

NEDERLANDSE VERENIGING VAN DAAD-ALUMNI

Privacy in Nederland en Duitsland

Gerrit-Jan Zwenne – 30 november 2011



drie privacy casus

Google Streetview

- almost unnoticed when introduced in the Netherlands, in Germany many privacy concerns
- Dutch DPA acts against WiFi-data collection, allegedly with global implications

Diginotar

- one of the most serious hacks ever
- almost lockdown of all government and many other websites
- call for security breach notification obligation

Telecom bewaarplicht

- bewaarplicht van verkeers- en gebruikers-gegevens
- t.b.v. voorkoming, opsporing en vervolging van ernstige criminaliteit



Google Streetview in Nederland

Google Streetview

- geïntroduceerd in voorjaar 2009, enige discussie over bekende Nederlanders, huisnummers en kentekens
- in voorjaar 2011 wel last onder dwangsom voor WiFi-gegevens

Tech / Internet

Google gaat privacy in Street View beter waarborgen

Laatste update: 4 september 2009 16:36

AMSTERDAM – Google gaat op Street View-foto's de privacy van afgebeelde personen beter waarborgen. De foto's van gezichten zullen beter en strenger gecensureerd worden.



Foto: AFP

Dit meldt Webwereld. Het besluit van Google komt na bezwaren van een Zwitserse privacywaakhond, die pleit voor het offline halen van de dienst. Volgens de waakhond zou het internetbedrijf zich niet aan de wet houden die de privacy van personen waarborgt.

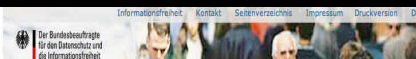
Google heeft daarop besloten de gezichten van personen die herkenbaar zijn op Street View beter te vervagen. Ook worden kentekenplaten van auto's slechter zichtbaar gemaakt.

Volgens Google is Zwitserland het eerste land waar extra op de privacy wordt gelet, maar zullen andere landen later volgen. De Europese Commissie gaf eerder al een waarschuwing af aan Google omtrent de privacy van personen in Street View.

Google Streetview in Duitsland

Google Streetview

- geïntroduceerd in najaar 2010, nadat er was voorzien in opt-out functie
- actualisering van beelden (voorsnog?) gestopt in voorjaar 2011
- heftige protesten tegen verzameling Wifi-gegevens



Google-Street-View-Fahrten werden auch zum Scannen von WLAN-Netzen genutzt

Datenschützer fordern sofortigen Ausbau der WLAN-Scanner aus Google-Street-View Fahrzeugen

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, hat über eine andere europäische Datenschutzbehörde erfahren, dass Google-Street-View-Fahrzeuge auch mit einem Scanner für WLAN-Netze ausgestattet waren.

Ein Vertreter von Google Inc. hat auf Nachfrage gegenüber dem zuständigen Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, Prof. Dr. Johannes Casper, eingeräumt, dass auch in Deutschland alle für den Internetdienst von Google Street View im Einsatz befindlichen Fahrzeuge mit technischen Geräten zur Kartografie von WLAN-Netzen ausgestattet seien. Eine schriftliche Antwort auf Fragen über die genauen technischen Vorgänge und Hintergründe dieser Erfassung haben wir von Google nicht erhalten. Eben wenig wurde uns bisher die Beschäftigung eines Google-Street-View-Fahrzeugs ermöglicht.

Damit erhärtet sich der Verdacht, dass die Fahrten für Google Street View in den letzten Jahren nicht nur zur Aufnahme von Straßensichten, sondern auch zur flüchtlingsdeckenden Erhebung und Speicherung gerade auch der von privaten Haushalten betriebenen WLAN-Netze genutzt wurden. Nach gegenwärtigen Erkenntnissen ist davon auszugehen, dass neben der örtlichen Erfassung, dem Verschlüsselungsstatus der Geräte, der weltweit eindeutigen MAC-Adresse auch der vom Betreiber vergebene Name (sogenannte SSID) gespeichert wurde. Bei letzteren verwendenden Privatpersonen nicht selten ihre Klarnamen oder andere auf sie hinweisende Informationen. Sowohl mit Blick auf die Benutzung des eigenen Namens als auch auf die Möglichkeit, die WLAN-Netze aufgrund ihrer örtlichen Lage Bewohnern von Häusern zuzuordnen, handelt es sich um die Erfassung und Speicherung personenbezogener Daten und deren Übertragung in die USA.

Hierzu erklärt Professor Dr. Johannes Casper: Das Vorgehen von Google ist nicht akzeptabel. Zu keiner Zeit war dieses rechtswidrige Scannen Gegenstand der geführten Gespräche über Google Street View. Die Betreiber von WLAN-Netzen haben von der heimlichen Speicherung ihres Netzwerks nichts bemerkt. An einer Verhinderung insbesondere der öffentlichen Verbreitung des Verschlüsselungsstatus haben sie aber ein großes Interesse. Informationen über den Verschlüsselungsstatus sind höchst missbrauchsanfällig und können durchaus dazu führen, dass entsprechende Daten als Wegweiser für Schwarzurfer genutzt werden. Ich fordere daher den sofortigen Ausbau aller entsprechenden Scanner. Die Fahrten für Google-Street-View dürfen erst wieder aufgenommen werden, wenn Google auf den Boden unserer Vereinbarung vom Juni 2009 zurückkehrt und die datenschutzwidrigen Fahrten zum Netzwerkeintrag einstellt.

Google Streetview wereldwijd....

Google Streetview

- mogelijk naar aanleiding van CBP last-ondwangsom implementeert Google opt-out
- via `_nomap` instructie in Wfi-router-naam

Wifi-gegevens af te schermen voor Google

Gepubliceerd: dinsdag 15 november 2011 11:11
Update: dinsdag 15 november 2011 11:23



Nederlanders kunnen zich vanaf dinsdag verzetten tegen verwerking van hun wifi-gegevens door internetgigant Google. Zij kunnen met hun computer hun draadloze netwerk zo instellen dat hun gegevens niet meer door Google verzameld en gebruikt worden. Dat meldde het College Bescherming Persoonsgegevens (CBP), dat aandrang op deze 'opt-out-mogelijkheid'.

- Google wist wifi-gegevens
- Google stapt naar rechter
- Google heeft spijt
- CBP dreigt google met dwangsom
- Google verzamelde data via Street View
- Bekijk het maar met je privacy

Google meldt op zijn weblog dat het bedrijf deze optie wereldwijd heeft ingevoerd. Internetters die gebruik willen maken van deze opt-out, hoeven alleen 'nomap' toe te voegen achter de bestaande netwerknaam van hun wifi-kastje.

Het privacycollege tikte Google afgelopen april op de vingers omdat het bedrijf met de rondrijdende Street View-auto's persoonlijke gegevens van burgers verzamelde. Deze gegevensverzameling was onrechtmatig, omdat Google het publiek hierover niet informeerde en geen mogelijkheid bood waarmee mensen zich konden verzetten tegen deze gang van zaken. Met de opt-outmogelijkheid komt Google tegemoet aan de wensen van het CBP.

Google had met de Street View-auto's ook inhoudelijke gegevens opgeslagen. Deze inhoudelijke gegevens zijn eerder dit jaar door Google vernietigd.

Diginotar

Google Streetview

- almost unnoticed when introduced in the Netherlands, in Germany many privacy concerns
- Dutch DPA acts against WiFi-data collection, allegedly with global implications

Diginotar

- one of the most serious hacks ever
- almost lockdown of all government and many other websites
- call for security breach notification obligation

Telecom bewaarplicht

- bewaarplicht van verkeers- en gebruikers-gegevens
- t.b.v. voorkoming, opsporing en vervolging van ernstige criminaliteit

Diginotar

Diginotar

- one of the most serious hacks ever
- almost lockdown of all government and many other websites
- call for security breach notification obligation



Telecoms Data Retention

Google Streetview

- almost unnoticed when introduced in the Netherlands, in Germany many privacy concerns
- Dutch DPA acts against WiFi-data collection, allegedly with global implications

Diginotar

- one of the most serious hacks ever
- almost lockdown of all government and many other websites
- call for security breach notification obligation

Telecoms Data Retention

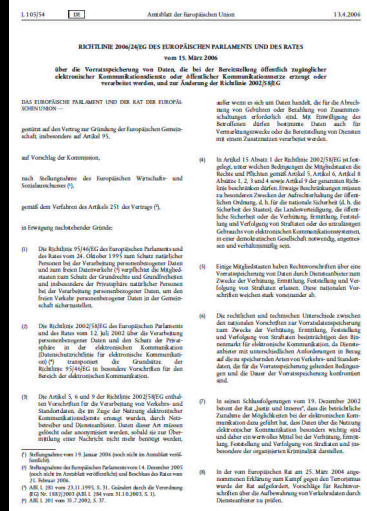
- bewaarplicht van verkeers- en gebruikersgegevens
- t.b.v. voorkoming, opsporing en vervolging van ernstige criminaliteit

bewaarplicht telecomgegevens

Telecom bewaarplicht

- bewaarplicht van verkeers- en gebruikers-gegevens
- t.b.v. voorkoning, opsporing en vervolging van ernstige criminaliteit

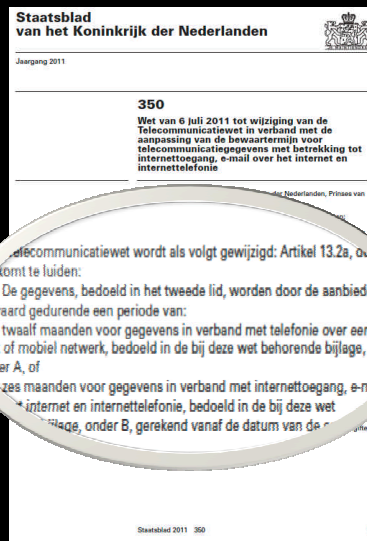
EHvJ 10 februari 2009, zaak C-301/06



bewaarplicht in Nederland

Telecom bewaarplicht

- veel discussie over te bewaren gegevens en bewaartermijnen, vooral in Eerste Kamer
- 12 maanden voor telefonie en internet, met toezegging dat termijn voor internet 6 maanden wordt...



bewaarplicht in Duitsland

Telecom bewaarplicht

- Bundesverfassungsgericht acht bewaarplicht ongrondwettelijk(!)
- vanwege ontbreken privacywaarborgen

Duitse bewaarplicht ongrondwettig. En in Nederland?

G.-J. Zwenne en F. Simons*

Op 1 maart jongstleden verklaarde het Duitse Bundesverfassungsgericht de Duitse implementatie van de Europese dataretentierichtlijn ongrondwettig. Volgens onze Minister van Justitie heeft het geen gevolgen voor Nederland. Uit rechts juridisch oogpunt heeft de minister niet ongelijk. De vraag nu is het Duitse constitutionele kerf recht echter wel machtsloos die ook in de discussie rond de Nederlandse bewaarplicht aan de orde is.

1. Inleiding

De Implementatiewet 2006/24/EG heeft onder de naam de Telecommunicatie- en Internetgegevens bewaarplicht zijn voor het onderscheiden, opgevoeren en vastleggen van essentiële communicatie ("essence of communication") ("Erkennend Verordening") van de Duitse wet op de Telecommunicatie ("Telekommunikationsgesetz") van de Duitse Bundestag. Het doel van de wet is om de veiligheid van de Duitse samenleving te waarborgen, te voorkomen dat de Duitse samenleving in de toekomst in de bewaarplicht geïmplementeerd is. Het doel van de wet is om de veiligheid van de Duitse samenleving te waarborgen, te voorkomen dat de Duitse samenleving in de toekomst in de bewaarplicht geïmplementeerd is.

2. Het BVG arrest

2.1 **Bewaarplicht niet a priori disproportioneel**
De Implementatiewet verklaart de telecommunicatie- en internetgegevens retentie van minimaal 30 maanden en het beroep naar voren van de data van de communicatie worden bewaard. In Duitsland heeft de regering gekozen voor de grootste bewaarplicht van het continent. Volgens het BVG, vooraf deze, in termen van de richtlijn dat minimale bewaarplicht minimum een kwart eeuw zal worden op het telecommunicatiepakket, een inbreuk met een redelijke de de richtlijn met een redelijke termijn. Maar dat doet niet afrekent met het dat een dergelijke bewaarplicht onder voorwaarden proportioneel kan zijn.

De Implementatiewet heeft een redelijke termijn als minimum eis. Het BVG begint met bepaling van de telecommunicatie als minimum en niet daarna de bepaling van de termijn. Het BVG begint met bepaling van de telecommunicatie als minimum en niet daarna de bepaling van de termijn. Het BVG begint met bepaling van de telecommunicatie als minimum en niet daarna de bepaling van de termijn.

Elke preventieve opslag van telecommunicatie- en internetgegevens aan de hand van een eerdere beslissing, indien deze voor een andere bestemming, aan de voor de rechtspraak of de rechterlijke instanties of de instellingen, die deze gegevens voor het bewaaren van zijn dossier als gerecht beschouwen. Er worden hierboven

* Gerrit-Jan Zwenne en Frank Simons zijn advocaten bij Breda & Breda De Oude Elzen, Groot- en Kleinhandelsrecht, en de Duitse rechtssystemen van de Universiteit Leiden.
1. Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenoteerd of vervaardigd in verband met de aanbesteding van openbare telecommunicatie- en internetdiensten of van openbare telecommunicatie- en internetdiensten.
2. BGH, NJW 2006, 1211.
3. Vgl. Ministeriaal Besluit Kennisgeving van 2006-03-20/06-12-1211.
4. BVG, I, BVerfGE 116, 346 van 1 maart 2006, Absatz 51-52; vgl. www.BVG.de/arschuldner/arschuldner.html.
5. Richtlijn 2006/24/EG van de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenoteerd of vervaardigd in verband met de aanbesteding van openbare telecommunicatie- en internetdiensten of van openbare telecommunicatie- en internetdiensten.
6. Art. 1, par. 1, lid 1, sub 1, van de Grondwet van 1990.
7. Art. 1, par. 1, lid 1, sub 1, van de Grondwet van 1990.
8. Overeenkomst.



<http://bit.ly/DAAD30nov2011>

#DAAD30nov2011



VRAGEN?

gerrit-jan.zwenne@twobirds.com

