BIG BROTHER AWARDS

JURYRAPPORT 2010

ORGANISATIE

De Big Brother Awards wordt geörganiseerd door Bits of Freedom:
http://www.bigbrotherawards.nl
http://www.bof.nl

OPMAAK

Verzorgd door Largetosti:
http://www.largetosti.com

DE GENOMINEERDEN

OVERHEID

BEDRIJVEN

VOORSTELLEN

PERSONEN

De genomineerden voor de Big Brother Awards 2010 zijn vastgesteld door de onafhankelijke expertjury.

OVER DE BIG BROTHER AWARDS

Met de Big Brother Awards worden elk jaar personen, bedrijven, overheden en voorstellen te kijk gezet die het afgelopen jaar bij uitstek controle op burgers en inbreuken op privacy hebben bevorderd.

DE NAAM

De prijs ontleent haar naam aan de totalitaire, alziende leider 'Big Brother' uit het boek 1984 van George Orwell.

INTERNATIONAAL

De eerste Big Brother Awards werden in 1998 georganiseerd door Privacy International in Engeland. Sindsdien vindt dit evenement in veel landen plaats.

ORGANISATIE DOOR BITS OF FREEDOM

De organisatie van de Nederlandse versie van de Big Brother Awards is in handen van stichting Bits of Freedom, een burgerrechtenbeweging die opkomt voor vrijheid op internet en voor privacy. Deze grondrechten zijn onmisbaar voor ieders sociale en persoonlijke vrijheid, voor maatschappelijke innovatie en voor een democratische rechtsstaat. Maar die vrijheid is niet vanzelfsprekend. Persoonlijke gegevens worden opgeslagen en geanalyseerd. Het internetverkeer van burgers wordt geanalyseerd, afgeknepen en geblokkeerd. De kracht van Bits of Freedom ligt in de combinatie van expertise, een constructieve lobby waar mogelijk, en scherpe publiekscampagnes waar nodig. De Big Brother Awards zijn een voorbeeld van het laatste. Meer informatie over Bits of Freedom vindt u op de website www.bof.nl.

De zevende editie van de Big Brother Awards Nederland, op 9 maart 2011, is mede mogelijk gemaakt door de hulp van talloze vrijwilligers, Pakhuis de Zwijger en ontwerpbureau Largetosti. Bits of Freedom wil hen hiervoor hartelijk bedanken.

Amsterdam, 28 februari 2011

OVER DIT RAPPORT

Voor u ligt het juryrapport waarin de nominaties voor de Big Brother Awards 2010 worden toegelicht. De winnaars van de Awards worden, net als de winnaars van de Publieksprijs en de Winston Award, bekend gemaakt op 9 maart 2011 tijdens een feestelijke prijsuitreiking in Pakhuis de Zwijger.

SINDS 20 JANUARI
kon het publiek kandidaten voordragen in vier categorieën: overheid, voorstellen, bedrijven en personen. De jury wil alle inzenders hartelijk bedanken: velen van u kwamen met goede motiveringen en nauwkeurige bronvermeldingen.

DAARNA KON DE JURY AAN DE SLAG
De jury is samengesteld uit experts op het gebied van internet, computerbeveiliging, informatierecht, consumentenproblematiek en journalistiek. De jury heeft tijdens de beraadslagingen in volledige onafhankelijkheid geopereerd. Bits of Freedom noch andere personen of organisaties hebben op enigerlei wijze invloed uitgeoefend op het oordeel van de jury.

DIT JAAR
heeft de jury slechts twee nominaties in de categorie voorstellen toegekend. Vanwege de val van het kabinet, de verkiezingen en de daaropvolgende lange formatieperiode heeft het kabinet in 2010 maar een beperkt aantal voorstellen kunnen doen. De categorie overheid echter telt vier nominaties: er waren simpelweg te veel zeer verschillende en ijzersterke nominaties.

De jury hoopt op een levendig maatschappelijk debat over de genomineerden, en wenst u veel leesplezier toe met dit rapport.


OVERHEID

DE BELASTINGDIENST

Verplicht burgerservice-nummer rondbazuinen

De Belastingdienst dwingt kleine ondernemers hun burgerservice-nummer (BSN) rond te bazuinen, terwijl de overheid bij wet heeft vastgelegd dat het BSN alleen in het verkeer tussen overheid en burger mag worden gebruikt. Freelancers – van de coach op de hoek tot de bekende Nederlander op televisie – gaan allemaal voor de bijl.

Nederland kent meer dan een half miljoen ZZP'ers: zelfstandige ondernemers zonder personeel. Zij krijgen van de Belastingdienst een BTW-nummer toegewezen dat gelijk is aan hun burgerservice-nummer. Dit BTW-nummer moet door de ondernemer op elke factuur worden vermeld. Ondernemers die niet BTW-plichtig zijn, moeten een zogenaamde 'verklaring arbeidsrelatie' (VAR) aanvragen; in het kenmerk daarvan is eveneens het BSN verwerkt. Ook deze verklaring moet – nota bene met een kopie van het identiteitsbewijs – aan al hun klanten worden verstrekt.

De Nederlandse overheid heeft de burger bij de introductie van het BSN voorgehouden dat het nieuwe nummer identiteitsfraude zou tegengaan. Critici zoals hoogleraar Prins (Universiteit Tilburg) zijn minder optimistisch. Zij merkt op dat het BSN veel breder wordt ingezet dan zijn voorganger, het sofi-nummer; dat betekent dat áls het misgaat de consequenties ook veel groter zijn. Iemands BSN geeft toegang tot alle informatie van deze persoon waarover de overheid beschikt. Dat zijn niet alleen iemands sociaalfiscale gegevens, maar ook gegevens over onderwijs, (para)medische en maatschappelijke zorg, en zelfs over justitiële aangelegenheden.

Aangezien het burgerservice-nummer de sleutel vormt tot een schat aan gegevens over iemand, is deze unieke en persoonsgebonden cijferreeks een goudmijn voor iedereen die onbevoegd toegang tot andermans gegevens zoekt. Bij de invoering van het BSN is daarom bij wet vastgelegd dat dit nummer uitsluitend mag worden gebruikt voor communicatie tussen de burger en de overheid. Uitzonderingen op die regel moeten bij wet zijn vastgelegd. Ander gebruik is niet toegestaan. De jury merkt op dat overheid haar eigen regels te buiten gaat.

De jury vind het onverantwoord dat de Belastingdienst kleine zelfstandigen dwingt hun burgerservice-nummer rond te bazuinen. De overheid negeert daarmee haar eigen wet- en regelgeving, en zet de bescherming van de identiteit van kleine ondernemers op het spel.

MEER INFORMATIE

Computerrecht, 'Het BurgerServiceNummer en de strijd tegen Identiteitsfraude' (2003)
http://arno.uvt.nl/show.cgi?fid=5938
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties over het burgerservicenummer, 'Neemt de kans op identiteitsfraude toe met de invoering van het burgerservicenummer?'
http://www.burgerservicenummer.nl/veelgestelde_vragen/vragen_en_antwoorden#v1026
Radio online, 'Online privacyprobleem BN'ers dankzij KvK' (04.04.09)
http://www.radio1.nl/contents/4912-online-privacyprobleem-bn-ers-dankzij-kvk

HET MINISTERIE VAN SZW: PANDBRIGADES EN HUISDOORZOEKINGEN

‘Wij komen even onderzoeken of u iets te verbergen hebt’

De Haagse Pandbrigade en het Rotterdamse Interventieteam leggen huisbezoeken af op zoek naar illegale activiteiten van bewoners. Alle huizen in een buurt worden systematisch afgewerkt op grond van een algemene verdenking tegen de wijk. Wanneer de brigade eenmaal ergens binnen is, wordt zowat alles onderwerp van onderzoek, tot aan leerplichtkwesties toe. Het ministerie van Sociale Zaken en Werkgelegenheid heeft een wetsvoorstel gelanceerd om een vergelijkbare aanpak landelijk in te voeren.

De gevolgen voor burgers zijn verstrekkend. Zo kon een Haagse bij thuiskomst opeens haar huis niet meer in: de Haagse Pandbrigade had het huis in haar afwezigheid doorzocht en had, om binnen te komen, het slot open geboord. Van het vermoeden van onrechtmatig gebruik van de woning (c.q. dat niet alle bewoners waren ingeschreven) bleek niets te kloppen. Ook in Rotterdam worden dergelijke huisbezoeken afgelegd: daar om de gemeentelijke basisadministratie te controleren.

Al in 2007 constateert Rotterdamse Ombudsman dat burgers het recht hebben om de doorzoeking te weigeren, maar dat zij in de praktijk 'onder oneigenlijke druk gezet worden om toestemming voor een huisbezoek te geven'. De gemeente laat zich bij het binnentreden 'niet van de beste kant zien' en burgers worden 'willens en wetens overrompeld'. De Ombudsman concludeert dat de bezoeken vaak 'het karakter van een fishing expedition' hebben.

De criteria voor een huisbezoek zijn minimaal: wie als een alleenstaande een woning met een andere alleenstaande deelt, kan al op visite rekenen. Dat geldt ook voor alleenstaande moeders die tijdens hun uitkeringsperiode een kind krijgen, of voor mensen die net een uitkering hebben aangevraagd. Soms is het voldoende om in een specifieke wijk te wonen: in sommige gebieden wordt huis-aan-huis gecontroleerd. Veel bezoeken zijn te danken aan de slechte gemeentelijke administratie, zeggen ambtenaren van de Haagse Pandbrigade. Omdat er geen sprake is van een gerichte verdenking, zijn burgers niet verplicht de brigades en teams binnen te laten. Maar veel burgers weten dat niet en vaak zijn ze sterk afhankelijk van de overheid die binnen komt stormen.

De samenleving heeft er baat bij als de gemeente haar administratie op orde krijgt, spijbelende kinderen naar school stuurt, fraude met sociale voorzieningen tegengaat en wijken veiliger maakt. Maar het ingezette instrument moet voldoen aan het proportionaliteits- en subsidiariteitsbeginsel. Staat de maatregel in verhouding tot het probleem, is hij noodzakelijk, is er geen andere weg? Deze praktijk maakt een enorme inbreuk op de persoonlijke levenssfeer van burgers. De jury vindt de categorische huisdoorzoekingen van de brigades en interventieteams op gespannen voet staan met het Europees Verdrag voor de Rechten van de Mens.

Het ministerie van Sociale Zaken heeft nu een wetsvoorstel ingediend om de interventieteams nationaal in te voeren. Elke uitkeringsgerechtigde kan bezoek van controleurs krijgen, ook zonder concrete verdenking van fraude. Wie de controleurs niet binnenlaat, kan worden gestraft met korting op of intrekking van de uitkering (kinderbijslag, AOW, bijstand). De jury vind het een draconisch plan: ambtenaren die huizen mogen doorsnuffelen zonder dat de bewoner ook maar ergens van wordt verdacht.

MEER INFORMATIE

Kamerstukken aangaande 'Een regeling in de sociale zekerheid van de rechtsgevolgen van het niet aantonen van de leefsituatie na het aanbod van een huisbezoek'
https://zoek.officielebekendmakingen.nl/dossier/31929
Rapport Ombudsman van Rotterdam, 'Baas in eigen huis' (02.11.07)
http://www.ombudsman.rotterdam.nl/publicaties/Eindrapport%20Baas%20in%20eigen%20Huis.pdf
Sargasso, 'Verdacht volgens de Haagse Pandbrigade' (16.08.10)
http://sargasso.nl/archief/2010/08/16/verdacht-volgens-de-haagse-pandbrigade/
Sargasso, 'Pandbrigade: Als we dan toch binnen zijn…' (17.08.10)
http://sargasso.nl/archief/2010/08/17/pandbrigade-binnen-zijn/
Sargasso, 'Haagse Pandbrigade: Verzet en vragen' (18.08.10)
http://sargasso.nl/archief/2010/08/18/haagse-pandbrigade-verzet-en-vragen/
Binnenlands Bestuur, 'Pandbrigade kuist Haagse wijken' (03.05.10)
http://www.binnenlandsbestuur.nl/pandbrigade-kuist-haagse-wijken.158102.lynkx
Vragen Haagse Stadspartij naar aanleiding van Haagse Pandbrigade (15.07.10)
http://www.haagsestadspartij.nl/index.php?action=artikel&artikel_ID=462
Brief Inspecteur Project Haagse Pand Brigade over controle bewoning (15.06.09)
http://www.denhaagtekijk.nl/Pandbrigade/brieve1.jpg
Brief Algemeen Directeur Dienst Stedelijke Ontwikkeling over voorgenomen huisbezoek van de Haagse Pand Brigade (10.07.09)
http://img18.imageshack.us/img18/8489/briefgemeentedeel1.jpg
http://img35.imageshack.us/img35/2174/briefgemeentedeel2.jpg
Gemeente Den Haag, 'De Haagse Pandbrigade – Verbeteren van de leefbaarheid en veiligheid in Den Haag' (14.12.09)
http://www.denhaag.nl/home/bewoners/to/De-Haagse-Pandbrigade.htm

DE NEDERLANDSE ZORGAUTORITEIT

De jury wordt er depressief van...

De Nederlandse Zorgautoriteit (NZa) negeert bewust een rechterlijke uitspraak en geeft zorgverzekeraars inzage in de diagnoses van psychiatrische patiënten. Psychiaters en psychotherapeuten worden daardoor verplicht om zowel hun beroepsgeheim als de privacy van hun patiënten te schenden.

De NZa houdt toezicht op de naleving van wet- en regelgeving door zorgaanbieders en zorgverzekeraars. In 2008 heeft de NZa psychiaters en psychotherapeuten de verplichting opgelegd om expliciet diagnostische gegevens op de DBC-declaraties te vermelden. (In een DBC (een diagnose-behandelcombinatie) is precies vastgelegd welke behandeling bij een diagnose hoort en welk prijskaartje daar aan mag hangen.) Daarmee komt ook een beschrijving van de symptomen van de patiënt en de geleverde behandeling in de administratie van de zorgverzekeraars terecht.

Veel psychiaters en psychotherapeuten hebben geprotesteerd: zij hebben een beroepseed afgelegd en dienen strikt vertrouwelijk om te gaan met hun kennis over hun patiënten. Psychische problemen zijn buitengewoon privacygevoelig en mogen onder geen beding aan derden worden meegedeeld, óók niet aan zorgverzekeraars. Wanneer patiënten er niet op kunnen bouwen dat hun diagnose en behandeling binnen de grenzen van de spreekkamer blijft, zullen zij niet meer openhartig kunnen praten met hun behandelaar.

In augustus 2010 is de NZa door het College van Beroep voor het

bedrijfsleven (CBb) tot de orde geroepen. Het CBb bevestigde het standpunt van de beroepsgroep en onderschreef het belang van de privacy van de patiënt en van het beroepsgeheim. De verplichting om de diagnose op de declaraties te vermelden werd geschorst.

Niettemin stellen de zorgverzekeraars nog altijd dusdanige eisen aan declaraties dat daaruit de diagnose eenvoudig kan worden afgeleid. De NZa weet dit, maar negeert de privacy-schendende consequentie ervan. Zij schrijft: 'De voorlopige voorziening beperkt zich [..] tot het [..] niet hoeven voldoen aan de verplichting om diagnose-informatie en lekenomschrijving op de DBC-factuur te vermelden. Dat [..] via omwegen uiteindelijk toch achterhaald kan worden op welke diagnose een factuur [..] betrekking heeft, is op zich geen onjuiste constatering, maar doet aan de inhoud van de voorlopige voorziening verder niet af.'

De NZa moet zich naar letter en geest aan de uitspraak conformeren, maar omzeilt beide doelbewust. De jury oordeelt dat het NZa daardoor zowel de medische privacy van patiënten als het beroepsgeheim van psychiaters en psychotherapeuten ernstig schendt.

MEER INFORMATIE

Uitspraak College van Beroep voor het bedrijfsleven (02.08.10)
http://www.rechtspraak.nl/ljn.asp?ljn=BN3056&u_ljn=BN3056
College van Beroep voor het bedrijfsleven, 'Grondslag tariefstructuur voor vrijgevestigde psychiaters door NZa onvoldoende onderzocht' (02.08.10)
http://www.rechtspraak.nl/Gerechten/CBb/Actualiteiten/Vermelding+diagnose+op+declaraties+voorlopig+van+de+baan.htm
E-mail Nederlandse Zorgautoriteit, 'negeren van rechterlijke uitspraak door ziektekostenverzekeraars' (15.11.10)
http://www.enrgin.nl/xdata/devrijepsych/Downloads/BriefNZa15november2010.pdf
E-mail helpdesk GGZ, 'Antwoord op de vraag of de diagnose zichtbaar of herleidbaar is' (05.10.10)
http://www.enrgin.nl/xdata/devrijepsych/Downloads/DBCOnderhoudhelpdesk.pdf
Vrij Nederland, 'Vrijuit praten bij de dokter kan weer' (12.08.10)
http://www.vn.nl/Archief/Samenleving/Artikel-Samenleving/Vrijuit-praten-bij-de-dokter-kan-weer.htm

HET OPENBAAR MINISTERIE

Pas op: reaguren maakt verdacht

Het Openbaar Ministerie vraagt regelmatig de gegevens op van bezoekers van journalistieke websites, zonder daarbij een gerechtelijk bevel te kunnen overleggen. Wanneer niet meteen aan het verzoek wordt voldaan, dreigt het OM met dwangmiddelen als arrestatie en gijzeling. Pas dus op als je naar een nieuwsbericht surft: soms vindt de politie het kennelijk nodig precies te weten wie dat bericht allemaal hebben gelezen. De jury vindt dat het Openbaar Ministerie met deze sleepnetacties een nominatie in de wacht sleept.

Nadat een lokale krant verslag doet van de Nieuwjaarsrellen in Culemborg, vordert Justitie prompt gegevens van iedereen die de website gedurende de eerste vier dagen van 2010 had bezocht. Justitie hoopt zo te kunnen achterhalen wie op welk moment het bewuste artikel heeft gelezen en wie erop heeft gereageerd. De krant weigert gelukkig: 'Justitie gooit een sleepnet uit en bekijkt vervolgens wat de vangst is.'

Een jaar later probeert Justitie het opnieuw, nu bij de website Crimesite. Onder een artikel over een ernstige mishandeling staan reacties van mogelijke getuigen. Justitie eist de IP-adressen op van twee mensen die op het bericht hebben gereageerd. Nadat de website de gevraagde informatie weigert af te staan, dreigt Justitie de hoofdredacteur te arresteren. Pogingen van de redactie om de situatie te bespreken met de officier van justitie blijven onbeantwoord.

In beide gevallen ging het OM haar boekje ver te buiten. Alleen van specifieke bezoekers mag eventueel een IP-adres worden opgevraagd. Maar dan moet er wel een gerichte verdenking jegens juist die persoon bestaan en is bovendien een rechterlijk bevel nodig. Het OM doet alsof het simpele lezen van een online krantenbericht al voldoende grond vormt voor een verdenking. In de Crimesite-kwestie behandelt het OM voorts mogelijke getuigen als waren zij verdachten – een gelijkstelling die bepaald niet op gaat.

Gelukkig heeft ook de Tweede Kamer kritiek op dergelijk gedrag. Naar aanleiding van Kamervragen van de leden Hennis-Plasschaert en Van der Steur (VVD) floot minister Opstelten het OM onlangs terug. De minister tekent aan dat voor zulke verzoeken een bevel van de rechter nodig is. In de hoop dat het OM zo haar lesje leert en zich voortaan zelf ook aan de wet houdt, nomineert de jury het Openbaar Ministerie.

MEER INFORMATIE

Culemborgse Courant, 'Officier van Justitie vordert internetverkeer CulemborgseCourant.nl' (15.02.10)
http://www.culemborgsecourant.nl/page/Nieuws-detail/Officier-van-Justitie-vordert-internetve.494804.news

Crimesite, 'Amsterdamse recherche dreigt hoofdredacteur Crimesite met arrestatie' (04.01.11)
http://www.crimesite.nl/crimesite/159-headlines/20416-amsterdamse-recherche-dreigt-hoofdredacteur-crimesite-te-arresteren.html

Antwoorden Kamervragen van de leden Hennis-Plasschaert en Van der Steur (17.02.11)
http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2011/02/18/173227-antwoorden-kamervragen-over-het-opvragen-van-ip-adressen-door-politie-en-justitie/2011z00200-antwoorden-kamervragen-over-het-opvragen-van-ipadressen-door-politie-en-justitie-24374.pdf

Bits of Freedom, 'Opsporingsdiensten teruggefloten; reaguren weer veilig?' (23.02.11)
https://www.bof.nl/2011/02/23/opsporingsdiensten-teruggefloten-reaguren-weer-veilig/


Ability to sleep under any cond is my biggest talent. Just slept ~9hrs on Chicago-Tokyo flight... In additn to ~2hrs on Boston-Chicago flt!

BEDRIJVEN

ABN AMRO: PRIVACY ANNO NU

Een bankrekening die rente trekt van jouw privacy

In september 2009 werd ABN AMRO betrapt: via haar website verzamelde de bank op steelse wijze – en bovendien onveilig – gegevens over haar bezoekers. Voor ABN bood het nieuwe jaar geen nieuwe kansen: de bank ging door met deze praktijk, nu alleen nog heimelijker. De ABN-klanten zijn het kind van de rekening.

Bij het bezoeken van de website van ABN AMRO werden achter de schermen een aantal cookies op de computer van de bezoeker geïnstalleerd. Die cookies waren niet alleen van de bank maar ook van andere partijen, zoals Ilsemedia en 2o7.net. Alleen wie zogenaamde 'browser plug-ins' gebruikte, merkte dat zijn gegevens aan andere partijen beschikbaar werden gesteld.

De bank werd hiervoor publiekelijk op de vingers getikt door digitaal onderzoeksbureau Unit 10. Dat mocht niet baten. De bank verstopte de truc dieper in de broncode van haar website, zodat de plug-ins niet langer alarm konden slaan wegens de aanwezigheid van onveilige en ongewenste scripts. De gegevens worden nog steeds verzameld en aan derden verstrekt. ABN AMRO verklaart dat haar eigen privacyvoorwaarden niet van toepassing zijn op websites waarmee de website van de bank verbonden is. Oftewel: wij doen gerust aan privacy hoor, we sluizen uw gegevens alleen door aan bedrijven die dat niet hoeven te doen.

Klanten van ABN AMRO hebben geen alternatief: ze kunnen niet aangeven of ze ABN AMRO wel of niet toestemming geven om hun gegevens te (laten) gebruiken. Wanneer gebruikers met veel technische kunstgrepen wisten te vermijden dat de bank hun privégegevens ontfutselt en doorsluist, konden ze daarna opeens niet meer internetbankieren. Verder geeft ABN AMRO geen uitsluitsel over wat er nu precies gebeurt met de gegevens die ze verzamelt en wat een derde partij als Omniture daarmee doet. Tot overmaat van ramp vindt het doorsluizen van de bezoekersinformatie plaats via een onversleutelde – en dus onveilige – verbinding.

Het is dus onduidelijk hoe hoog de 'digitale rente' is bij dé bank. Wat de jury wel weet: de klant betaalt de privacyrekening.

MEER INFORMATIE

Unit 10, 'Internetbankieren: Rode kaart voor dé Bank' (24.02.10)
http://www.unit10.nl/nieuws.htm#Internetbankieren:_Rode_kaart_voor_d%C3%A9_Bank
Security, 'ABN AMRO krijgt rode kaart wegens Omniture spyware' (24.02.10)
http://www.security.nl/artikel/32534/1/ABN_AMRO_krijgt_rode_kaart_wegens_Omniture_spyware.html
The Guardian, 'Plagued by the 2o7.net cookie' (24.04.08)
http://www.guardian.co.uk/technology/askjack/2008/apr/24/plaguedbythe2o7netcookie
Privacy statement ABN AMRO
http://www.abnamro.com/nl/footer/privacy-statement.html

HET TNO

Orwelliaanse techniek: een echte Big Brother HIT

Onderzoeksbureau TNO ontwikkelt technologie om verdacht gedrag in openbare gelegenheden op te sporen. Hun lijst is – hoe verrassend – niet openbaar, maar het dragen van een dikke jas wordt afgeraden. Het TNO richt wederom haar pijlen op de controle van burgers en perkt hun privacy in, op zoek naar die ene hit.

De 'Hostile Intent Technology' (HIT) van het TNO bestaat uit een configuratie van camera's, sensoren en software gericht op de interpretatie van gedrag. 'HIT identificeert afwijkende gedragingen zoals wilde gebaren en korte interacties tussen mensen. Door de interpretatie van het gedragspatroon is in veel gevallen een voorspelling over verkeerde bedoelingen, of "hostile intent", mogelijk,' claimt het onderzoeksbureau.

Het sleutelwoord is 'afwijkend gedrag'. Wie zich raar gedraagt, is vast rare dingen van plan. Maar zoals het TNO nota bene in haar eigen promotiefilmpje moet toegeven: 'Daar is geen wetenschappelijk bewijs voor.' Om die reden is de Sectie Forensische Psychologie van de Universiteit Maastricht zeer sceptisch over HIT: 'De kans dat een systeem als Hostile Intent Technology onze samenleving veiliger gaat maken [is] klein. Dit om de eenvoudige reden dat we geen idee hebben wat voor soort gedrag nu bijvoorbeeld een terroristische aanslag voorspelt. Analyses van de aanslagen in New York en Londen lieten juist zien dat de daders zich opmerkelijk normaal gedroegen.' Welke gedragingen het TNO niet zinnen, is onduidelijk: we kregen nul op rekest toen we de lijst van 'verdachte' gedragingen opvroegen bij TNO. Vooralsnog kan

de jury alleen maar concluderen dat het TNO en passant een breed scala aan gedragingen als 'verdacht' bestempelt: schuw zijn, wilde gebaren maken, korte interacties hebben, en – u raadt het al – een dikke jas dragen. Je zult maar een jolige bui hebben, kouwelijk zijn aangelegd of spastisch wezen...

De jury nam de HIT-plannen aanvankelijk weinig serieus. Immers, al in 2002 won TNO een Big Brother Award voor door haar ontwikkelde software met exact dezelfde oogmerken (de zogeheten 'automatische agressie detector video software'), waar we sindsdien gelukkig nooit meer van hebben vernomen. HIT is echter in 2010 getest tijdens live oefeningen met de politie, de marechaussee en particuliere bewakingsdiensten, onder meer op Amsterdam Centraal Station.

TNO vuurt met haar uitvinding in het donker hagel af op vlooien. Laten we hopen dat een tweede Big Brother-nominatie helpt om ook HIT te laten floppen.

MEER INFORMATIE

TNO Magazine, 'Afwijkend gedrag signaleren om aanslagen te voorkomen' (02.2010)
http://www.tno.nl/images/shared/overtno/magazine/tno_mag_2_feb_2010_15.pdf
Forensische Psychologie Blog van de Universiteit Maastricht, 'Hostile Intent' (10.01.11)
http://forensischepsychologie.wordpress.com/2011/01/10/hostile-intent/
Beveiliging Nieuws, 'Hostile Intent Technology van TNO', (09.12.10)
http://www.beveiligingnieuws.nl/video/253/Hostile_Intent_Technology_van_TNO.html
De Naakte Mens, 'Software kijkt of u gevaarlijk bent' (03.05.10)
http://www.denaaktemens.nl/2010/05/03/software-kijkt-of-u-gevaarlijk-bent/

TRANS LINK SYSTEMS EN DE VIJF GROOTSTE OV-BEDRIJVEN

OV-chipkaart op een dood spoor

Met de OV-chipkaart negeert Trans Link Systems al jaren alle kritiek op de beroerde manier waarop het bedrijf omgaat met de privacy van reizigers. Ook blijkt de kaart zo lek als een mandje. Niettemin blijft Trans Link haar speeltje doordrukken. Deze hardleerse houding en de dramatische gevolgen voor reizigers tonen het aan: Trans Link staat met de OV-chipkaart op een dood spoor.

De vijf grootste OV-bedrijven van Nederland hebben Trans Link Systems opgericht om een gezamenlijk elektronisch betaalsysteem in het openbaar vervoer te realiseren: de OV-chipkaart. Inmiddels heeft dit elektronische betaalmiddel in veel regio's de strippenkaart vervangen. 'Voorop staat het gemak voor de reiziger' en 'Alle deelnemende OV-bedrijven en kaartuitgever Trans Link Systems gaan zorgvuldig om met uw persoonsgegevens', belooft het bedrijf op haar website.

De praktijk is anders. De regionale uitrol van de OV-kaart in 2010 bracht steeds meer organisatorische en administratieve problemen aan het licht: studenten die maandenlang geen werkende kaart kregen. Studenten die verplicht moeten in- en uitchecken terwijl ze een overal geldige kaart hebben. Kaarten die het wisselen tussen eerste- en tweedeklas onmogelijk maken.

Poortjes die niet werken. Machines die zomaar 'gratis saldo' opladen. Gelukkig voor Trans Link Systems beperkt de jury zich tot de privacy-aspecten van de kaart. Ook die zijn niet gering. Nederland is het land waar via de OV-kaart de reisgegevens van burgers het langst worden vastgelegd: maar liefst 7 jaar. Dat is op zich al een buitengewoon ernstige privacyschending. Dat de promotiewebsite 'Ervaar het OV' – door Trans Link in samenwerking met de provincie Gelderland opgezet – in 2010 maandenlang zo lek bleek dat de data van de daar geregistreerde 168.000 mensen feitelijk op straat lag, boezemt evenmin veel vertrouwen in. Onder de vele hacks waarvoor de OV-chipkaart zich makkelijk leent – kaarten kunnen thuis worden opgeladen en reistrajecten kunnen thuis worden 'ingevoerd' – vallen helaas ook privacyhacks. Kaarten van andere reizigers kunnen eenvoudig op afstand worden uitgelezen en later gekloond.

Trans Link is uitvoerig gewaarschuwd. Het bedrijf kreeg eerder van deze jury een nominatie (2005) en een prijs (2007); deskundigen toonden al in 2008 aan dat het product 'onherstelbaar kapot' is. Het College Bescherming Persoonsgegevens tikte Trans Link Systems vorig jaar ernstig op de vingers wegens het handelen in strijd met de Wet Reisgegevens en het 'niet beschikken over een verantwoord beleid voor bewaartermijnen'. De OV-chipkaart is definitief stuk. Het antwoord van Trans Link Systems? Dreigen met een rechtszaak tegen een boodschapper van het slechte nieuws, en: zelfs kijken of de OV-kaart voortaan ook als betalingsmiddel kan worden gebruikt.
De jury is ontsteld door zoveel gestuntel en hardleersheid. Zelfs de politiek brengt Trans Link Systems inmiddels in verband met 'Big Brother'. Een nominatie voor de Big Brother Awards kan opnieuw niet uitblijven.

MEER INFORMATIE

College Bescherming Persoonsgegevens, Onderzoek naar Verwerking van persoonsgegevens ten behoeve van de studenten OV-chipkaart bij Trans Link Systems B.V. te Amersfoort' (12.2010)
http://www.cbpweb.nl/downloads_rapporten/rap_2010_ovchip_db_tls.pdf
College Bescherming Persoonsgegevens, 'Onderzoek studenten OV-chipkaart' (09.12.10)
http://www.cbpweb.nl/Pages/pb_20101209_ov-chip.aspx
Trouw, 'Studenten ov-chipkaart geeft problemen' (31.08.10)
http://www.trouw.nl/nieuws/nederland/article3187981.ece/Studenten_ov-chipkaart_geeft_problemen.html
NOS, 'Lek in website aanvragen ov-kaart' (18.05.10)
http://nos.nl/artikel/158104-lek-in-website-aanvragen-ovkaart.html
Webwereld, 'OV-chipkaart nu door iedereen te kraken' (05.11.10)
http://webwereld.nl/nieuws/67699/ov-chipkaart-nu-door-iedereen-te-kraken.html
Z24, 'Trans Link bezint zich op juridische stappen tegen Webwereld' (16.02.11)
http://www.z24.nl/z24geld/autos_reizen/artikel_201481.z24/Translink_bezint_zich_op_juridische_stappen_tegen_Webwereld.html
Nu, 'OV-chipkaart getest als betaalpas' (05.01.11)
http://www.nu.nl/binnenland/2415467/ov-chipkaart-getest-als-betaalpas.html
Webwereld, 'Politiek fel over privacyschending OV-chipkaart' (25.01.10)
http://webwereld.nl/nieuws/64956/politiek-fel-over-privacyschending-ov-chipkaart.html
Webwereld, 'OV-chipkaart onterecht privacyonvriendelijk' (27.01.10)
http://webwereld.nl/nieuws/64974/ov-chipkaart-onterecht-privacyonvriendelijk.html

VOORSTELLEN

DEEP PACKET INSPECTION

Na succes in China en Egypte nu ook in Nederland?

De afluistertechnologie 'Deep Packet Inspection' (DPI) maakt het mogelijk om de inhoud van al het internetverkeer te inspecteren en te analyseren. De inzet van DPI is in flagrante strijd met het grondrecht op privacy en in het bijzonder met het briefgeheim. En hoewel het gebruik van DPI voorbehouden lijkt aan landen als China en (Mubarak) Egypte, staat de technologie ook hier op de politieke agenda.

Met DPI kan worden bijgehouden welke webpagina's een internetgebruiker bezoekt, wat er in bestanden zit die zij downloaden, en kan worden geïnspecteerd wat internetgebruikers elkaar mailen. Desgewenst kan met behulp van DPI een deel van dat verkeer worden geblokkeerd.
In veel Westerse landen, waaronder ook Nederland, wordt de inzet van DPI geregeld geopperd ten behoeve van internetfilters waarmee ongewenste inhoud kan worden gesignaleerd of geblokkeerd. Denk aan filters voor kinderporno of filters om auteursrechtinbreuk tegen te gaan. Maar DPI inzetten om specifieke websites, diensten, bestanden of afbeeldingen ontoegankelijk te maken, betekent onvermijdelijk dat ál het internetverkeer wordt afgeluisterd en geanalyseerd. Anders gezegd: de inzet van DPI behelst een permanente internettap voor alle Nederlandse internetgebruikers.

Het moge duidelijk zijn dat DPI zodoende in flagrante strijd is met het

grondrecht op privacy en in het bijzonder met het briefgeheim, dat beschermd wordt in de Nederlandse Grondwet en in het Europees Verdrag voor de Rechten van de Mens. Het is onacceptabel om zonder concrete verdenking het internetverkeer van alle burgers (benevens dat van instellingen en bedrijven) af te luisteren. Deze bezwaren zijn in het kader van de handhaving van het downloadverbod in 2009 ook al uitgebreid aan de orde gekomen en hebben toen tot grote publieke weerstand geleid. Maar plannen voor DPI blijven desondanks de kop opsteken.

Na Kamervragen van de SP bleek recent dat het ministerie van Veiligheid en Justitie onderzoek doet naar de inzet van DPI. De jury acht het de hoogste tijd dat het ministerie afscheid neemt van de gedachte dat Nederland veiliger wordt door ieders internetverkeer tot op de laatste bit en byte controleren.

MEER INFORMATIE

Tweakers, 'Deep packet inspection mogelijk ingezet tegen kinderporno' (03.12.10)
http://tweakers.net/nieuws/71104/deep-packet-inspection-mogelijk-ingezet-tegen-kinderporno.html
Webwereld, 'Justitie overweegt internet permanent te tappen' (19.02.11)
http://webwereld.nl/nieuws/67999/justitie-overweegt-internet-permanent-te-tappen.html
Freepress, 'Questions Raised About U.S. Firm's Role in Egypt Internet Crackdown' (19.02.11)
http://www.freepress.net/press-release/2011/1/28/questions-raised-about-us-firms-role-egypt-internet-crackdown

SLIM PRIJZEN REGIORING

Krijg geld om van uw telefoon een spionagekastje te maken

Stadsregio Arnhem Nijmegen geeft geld voor uw whereabouts. SLIM Prijzen is een project waaraan automobilisten vrijwillig kunnen basis deelnemen en waarbij deelnemers, tegen een financiële vergoeding, toestemming geven voor het registreren en verwerken van hun ritgegevens. Het doel: bewustwording over en het voorkomen van files. De jury nomineert SLIM Prijzen, omdat de opzet van het systeem anonimiteit niet waarborgt en ondertussen automobilisten klaarmaakt voor de controlemaatschappij.

Met behulp van GPS in de telefoon of PDA wil SLIM Prijzen registreren hoeveel, waar en wanneer een deelnemer rijdt. Camera's op meet- en controlepunten registreren tevens of, hoe laat en wanneer de deelnemers langsrijden. Iedere deelnemer is op grond van de voorwaarden verplicht een logboek bij te houden. Bij aanvang van de 'beloningsperiode' wordt deelnemers een bedrag in het vooruitzicht gesteld. Zij worden hierop vervolgens € 4,- gekort voor elke keer dat zij tijdens de spits op de RegioRing rijden.

Billboards, abri's en advertenties in de regionale dagbladen volstonden klaarblijkelijk niet om genoeg vrijwillige deelnemers te overtuigen. Bij ruim 30.000 automobilisten die zich niet hadden aangemeld, viel daarom 'spontaan' een herinnering op de deurmat om alsnog deel te nemen. Aan de hand van

kentekenregistraties is was namelijk op voorhand bepaald wie aan dit project zouden kunnen deelnemen.

De initiatiefnemers van SLIM Prijzen – de stadsregio Arnhem Nijmegen, de gemeente Nijmegen en het ministerie van Verkeer en Waterstaat (het huidige ministerie van Infrastructuur en Milieu) – geven zich onvoldoende rekenschap van de privacyaspecten van hun plan. Dat bleek al uit het ongevraagd in kaart brengen en benaderen van mogelijke deelnemers aan het project. Het minutieus observeren van de verkeersgedragingen van de deelnemende automobilisten staat in geen enkele verhouding tot het doel van het project – filebestrijding en bewustwording – of de achterliggende problematiek. Bovendien is er geen enkel mechanisme overwogen om te voorkomen dat politie en justitie, wanneer deze gegevens 'er nu eenmaal toch zijn', erin willen grasduinen.

De privacyaspecten van mobiliteitsvraagstukken wordt ernstig verwaarloosd door overheidsinstanties, getuige de vele voorstellen die de jury de afgelopen jaren de revue zag passeren. Melanie Schultz van Haegen, de minister van Infrastructuur en Milieu, roemde dit sterk aan rekeningrijden verwante voorstel dan ook ongegeneerd: het 'werkt echt goed om de overlast te beperken', meende zij.

De jury ziet dit project allerminst als een lichtend voorbeeld. Het voorstel laat echter wel uitmuntend zien hoe de spanning tussen privacy en mobiliteit in de 21e eeuw juist niet moet worden opgelost.

MEER INFORMATIE

Website SLIM Prijzen
www.slimprijzen.nl/
Privacy Protocol Slim Prijzen (26.11.10)
https://www.slimprijzen.nl/downloads/Privacy%20Protocol%20SLIM%20Prijzen%20Tweede%20Fase%20v2.5.pdf
Herinnering SLIM Prijzen bij 30.000 automobilisten (27.01.10)
https://www.slimprijzen.nl/pages/?pageid=80
Speech van minister van Infrastructuur en Milieu, Melanie Schultz van Haegen, bij starthandeling traject wegverbreding A50 Ewijk-Valburg, maandag 31 januari 2011 (19.02.11)
http://www.rijksoverheid.nl/regering/het-kabinet/bewindspersonen/melanie-schultz-van-haegen-maas-geesteranus/toespraken/2011/01/31/a50-op-de-schop.html

PERSONEN

DE GEBRUIKERS VAN FACEBOOK

Je beste vriend als beste verklikker

Op Facebook wordt het gelukkig beter mogelijk om je privacy-instellingen te regelen en zo te bepalen wie toegang tot welke gegevens krijgt. Maar nu zijn het je medegebruikers die zulke afgeschermde persoonlijke informatie desalniettemin in handen van derden kunnen spelen. Zodra je ingaat op een applicatie die je vrienden je via Facebook sturen – een spelletje of een quiz – krijgt zo'n app de volledige toegang tot al je gegevens, ook al had je ze nog zo netjes afgeschermd. Zo worden je beste vrienden je beste verklikkers.

'Iedereen' zit op Facebook. Leuk, maar je kunt ook er ook bijna niet meer omheen. Met wereldwijd meer dan 500 miljoen gebruikers bezit het bedrijf een immense hoeveelheid informatie over een fors deel van de wereldbevolking. Van persoonsgegevens als naam, adres, telefoonnummer en e-mail, tot informatie over dagindeling ('Ik zit nog tot zes uur op mijn werk'), seksuele voorkeur en geloofsovertuiging. Al deze informatie hebben gebruikers zelf toevertrouwd aan de servers van Facebook. Met de juiste privacy-instellingen zou het in theorie mogelijk moeten zijn om deze informatie binnen Facebook te houden, en die slechts te delen met mensen die je zelf uitkiest.

De jury ziet dat de netwerksite het haar gebruikers echter notoir moeilijk maakt om hun zelfgekozen mate van privacy te bewaren. Er worden permanent nieuwe opties en instellingen doorgevoerd die eerdere afschermingen ongedaan maken. Ook werkt Facebook samen met schimmige

apps die op hun beurt gebruikers ontfutselen. Voorts is er reden tot zorg nu Facebook naar de beurs wil. Wie worden de grootaandeelhouders van het bedrijf, en dus mede-eigenaar van al die gegevens? Hoe gaan zij om met die gegevens? Het rampscenario waarvan de jury even verbleekte, was een meerderheidsbelang van een overheid – ongeacht welke.

Minder bekend is het vriendenverraad dat Facebook haar leden laat plegen. Dat gebeurt via de talloze 'grappige' apps. Vorig jaar werd bekend dat populaire apps (zoals FarmVille en Texas HoldEm Poker) zichzelf bij gebruik automatisch toegang verschaffen tot al iemands gegevens, ongeacht of die afgeschermd zijn of niet.

Dat principe maakt vrienden op Facebook tot elkaars verklikkers. Wie zijn gegevens enigszins heeft afgeschermd en ze bijvoorbeeld alleen met een selecte groep vrienden deelt, is de klos wanneer een van die vrienden zichzelf ertoe laat verleiden om zo'n data-zuigende app te gebruiken. Je vriend heeft toegang tot jouw gegevens, de app heeft volledige toegang tot al zijn gegevens. Ergo: die vriend verleent derden via de achterdeur, en zonder dat jij daar weet van hebt, automatisch toegang tot al jouw gegevens.
Wie op Facebook zijn privacy wil bewaren, kan zijn vrienden niet langer vertrouwen. Reden voor de jury om de gebruikers van Facebook te nomineren.

Privacytip van de jury: Je kunt je verdedigen tegen de onnadenkendheid van je vrienden op Facebook door je instellingen aan te passen. Ga naar Account -> Privacy Settings. Linksonder, bij het kopje Apps and websites, klik je op Edit your settings. Op de volgende pagina, achter Information accessible through your friends, staat de knop die je zoekt: Edit settings. Bekijk eerst rustig alle soorten informatie die je vrienden zomaar over je hebben weggegeven, en vink daarna alle achttien (!) items netjes af. Deel deze privacytip daarna met al je Facebookvrienden. Dát is pas vriendschap!

MEER INFORMATIE

Facebook, '500 Million Stories' (21.07.10)
http://blog.facebook.com/blog.php?post=409753352130
Wall Street Journal, 'Facebook in Privacy Breach' (18.10.10)
http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html
Tweakers, 'Facebook-apps sluisden id's van gebruikers door naar derden' (18.10.10)
http://tweakers.net/nieuws/70272/facebook-apps-sluisden-ids-van-gebruikers-door-naar-derden.html
TechCrunch.com, 'Scamville: The social gaming ecosystem of hell' (31.10.09)
http://techcrunch.com/2009/10/31/scamville-the-social-gaming-ecosystem-of-hell/

IVO OPSTELTEN

Van het kastje in de auto naar het kastje aan de muur

VVD-Kamerleden Charlie Aptroot en Fred Teeven haalden in 2009 fel uit naar de voorgestelde kilometerheffing: ze vonden dat 'echt een "Big Brother is watching you"-verhaal' en 'een enorme aantasting van de privacy'. De minister van Veiligheid en Justitie, Ivo Opstelten – eveneens lid van de VVD – meent echter dat privacy niet in het geding is bij een minstens even ingrijpend en deels vergelijkbaar systeem: automatische kentekenherkenning. Opstelten wil het bewaren en verwerken van de kentekens van alle passerende automobilisten tot wet verheffen. Dat is pas écht een 'Big Brother is watching you'-verhaal, vindt de jury.

De politie maakt al geruime tijd gebruik van automatische kentekenherkenning (ANPR). Hiermee scant zij alle kentekens op de weg om te controleren of die in haar bestanden voorkomen. Treffen ze een kenteken waarmee iets aan de hand is (een 'hit'), dan mag de politie in actie komen. Alle 'no-hits' – scans van onschuldige kentekens – moeten echter direct worden vernietigd.

Desondanks bewaarden twee politiekorpsen deze no-hits, soms 10 dagen (korps IJsselland), soms zelfs 120 dagen (korps Rotterdam). Het College Bescherming Persoonsgegevens onderzocht de kwestie en velde in januari 2010 een hard oordeel: 'De twee politiekorpsen erkennen dat zij no-hits verwerken én dat hiervoor geen wettelijke basis is. Het CBP kan niet anders dan concluderen

dat deze korpsen willens en wetens de wet overtreden.' Ter illustratie van de ernst en omvang van deze moedwillige overtreding: het CBP berekende dat korps Rotterdam circa 58 miljoen kentekenscans onwettelijk had opgeslagen.

In plaats van te eisen dat zijn wetshandhavers de wet naleefden, besloot de minister van Veiligheid en Justitie dit illegale gedrag riant te belonen. In januari 2011 publiceerde Ivo Opstelten een voorstel om voortaan alle gescande kentekens, inclusief de no-hits, te verwerken en vier weken te bewaren. (Een eerder voorstel van zijn voorganger Hirsch Ballin beperkte zich nog tot 10 dagen.) Daarnaast krijgt de politie van de minister een vrijbrief om deze gegevens te gebruiken om het reisgedrag van automobilisten in kaart brengen. Naast het kenteken en de foto van het voertuig zullen ook gegevens bewaard worden over locatie, datum en tijdstip van de scan.

Plannen voor rekeningrijden (de zg. kilometerheffing) strandden in 2009 op grote zorgen over de privacy van automobilisten. De VVD nam dat bezwaar hoog op; De Telegraaf sprak zelfs over 'spionagekastjes'. De heffingsmeter in de auto zou immers voortaan nauwkeurig alle vervoersbewegingen van automobilisten registreren, door bij te houden wanneer de auto zich waar bevond.
Aangezien een kastje in de auto een serieuze privacyschending vormt, ontgaat het de jury waarom een vergelijkbaar kastje langs de weg wel acceptabel zou zijn. Daarboven: nu eenduidig is vastgesteld dat het bewaren van onschuldige nummerscans een wetsovertreding is, is dat uitsluitend reden om de handhaving van de wet beter na te leven – niet om die wet dan maar aan te passen. Door echter voor dat laatste te kiezen, degradeert de minister wetgeving tot een gelegenheidsargument: iets waaraan alleen burgers zich hebben te houden. Redenen genoeg voor de jury om Ivo Opstelten te nomineren in de categorie personen.

MEER INFORMATIE

Ministerie van Veiligheid en Justitie, 'Opstelten: 'alle kentekengegevens vier weken bewaren' (10.01.11)
http://www.rijksoverheid.nl/ministeries/venj/nieuws/2011/01/11/opstelten-alle-kentekengegevens-vier-weken-bewaren.html
Concept-wetsvoorstel regeling van het vastleggen en bewaren van kentekengegevens door de politie (20.12.10)
http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/regelingen/2011/01/11/wetsvoorstel-regeling-van-het-vastleggen-en-bewaren-van-kentekengegevens-door-de-politie/conceptwetsvoorstel20december.pdf
College bescherming persoonsgegevens, 'Politiekorpsen handelen in strijd met de wet bij toepassing ANPR' (28.01.10)
http://www.cbpweb.nl/Pages/pb_20100128_anpr.aspx
Security, 'Politie wil alle kentekens vier weken bewaren' (11.01.11)
http://www.security.nl/artikel/35777/Politie_wil_alle_kentekens_vier_weken_bewaren.htmlml

ROB VAN DOORN

GroenLinks krijgt de binnenstad eindelijk autoloos

In veel gemeentes moeten mensen het kenteken van hun voertuig intoetsen wanneer ze een parkeerbewijs willen kopen, en steeds vaker worden papieren parkeerschijven en -vergunningen vervangen door digitale systemen. Nu wil de Haarlemse wethouder Rob van Doorn dat bewoners van de binnenstad bovendien doorgeven wanneer zij bevriende automobilisten op bezoek krijgen, welke auto dat bezoek dan gebruikt en wanneer ze weer vertrekken. De jury wil voorlopig niet meer in Haarlem op visite.

Bij het registreren van kentekens bij parkeerbewijzen is het privacygevaar evident: waarom zou je een parkeerkaartje expliciet willen koppelen aan het kenteken van de geparkeerde auto? Een betaalbewijs volstaat. Vastleggen welke auto waar, wanneer en hoe lang staat geparkeerd, kan alleen maar dienen om het fijnmazige net van burgervolgsystemen verder te verfijnen. Tot voor kort werd het bezoek van binnenstadbewoners gelukkig gespaard: de binnenstadbewoner gaf zijn bezoekers een daartoe bestemde parkeerschijf te leen.

De Haarlemse wethouder Rob van Doorn stelde een volgende stap voor, waarmee binnenstadsbezoek beter kan worden gemonitord. Met de huidige digitale parkeersystemen weet je tenslotte wel waar een auto staat, maar heb je nog geen idee waar de bestuurder van die auto uithangt, noch of die bestuurder wel een geldige excuus heeft om in de binnenstad te willen parkeren.
Van Doorn stelde een digitale bezoekerspas voor. Haarlemse binnenstadbewoners krijgen een parkeerpas met een unieke activeringscode; de pas is alleen geldig in de wijk van de pashouder. Wanneer zo'n binnenstadbewoner bezoek krijgt dat met de auto is gekomen, dient de pashouder (per sms of via een website) terstond kenteken, tijd van aankomst en van vertrek van het bezoek aan de gemeente door te geven.

Sinds oktober wordt met deze bezoekerspas geëxperimenteerd. In december werd wegens de vele protesten een half jaar uitstel van algehele invoering bedongen: de proefwijk stelde het niet bijster op prijs dat de gemeente nu precies wist welk gemotoriseerd bezoek ze ontvangen.
Overigens was de wethouder vergeten bij het CBP navraag te doen of zijn beleid wel in overeenstemming met de privacywetgeving was. Hij voorzag echter geen problemen: volgens de wethouder worden de gevorderde gegevens 'niet bewaard' en kan er 'dus' geen misbruik of ongewenste koppeling plaatsvinden.
De jury biedt wethouder Van Doorn met plezier een basiscursus 'digitale gegevens' aan. Maar ze komt niet met de auto.

MEER INFORMATIE

Brief wethouder Van Doorn, 'Digitale bezoekersparkeervergunning' (01.12.10)
http://www.burgwalhaarlem.nl/brief%20wethouder.pdf
Gemeente Haarlem, 'Invoering van digitale bezoekersparkeervergunning vier maanden uitgesteld' (15.12.10)
http://www.haarlem.nl/nieuws/nieuwsbericht/artikel/invoering-van-digitale-bezoekersparkeervergunning-vier-maanden-uitgesteld/
BurgwalHaarlem, 'Digitale bezoekersvergunning houdt gemoederen bezig' (15.12.10)
http://burgwalhaarlem.blogspot.com/2010/12/digitale-bezoekersvergunning-houdt.html

OVER DE JURY

KARIN SPAINK

(voorzitter) is columnist en publicist. Ze schrijft onder meer voor Het Parool, werkt aan een boek over de geschiedenis van XS4ALL en is hoofdredacteur van een serie boeken over internet en maatschappij. Van 1999 tot 2006 was zij voorzitter van Bits of Freedom.

ANTOINETTE HERTSENBERG

is programmamaakster en presentatrice van TROS Radar en Opgelicht?! Zij is in 2009 door het vaktijdschrift Villamedia uitgeroepen tot Journalist van het Jaar.

MELANIE RIEBACK

is assistant professor aan de Vrije Universiteit. Haar onderzoek naar de beveiliging van RFID's mocht op veel aandacht rekenen. Ze is met name geïnteresseerd in de vraag hoe mensen kunnen voorkomen dat zijzelf en hun spullen permanent worden uitgelezen.

BART DE KONING

is journalist en schrijft over politiek, economie en recht. Hij schreef onder andere voor Algemeen Dagblad, Quote, FemBusiness en HP/De Tijd. In 2008 publiceerde hij het boek Alles onder controle, waarin hij uitlegt waarom de overheid de burger tegenwoordig niet meer vertrouwt.

NICO VAN EIJK

is hoogleraar Media- en Telecommunicatierecht aan de Universiteit van Amsterdam (IViR). Tevens is hij voorzitter van de Vereniging voor Media- en Communicatierecht, redactielid van het tijdschrift Computerrecht en lid van de raad van toezicht van de Nederlandse Publieke Omroep.

MEDE MOGELIJK GEMAAKT DOOR

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

PAKHUIS DE ZWIJGER*

BIG BROTHER AWARDS

ARSENOSTI

nlnet FOUNDATION

De genomineerden voor de Big Brother Awards 2010 zijn vastgesteld door de onafhankelijke expertjury. Deze organisaties hebben geen invloed gehad op het oordeel van de jury.