aan hun berichten om die berichten van context te voorzien.[40] Ook de browsers Firefox en Chrome hebben de Google GLS als standaard geolocatieserver ingesteld, zodanig dat derde partijen via de browser de locatie van de gebruiker kunnen opvragen.

Google stelt dat via de Google GLS en de API geen precieze informatie wordt verstrekt over het netwerk, alleen een plaatsbepaling: *"De GLS en de locatie gebaseerde diensten van Google maken de SSID en MAC adressen of andere netwerk informatie die gerelateerd is aan een WiFi toegangspunt, niet openbaar (een apparaat van een gebruiker kan deze informatie wel onafhankelijk detecteren)(...)."*[41]

Iedereen kan deze plaatsbepalingsdienst gebruiken, ofwel door zelf software te installeren die Google kosteloos ter beschikking stelt of door het intypen van een MAC-adres op de website van een derde partij die deze software heeft geïnstalleerd op zijn server. De Google GLS toont vervolgens als resultaat een berekende locatie voor die wifi-router.

[40] Google, 'Data collected by Google cars', 27 april 2010, URL: http://googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html
[41] Brief van Google van 8 juni 2010, bijlage, blz. 4.

Het CBP heeft in de *payload data* gezocht naar MAC-adressen en 75 stuks aangetroffen van waarschijnlijke printservers.[42] Dergelijke printservers vormen een onderdeel van het wifi-netwerk, en worden gebruikt als twee mensen in een gezin bijvoorbeeld draadloos van dezelfde printer gebruik willen maken. De printserver zendt dezelfde signalen uit als een wifi-router. Daarom zijn dergelijke printservers ook opgeslagen in de Google GLS als internet *access points.*

Het CBP heeft deze 75 MAC-adressen ingevoerd in de Google GLS en als antwoord voor 45 van deze MAC-adressen een berekende locatie gekregen.[43] Het CBP heeft elk van deze 45 locaties nader bekeken op satellietniveau (via Google Maps) en onderzocht hoeveel huizen het maximaal betrof. Dat varieert van 1 boerderij in Overijssel tot maximaal 65 appartementen in een woonwijk in Helmond. Het gemiddelde aantal woningen of appartementen per MAC-adres is 8. De onderzochte MAC-adressen blijken verspreid over heel Nederland, zowel afkomstig uit plattelandsgebieden als uit steden. Daarmee biedt deze set een representatief beeld van de nauwkeurigheid van de plaatsbepaling van de wifi-routers. Zie **bijlage III** voor een plattegrond van de onderzochte MAC-adressen.

Verkregen gegevens over MAC-adres <x[44]> via Google Maps API

"latitude":51.8579504
"longitude":4.5237314
"country":"The Netherlands"
"country_code":"NL"
"region":"South Holland"
"city":"Barendrecht"
"street":"Serenadelaan"
"street_number":"<x[47]>"
"postal_code":"2992"
"accuracy":36.0

Volgens de Google GLS woont de gebruiker van de printserver met dit MAC-adres in de Serenadelaan in Barendrecht, tussen de huisnummers <x[47]>.

De plaatsbepaling van dit MAC-adres heeft volgens de GLS een nauwkeurigheid ("accuracy") van 36 meter.

[42] De gebruikte zoekopdracht is: "ngrep -q -I tt-merged-1to20.pcap 'mac=' > tt-mac-1.out $ cat tt-mac-1.out | grep -Erhio 'x-hp-mac=.....' | sort | uniq"
[43] Van de 75 MAC-adressen bleken er 30 onbekend in de Google GLS.
[44] Door het CBP geanonimiseerde versie van het MAC-adres. Het origineel is beschikbaar in het onderzoeksdossier van het CBP.

Via Google Maps kunnen de lengte- en breedtegraad grafisch worden weergegeven. Ingezoomd op de combinatie van kaart en satellietgegevens blijkt dat het bij benadering gaat om twee rijtjes huizen in een woonwijk in Barendrecht.[45] Het betreft maximaal 9 verschillende zelfstandige huizen.

Andere MAC-adressen in de door het CBP onderzochte set hebben volgens de GLS een nauwkeurigheid ("accuracy") van 24 meter.[46]

Verkregen gegevens over MAC-adres <x[47]> via Google Maps API

"latitude": <x[47]>
"longitude": <x[47]>
"country":"The Netherlands"
"country_code":"NL"
"region":"Overijssel"
"city":"Losser"
"street":"<x[47]>"
"street_number":"<x[47]>"
"postal_code":"7587"
"accuracy":24.0

Door in te zoomen op de lengte- en breedtegraad in Google Maps blijkt dat het om één boerderij gaat (met stal) in een ruraal gebied in Overijssel.

[45] Het CBP heeft gebruik gemaakt van de website http://samy.pl/mapxss/.
[46] 13 van de 45 MAC-adressen hebben een nauwkeurigheid van 24 meter, de overigen van 36 meter.
[47] Door het CBP geanonimiseerde versie. Het origineel is beschikbaar in het onderzoeksdossier van het CBP.

<Afbeelding[48]>

Verkregen gegevens over MAC-adres <x[48]> via Google Maps API

"latitude":52.2108823
"longitude":5.1808856
"country":"The Netherlands"
"country_code":"NL"
"region":"North Holland"
"city":"Hilversum"
"street":"Diependaalselaan"
"street_number":"<x[48]>"
"postal_code":"1213"
"accuracy":36.0

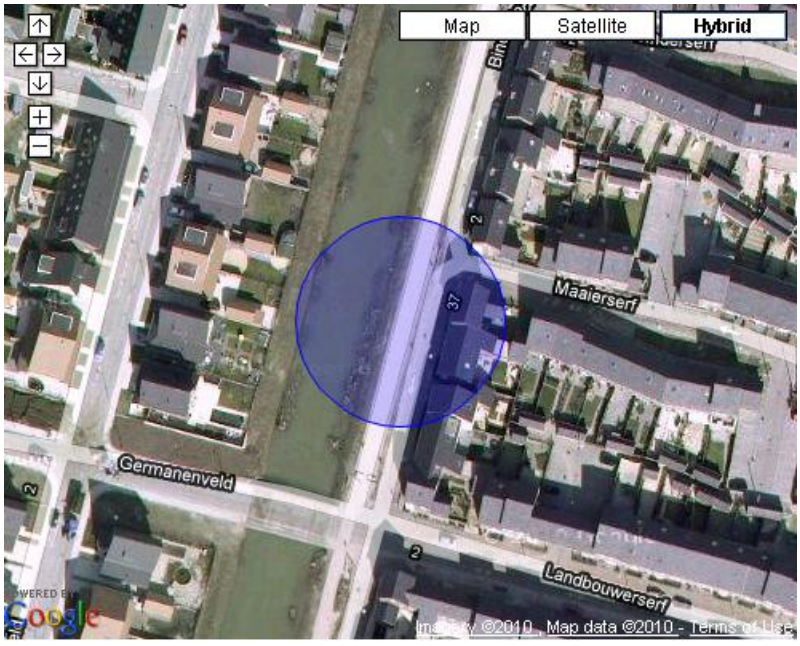
Uit dit voorbeeld blijkt dat de nauwkeurigheid van de plaatsbepaling niet beperkt is tot plattelandsgebieden. Ook in Hilversum blijken er 3 huizen aanwijsbaar te zijn als adres van het betreffende internet access point.

[48] Idem.

Dezelfde nauwkeurigheid, tot op 3 huizen, geldt voor een MAC-adres in Arnhem.

Verkregen gegevens over MAC-adres <x[49]> via Google Maps API

"latitude":51.9477717
"longitude":5.848366
"country":"The Netherlands"
"country_code":"NL"
"region":"Gelderland"
"city":"Arnhem"
"street":"<x[49]>"
"street_number":"<x[49]>"
"postal_code":"6846"
"accuracy":24.0



Op basis van de signaalsterkte van de wifi-router kan vervolgens het precieze adres worden bepaald waar de wifi-router zich bevindt. Google kan dat zelf, vanachter zijn eigen burelen doen, mede met behulp van andere gegevens waarover Google beschikt, waaronder de nieuwe gegevens over wifi-routers die Google voortdurend ontvangt van de gebruikers van zijn geolocatiediensten.

Derde partijen kunnen eveneens het precieze adres achterhalen, door met behulp van een smartphone of laptop rond te lopen in de buurt waar de wifi-router zich volgens de Google GLS ongeveer bevindt (gemiddeld 8 huizen). Er zijn gratis applicaties voor smartphones en er is allerlei gratis software voor laptops waarmee de signaalsterkte op een grafische manier in beeld wordt gebracht, in de vorm van balken of in de vorm van een radarscherm. Omdat de gebruiker de signaalsterkte ziet in combinatie met het MAC-adres en de netwerknaam, kan het precieze apparaat makkelijk herkend en gelokaliseerd worden. Hoe dichter de gebruiker in de buurt komt van het precieze huis waar de wifi-router zich bevindt, hoe sterker de signaalsterkte.

[49] Idem.

Peilingen met behulp van deze applicaties/software zijn eenvoudig, consistent en reproduceerbaar.[50]

3.4 Informatie

Op 22 april 2010 maakten twee Duitse toezichthouders op de bescherming van persoonsgegevens (de toezichthouder van Hamburg en de federale Duitse toezichthouder) bekend dat Google met de Street View auto's Wifi-gegevens verzamelde.[51] Op 27 april 2010 maakte Google bekend dat met de Street View auto's gegevens over wifi-netwerken werden verzameld.[52] Het bedrijf stelde toen alleen gegevens *over* (het bestaan van) wifi-netwerken te verzamelen. De verzameling van gegevens met betrekking tot wifi-netwerken zou beperkt zijn tot MAC-adressen en SSID's (netwerknamen). Het bedrijf stelde expliciet géén *payload data* te verzamelen, d.w.z. inhoudelijke communicatiegegevens afkomstig uit wifi-routers. "*However, all data payload from data frames are discarded, so Google never collects the content of any communications.*"[53]

Op 14 mei 2010 maakte Google bekend dat hij bij het verzamelen van gegevens over wifi-netwerken wel *payload data* had opgenomen en bewaard.[54] Het bedrijf was op 5 mei 2010 om inzage gevraagd door de Hamburgse toezichthouder in de verzamelde gegevens, en Google verklaarde dat het op dat moment ontdekte dat toch inhoudelijke gegevens waren bewaard. "*Nine days ago the data protection authority (DPA) in Hamburg, Germany asked to audit the WiFi data that our Street View cars collect* (...). [We said] *we did not collect payload data (information sent over the network). But it's now clear that we have been mistakenly collecting samples of payload data from open (i.e. non-password-protected) WiFi networks, even though we never used that data in any Google products*."[55] Google deelde voorts mee dat het bedrijf gestopt was met het verzamelen van (alle soorten) Wifi-gegevens via zijn Street View auto's. "*In addition, given the concerns raised, we have decided that it's best to stop our Street View cars collecting WiFi network data entirely.*" Google vermeldde daarbij niet dat het bedrijf doorlopend gegevens over wifi-routers verzamelt via de gebruikers van zijn geolocatiediensten.

Na een verzoek van de Ierse toezichthouder op de bescherming van de persoonsgegevens om alle in Ierland verzamelde *payload data* te vernietigen, heeft Google opdracht gegeven aan een Amerikaans beveiligingsbedrijf om toe te zien op het scheiden van de *payload data* van de overige gegevens *over* wifi-netwerken. De *payload data* zijn vervolgens in een aparte map per land

---

[50] Zie de whitepaper 'Converting Signal Strength Percentage to dBm Values' van het Amerikaanse bedrijf WildPackets, Inc. uit 2002, URL: http://www.wildpackets.com/elements/whitepapers/Converting_Signal_Strength.pdf en het artikel 'Modeling Signal Attenuation in IEEE 802.11Wireless LANs - Vol. 1' (juli 2005) van informatica-student Daniel B. Faria van de Amerikaanse Stanford Universiteit.

[51] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 'Google-Street-View-Fahrten werden auch zum Scannen von WLAN-Netzen genutzt', persbericht 22 april 2010, URL: http://www.bfdi.bund.de/cln_136/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2010/GoogleWLANScanning.html

[52] Bron: Google, 'Data collected by Google cars', 27 april 2010, URL: http://googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html. Google schrijft: "*This blog also addresses concerns raised by data protection authorities in Germany.*"

[53] Bron: Google, 'Copy of Google's submission today to several national data protection authorities on vehicle-based collection of wifi data for use in Google location based services', 27 April 2010, blz. 2-3, URL: http://www.google.com/googleblogs/pdfs/google_submission_dpas_wifi_collection.pdf

[54] Bron: Google, 'WiFi data collection: An update', 14 mei 2010, URL: http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html

[55] Idem.

opgeslagen op servers in Californië en North Carolina in de Verenigde Staten. Google heeft deze verklaring op 17 mei 2010 gepubliceerd in zijn weblog.[56]

De Google webpagina's over Street View, inclusief een privacy-verklaring, en de Google algemene privacy-verklaring bevatten geen concrete informatie over het verwerken van gegevens *over* wifi-routers.[57] In zijn algemene privacy-verklaring informeert Google gebruikers niet over het feit dat Google bij het algemene publiek gegevens over wifi-routers heeft verzameld. Google stelt dat alleen bij het *gebruik* van locatiediensten telefonie-gegevens van *gebruikers* van deze diensten worden verwerkt, zoals GPS en de mastgegevens van de mobiele operators:

Location data – Google offers location-enabled services, such as Google Maps for mobile. If you use those services, Google may receive information about your actual location (such as GPS signals sent by a mobile device) or information that can be used to approximate a location (such as a cell ID).

Google heeft daarnaast een groot aantal aparte privacy-verklaringen voor verschillende diensten. Deze clausules zijn ook weer gericht op specifieke afnemers van bepaalde Google producten of diensten en niet op het algemene publiek waarvan Google de gegevens over wifi-routers heeft verzameld. De privacy-verklaringen voor de door Google zelf ontwikkelde browser Chrome bevat sinds 9 mei 2010 de volgende passage over geolocatiediensten:

If you use Google Chrome's location feature which allows you to share your location with any site, Google Chrome will send local network information to Google Location Services to get an estimated location. The local network information includes, depending on the capabilities of your device, information about the wifi routers closest to you, cell ids of the cell towers closest to you, the strength of your wifi or cell signal, and information about your device such as your device's IP address. We use the information to process the location request and to operate, support, and improve the overall quality of Google Chrome and Google Location Services. Information collected above will be anonymized and aggregated before being used by Google to develop new features or products and services, or to improve the overall quality of any of Google's other products and services.[58]

Ten slotte heeft Google een aparte privacy-verklaring over het gebruik van geolocatiediensten in de browser Firefox. In deze verklaring wordt het gebruik van wifi-routers als volgt genoemd:

Information we collect
• If you allow a website to get your location via this service, we will collect, depending on the capabilities of your device, information about the wifi routers closest to you, cell ids of the cell towers closest to you, and the strength of your wifi or cell signal. We use this information to return an estimated location to the Firefox browser and the Firefox browser sends the estimated location to the requesting website. For each request sent to our service, we also collect IP address, user agent information, and unique identifier of your client. We use this information to distinguish requests, not to identify you.

---

[56] Bron: Google, 'WiFi data collection: An update', update van 17 mei 2010 met hyperlink naar http://www.google.com/press/pdf/ISEC_Letter.pdf. Dit is een verklaring van het Amerikaanse beveiligingsbedrijf iSEC Partners Inc. dat de gegevens op 15 en 16 mei 2010 gescheiden zijn.
[57] Bron: Google, Nederlandstalige privacy-verklaring bij Street View, URL: http://maps.google.com/intl/nl/help/maps/streetview/privacy.html. Algemene Nederlandstalige privacy-verklaring van Google (laatst gewijzigd 11 maart 2009), URL: http://www.google.nl/intl/nl/privacypolicy.html
[58] Bron: Google, Chrome Privacy Notice, 4 mei 2010, URL: http://www.google.com/chrome/intl/en/privacy.html. NB! deze informatie was nog niet aanwezig in de privacy-verklaringvan 9 februari 2010.

Uses
• We use all the information above to process the Firefox geolocation requests. We also use all the information above to operate, support, and improve the overall quality of the Google Location Service[59].

In deze informatie, gericht op de specifieke doelgroep van gebruikers van deze browsers voorzover zij geolocatiediensten gebruiken, bevestigt Google dat het bedrijf beschikt over een database met locaties van wifi-routers. Het bedrijf geeft bovendien aan doorlopend nieuwe MAC-adressen te verwerken in combinatie met signaalsterkte.

De melding die Google bij het CBP heeft gedaan op 4 februari 2010 voor de dienst Street View, onder nummer m1426715, beschrijft alleen de verwerking van foto's. Als verantwoordelijke is Google Inc. aangewezen, gevestigd in Mountain View, Californië, in de Verenigde Staten.

De melding bevat geen informatie over het verwerken van Wifi-gegevens. Google heeft geen andere meldingen gedaan bij het CBP.

3.5 Doeleinden verwerking

3.5.1 Doeleinden verwerking payload data

Volgens Google is de software per ongeluk ingesteld op het opvangen van de inhoudelijke communicatie uit onbeveiligde wifi-netwerken.[60] Google verklaart: "*Google heeft payload data niet gebruikt in enig Google product of dienst en heeft geen WiFi informatie die is verzameld door middel van de Street View auto's gebruikt voor profileringactiviteiten gericht op individuele eindgebruikers.*"[61]

3.5.2 Doeleinden verwerking gegevens over wifi-routers

Uit de schriftelijk ingewonnen inlichtingen blijkt dat Google gegevens *over* (het bestaan van) wifi-routers gebruikt om via een geolocatie server plaatsbepalingsdiensten aan te bieden aan gebruikers van mobiele communicatieapparatuur (laptops of GSM's) en ten behoeve van route navigatie. Google stelt niet voornemens te zijn om een database te publiceren van MAC-adressen, SSID's en hun berekende locatie.[62]

4. Beoordeling

4.1 Verantwoordelijke

[59] Bron: Google, Google Location Service in Mozilla Firefox Privacy Policy, 24 april 2009, URL: http://www.google.com/privacy-lsf.html
[60] Google schrijft: *So how did this happen? Quite simply, it was a mistake. In 2006 an engineer working on an experimental WiFi project wrote a piece of code that sampled all categories of publicly broadcast WiFi data. A year later, when our mobile team started a project to collect basic WiFi network data like SSID information and MAC addresses using Google's Street View cars, they included that code in their software – although the project leaders did not want, and had no intention of using, payload data.* Bron: http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html (originele blogposting van 14 mei 2010).
[61] Brief van Google van 8 juni 2010, bijlage, blz. 8.
[62] Idem. Google schrijft: "*Google publiceert de WiFi netwerk informatie die zij heeft verzameld met de Street View auto's niet en heeft daarvoor ook geen plannen.*"

Op grond van artikel 1, onder d, Wbp is de verantwoordelijke *de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt*.

Artikel 4, derde lid, Wbp bepaalt: *Het is een verantwoordelijke als bedoeld in het tweede lid, verboden persoonsgegevens te verwerken, tenzij hij in Nederland een persoon of instantie aanwijst die namens hem handelt overeenkomstig de bepalingen van deze wet. Voor de toepassing van deze wet en de daarop berustende bepalingen, wordt hij aangemerkt als de verantwoordelijke.*

Google Inc, gevestigd in Mountain View, Californië in de Verenigde Staten, heeft de doeleinden vastgesteld voor de verwerking van gegevens over wifi-routers. Google Inc. heeft tevens de middelen vastgesteld om deze gegevens te verzamelen. Uit de schriftelijk ingewonnen inlichtingen blijkt dat Google Inc. contracten heeft gesloten met de Nederlandse vestiging van een internationaal uitzendbureau om de chauffeurs in te huren voor de Street View auto's. Tevens blijkt dat Google Inc. verantwoordelijk is voor de apparatuur en programmatuur om de gegevens te verzamelen en verder te verwerken. Google Netherlands B.V. is opgetreden als lokaal vertegenwoordiger van Google Inc., conform artikel 4, derde lid, Wbp. Google Inc. is daarmee verantwoordelijke in de zin van artikel 1, onder d, Wbp, zoals lokaal vertegenwoordigd door Google Netherlands B.V.

In zijn zienswijze op de voorlopige bevindingen van het CBP stelt Google geen verantwoordelijke te zijn conform artikel 1, onder d, Wbp voor het verzamelen van gegevens *over* en *afkomstig uit* wifi-routers. Google geeft een verschillend argument voor de twee verwerkingen.

Google zou niet verantwoordelijk zijn voor het verzamelen van de gegevens *over* wifi-routers omdat dit geen persoonsgegevens zijn. Dit argument kan niet worden aanvaard, omdat, zoals hierna wordt beargumenteerd, gegevens over wifi-routers persoonsgegevens zijn.

Google stelt voorts in zijn zienswijze dat hij evenmin als verantwoordelijke kan worden beschouwd voor het verzamelen van de persoonsgegevens in de *payload data* omdat het bedrijf tot mei 2010 niet op de hoogte was van, en geen doel had met, het verzamelen van deze gegevens. "*Google stelt zich op het standpunt dat het voor een organisatie onmogelijk is een verantwoordelijke te zijn indien er door die organisatie met het verwerken van de persoonsgegevens geen doel wordt nagestreefd.*"[63]

Google lijkt te impliceren dat een partij niet verantwoordelijk is zolang die partij geen duidelijk doel bepaalt voor het verzamelen van gegevens. Daarmee zou de toepasselijkheid van de wet afhankelijk zijn van bewustzijn of intenties. Dat is niet het geval. Het wettelijke begrip 'verantwoordelijke' moet objectief worden bezien, niet subjectief.

Het gaat in deze context niet om een eenmalig incident, maar om het systematisch, gedurende twee jaar in Nederland (en elders in de wereld) opvangen en vastleggen van vertrouwelijke communicatiegegevens uit onbeveiligde wifi-routers. Het 'niet weten' dat er op dergelijke grote schaal en langdurig gegevens worden verzameld, is een gevolg van de wijze waarop Google zijn bedrijfsvoering heeft ingericht, dat wil zeggen, doel en middelen voor de gegevensverwerking door de organisatie heeft bepaald. Google heeft, door zijn bedrijfsvoering op deze wijze in te richten, willens en wetens de mogelijkheid aanvaard dat gegevens worden verzameld zonder duidelijk bepaald doel.

[63] Zienswijze Google, paragraaf 77, blz. 26.

Voorts zijn de persoonsgegevens verzameld en verwerkt in de georganiseerde activiteit van het rondrijden met Street View auto's, heeft Google het personeel ingehuurd dat de auto's bestuurde en heeft Google de auto's op zodanige wijze technisch toegerust dat *payload data* konden worden verzameld en vastgelegd. Ten aanzien van deze activiteit heeft Google doel en middelen vastgesteld.

4.2 Rechtsmacht

Artikel 4, tweede lid, Wbp bepaalt:

2. Deze wet is van toepassing op de verwerking van persoonsgegevens door of ten behoeve van een verantwoordelijke die geen vestiging heeft in de Europese Unie, waarbij gebruik wordt gemaakt van al dan niet geautomatiseerde middelen die zich in Nederland bevinden, tenzij deze middelen slechts worden gebruikt voor de doorvoer van persoonsgegevens.

Het staat vast dat Google Inc. geen vestiging heeft (aangewezen) in de Europese Unie. Google Inc. heeft op Nederlands grondgebied gegevens verzameld met betrekking tot wifi-netwerken met gebruikmaking van in Nederland rondrijdende auto's en middelen waaronder apparatuur. Het betreft hier "al dan niet geautomatiseerde middelen" waarmee persoonsgegevens worden verwerkt zoals bedoeld in artikel 4, tweede lid, Wbp. De Wbp is derhalve van toepassing op de verwerking van persoonsgegevens *over* en *afkomstig uit* wifi-routers door Google Inc. in de Verenigde Staten, zoals lokaal vertegenwoordigd door Google Netherlands B.V.

4.3 Persoonsgegevens

Volgens artikel 1, aanhef en onder a, Wbp wordt onder een persoonsgegeven verstaan: *elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon*. 'Verwerking' van persoonsgegevens is gedefinieerd in artikel 1, onder b, Wbp en omvat onder meer het vastleggen, verzamelen en bewaren van persoonsgegevens.

Ingevolge de memorie van toelichting bij de Wbp moeten als persoonsgegevens worden beschouwd "*alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon*".

Ook gegevens die niet betrekking hebben op een bepaalde persoon, maar bijvoorbeeld op een product of een proces, kunnen soms informatie verschaffen over een bepaalde persoon. In de memorie van toelichting[64] worden in dit verband telefoonnummers, kentekens van auto's en postcodes met huisnummers genoemd.

Niet is vereist dat iedere mogelijkheid de gegevens met betrekking tot personen te gebruiken, is uitgesloten. Is deze mogelijkheid weliswaar theoretisch aanwezig maar is ondenkbaar dat dit ook daadwerkelijk gebeurt, dan kan ervan worden uitgegaan dat de gegevens niet als persoonsgegevens worden aangemerkt. De wetgever merkt in dit verband expliciet op: "*Indien het daarentegen mogelijk is de gegevens te gebruiken om fraude op te sporen, dan is sprake van een persoonsgegeven. Daarbij is niet relevant of de bedoeling de gegevens voor dat doel te gebruiken ook aanwezig is. Er is reeds sprake van een persoonsgegeven wanneer het gegeven voor een dergelijk op de*

[64] Memorie van Toelichting bij de Wbp, blz. 46-47.

persoon gericht doel, kan worden gebruikt."[65] Dat een gegeven ook een persoonsgegeven kan zijn als de verwerking niet tot doel heeft om de betrokkenen te identificeren, wordt eveneens bevestigd door de gezamenlijke Europese toezichthouders verenigd in de werkgroep artikel 29.

Voorts moet de persoon zijn geïdentificeerd of althans direct of indirect identificeerbaar zijn.

Van *direct* identificerende gegevens is sprake wanneer gegevens betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig vast te stellen is.[66]

Hiervan te onderscheiden zijn *indirect* identificerende gegevens. Er is sprake van indirect identificeerbare gegevens indien gegevens ontdaan zijn van naam, maar door combinatie met andere gegevens weer teruggebracht kunnen worden tot een bepaalde persoon. De MvT bepaalt in dit verband: "*uitgegaan moet worden van een redelijk toegeruste verantwoordelijke. In concrete gevallen moet echter wel rekening gehouden worden met de bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke*"**.**[67]

Een gegeven dat op een bepaald moment nog "*redelijkerwijs niet identificeerbaar*" is omdat identificatie een disproportionele aanwending van geld en middelen zou vergen, en daarom niet als persoonsgegeven kan worden aangemerkt, kan met voortschrijdende informatietechnologie tot een persoonsgegeven worden omdat de identificatie dan gemakkelijk is geworden. Het omslagpunt zal afhangen van de beoordeling van de mogelijkheden van de techniek in het concrete geval.[68]

Specifiek over het voortschrijden van de technologie schrijft de wetgever: "*Bij het voortschrijden van informatietechnologie moet rekening worden gehouden met het feit dat waar voorheen wellicht nog sprake is was van een onevenredige inspanning (en dus niet van een persoonsgegeven), deze inspanning geringer wordt met het beschikbaar komen van nieuwe technieken. Wat dus bij een bepaalde stand van de techniek als anoniem, want redelijkerwijs niet op een persoon herleidbaar gegeven, kan worden beschouwd, kan door technische ontwikkelingen alsnog een persoonsgegeven worden gelet op de toegenomen mogelijkheden tot herleiding.*"[69]

4.3.1 Gegevens over wifi-routers

Feitelijk staat vast dat Google de volgende gegevens over wifi-routers heeft verzameld: het wereldwijd uniek identificerend nummer van de hardware (BSSID), de berekende locatie, de signaalsterkte en in veel gevallen de SSID (de netwerknaam). De combinatie van het MAC-adres en de berekende locatie is opgeslagen in de Google GLS.

De verzamelde MAC-adressen van wifi-routers, in combinatie met de berekende locatie, zijn in deze context persoonsgegevens in de zin van artikel 1, onder a, Wbp omdat het uniek identificerende nummers zijn waarmee individuele houders geïdentificeerd kunnen worden.

---

[65] Idem, blz. 47. WP29 Opinie 4/2007 over het begrip persoonsgegevens, blz. 18. Zie ook: Rechtbank 's Gravenhage, 2 April 2010, LJN BM1481.
[66] MvT bij de Wbp, blz. 48.
[67] Idem, blz. 49. Zie ook: CBP 30 juni 2003, z2003-0477.
[68] Idem, blz. 1-2.
[69] Idem, blz. 49.

Daarbij is van belang dat MAC-adressen unieke hardware onderscheiden[70] en dat die hardware, in de context van geolocatie diensten, onverbrekelijk verbonden is met de locatie van een houder.[71]

In de specifieke toepassing van de Google GLS zijn immers niet alleen 3.606.579 MAC-adressen van wifi-routers opgenomen, maar ook van elke router een berekende plaatsbepaling. Dit rapport bevat voorbeelden van de plaatsbepaling van MAC-adressen in de Google GLS. In de onderzochte MAC-adressen varieert de nauwkeurigheid van de plaatsbepaling tussen de 24 en de 36 meter, met een bereik van gemiddeld 8 appartementen of zelfstandige woningen.

Het is een feit dat Google de signaalsterkte verwerkt van wifi-routers, zoals blijkt uit het Stroz Friedberg rapport. Uit de specifieke privacy-verklaringen voor de gebruikers van de geolocatiediensten in de browsers Chrome en Firefox blijkt dat Google doorlopend nieuwe gegevens ontvangt over nieuwe en reeds in kaart gebrachte wifi-routers via de gebruikers van zijn geolocatiediensten, waaronder het BSSID en de signaalsterkte. Hierdoor worden de locatieberekeningen in de Google GLS steeds preciezer.

Google zelf beschikt daarmee bij uitstek over de middelen om de individuele eigenaren van de wifi-routers te kunnen identificeren. De inspanning die Google zou moeten verrichten om met behulp van deze reeds aanwezige gegevens, en de doorlopende metingen de huiseigenaren te identificeren, valt niet onevenredig te noemen, zeker niet in het licht van het feit dat juist Google beschikt over een enorm potentieel aan capabele technici en informatici. Google kan deze identificatie vanachter zijn eigen burelen uitvoeren, op basis van gegevens die het bedrijf zelf al heeft, en dagelijks ontvangt.

Ook anderen dan Google kunnen met behulp van de Google GLS bepalen waar een wifi-router zich bevindt. Nadat via de Google GLS ongeveer de locatie is achterhaald (gemiddeld 8 woningen), kan iedereen het specifieke adres van de wifi-router met het betreffende MAC-adres. vervolgens zelf makkelijk achterhalen, door in de buurt van de aangegeven woningen zelf met een laptop of wifi-geschikte mobiele telefoon, met behulp van gratis verkrijgbare software of applicaties, de signaalsterkte te peilen van de aanwezige MAC-adressen, totdat men bij de juiste houder is aangekomen.

Google stelt desalniettemin in zijn zienswijze op de voorlopige bevindingen dat het "onmogelijk" zou zijn om een individuele wifi-router te identificeren, omdat de locatieberekening van een wifi-router in de GLS naar meerdere adressen in één straat verwijst, en niet naar één specifiek huis. "*Het is voor iemand die uitsluitend over een SSID, BSSID of draadloos MAC-adres in combinatie met de door Google berekende locatie-informatie beschikt onmogelijk om het desbetreffende draadloze apparaat (of, met betrekking tot de SSID, apparaten) te identificeren*."

Zoals in het bovenstaande is uiteengezet, is dat feitelijk onjuist. Google miskent voorts dat bij het criterium van de herleidbaarheid ingevolge de MvT uitgegaan moet worden "*een redelijk*

[70] Het MAC-adres is ingebrand in de hardware en kan nooit gewijzigd worden. Met bepaalde software is het wel mogelijk om een ander MAC-adres te emuleren (na te bootsen). Dit is geen eenvoudige handeling. Het proces heet 'cloning' of 'spoofing'.
[71] Er is jurisprudentie in Nederland over een specifieke internetgebruiker die in een politie-onderzoek opgespoord is aan de hand van zijn MAC-adres. Zie: Rechtbank 's Gravenhage, 2 April 2010, LJN BM1481, URL: http://jure.nl/bm1481. Een stalker kan voor het flatgebouw gaan staan of in het gedeelte van de straat waar het MAC adres is gelocaliseerd en kan zijn of haar doelwit op dat moment makkelijk identificeren.

toegeruste verantwoordelijke. In concrete gevallen moet echter wel rekening gehouden worden met de bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke."[72]

De omstandigheid dat in sommige gevallen een MAC-adres in combinatie met de berekende locatie niet of niet zonder onevenredige inspanning tot een individu te herleiden is, doet aan het bovenstaande niets af.

Google stelt voorts: "*Zelfs indien een afzonderlijke woning geïdentificeerd kan worden, zoals onlangs is geïllustreerd door een recente uitspraak van de rechtbank Rotterdam in B/Schoonderwoerd, hoeft het niet zo te zijn dat met informatie waarmee een specifiek huis is geïdentificeerd ook de persoon (of de personen) die dat huis woont is geïdentificeerd: alleen de identiteit van het pand is achterhaald en dat geldt niet als een persoonsgegeven.*"[73]

In de aangehaalde zaak B/Schoonderwoerd gaf de rechter een beknopte overweging ten overvloede, dat een waardegeschiedenis van een huis in beginsel niet kan worden aangemerkt als een persoonsgegeven. De zaak betreft geen vergelijkbaar geval. De verzoeker was niet ontvankelijk in de hoofdzaak omdat hij de verkeerde B.V. had aangeschreven. In deze beknopte overweging is de rechtbank niet toegekomen aan de vraag of de betreffende persoon *indirect* kan worden geïdentificeerd. De wetgever had bovendien al bepaald dat de combinatie van postcode met huisnummer in veel gevallen een persoonsgegeven is. "*Tevens dienen telefoonnummers, kentekens van auto's en postcodes met huisnummers onder omstandigheden als een persoonsgegeven te worden aangemerkt.*"[74]

Ten aanzien van de netwerknamen is vastgesteld dat apparatuur een zelfgekozen naam kan dragen, die direct identificerend kan zijn (voornaam en achternaam in combinatie met de berekende locatie) of indirect identificerend (de combinatie van een netwerknaam met het unieke MAC-adres in combinatie met de berekende locatie). Ook standaard netwerknamen als "SpeedtouchBFCB8F" zijn daarom persoonsgegevens in de zin van artikel 1, onder a, Wbp, in de door Google verwerkte combinatie met MAC-adres en berekende locatie.

4.3.2 Payload data

Vast staat dat Google op grote schaal inhoudelijke communicatiegegevens heeft verzameld afkomstig uit onbeveiligde wifi-routers in heel Nederland. De *payload data* bevatten bijna 6 miljoen analyseerbare *packets.* Veel *packets* bevatten persoonsgegevens als gedefinieerd in artikel 1, onder a, Wbp, zoals namen, e-mailadressen, mobiele telefoonnummers en namen van computers, laptops en iPhones waarin voor- en/of achternamen voorkomen. Aan de hand van deze gegevens kunnen personen gemakkelijk worden geïdentificeerd, door de naam op te zoeken in een telefoonboek of door te bellen of te e-mailen.

In totaal heeft Google in Nederland 16.640 e-mailadressen verzameld. E-mailadressen zijn in de meeste gevallen persoonsgegevens omdat ze betrekking hebben op en herleidbaar zijn naar een natuurlijke persoon, ook als die persoon een zakelijk e-mailadres gebruikt, zoals Jan@bedrijfsnaam.nl.

[72] MvT bij de Wbp, blz. 48. Zie ook CBP 30 juni 2003, z2003-0477.
[73] Zienswijze Google, paragraaf 107, blz. 34.
[74] MvT bij de Wbp, blz. 46-47.

In het DNS-verkeer (verzoeken aan de servers die domeinnamen vertalen in IP-adressen) is 2.205 keer een (unieke) voornaam gevonden, een unieke combinatie van voornaam en achternaam, al dan niet in combinatie met een MAC-adres. Deze gegevens zijn eveneens persoonsgegevens, zeker in combinatie met het feit dat Google bij elk *packet* de nauwkeurige plaatsbepaling van de auto heeft bewaard. Ook hierbij dient rekening te worden gehouden met het feit dat Google zelf bij uitstek in staat is om deze personen te identificeren.

Omdat bij elk *packet* ook de precieze locatiegegevens van de auto zijn bewaard, is de kring van mogelijke personen met dezelfde naam zeer klein en zijn de betrokkenen dus zonder onevenredige inspanning identificeerbaar.

Vaak zijn er ook meerdere *packets* van 1 gebruiker opgevangen. Die kunnen aan elkaar gekoppeld worden omdat er een (intern) IP-adres in voorkomt en/of een e-mailadres. Juist vanwege zijn grote scala aan online diensten en zijn enorme potentieel aan uiterst capabele technici en informatici is Google bij uitstek in staat om zonder onevenredige inspanning een persoon te kunnen identificeren op basis van dergelijke gegevens. In de opinie over persoonsgegevens hebben de gezamenlijke Europese toezichthouders op de bescherming van persoonsgegevens, verenigd in de "Artikel 29 Werkgroep", vastgesteld dat een persoonsgegeven identificeerbare personen betreft als de persoon "redelijkerwijs", "met alle middelen" geïdentificeerd kan worden. "*Indien, rekening houdende met "alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn", die mogelijkheid niet bestaat of verwaarloosbaar is, mag de persoon niet als "identificeerbaar" worden beschouwd en geldt de informatie niet als "persoonsgegeven*".[75]

Google stelt dat de payload data geen persoonsgegevens waren toen Google de gegevens verzamelde en vastlegde. "*Deze gegevens vormen geen persoonsgegevens wanneer ze op de harde schijven van Street View worden bewaard, omdat ze in een proprietary binair formaat worden opgeslagen en afzonderlijke personen daarom niet direct of indirect geïdentificeerd kunnen worden uit deze data. Wanneer de payload data in een voor mensen leesbare vorm geconverteerd worden, kunnen ze in uitzonderlijke gevallen kleine hoeveelheden gefragmenteerde persoonsgegevens bevatten.* "[76]

Het feit dat Google de gegevens in binair formaat heeft opgeslagen, betekent niet dat de gegevens daarmee niet leesbaar zouden zijn. Binair betekent dat informatie op een hele efficiënte manier in de vorm van nullen en enen wordt opgeslagen. Vast staat dat Google over de middelen beschikt om deze binaire informatie te vertalen in menselijk leesbaar formaat, en dat Google deze middelen (de codex software) ook vanaf het eerste moment dat met de auto's gegevens over Wifi-netwerken werden verzameld, heeft gebruikt om de gegevens over de wifi-netwerken te kunnen verwerken in de Google GLS. Het binaire formaat is daarmee een vorm van pseudo-anonimisering, die aan de beoordeling van het CBP geen afbreuk doet.

Of Google de gegevens ooit gebruikt heeft of zou willen gebruiken voor een bepaald doel, en of een dergelijke verwerking schade zou kunnen berokkenen aan betrokkenen, is in dit geval niet relevant. Op grond van de uitspraak van het Europees Hof voor de Rechten van de Mens in de zaak Amann[77] vormt louter het verzamelen en bewaren van persoonsgegevens een inbreuk op de

[75] WP29 Advies 4/2007 over het begrip persoonsgegevens, aangenomen 20 juni 2007, URL Nederlandstalige versie
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_nl.pdf
[76] Zienswijze Google, paragraaf 7, ii, onder a, blz. 5.
[77] EHRM 16 februari 2000 *(Amann)*.

door artikel 8 van het Europees Verdrag van de Rechten van de Mens beschermde persoonlijke levenssfeer en correspondentie.

Het Hof overweegt:

"The Court reiterates that the storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding (see, mutatis mutandis, the Leander judgment cited above, p. 22, § 48, and the Kopp judgment cited above, p. 540, § 53)."[78]

Bijzondere persoonsgegevens

De door Google verzamelde gegevens bevatten ook *bijzondere* persoonsgegevens als gedefinieerd in artikel 16 Wbp, zoals een uitgebreid psychologisch rapport over een jongen met een ernstige leerachterstand. Het rapport bevat zijn voornaam, achternaam, adres en geboortedatum.

Communicatiegegevens

Uit het onderzoek blijkt dat Google veel inhoudelijke communicatiegegevens heeft opgevangen en opgeslagen, zoals de combinatie van loginnaam, wachtwoord en e-mail/FTP-server, betalingsgegevens met betrekking tot beleggingen of een overzicht van ontvangen e-mail.

Hoewel de Wbp geen aparte definitie kent van *gevoelige* communicatiegegevens, bestaat er in het maatschappelijk verkeer geen twijfel dat dergelijke persoonsgegevens met de hoogste mate van vertrouwelijkheid dienen te worden behandeld.

Google betwist dit. "*Google aanvaardt niet dat niet-versleutelde communicatiegegevens die door heel Nederland publiekelijk via onbeveiligde Wifi-netwerken verzonden worden, 'gevoelige communicatiegegevens' zijn, zoals het CBP in het rapport stelt.*"[79] Google stelt dat de gegevens niet gevoelig zijn omdat radiosignalen in de lucht geen strafrechtelijke bescherming genieten: "*in het artikel waarin het onderscheppen van persoonlijke elektronische berichten wordt verboden (artikel 139c Wetboek van Strafrecht), worden specifiek radiosignalen uitgesloten die eenvoudig met een rechtmatig verkrijgbaar ontvangstapparaat ontvangen kunnen worden.*"[80]

De vertrouwelijkheid van communicatie vloeit rechtstreeks voort uit internationale verdragen als het EVRM en Handvest van de grondrechten van de Europese Unie. Uit jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) blijkt dat zowel de inhoud van, als informatie over elektronische communicatie, bescherming genieten op grond van artikel 8, eerste lid, EVRM.[81]

Hoewel het begrip 'correspondentie' uit het EVRM niet expliciet van toepassing is op elektronische communicatie, heeft het EHRM de bescherming successievelijk van toepassing

[78] Idem, paragraaf 70, zie ook 68-69.
[79] Zienswijze Google, paragraaf 70, blz. 24.
[80] Idem.
[81] De Hoge Raad heeft in HR 9 januari 1987 (*Bespiede bijstandsmoeder*) expliciet erkend dat art. 8 EVRM een horizontale werking heeft, dwz, een recht is waarop burgers zich kunnen beroepen ten aanzien van andere burgers en bedrijven.

geacht op telefoongesprekken (Klass), telefoonnummers (Malone) en het heimelijk opnemen van conversaties met afluisterapparatuur (P.G. & J.H.).[82]

In de zaak Huvig overwoog het Hof dat het afluisteren van telefoongesprekken een ernstige inbreuk vormt op het privéleven en de correspondentie: "*Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.*"[83]

In de zaak Copland[84] breidde het Hof de bescherming expliciet uit naar e-mail correspondentie en internetgebruik. Het Hof overwoog: "*Accordingly, the Court considers that the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8.*"

Veelzeggend is het feit dat in het Handvest van de grondrechten van de Europese Unie het begrip 'correspondentie' vervangen is door het veel bredere begrip 'communicatie' in artikel 7.

Dat inhoudelijke communicatiegegevens algemeen gezien worden als zeer vertrouwelijke gegevens blijkt voorts uit het feit de Europese richtlijn *bewaarplicht verkeersgegevens telecommunicatie* inhoudelijke gegevens, zoals de onderwerpsregel van e-mail en webverkeer, nadrukkelijk heeft uitgezonderd van de bewaarplicht. Het preventief opslaan van deze gegevens van alle burgers ten behoeve van de opsporing zou een te grote inbreuk maken op het fundamentele recht op bescherming van de persoonlijke levenssfeer en correspondentie (artikel 8 EVRM).

Het overzicht van ontvangen e-mail maakt duidelijk hoe indringend het beeld is dat verkeersgegevens over telecommunicatie kunnen geven van iemands persoonlijke leven. Op basis van de timing van de e-mails, de adressen van de verzenders en vooral de onderwerpsregel valt een nauwkeurig beeld te reconstrueren van momenten uit het leven van deze betrokkene, zijn interesses en zijn loopbaanontwikkeling.

Een ander voorbeeld van dergelijke gevoelige communicatiegegevens zijn sommige zoekopdrachten bij de Google zoekmachine. Zoekopdrachten als "hoeveel weken zwanger" "groene poep baby" en "thuiszorg winkel TWELLO" wijzen op dringende medische vragen Het feit dat iemand kennelijk een bruidsjurk wil huren, geeft een indicatie van welstand.

Een zoekopdracht hoeft geen betrekking te hebben op een behoefte van de betrokkene zelf. Een betrokkene kan ook voor een familielid, kennis of bijvoorbeeld in het kader van een werkstuk op school op zoek gaan naar informatie. Toch hebben de zoekopdrachten wel degelijk *betrekking* op een specifieke betrokkene, omdat zij een duidelijke indicatie geven van diens belangstelling en behoeftes. De bedoeling van *behavioural advertising* is bijvoorbeeld om gerichte reclame te tonen aan betrokkenen op basis van hun internetgedrag. Daarbij maakt het niet uit of de betrokkene het getoonde product of de aanbevolen dienst voor zichzelf aanschaft, of voor een derde.

---

[82] EHRM 6 september 1978 (*Klass*), EHRM 2 augustus 1984 (*Malone*), NJ 1988, 534, EHRM 25 september 2001 *(P.G. en J.H. v. Verenigd Koninkrijk),* nr 44787/98.
[83] EHRM 24 april 1990, NJ 1991, 523 (*Huvig*) § 32.
[84] EHRM 3 april 2007 *(Copland v. Verenigd Koninkrijk)*.

Diezelfde gevoeligheid geldt voor de laatst bezochte websites, de *referrers*.

Een zoekopdracht naar porno kan een betrokkene in ernstige verlegenheid brengen. In het onderzochte geval blijkt een betrokkene meerdere websites te hebben bezocht met onmiskenbaar pornografische inhoud en daar specifieke bestanden te hebben bekeken. Deze betrokkene is eveneens identificeerbaar, omdat van elke zoekopdracht een locatie valt te berekenen van de wifi-router.

Met de combinatie van loginnaam en wachtwoord voor een e-mailserver kan de inhoud van alle inkomende en uitgaande e-mail van een (op dat moment identificeerbare) betrokkene worden (mee-)gelezen. Google heeft 56 van deze combinaties opgeslagen. Google kan hierdoor in theorie inzicht verkrijgen in kopieën van verzonden e-mails op de server (voorzover een betrokkene die heeft bewaard), en kan deze e-mails lezen en kopiëren. Datzelfde geldt voor contactgegevens in een adresboek.

4.4 Informatie

Artikel 33 Wbp bepaalt dat de verantwoordelijke *vóór het moment van de verkrijging* de betrokkene dient te informeren over zijn identiteit en de doeleinden van de verwerking. Daarbij dient de verantwoordelijke op grond van artikel 33, derde lid, Wbp nadere informatie te verstrekken *voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.* (onderstreping CBP).

Artikel 34 Wbp bepaalt: *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* (dwz identiteit, doeleinden en nadere informatie als in artikel 33 Wbp, uitleg CBP)*, 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*.

Daarbij geldt op grond van het vierde lid van artikel 34 Wbp dat de verantwoordelijke niet hoeft te informeren *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.*

Artikel 27, eerste lid, Wbp bepaalt: *Een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens die voor de verwezenlijking van een doeleinde of verscheidene samenhangende doeleinden bestemd is, wordt alvorens met de verwerking wordt aangevangen gemeld bij het College of de functionaris*.

4.4.1 Gegevens over wifi-routers

Google heeft met zijn Street View auto's gegevens verzameld over (het bestaan van) ruim 3,6 miljoen wifi-routers in Nederland. Vast staat dat Google de inwoners van Nederland met een wifi-router niet voorafgaand en niet tijdens de verzameling heeft geïnformeerd over de verwerking van deze persoonsgegevens. Google heeft de verwerking van wifi-gegevens tot op heden niet verwerkt in zijn algemene privacy-verklaring, noch in de specifieke toelichtingen bij Maps en Street View. De enige informatie die Google ter beschikking stelt gaat over het doorlopend verzamelen van wifi-gegevens en is gericht op de specifieke doelgroep van

gebruikers van de browsers Chrome en Firefox voorzover zij gebruik maken van de geolocatiediensten. Deze informatie is niet gericht op de betrokkenen van wie de wifi-router door Google in kaart is gebracht.

Vast staat ook dat Google de verwerking van persoonsgegevens niet heeft gemeld bij het CBP. Google heeft op 4 februari 2010 een melding gedaan bij het CBP van het verwerken van fotografische gegevens ten behoeve van de dienst Street View, maar deze melding bevat geen informatie over het verzamelen van gegevens over wifi-routers.

Met de verplichting om voorgenomen gegevensverwerkingen te melden bij de toezichthouder, heeft de wetgever transparantie beoogd van gegevensverwerkingen, zodat betrokkenen in staat zijn om te controleren wat de doeleinden zijn van bepaalde gegevensverwerkingen.

"Aanmelding heeft tot doel de transparantie van de gegevensverwerking te bevorderen. De handelingsvrijheid van een ieder om voor op zichzelf gerechtvaardigde doeleinden gegevens te verwerken, wordt ingeperkt door de grondwettelijk gewaarborgde vrijheid van de betrokkene om niet onnodig aan verwerking van hem betreffende gegevens te worden onderworpen. Dit leidt enerzijds tot het materiële voorschrift dat de belangen van de verantwoordelijke en de betrokkene tegen elkaar moeten worden afgewogen; anderzijds tot het procedurele voorschrift dat de afweging controleerbaar dient te zijn."[85]

In zijn zienswijze op de voorlopige bevindingen heeft Google aangegeven dat niet artikel 33 Wbp van toepassing is op de gegevensverzameling, maar artikel 34 Wbp. Het bedrijf doet tegelijkertijd een beroep op de uitzondering van artikel 34, vierde lid, Wbp om houders van wifi-routers niet te hoeven informeren.
"*Afgezien van het feit dat Google vindt dat Wifi-netwerkinformatie niet als persoonsgegeven geldt, erkent Google niet dat zij een wettelijke informatieplicht heeft geschonden.* (...) [Google zou] *zich disproportioneel moeten inspannen teneinde alle betrokkenen (wie dat ook mogen zijn) die gekoppeld zijn aan de miljoenen SSID's, BSSID's en MAC-adressen die publiekelijk via Wifi-netwerken in iedere regio van Nederland zijn uitgezonden, melding te doen van het feit dat Google deze gegevens aan het verzamelen was. Google zou vrijgesteld zijn van de informatieplicht op grond van artikel 34 lid 4 Wbp."*[86]

Google heeft de gegevens over de wifi-routers zelf verzameld, bij de voordeur van betrokkenen, door rond te rijden met de Street View auto's. Omdat Google nooit bekend heeft gemaakt dat de Street View auto's naast foto's van huizen ook gegevens verzamelden over wifi-routers, is er *de facto* sprake van heimelijke gegevensverzameling. Google heeft betrokkenen daardoor ook niet in de gelegenheid gesteld hun gedrag aan te passen, bijvoorbeeld door hun router uit te zetten op het moment dat de Street View auto's langsreden of anderszins bezwaar te maken tegen opname van de hen betreffende gegevens in de Google GLS.

In de memorie van toelichting bij de Wbp wordt het voorbeeld gegeven van camera-toezicht. Als dat heimelijk geschiedt, is artikel 34 Wbp van toepassing.

De gegevensvergaring met behulp van videocamera's kan onder artikel 33 worden geschaard indien het geen geheime observatie betreft. Indien de betrokkene op de hoogte is van de aanwezigheid van camera's en hij eveneens weet voor welk doel deze gebruikt worden, heeft hij de mogelijkheid zich hieraan te onttrekken.

[85] Memorie van Toelichting Wbp, blz. 132-133.
[86] Zienswijze Google, paragraaf 124, blz. 40.

Doet hij dat niet dan kan gesteld worden dat hij zijn persoonsgegevens voor het desbetreffende doel bewust ter beschikking heeft gesteld.[87]

Het feit dat Google de gegevens heimelijk heeft verzameld, ontslaat het bedrijf niet van de verplichting om op grond van artikel 34, eerste lid, onder a, Wbp betrokkenen te informeren op het moment van vastlegging van de gegevens.

Het CBP deelt de kwalificatie niet dat informeren een onevenredige inspanning zou vergen. Het CBP begrijpt ook niet waarin deze inspanning verschilt van de wijze waarop Google bijvoorbeeld in Duitsland betrokkenen heeft geïnformeerd over het voornemen om op bepaalde tijden in bepaalde gebieden foto's van huizen te maken voor de dienst Street View, later gevolgd door informatie over het voornemen tot publicatie van deze foto's over te gaan, en de mogelijkheden voor betrokkenen om zich te verzetten tegen de publicatie van hen betreffende gegevens.

Ook in Nederland waren voldoende middelen beschikbaar om betrokkenen te informeren over de gegevensverzameling, zoals aangekondigde routes via websites, persberichten, gerichte advertenties en herkenbaarheid van de betreffende auto's. Er zijn eveneens voldoende middelen beschikbaar om betrokkenen alsnog adequaat te informeren over de gegevensverwerking. Gegeven de enorme omvang van de gegevensverzameling, de belangen van betrokkenen om te weten dat er gegevens over hen worden verzameld en voor welk doel, en hoe zij zich daaraan kunnen onttrekken en gegeven de mogelijkheden die Google ter beschikking staan in deze voor publieke informatievoorziening, is een dergelijke invulling van de informatieplicht in deze context zeker niet disproportioneel.

Door het negeren van de plicht om betrokkenen in Nederland te informeren over het verzamelen en verwerken van gegevens over wifi-routers heeft Google in strijd gehandeld met artikel 34 Wbp. Door de voorgenomen verwerking niet te melden bij het CBP, heeft Google in strijd gehandeld met artikel 27 jo. 28 Wbp.

4.4.2 Payload data

Google heeft gedurende twee jaar bijna 30 gigabyte aan inhoudelijke communicatiegegevens verzameld in Nederland. Vast staat dat Google betrokkenen noch het CBP op voorhand heeft geïnformeerd over het verzamelen van deze *payload data*. Na een aanvankelijke ontkenning (op 27 april 2010) heeft het bedrijf later bekend gemaakt (op 14 mei 2010) dat er toch per ongeluk *payload data* waren verzameld. Google heeft in ieder geval voor 27 april 2010 niet aan de informatieplicht ex artikel 34 Wbp voldaan. Ook sinds die tijd heeft Google het Nederlandse publiek niet geïnformeerd over de verwerking van hen betreffende gegevens, noch voldaan aan de verplichting om de voorgenomen verwerking te melden bij het CBP.

4.5 Doeleinde en grondslag

Conform artikel 7 Wbp dient de verantwoordelijke *welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden* te hebben voor de gegevensverzameling.

Op grond van artikel 8 Wbp dient de verantwoordelijke een grondslag te hebben voor de gegevensverwerking. In casu komen daarvoor twee rechtvaardigingsgronden in aanmerking: toestemming en noodzaak.

[87] Memorie van Toelichting Wbp, blz. 155-157.

Artikel 8, aanhef en onder a, respectievelijk f, Wbp, bepaalt: *Persoonsgegevens mogen slechts worden verwerkt indien: (...)*

a. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;

f. 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 bescherming van de persoonlijke levenssfeer, prevaleert.

4.5.1 Gegevens over wifi-routers

Met betrekking tot het vastleggen van gegevens *over* wifi-routers en andere communicatie-apparatuur heeft Google het doeleinde van de verwerking pas bekend gemaakt nadat er publicitaire ophef was ontstaan over het feit dat Google met de Street View auto's gegevens over wifi-netwerken verzamelde. Google stelt de MAC-adressen en de berekende locatie nodig te hebben om een plaatsbepalingsdienst aan te kunnen bieden op internet, via de Google GLS.

Google heeft geen welbepaald of uitdrukkelijk omschreven doeleinde genoemd voor het registreren van de SSID (de netwerknaam van de wifi-routers). Dit gegeven kan een standaardnaam zijn die de fabrikant heeft meegegeven, maar ook een zelfgekozen combinatie van voor- en achternaam of adres met huisnummer. De combinatie van SSID, BSSID en de berekende locatie is een persoonsgegeven. Door het ontbreken van informatie over de precieze verwerkingsdoeleinden van de SSID's handelt Google in strijd met artikel 7 Wbp.

Google heeft geen toestemming gevraagd aan betrokkenen voor het verzamelen van de BSSID's, de SSID's en de signaalsterkte. De enige andere toepasselijke grondslag voor deze gegevensverwerking is artikel 8, onder f, Wbp. Bij die rechtvaardigingsgrond dient het eigen gerechtvaardigde belang afgewogen te worden tegen de rechten en vrijheden van betrokkenen, in het bijzonder de bescherming van hun persoonlijke levenssfeer. Een verantwoordelijke die zich op deze grondslag wil beroepen, moet aantonen dat de verwerking noodzakelijk is en dat het doel niet anderszins of met minder ingrijpende middelen gediend kan worden. Na deze afweging van proportionaliteit en subsidiariteit volgt een tweede afweging, waarbij de belangen van de betrokkene een zelfstandig gewicht in de schaal leggen tegenover het belang van de verantwoordelijke. 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.

Ten aanzien van het verzamelen van MAC-adressen van wifi-routers in combinatie met de berekende locatiegegevens en de signaalsterkte ten behoeve van het kunnen aanbieden van een nieuw product (de GLS), waarnaar vraag is in de markt, is een beroep mogelijk op artikel 8, onder f, Wbp, de noodzaak om deze gegevens te verzamelen ten bate van een gerechtvaardigd belang, mits Google in een aantal waarborgen voorziet om te voorkomen dat het belang van betrokkenen bij de bescherming van hun persoonlijke levenssfeer prevaleert.

In zijn zienswijze stelt Google dat toepasselijkheid van de Wet bescherming persoonsgegevens een belemmering zou opwerpen voor de ontwikkeling van nieuwe cartografische diensten. "*Indien het CBP en/of de Artikel 29 Werkgroep door spelers op de digitale kaartenmarkt gebruikelijk verzamelde Wifi-netwerkinformatie als persoonsgegeven aanmerkt (al dan niet in combinatie met GPS-coördinaten), zou dit vergaande gevolgen hebben voor deze grote, snelgroeiende branche. (...) Een dergelijke*

classificatie zou de toekomstige groei van de markt voor digitale kaarten in EMEA belemmeren en de ontwikkeling van nieuwe kaartproducten verhinderen."[88] Google motiveert dit niet. Google geeft niet aan welke potentiële belemmeringen of verhinderingen veroorzaakt zouden worden door de kwalificatie persoonsgegeven.

Voorop staat dat verantwoordelijken gerechtvaardigde belangen kunnen hebben bij de ontwikkeling van innovatieve nieuwe diensten op internet waar vraag naar bestaat. Conform artikel 8, onder f, Wbp dient daarbij rekening te worden gehouden met de impact van deze diensten op de persoonlijke levenssfeer van betrokkenen. Verantwoordelijken dienen waarborgen in te bouwen om onevenredige benadeling te voorkomen. Van een potentiële belemmering van de toekomstige groei of van verhindering van de ontwikkeling van nieuwe kaartproducten door het inbouwen van waarborgen (*privacy by design*) is geenszins sprake.

In casu heeft Google betrokkenen niet geïnformeerd over de verwerking van gegevens over wifi-routers. Een zorgvuldige gegevensverwerking vereist dat betrokkenen actief geïnformeerd worden over het vastleggen van hen betreffende persoonsgegevens en de specifieke doeleinden waarvoor deze gegevens worden verzameld en verwerkt.

Google dient rekening te houden met het risico van ernstige privacy-inbreuken door de traceerbaarheid van internetgebruikers via het MAC-adres van hun wifi-router in combinatie met de steeds nauwkeuriger wordende localisatie. In bijzondere gevallen, zoals bijvoorbeeld bij gevaar van *stalking* als een betrokkene verhuist naar een nieuwe woonplaats maar daar opnieuw opgespoord kan worden onder hetzelfde MAC-adres, moet in dat kader voorzien zijn in de mogelijkheid van verzet als bedoeld in artikel 40 Wbp. Daarbij is van belang dat de waarborgen steeds aangepast zijn aan de voortschrijdende technische mogelijkheden tot identificatie van betrokkenen.

De wijze van gegevensverzameling tot nu toe door Google geeft onvoldoende blijk van een evenredige belangenafweging (proportionaliteitsbeginsel). Daarbij dient mede in aanmerking te worden genomen dat indien het gerechtvaardigd belang van de verantwoordelijke anderszins of met minder ingrijpende middelen wordt gediend, de gegevensverwerking niet is toegestaan (subsidiariteitsbeginsel). Google kan de SSID's (netwerknamen) weglaten uit de Google GLS en volstaan met de combinatie van BSSID's en hun berekende locaties om een plaatsbepalingsdienst aan te bieden. Door het ontbreken van een noodzaak om de SSID's te verwerken, kan er geen sprake zijn van een gerechtvaardigd doeleinde voor het verzamelen ervan.

Google heeft door het verzamelen van de gegevens over wifi-routers in strijd gehandeld met artikel 7 (doeleinde) en artikel 8 Wbp (grondslag). Voor het verzamelen van SSID's (netwerknamen) ontbreekt een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde. Tevens ontbreekt een grondslag voor het verzamelen van de SSID's, in casu toestemming of gerechtvaardigd belang.

4.5.2 Payload data

Met betrekking tot het verzamelen van de *payload data* heeft Google in antwoord op vragen van het CBP en publiekelijk erkend geen (gerechtvaardigd) doeleinde te hebben. Google is na de ontdekking wereldwijd gestopt met het verzamelen en verwerken van de inhoudelijke communicatiegegevens.

[88] Zienswijze Google, paragraaf 117, blz. 37-38.

Gelet op het ontbreken van een gerechtvaardigd doeleinde van Google om vertrouwelijke communicatiegegevens te verzamelen en het vertrouwelijke karakter van sommige verzamelde persoonsgegevens kan Google zich niet beroepen op een gerechtvaardigd belang om de gegevens te verzamelen, dwz een grondslag in artikel 8, onder f, Wbp. Ook van toestemming is geen sprake, laat staan van de *uitdrukkelijke* toestemming die op grond van artikel 16 Wbp vereist is om het verbod te doorbreken op de verwerking van *bijzondere* persoonsgegevens. Google heeft hierdoor geen grondslag voor de gegevensverwerking.

Google heeft door het verzamelen van de *payload data* in strijd gehandeld met de verplichting uit artikel 7 om een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde te hebben voor de gegevensverzameling. Google heeft tevens in strijd gehandeld met artikel 8 Wbp door het ontbreken van een grondslag, in casu toestemming of gerechtvaardigd belang. Bij het verzamelen van *bijzondere* persoonsgegevens heeft Google tevens in strijd gehandeld met artikel 16 Wbp, het verbod op de verwerking van *bijzondere* persoonsgegevens.

4.6 Zorgvuldigheid

In artikel 6 Wbp is bepaald dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze dienen te worden verwerkt.

Alle in de onderhavige context geconstateerde onrechtmatigheden werken door in de beoordeling op grond van artikel 6 Wbp.

Ten aanzien van de verzameling van gegevens *over* wifi-routers staat vast dat Google in Nederland ruim 3,6 miljoen unieke wifi-routers in kaart heeft gebracht. Google heeft deze persoonsgegevens heimelijk verzameld, zonder enige informatie te verstrekken aan betrokkenen over het doeleinde van deze verzameling, niet rechtstreeks en niet indirect via een melding bij het CBP. Door dit gebrek aan informatie kan Google geen behoorlijke en zorgvuldige gegevensverwerking waarborgen.

Bij een behoorlijke en zorgvuldige werkwijze hoort het toepassen van *privacy by design* om te voorkomen dat gegevens worden verwerkt die niet noodzakelijk zijn voor het (gerechtvaardigde) doel. Google had maatregelen moeten treffen om te waarborgen dat er binnen zijn bedrijfsvoering niet per ongeluk of zonder aan de eisen van de wet te voldoen, op deze schaal persoonsgegevens worden verzameld.

Door het feit dat Google geen gerechtvaardigd doeleinde heeft en geen grondslag voor het verzamelen en verwerken van *payload data*, heeft Google in strijd gehandeld met de wet. Het is op zijn minst onzorgvuldig dat Google gedurende twee jaar in Nederland heeft rondgereden zonder - zoals het bedrijf aangeeft - te merken dat er zoveel *payload data* werden opgeslagen. Door de software op voorhand anders in te stellen (*false* of *true*) had Google kunnen voorkomen dat er überhaupt *payload data* werden verzameld. Google stelt dat het verzamelen van de payload data een vergissing was van een individuele programmeur: "*Quite simply, it was a mistake. In 2006 an engineer working on an experimental WiFi project wrote a piece of code that sampled all categories of publicly broadcast WiFi data.*"

In zijn zienswijze stelt Google: "*Google is doende aanzienlijke herstelmaatregelen te implementeren en is haar werkmethodes aan het verbeteren teneinde te voorkomen dat zich in de toekomst nogmaals een incident voordoet waarbij per ongeluk Wifi payload data verzameld worden.*"[89]

Wat daar ook van zij, kennelijk had Google binnen zijn bedrijfsvoering in dit geval geen, althans onvoldoende, voorzieningen getroffen om te voorkomen dat, al dan niet bewust, op medewerkersniveau beslissingen worden genomen èn kunnen worden uitgevoerd die grote privacyrisico's met zich brengen.

Als gevolg van de wijze waarop Google als onderneming in dit geval heeft geopereerd, zijn de privacyrechten van grote groepen betrokkenen geschonden. Juist vanwege de aard van de bedrijfsactiviteiten van Google en de specifieke expertise die in verband hiermee aanwezig is, mag van Google worden verwacht dat zij opereert met inachtneming van de eisen die de Wbp stelt en dat Google zich voorafgaand aan de uitvoering van activiteiten rekenschap geeft van de risico's en de gevolgen die de wijze van opereren van het bedrijf heeft op de rechten van individuele betrokkenen. De onrechtmatigheid van de werkwijze van Google inzake het verzamelen van Wifi-gegevens is niet toerekenbaar aan een individuele programmeur, maar aan de vennootschap die dit risico neemt.

Google heeft door deze onzorgvuldige werkwijze in strijd gehandeld met artikel 6 Wbp.

5. Conclusie

Google heeft van maart 2008 tot mei 2010 in Nederland rondgereden met Street View auto's. Deze auto's hebben gegevens verzameld *over* alle wifi-routers die aanstonden op het moment dat de auto langsreed en inhoudelijke communicatie *afkomstig uit* onbeveiligde wifi-routers.

Van 63% van de huishoudens en bedrijven in Nederland met een breedbandverbinding heeft Google de wifi-router letterlijk in kaart gebracht, in de zin dat het unieke identificerende MAC-adres van de router is vastgelegd in combinatie met de berekende locatie. Ook als de houder van de wifi-router zijn communicatie had beveiligd, heeft Google toch informatie over de router vastgelegd. De combinatie van een MAC-adres van een wifi-router met de berekende locatie is in deze context een persoonsgegeven.

Google heeft door het verzamelen van de gegevens over wifi-routers in strijd gehandeld met artikel 7 (doeleinde) en artikel 8 Wbp (grondslag).Voor het verzamelen van SSID's (netwerknamen) ontbreekt een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde. Tevens ontbreekt een grondslag voor het verzamelen van de SSID's, in casu toestemming of gerechtvaardigd belang.

Google heeft in strijd gehandeld met artikel 34 Wbp door het negeren van de plicht om betrokkenen in Nederland te informeren over het verzamelen en verwerken van gegevens over wifi-routers. Door de voorgenomen verwerking niet te melden bij het CBP, heeft Google in strijd gehandeld met artikel 27 jo. 28 Wbp.

Google heeft in Nederland tevens op grote schaal gegevens verzameld afkomstig *uit* onbeveiligde wifi-netwerken, de zogenaamde *payload data*. In twee jaar tijd heeft het bedrijf bijna

[89] Zienswijze Google, paragraaf 133, blz. 42.

30 gigabyte aan gegevens opgeslagen, waarvan bijna 70% analyseerbaar blijkt te zijn. Uit het onderzoek blijkt dat deze gegevens geen onbetekenende fragmenten zijn. Van betrokkenen kunnen 2 tot 2.500 *packets* zijn opgevangen. Deze *packets* kunnen aan elkaar gekoppeld worden en daaruit kan een indringend beeld ontstaan van een betrokkene, zoals het feit dat iemand een grote hoeveelheid aandelen koopt, met naam, e-mailadres en bankrekeningnummer.

Soms kan 1 *packet* al een overvloed aan *bijzondere* persoonsgegevens bevatten, zoals in het beschreven geval van het uitgebreide psychologische rapport over een minderjarige jongen met een ernstige leesachterstand. Het rapport bevat zijn voornaam, achternaam, adres en geboortedatum.

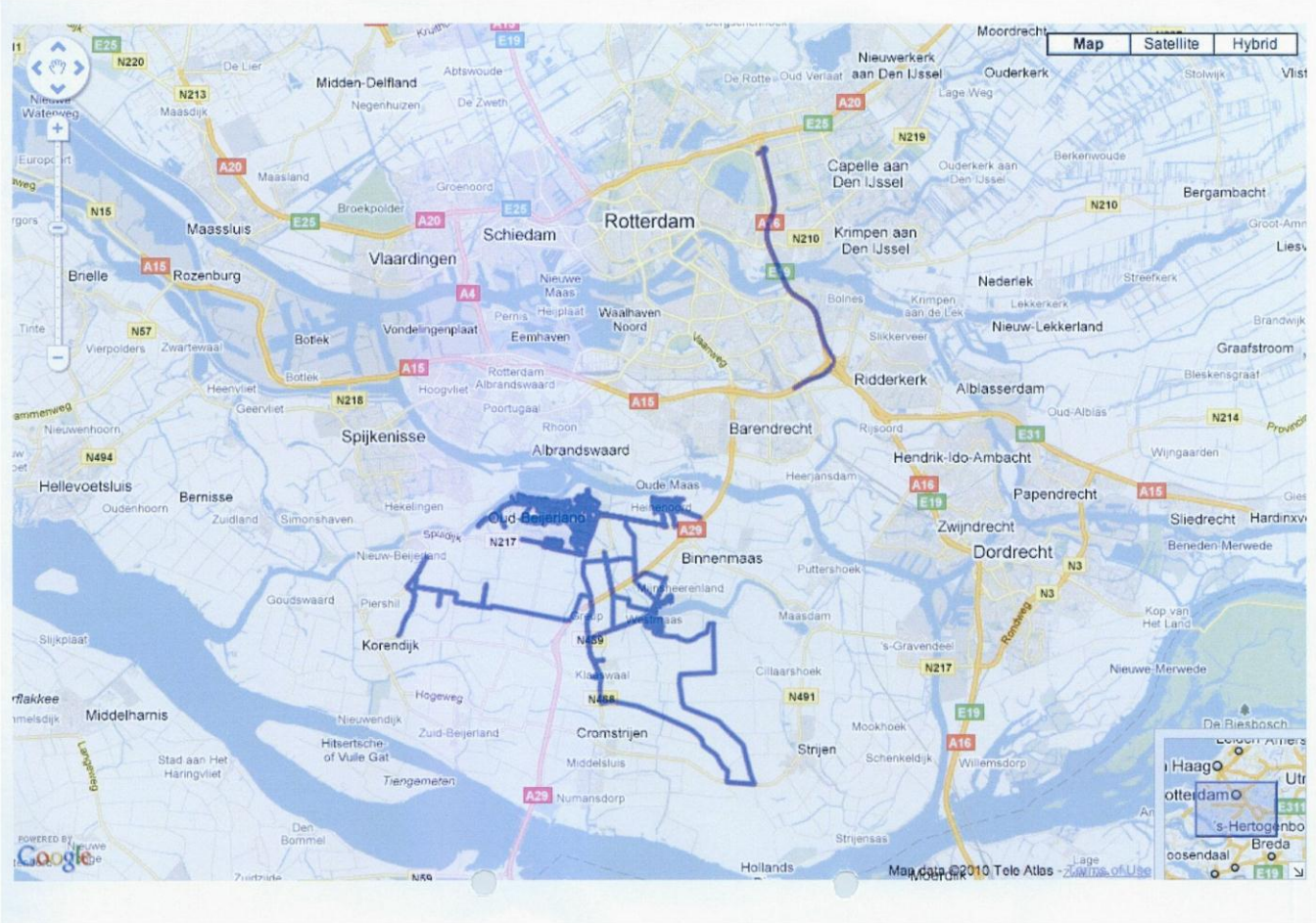
In het geanalyseerde verkeer zijn talloze persoonsgegevens aangetroffen, variërend van voornaam-achternaam tot e-mailadres en van zoekopdrachten bij Google tot bezoek aan pornografische websites.

Google heeft door het verzamelen van de *payload data* in strijd gehandeld met de verplichting uit artikel 7 om een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde te hebben voor de gegevensverzameling.

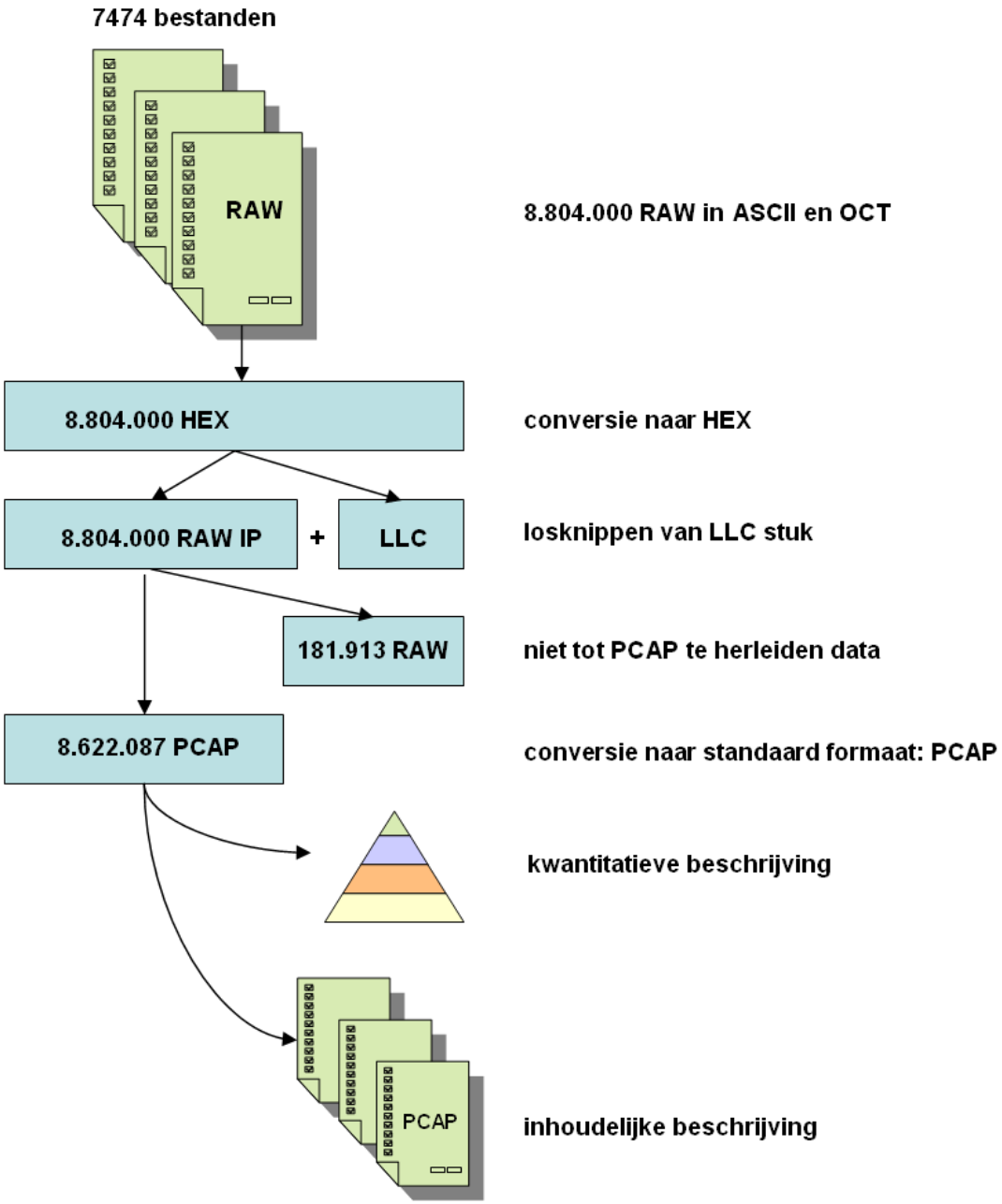
Google heeft tevens in strijd gehandeld met artikel 8 Wbp door het ontbreken van een grondslag, in casu toestemming of gerechtvaardigd belang. Bij het verzamelen van *bijzondere* persoonsgegevens heeft Google tevens in strijd gehandeld met artikel 16 Wbp, het verbod op de verwerking van *bijzondere* persoonsgegevens.

Het is onzorgvuldig dat Google gedurende twee jaar met Street View auto's in Nederland heeft rondgereden zonder te merken dat er zoveel *payload data* werden opgeslagen. Door een andere keuze te maken bij het inrichten van de software (*false* ipv *true*) had Google kunnen voorkomen dat er überhaupt *payload data* werden verzameld. Het valt Google te verwijten dat het bedrijf bewust grote privacyrisico's heeft genomen door in zijn bedrijfsvoering geen, althans onvoldoende, voorzieningen te treffen om deze grootschalige inbreuk op privacyrechten te voorkomen. Door het ontbreken van een grondslag en door zijn onzorgvuldige werkwijze heeft Google ten aanzien van de *payload data* in strijd gehandeld met artikel 6 Wbp.

BIJLAGE I - Plattegrond gegevens op door het CBP onderzochte harde schijf (kopie print Google)



BIJLAGE II - Stroomschema analysemethode CBP



BIJLAGE III - Plattegrond Nederland met door het CBP onderzochte locatie van MAC-adressen