BIG BROTHER AWARDS 2009

GENOMINEERDEN

DESIGN BY ERJEE.NET

De Big Brother Awards
is een initatief van

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

De genomineerden

Overheid

Bedrijven

Voorstellen

Personen

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 award ontleent zijn naam aan de totalitaire leider “Big Brother” uit het boek 1984 van George Orwell. De eerste Big Brother Awards werden georganiseerd door Privacy International. De prijzen worden inmiddels in vele andere landen uitgereikt.

Het prijzengala op 5 februari 2010 is alweer de zesde editie in de geschiedenis van de Big Brother Awards Nederland. In 2007 werden de Awards voor het laatst uitgereikt. Op deze website kunt u alle informatie vinden over de Big Brother Awards 2009 en alle eerdere edities, inclusief de juryrapporten, puibliciteit en sfeer-impressies.

De organisatie van de Nederlandse versie van de Big Brother Awards is in handen van Stichting Bits of Freedom. Bits of Freedom is een beweging die privacy en communicatievrijheid in de digitale wereld verdedigt. Twee belangrijke thema’s waar zij zich op richt, zijn de verzameldrift van de overheid, en een open en voor iedereen toegankelijk internet. Bits of Freedom geeft gestalte aan haar werkzaamheden via een constructieve lobby en publiekscampagnes, zoals de Big Brother Awards. Meer informatie over de geschiedenis en de heroprichting van Bits of Freedom vindt u via de website www.bof.nl.

De Big Brother Awards Nederland worden mede mogelijk gemaakt door de steun van talloze vrijwilligers, debatcentrum De Balie, Brinkhof, Stichting NLnet en SURFnet. Bits of Freedom wil hen hiervoor hartelijk danken.

Amsterdam, 28 januari 2010

Over dit rapport

Voor u ligt het juryrapport "Genomineerden Big Brother Awards 2009". In het rapport worden de nominaties voor de Big Brother Awards 2009 uit de doeken gedaan en nader toegelicht. De winnaars van de Big Brother Awards zullen, net als de winnaars van de Publieksprijs en de Winston Award, onthuld worden op 5 februari 2010 tijdens een feestelijke prijsuitreiking in debatcentrum De Balie in Amsterdam.

Sinds 8 december 2009 heeft het publiek massaal gehoor gegeven aan de oproep kandidaten voor te dragen in vier categoriën: 'overheid', 'bedrijfsleven', 'voorstellen' en 'personen'. Nog nooit eerder ontving de jury zoveel inzendingen. Een woord van dank gaat uit naar alle inzenders, die vaak goede motiveringen en nauwkeurige bronvermeldingen aan de dag wisten te leggen.

Na het sluiten van de deadline voor inzendingen was de jury aan slag. De jury is samengesteld uit experts op het gebied van informatierecht, copmputerbeveiliging, antropologie, journalistiek en nieuwe media. Zij heeft tijdens de beraadslagingen in volledige onafhankelijkheid geopereerd. Bits of Freedom noch andere betrokken organisaties hebben op enige wijze invloed uitgeoefend op het oordeel van de jury.

Na het verschijnen van dit rapport hebben de genomineerden een week de tijd om het leven te beteren en inhoudelijk te reageren op de nominatie. Deze reactie laat de jury meewegen in haar oordeel wie er gelauwerd wordt met een Big Brother Award 2009.

De jury hoopt op een levendig maatschappelijk debat over de genomineerden, en wenst u veel leesplezier toe met het juryrapport "Genomineerden Big Brother Awards 2009".

Nominaties categorie Overheid

DESIGN BY ERJEE.NET

De DNA-databank voor kinderen

Een genetisch strafblad voor jeugdzondes

Kinderen die in het jeugdstrafrecht verzeild raken, moeten steeds vaker hun DNA afstaan. Van 12.000 kinderen zijn de profielen al opgeslagen in de Nederlandse DNA-databank, en hun aantal groeit snel. Dit gebeurt ook bij relatief lichte vergrijpen zoals een fikkie stoken of graffiti spuiten, of als een taakstraf wordt opgelegd. Kinderen komen hier niet meer vanaf, ook niet als ze eenmaal volwassen zijn, aangezien de profielen 20 tot 30 jaar worden opgeslagen. Dit genetische strafblad voor kinderen werkt stigmatiserend en bevat gevoelige informatie over het kind. De jury nomineert de DNA-databank voor kinderen vanwege de stevige inbreuk die dit genetische strafblad voor jeugdzondes maakt op de privacy van het kind.

Nadat een wetswijziging in 2005 dit mogelijk maakte, wordt het profiel van steeds meer kinderen in de DNA-databank opgeslagen. In 2006 waren het er 1.627; inmiddels zijn het er al bijna tien maal zoveel (11.693). Het Nederlands Forensisch Instituut, dat de DNA-databank beheert, publiceerde de cijfers pas naar aanleiding van een Wob-verzoek van de organisatie Defence for Children. Eerder was geen sprake van openheid over de aantallen.

De opslag van DNA-profielen in databanken werkt stigmatiserend: één jeugdzonde, en het kind zit de rest van zijn leven vast aan een genetisch strafblad waar hij niet van af komt. Een achteloos weggegooide sigaret met DNA-sporen kan genoeg zijn om iemand jaren later van zijn bed te lichten. De profielen bevatten bovendien gevoelige informatie over ras en genetische

verwantschap. Het is niet te voorspellen wat de overheid hier in de toekomst mee zal doen.

De jury heeft de DNA-databank voor kinderen genomineerd, omdat juist kinderen een goede privacybescherming verdienen. Jeugdzonden zouden niet jaren later nog moeten leiden tot stigmatisering. Dat DNA-profielen van kinderen van alle leeftijden voor allerlei vergrijpen worden opgeslagen, doet geen recht aan dat uitgangspunt. De gedachte dat kinderen in het jeugdstrafrecht anders behandeld zouden moeten worden dan in het normale strafrecht, wordt door deze ontwikkeling bovendien verlaten.

Meer informatie

Wet DNA-onderzoek bij veroordeelden (26.01.10)
http://wetten.overheid.nl/BWBR0017212/geldigheidsdatum_26-01-2010
Brief van het NFI naar aanleiding van het Wob-verzoek (02.12.09)
http://www.nederlandsforensischinstituut.nl/Images/09-734%20Defence%20for%20Children_besluit%20WOB-verzoek%202009_tcm68-239271.pdf
Website Nederlands Forendisch Instituut
http://www.nederlandsforensischinstituut.nl/
Website Defence for Children
http://www.defenceforchildren.nl/

De nieuwe Paspoortwet

Twee vingerafdrukken van alle Nederlanders in één opsporingsregister

Op grond van de nieuwe Paspoortwet moet iedere Nederlander vanaf 21 september 2009 vier vingerafdrukken afgeven bij het aanvragen van een nieuw reisdocument. Twee daarvan worden opgeslagen in een centrale overheidsdatabank waartoe de Officier van Justitie onder bepaalde voorwaarden toegang zal krijgen. Het bewaren van vingerafdrukken van alle Nederlanders op één plek vormt een ernstige privacyschending. Het risico op identiteitsfraude is substantieel. Centrale opslag maakt controle op de mate waarin en de voorwaarden waaronder de gegevens worden gebruikt, moeilijk zo niet onmogelijk; en een hack van de database heeft potentieel desastreuze gevolgen. De jury is zeer kritisch over de nieuwe wet, en constateert dat de Nederlandse overheid hiermee veel verder gaat dan de ons omringende landen.

Europese regelgeving verplicht alle lidstaten twee vingerafdrukken af te nemen van burgers die een nieuw reisdocument aanvragen, en deze op een chip in het reisdocument op te slaan. Hiermee wordt beoogd Europese paspoorten betrouwbaarder te maken. De Nederlandse versie gaat echter veel verder. Volgens de Paspoortwet moet iedere burger twee extra vingerafdrukken afstaan, die vervolgens in een centrale databank zullen worden opgeslagen. Bovendien heeft de Officier van Justitie onder bepaalde voorwaarden toegang tot deze landelijke databank. Daarmee wordt het doel van de Europese regelgeving - het bestrijden van paspoortfraude - ruimschoots voorbijgestreefd. 'De centrale

reisdocumentenadministratie krijgt in feite de functie van een opsporingsregister', schrijft het College Bescherming Persoonsgegevens (CBP). Nederland is volgens het CBP het eerste land in Europa dat een landelijke databank aanlegt naar aanleiding van de reisdocumentenadministratie.

Voorheen werd de vingerafdruk alleen afgenomen van verdachten. Nu belanden de vingerafdrukken van alle Nederlanders in een landelijk opsporingsregister. Een recente uitspraak van het Europees Hof voor de Rechten van de Mens (EHRM) heeft strenge criteria geformuleerd voor de opslag van vingerafdrukken en DNA-materiaal in een landelijke databank; dat de vingerafdrukken van niet-veroordeelden in een Britse landelijke databank waren opgenomen, heeft het Europese Hof in ferme bewoordingen teruggefloten. Alleen veroordeelden mogen aldus worden geregistreerd, stelde het Europees Hof. Ondanks deze uitspraak, herhaaldelijke adviezen van het CBP, wetenschappers, privacywaakhonden, juristen en zelfs de Verenigde Naties negeert de overheid de bezwaren consequent. Dit leidde tot een brede discussie in de samenleving, aangewakkerd door een satirische tatoeagefolder van kunstenaarscollectief 'Het Nieuwe Rijk'. Daarnaast heeft de stichting 'Privacy First' besloten een bodemprocedure te starten, zodat de rechter zich zal buigen over de vraag of de nieuwe Paspoortwet in strijd is met de grondwet en het EVRM.

Naast deze fundamentele bezwaren herkent de jury tenminste twee privacyrisico's in de nieuwe Paspoortwet, te weten identiteitsfraude en function creep. Als de vingerafdrukken van alle burgers verzameld en op één plek bewaard worden, wordt met de databank een nieuwe goudmijn voor criminelen in het leven geroepen. Een vingerafdruk is eenvoudig te kopiëren, en met een nagemaakte vingerafdruk kan een slimme crimineel de illusie wekken dat iemand anders op een plaats delict is geweest. Zo wordt de politie op een dwaalspoor gezet, en een onschuldige

burger verdacht. En als de centrale databank wordt gehackt, liggen al onze vingerafdrukken op straat en is forensisch onderzoek op basis van vingerafdrukken op plaatsen delict voorgoed onmogelijk geworden. Daarnaast vormt de aanleg van de databank de opmaat voor function creep: toekomstig gebruik van de vingerafdrukken voor andere doelen van waarvoor zij oorspronkelijk verzameld zijn. Ook het CBP heeft dit opgemerkt. Het lijkt alsof de overheid amper heeft nagedacht over dit soort complexe, langetermijn-consequenties van centrale opslag.

De jury is zeer kritisch over de centrale opslag van de vingerafdrukken, en de opsporingsfunctie van de databank. Zij heeft bij de nominatie laten meewegen dat de Nederlandse overheid beduidend verder is gegaan dan de ons omringende landen, en dat de serieuze privacybezwaren in de wind werden geslagen.

Meer informatie

De Paspoortwet (26.01.10)
http://wetten.overheid.nl/BWBR0005212/geldigheidsdatum_26-01-2010
Memorie van Toelichting bij de wijziging van de Paspoortwet (2007/2008)
http://parlis.nl/KST115300
Advies CBP, 'Centrale reisdocumentenadministratie in strijd met EVRM' (30.03.07)
http://www.cbpweb.nl/Pages/adv_z2007-00010.aspx?refer=true
Uitspraak EHRM S. and Marper v. The United Kingdom**, samenvatting door het NJCM, (04.12.08)**
http://www.njcm.nl/site/jurisprudentie/show/51
NRC Handelsblad, 'Men realiseert zich te laat hoe ingrijpend de nieuwe Paspoortwet is' (24.07.09)
http://www.nrc.nl/opinie/article2309629.ece/Men_realiseert_zich_te_laat_hoe_ingrijpend_de_nieuwe_Paspoortwet_is
CQC, 'Jelte haalt vingerafdrukken', o.m. van minister Hirsch Ballin (30.09.09)
http://www.youtube.com/watch?v=EpC0koSsjpc
Dialogue Box, 'Vinderafdruk namaken is eenvoudig' (30.11.08)
http://www.youtube.com/watch?v=VZT1CVWal2w
Netwerk, 'Nieuw paspoort met vingerafdrukken onveilig?' (27.06.09)
http://www.youtube.com/watch?v=b3YPlu3NeIY&feature=player_embedded#

Het Centraal Informatiepunt Onderzoek Telecommunicatie

Het telefoonboek van de opsporingsdiensten vindt gretig aftrek en dijt uit

Bij het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) komen de gretigheid en slordigheid van opsporingsdiensten sterk tot uitdrukking. Via deze centrale bevragingsmodule vroegen politie en justitie in 2008 circa drie miljoen (!) keer de klantgegevens van telecomgebruikers op – een verbluffend aantal dat jaarlijks met 33% stijgt. Tegelijkertijd blijken opsporingsdiensten de wettelijke privacywaarborgen niet te kennen, of niet te willen treffen. Dit is voor de jury op zich al voldoende reden om het CIOT te nomineren voor een Big Brother Award. Maar de overheid wil het CIOT, dat aantoonbaar slordig omspringt met onze privacy, de beheerder maken van de gegevens die via de bewaarplicht zullen worden verzameld. Het CIOT moet het privéleven en het sociale netwerk van iedere burger tot op de seconde en tot op de millimeter traceerbaar maken. Daarmee komt de nominatie van het CIOT ook de beleidsmakers toe.

Sinds een aantal jaren moeten telecomaanbieders dagelijks al hun klantgegevens uploaden naar het CIOT. Het gaat onder meer om naam, adres, telefoonnummer, e-mailadres, IP-adres en login-gegevens van alle klanten. Het OM en de politie kunnen deze klantgegevens via vaste pc's op hun werkplek opvragen, wanneer zij onderzoeken of een bepaald e-mailadres of telefoonnummer gerelateerd kan worden aan 'een verdachte' van 'een misdrijf'. De praktijk leert dat opsporingsdiensten gretig gebruik maken van

deze dienst. In 2001 ontvingen Nederlandse telecommunicatieaanbieders het gehele *jaar* circa 300.000 verzoeken om klantgegevens. In 2008 was dit aantal vertwaalfvoudigd naar ongeveer 300.000 verzoeken per *maand*. De projectie van het aantal bevragingen van het CIOT in 2001 is daarmee mijlenver achtergebleven bij de realiteit: waar men in 2001 nog uitging van een lange termijn stijging naar circa 900.000 aanvragen, staat de teller op 3 miljoen en laten de aanvragen een explosieve exponentiële toename zien van circa 33% per jaar.

De gretigheid van de opsporingsdiensten gaat gepaard met verwijtbare slordigheid, zo bleek uit een WOB-verzoek. Opsporingsdiensten bevragen het CIOT onrechtmatig en springen gemakzuchtig om met de privacy van telecomgebruikers. Zo wordt in cruciale gevallen geen proces-verbaal opgesteld, is er geen controle op de bevragingen. en vragen opsporingsambtenaren om gegevens waartoe zij geen bevoegdheid hebben. De jury is geschrokken van de constateringen dat sommige opsporingsdiensten privacy als 'een administratieve last' ervaren en dat PIN-codes zijn uitgewisseld tussen verschillende ambtenaren, zodat ook ongeautoriseerde ambtenaren toegang kregen tot het CIOT. De jury ziet in deze cocktail van gretigheid en slordigheid een privacyschending van alle telecommuncatiegebruikers – en daarmee in feite van alle Nederlanders.

De jury maakt zich bovendien grote zorgen over de mogelijke uitbreiding van het CIOT in het kielzog van de Wet bewaarplicht telecommunicatiegegevens. Tijdens een informatiemiddag voor telecomaanbieders op 14 oktober 2009 werd niet weersproken dat de overheid de verplicht bewaarde verkeers- en locatiegegevens van alle telecomgebruikers via het CIOT raadpleegbaar wil maken. Een grove schending van de privacy – de Wet bewaarplicht telecommunicatiegegevens – wordt zo ook nog centraal uitgevoerd, waardoor het risico op privacyinbreuken

exponentieel toeneemt. De jury begrijpt niet waarom dit proces in geheimzinnigheid wordt gehuld en waarom er zoveel haast bij is. Het gaat immers om een uitbreiding met een enorme impact. Daarnaast is het buitengewoon bevreemdend dat niet eerst de huidige problemen bij het CIOT worden aangepakt, alvorens de organisatie nieuwe taken toebedeeld krijgt.

Bij haar keuze voor het CIOT, heeft de jury de datahonger en de laksheid van de opsporingsdiensten zwaar laten meewegen. Het gebrek aan bewustzijn van deze opstelling van opsporingsdiensten en het gebrek aan transparantie over de nieuwe plannen, is voor de jury doorslaggevend om de beleidsmakers rondom het CIOT te nomineren voor een Big Brother Award.

Meer informatie

Website CIOT
http://www.justitie.nl/onderwerpen/opsporing_en_handhaving/ciot/
Memorie van Toelichting bij de Wet vorderen gegevens telecommunicatie, p.17 (PDF) (2001/2002)
https://zoek.officielebekendmakingen.nl/kst-28059-3.pdf
Rejo Zenger, 'Eindrapport audit CIOT 2008', resultaat Wob-verzoek (11.09.09)
https://rejo.zenger.nl/focus/1253127301.php
Presentatie Informatiemiddag Bewaarplicht Telecommunicatiegegevens, vanaf sheet 33 (14.10.09)
https://www.bof.nl/live/wp-content/uploads/2010/01/Microsoft-PowerPoint-Bewaarplicht-Telecommunicatiegegevens-samengevoegd-2.pdf
Webwereld, 'Kabinet centraliseert bewaarplichtdata', (19.10.09)
http://webwereld.nl/nieuws/64011/-kabinet-centraliseert-bewaarplichtdata-.html

Nominaties categorie Bedrijven

DESIGN BY ERJEE.NET

De illegale verzamelpraktijken van Advance

Quizmasters verdienen goed geld met je echte leeftijd

Advance Concepts BV (Advance) oogstte onder het mom van leuke quizjes de afgelopen jaren gevoelige informatie van meer dan twee miljoen mensen, en verkocht die geaggregeerde informatie vervolgens door aan bedrijven. Advance schond daarmee de privacy van miljoenen Nederlanders en misleidde haar bezoekers. Het College Bescherming Persoonsgegevens (CBP) stelde vast dat Advance de Wet bescherming persoonsgegevens op 7 verschillende manieren heeft overtreden. De gevoeligheid van de gegevens, de schaal van de privacyinbreuk en de misleiding door Advance verdienen een nominatie voor een Big Brother Award.

Advance beheert verschillende interactieve websites waar bezoekers quizjes kunnen invullen, zoals 'Je echte leeftijd' en 'De waarde van je woning'. Gebruikers vulden daar uitgebreide vragenlijsten in over onderwerpen als gezondheid ('wat is je bloeddruk?'), seks ('hoe vaak masturbeer je?') en financiële situatie ('wat zijn je bezittingen waard?'). Op die manier heeft Advance gegevens van ongeveer 2,2 miljoen Nederlanders verzameld: door de informatie van de quizzen te combineren, wist Advance van circa 300.000 mensen meer dan 100 persoonskenmerken te achterhalen, aldus Webwereld. Advance koppelde die gegevens vervolgens aan de persoon die de quiz

had ingevuld. Ze verkocht daarmee ontwikkelde profielen aan bedrijven en stuurde namens bedrijven gerichte marketing aan geprofileerde doelgroepen.

Het CBP constateerde dat Advance handelde in strijd met de Wet bescherming persoonsgegevens. Advance heeft bezoekers onvoldoende geïnformeerd over het feit dat hun gegevens werden verzameld, gecombineerd, doorverkocht en gebruikt voor direct marketing. Voor de verzameling en verwerking van medische gegevens geldt bovendien in beginsel een verbod, en Advance handelde in strijd hiermee. Door persoonsgegevens van miljoenen Nederlanders in kaart te brengen en door te verkopen aan onder meer Amerikaanse bedrijven, schond Advance de wet, de privacy en het vertrouwen van miljoenen Nederlanders.

De jury is van oordeel dat Advance een nominatie verdient vanwege de schaal, de gevoeligheid en de misleiding. Niet alleen heeft Advance een belangrijk deel van de Nederlandse bevolking door middel van testjes in kaart gebracht, maar de informatie die zij verzamelde over haar bezoekers en doorverkocht betrof ook nog eens intieme details. Dat zij dit deed onder het mom van een leuke quiz, maakt het alleen maar ernstiger. Inmiddels heeft Advance aangekondigd de opgebouwde profielen te zullen vernietigen, en voortaan binnen de richtlijnen van het CBP te zullen opereren. Dat klinkt bemoedigend, maar omdat Advance aangeeft dat zij het niet met de conclusies van het CBP eens is, heeft zij de bezwaren kennelijk niet écht begrepen.

Meer informatie

Volkskrant, 'Je hele privéleven op internet' (13.02.09)
http://www.volkskrant.nl/multimedia/article1148632.ece/Je_hele_priveleven_op_internet
Onderzoek CBP naar verwerking persoonsgegevens door Advance (15.12.09)
http://www.cbpweb.nl/downloads_pb/pb_20091218_advance_bevindingen.pdf
Persbericht 'Advance past privacybeleid aan op basis van CBP onderzoek' (18.12.09)
http://www.advance.nl/nl/nieuws/interactief_nieuws/advance_past_privacybeleid_aan_op_basis_van_cbp_onderzoek_49

Albert Heijn voor de proef 'TiP2Pay'

Thumbs down voor vingerafdrukbetaling

Twee weken nadat Albert Heijn een proef begon met vingerafdrukbetaling, werd TiP2Pay al gekraakt. Tot verbazing van de jury noemt een woordvoerder TiP2Pay niettemin 'een succesvolle proef'. Albert Heijn geeft zich te weinig rekenschap van de fraudegevoeligheid van de vingerafdruk en het onderliggende probleem van vingerafdrukbetaling: de databank waarin de vingerafdrukken worden opgeslagen en gekoppeld met financiële gegevens en identiteitsdocumenten. Deze databank is een potentiële schatkist voor criminelen enerzijds, en opsporingsdiensten – die toegang tot deze vingerafdrukkendatabank zullen afdwingen – anderzijds. Weinig identiteitskenmerken zijn zo eenvoudig te vervalsen als de vingerafdruk. Bij al deze security- en privacyimplicaties lijkt Albert Heijn niet te hebben stilgestaan.

TiP2Pay startte als proef in een filiaal in Breukelen op 17 juni 2008. Het doel van de proef was 'om te kijken of klanten enthousiast zijn over deze nieuwe manier van betalen'. Met de vingerafdrukbetaling zou dit 'snel, gemakkelijk en veilig' kunnen. De veiligheid was echter al binnen twee weken onderuit gehaald door biometrie-expert Ton van der Putte, die met een rubberen kopie van een vingerafdruk gewoon kon betalen. Albert Heijn reageerde vervolgens door te stellen dat klanten geen enkel risico lopen. 'Complete onzin', volgens expert Van der Putte: 'eens gestolen is voor altijd gestolen.' Met een simpele vervalsing

kunnen mensen boodschappen doen op andermans rekening.

Albert Heijn heeft het onderliggende probleem van vingerafdrukbetaling nooit geadresseerd. De supermarkt heeft vijf miljoen vaste klanten, waardoor de brede acceptatie van deze betaalmethode de grootste biometrische databank van Nederland zou creëren – na de vingerafdrukkendatabank ORRA vanwege de nieuwe Paspoortwet (die een nominatie ontvangt in de categorie Overheid). De vingerafdruk van een klant is gekoppeld aan de financiële gegevens, eventuele kortingsprogramma's en de identiteitsbewijzen van al die klanten. Het risico dat de gegevens van een groot deel van de bevolking op straat komt te liggen neemt daarmee toe. Dit zou niet alleen het gebruik van de vingerafdruk als opsporingsmiddel ondermijnen, maar is vooral koren op de molens van identiteitsfraudeurs en andere criminelen. Ook kunnen opsporingsdiensten eenvoudig toegang verwerven tot deze databank via de Wet bevoegdheden vorderen gegevens. De databank zou daarmee de privacy van burgers onder druk zetten.

Juist van één van de leidende retailbedrijven in Nederland verwacht de jury meer prudentie. Ook al betrof het een proef, het naïeve Albert Heijn begeeft zich op glad ijs en onderkent de risico's van vingerafdrukbetaling en het aanleggen van een omvangrijke biometrische databank onvoldoende. Met een nominatie voor een Big Brother Award, wil de jury de vinger op de zere plek leggen.

Meer informatie

Persbericht 'Albert Heijn en Equens introduceren TiP2Pay' (17.06.08)
http://www.ah.nl/albertheijn/persberichten/article.jsp?id=486644
Webwereld, 'Onderzoeker kraakt vingerafdrukbetaling Albert Heijn' (30.06.08)
http://webwereld.nl/nieuws/51680/onderzoeker-kraakt-vingerafdrukbetaling-albert-heijn.html
Security.nl, 'Albert Heijn doet biometrisch betalen in de ijskast' (17.03.09)
http://www.security.nl/artikel/28006/1/Albert_Heijn_doet_biometrisch_betalen_in_de_ijskast.html
Wet bevoegdheden vorderen gegevens, art. 126nd lid 1, p.4
http://www.eerstekamer.nl/9370000/1/j9vvhwtbnzpbzzc/vh2wcehpgxmf/f=y.pdf

T-Mobile en Vodafone: doorgifte van sms-inhoud aan opsporingsdiensten

Telecomproviders nemen de 'stomme tap' wel erg letterlijk

'Niet nadenken, gewoon doen.' Iets van die strekking moet bij telecomproviders T-Mobile en Vodafone jarenlang de heersende mentaliteit zijn geweest. Totdat op 30 mei 2009 bekend werd dat beide bedrijven ook de inhoud van sms-berichten meeleverden als de opsporings- en inlichtingendiensten de verkeersgegevens van hun klanten vorderden. T-Mobile en Vodafone hebben de privésfeer en het vertrouwen van hun klanten te grabbel gegooid. Dit klemt des te meer daar beide tenminste vier maanden daarvoor al van hun fout op de hoogte waren gesteld tijdens een overleg met de opsporings- en inlichtingendiensten.

Zowel de Officier van Justitie als de AIVD kunnen van telecomproviders de levering van verkeersgegevens van sms-berichten vorderen: gegevens over telefoonnummers, geadresseerde, datum en tijdstip van een smsje. Daarnaast hebben zij de bevoegdheid om voor een beperkte periode toekomstige verkeersgegevens te vorderen. De verkeersgegevens worden in dat geval real-time geleverd – de zogenaamde 'stomme tap'. Het absoluut niet de bedoeling dat bij zo'n stomme tap ook de inhoud van een smsje wordt meegeleverd. Daarvoor bestaat een aparte wettelijke regeling,

namelijk het aftappen van telecommunicatie, waarvoor de toestemming van de rechter-commissaris of de minister nodig is. Toch hebben T-Mobile en Vodafone de inhoud van sms-berichten meegeleverd bij deze stomme taps, en zijn zij hiermee doorgegaan nadat zij hierop werden gewezen door de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD). Bij één stomme tap, ontving de AIVD 'binnen geringe tijd zelfs 150 sms-berichten'. T-Mobile en Vodafone verdedigden zichzelf aanvankelijk door te zeggen dat het technisch gezien onmogelijk was inhoud en vorm van smsjes te scheiden. Collega KPN meldde echter prompt dat zij de real-time verstrekking van sms-berichten wel kan filteren op inhoud. Anders gezegd: het was onwil, geen onvermogen.

Het jarenlang systematisch doorgeven van de inhoud van sms-berichten vormt een ernstige privacyschending van de klanten van T-Mobile en Vodafone. De AIVD beschouwt deze berichten namelijk als 'bijvangst: We vragen er niet om, maar het komt wel mee. Dat is natuurlijk een lastig dilemma', alus een woordvoerder van de AIVD. De inlichtingendiensten hebben de onterecht ontvangen gegevens wél bestudeerd, zo bleek.

Het CTIVD geeft terecht aan dat de inhoud van sms-berichten valt onder het telefoongeheim van artikel 13 van de Grondwet. Merkwaardig genoeg wordt de toezichthouder hierin niet gesteund door minister Ter Horst, die het kennisnemen van de smsjes goedkeurt omdat de inlichtingendiensten nooit hadden gevraagd om de inhoud van de berichten. Zij doet de kwestie af met het bevel de sms-inhoud voortaan apart op te slaan en het gebod haar om toestemming achteraf te vragen. Maar dan is de buit natuurlijk al binnen. Los van de beschamende reactie van minister Ter Horst – de jury nomineert haar niet voor niets in de categorie Personen – hadden T-Mobile en Vodafone deze privacyschending kunnen en moeten voorkomen door na het overleg in februari hun verantwoordelijkheid te nemen. Pas toen

het schandaal aan het licht kwam, werkten de telecomproviders inderhaast aan een oplossing.

Vooral dit laatste aspect heeft de jury zwaar laten meewegen in haar oordeel de beide bedrijven te. Klanten moeten erop kunnen vertrouwen dat de telecomprovider hun privacy waarborgt. T-Mobile en Vodafone gooiden de smsjes echter zonder na te denken over de schutting. Zelfs na een overleg werden de benodigde maatregelen niet getroffen. Dat getuigt volgens de jury van laksheid en onwil. Ondertussen werd de 'bijvangst' gebruikt door de AIVD. Dit maakte het door beide bedrijven in het leven geroepen risico op privacyschending compleet.

Meer informatie

Toezichtsrapport CTIVD nr. 19, 'De inzet van de afluisterbevoegdheid en de signaalinterceptie door de AIVD (2009)
http://www.ctivd.nl/?download=CTIVD rapport 19.pdf
Officiële reactie minister Ter Horst (20.02.09)
http://www.ctivd.nl/?download=KST128316.pdf
NRC Handelsblad, 'SMSjes gaan ongevraagd naar de politie' (30.05.09)
http://www.nrc.nl/binnenland/article2256668.ece/Smsjes_gaan_ongevraagd_naar_politie
Webwereld, 'SMS-tap schendt mogelijk de grondwet' (03.06.09)
http://webwereld.nl/nieuws/58967/-sms-tap-vodafone-en-t-mobile-schendt-grondwet-.html

Nominaties categorie Voorstellen

DESIGN BY ERJEE.NET

De introductie van het downloadverbod

Handhaving van auteursrecht nu ook in de huiskamer

Als het aan het aan het kabinet en de Commissie Gerkens ligt, wordt het zonder toestemming downloaden van muziek, tv-series en films binnen een paar jaar verboden. Tegelijkertijd zou de thuiskopieheffing op dragers (zoals cd's, dvd's en m3-spelers) worden afgeschaft. Men geeft zich er geen rekenschap van dat, om dit downloadverbod te handhaven, de online activiteiten van alle Nederlanders nauwgezet zouden moeten worden gecontroleerd. Met dit voorstel dringt de handhaving van auteursrechten binnen in de huiskamer van iedere Nederlander.

Het omstreden voorstel zal miljoenen Nederlanders criminaliseren voor een activiteit die nu gewoon is toegestaan onder de thuiskopie-exceptie van de Auteurswet. Uit een recent verschenen rapport van het TNO blijkt dat meer dan vier miljoen Nederlanders wel eens een inbreukmakend muziekje of filmpje hebben gedownload. De Commissie Gerkens stelt bovendien voor bij de handhaving van het verbod gebruik te maken van 'Deep Packet Inspection' (DPI). Deze techniek maakt het mogelijk om alle internetverkeer op inhoud te controleren. Later heeft Gerkens aangegeven dat zij een 'waarschuwingsscherm' op filesharingsites zou willen publiceren, maar zij heeft niet ondubbelzinnig afstand genomen van de inzet van DPI in het kader van de introductie van een downloadverbod.

Voorstanders van dit voorstel lijken zich geen rekenschap te geven van de gevolgen voor de privacy van de internetgebruiker. Alle inhoud van al het internetverkeer moet continu in de gaten gehouden worden om te controleren of mogelijk onrechtmatig materiaal wordt gedownload. In het ergste geval zal ook encryptietechnologie verboden moeten worden, wat internetbankieren en veilig e-mailen onmogelijk zou maken. Dit voorstel vergroot ook de kans op censuur. In veel gevallen is het namelijk niet eenvoudig vast te stellen of sprake is van inbreuk op een auteursrechtelijk beschermd werk. Invoering van de voorgestelde technologie maakt het in theorie mogelijk om zonder voorafgaande toetsing door een rechter de toegang tot informatie te blokkeren of de informatie te verwijderen. Tegelijkertijd staat het vermeende negatieve effect van filesharing op de productie van cultuur allerminst vast. Uit Brits onderzoek blijkt zelfs dat filesharers meer muziek kopen.

Het minutieus observeren van alle gedragingen van alle internetgebruikers staat in geen enkele verhouding tot het veronderstelde probleem, waarvan het bovendien nog onzeker is of een downloadverbod de oplossing zal zijn. De voorgestelde handhaving van het downloadverbod zet tevens het open karakter van het internet op losse schroeven. De overheid en de entertainmentindustrie moeten nadenken over de stimulering van de productie en verspreiding van cultuur, zonder dat de internetgebruiker vergaand wordt gecontroleerd en gecriminaliseerd.

Meer informatie

Rapport Commissie Gerkens (herdruk) (2008/2009)
http://www.tweedekamer.nl/images/Herdruk_rapport_auteursrecht_118-191067.pdf
Kabinetsreactie op rapport Commissie Gerkens (30.10.09)
http://www.justitie.nl/images/Kabinetsreactie%20wg%20Gerkens%20eindversie_tcm34-229079.pdf
NU.nl, 'Handhaven downloadverbod strijdig met privacy' (Video) (18.12.09)
http://www.nu.nl/internet/2147164/handhaven-downloadverbod-strijdig-met-privacy.html
NRC.next, 'Zeg nee tegen het repressieve downloadverbod', (21.12.09)
http://www.bbrussen.nl/2009/12/21/zeg-nee-tegen-het-repressieve-downloadverbod/

Onderzoeksrapport TNO, IViR, SEO, 'Ups and downs: Economische en culturele gevolgen van file sharing' (12.01.09)
www.ez.nl/dsresource?objectid=161961&type=PDF
NRC Handelsblad, 'Downloadverbod slecht voor creativiteit' (19.01.10)
http://www.nrc.nl/economie/article2462306.ece/Verbod_op_downloaden_slecht_voor_creativitei
The Register, Downloadverbod stimuleert versleuteling dataverkeer (23.10.09)
http://www.theregister.co.uk/2009/10/23/filesharing_crypto/
Tweakers, 'Brits onderzoek: filesharers kopen meer muziek' (02.11.09)
http://tweakers.net/nieuws/63458/brits-onderzoek-filesharers-kopen-meer-muziek.html
Tweakers, 'SP pleit voor waarschuwingsscherm voor downloadsites' (18.12.09)
http://tweakers.net/nieuws/64422/sp-pleit-voor-waarschuwingsscherm-voor-downloadsites.html

De mobiele naaktscanner van de politie

Oom Agent komt u preventief naaktfotograferen

Daags nadat Hirsch Ballin in allerijl besloot naaktscanners op Schiphol in te voeren, wil ook de politie een mobiele naaktscanner ontwikkelen. De scanner zou binnen drie jaar beschikbaar moeten zijn voor alle korpsen, en zou ook 'heimelijk' op openbare plaatsen moeten kunnen worden gebruikt. De jury is van oordeel dat *function creep* zelden zo snel plaatsvond: van een middel ter bestrijding van terrorisme tot een middel dat in alledaags politiewerk kan worden ingezet.

In samenwerking met de landelijke ondersteuningsdienst van de politie Voorziening tot samenwerking Politie Nederland (VtsPN), werkt het politiekorps Rotterdam-Rijnmond aan de ontwikkeling van de mobiele naaktscanner, waarvoor het een subsidie van een half miljoen euro zal ontvangen van het ministerie van Binnenlandse Zaken. Met behulp van een dergelijke scanner zal de politie in staat worden gesteld om door de kleding van gescande personen heen te kijken. Hoewel de politie Rotterdam heeft aangegeven dat de mobiele naaktscanner zal dienen als alternatief voor preventief fouilleren, ziet het korps al mogelijkheden om de scanner in vele andere situaties toe te passen, zoals bij grote evenementen of in (semi)publieke ruimten als winkelcentra en het openbaar vervoer.

De inbreuk op de privacy van burgers is op zijn minst serieus te noemen. De mobiele scanners kunnen het lichaam ongemerkt 'aflezen' vanaf een afstand tot meer dan tien meter. De jury ziet –

naast het gevaar dat men zich anders zal gedragen als men continu wordt geobserveerd - de toepassing van de mobiele naaktscanner als een aantasting van de lichamelijke integriteit. In dit geval is het niet de fysieke aanraking van het lichaam die deze lichamelijke integriteit aantast, maar de observatie en doorlichting van het lichaam zelf, zonder medeweten en zonder toestemming van de geobserveerde persoon. Corien Prins, hoogleraar privacyrecht aan de Universiteit Tilburg, wijst erop dat niet alleen de observatie zelf problematisch is, maar dat ook de opslag en de verwerking van deze informatie eveneens de privacy van burgers kan aantasten. Hoe lang zullen de beelden bewaard blijven, voor wat voor doeleinden mag men de opgeslagen informatie gebruiken en wie heeft er toegang tot deze informatie?

De jury observeert opnieuw een duidelijk geval van function creep. Waar de naaktscanners op Schiphol terroristische aanslagen proberen te voorkomen, manifesteert zich daags na het besluit deze te introduceren een roep om mobiele naaktscanners op straat. Het vormt een vervanging van preventief fouilleren. Maar waar de mogelijkheid tot preventief fouilleren ingevolge artikel 151b van de Gemeentewet is beperkt tot een door de burgemeester aangewezen gebied voor bepaalde tijd, lijkt dit plan heel Nederland bij voorbaat als 'veiligheidsrisicogebied' te bestempelen. Het zal mogelijk worden om iedereen op afstand preventief te scannen.

De bestrijding van criminaliteit is een uiterst belangrijk doel, maar de jury vindt dat het voorstel onvoldoende rekening houdt met de maatschappelijke risico's van deze technologie. Eerst moet worden vastgesteld wat de mogelijke nadelen van de toepassing van deze technologie kunnen zijn. Daarnaast betwijfelt de jury ten zeerste of de veronderstelde 'dreigingssituatie op straat' een dergelijk ingrijpende inbreuk op de privacy en lichamelijke integriteit van burgers vereist. Niet alleen is het kwestieus of er sprake is van een dergelijke dreiging in Nederland, het is ook

onzeker of deze situatie effectief kan worden bestreden door toepassing van de mobiele naaktscanner door de politie.

Meer informatie

NRC Handelsblad, 'Politie: mobiele scanners bouwen' (07.01.10)
http://www.nrc.nl/binnenland/article2453129.ece/Politie__mobiele_scanners_bouwen
NRC.next blog, 'Politie Rotterdam: Die securityscanner kunnen we op straat ook wel gebruiken' (07.01.10)
http://www.nrcnext.nl/blog/2010/01/07/politie-rotterdam-die-securityscanner-kunnen-we-op-straat-ook-wel-gebruiken/
De Pers, 'De verkeerde bodyscanners zijn besteld' (07.01.10)
http://www.depers.nl/binnenland/366577/Verkeerde-naaktscanners-besteld.html
Elsevier, 'Kritiek op bodyscan; NCTb vaag over werking' (08.01.10)
http://www.elsevier.nl/web/Nieuws/Nederland/255188/Kritiek-op-bodyscan-NCTb-vaag-over-werking.htm

Het INDECT-project

Europees werkgelegenheidsprogramma voor ex-KGBers

Europa werkt aan een Orwelliaans informatiesysteem voor de observatie van haar burgers. Het project INDECT, dat door 17 Europese partijen wordt ontwikkeld, moet het mogelijk maken om vanuit de lucht, vanaf de straat en online 'abnormaal gedrag' en geweld automatisch te detecteren. Het project heeft bijna 11 miljoen euro subsidie gekregen van de Europese Unie. Doel van het systeem: 'observation, searching and detection for security of citizens in urban environment.' De jury nomineert het Europese surveillanceproject INDECT, dat veel weg heeft van een Europees werkgelegenheidsprogramma voor ex-KGB'ers.

Het systeem moet het gedrag van iedere burger in de publieke ruimte registreren en analyseren door middel van een heel Europa omvattend netwerk van camera's en andere observatiemiddelen. De geregistreerde gegevens zouden beschikbaar moeten zijn voor Europese opsporingsambtenaren. Daarnaast wil men 'agents' ontwikkelen die permanent en volautomatisch online 'public resources' zoals websites, internetfora, p2p-netwerken en zelfs individuele computers observeren. Met andere woorden: men wil het gedrag in zowel de openbare ruimte als online van iedere burger in Europa kunnen observeren en analyseren.

Het project staat nog in de kinderschoenen en het uitgetrokken budget is natuurlijk (en gelukkig) volstrekt onvoldoende voor een project van deze omvang. Maar de omschrijving op de website en het promotiefilmpje van INDECT bieden een leerzaam inkijkje in

de ambities van het onderzoeksproject en een deel van de Europese overheid.

Het is de jury nog onbekend wie op welke gronden en voor welke doeleinden de verkregen informatie mag gebruiken. Hoewel het project volgens de website een 'Ethics board' heeft dat toeziet op de ethisch-juridische aspecten, spreekt de website alleen over het lidmaatschap van vertegenwoordigers van Noord-Ierse politiediensten. De jury twijfelt niet zozeer aan de integriteit van deze vertegenwoordigers, maar vraagt zich af of in de 'Ethics board' alleen de opsporingsdiensten of ook andere groepen uit de samenleving vertegenwoordigd zouden moeten zijn.

Met een enkele verwijzing naar de bescherming van de veiligheid van Europese burgers, is de noodzaak van een dergelijk project nog niet aangetoond. De ambitieuze plannen van INDECT vereisen op zijn minst een grondige analyse van de mogelijke burgerrechtelijke risico's die aan een dergelijk overkoepelend systeem kleven. De jury is ziet deze eenzijdige visie op de veiligheidsproblematiek in Europa als een stap op weg naar een politiestaat.

Meer informatie

Project INDECT
http://www.indect-project.eu/
Promotievideo Project INDECT
htttp://www.volksopstand.net/index.php?option=com_hwdvideoshare&task=viewvideo&Itemid=4&video_id=88
Europese Commissie, Seventh Framework Research Funding Programme (FP7)
http://cordis.europa.eu/fetch?CALLER=FP7_PROJ_EN&ACTION=D&DOC=4&CAT=PROJ&QUERY=011f30e52539:b685:00e1e967&RCN=89374
Telegraph, 'EU funding 'Orwellian' artificial intelligence plan to monitor public for "abnormal behaviour"' (19.09.09)
http://www.telegraph.co.uk/news/uknews/6210255/EU-funding-Orwellian-artificial-intelligence-plan-to-monitor-public-for-abnormal-behaviour.html

Nominaties categorie Personen

DESIGN BY ERJEE.NET

Guusje ter Horst, minister van Binnenlandse Zaken en Koninkrijksrelaties

'Privacy maakt Nederland minder veilig'

De jury erkent dat minister Ter Horst een grote verantwoordelijkheid heeft om de handhaving van de openbare orde in goede banen te leiden. Maar de bewindsvrouw betoont zich onevenredig vaak ongevoelig voor de privacygevolgen. Door haar eenzijdige focus op vermeende functionaliteit en efficiëntie, en haar gebrek aan begrip voor het belang van privacybescherming, bouwt zij mee aan de instrumenten van een politiestaat. Tijdens haar korte bewind heeft de minister talloze wapenfeiten op haar naam gezet, die een nominatie voor een Big Brother Award verdienen. Onderstaande selectie levert een gevarieerd en triest beeld op.

Onder het bewind van minister Ter Horst is de opslag van vingerafdrukken in het kader van het biometrisch paspoort ingevoerd. Waar zij geregeld verwijst naar een verplichting die zou voortvloeien uit Europese regelgeving, bestaat die verplichting niet ten aanzien van de verzameling van twee extra vingerafdrukken en de centrale opslag daarvan in een landelijke databank. Ter Horst luistert niet naar kritiek over veiligheid (een beveiligingslek is mogelijk rampzalig), noodzaak (buurlanden hanteren minder ingrijpende oplossingen) en function creep (de Officier van Justitie krijgt toegang tot de vingerafdrukkendatabank), terwijl haar ministerie critici de mond

snoert door aangifte te doen.

De jury neemt het minister Ter Horst kwalijk dat zij na de mislukte aanslag op eerste Kerstdag direct overging tot het plaatsen van naaktscanners op Schiphol. De aanpak is tekenend voor de wijze waarop de bewindsvrouw veiligheid en privacy afweegt. Privacy is volgens haar iets vaags. We moeten de overheid gewoon eens vertrouwen, want die heeft het beste met ons voor. Maar volgens de jury is in veel gevallen sprake van wat veiligheidsdeskundige Bruce Schneier 'veiligheidstheater' noemt.

Haar ministerie voert het burgerservicenummer (BSN) breed in. Dit unieke nummer maakt het mogelijk om informatie tussen zorg, onderwijs, inkomsten, uitkeringen, fiscale gegevens en reisgegevens van studenten te koppelen. De minister is doof voor de bezwaren dat het BSN tot een cascade van fouten in al deze gekoppelde systemen kan leiden, waardoor burgers ernstig in de problemen kunnen raken.

Dit jaar joeg de minister haar eigen politieagenten tegen zich in het harnas toen ze bekend maakte dat het DNA van alle agenten in een databank opgenomen moest worden. Op die manier zouden dwaalsporen op plaatsen delict kunnen worden voorkomen. Een belangrijk deel van de agenten wilde hun DNA echter niet afstaan, omdat zij dit een inbreuk op hun privacy vonden.

Minister Ter Horst lijkt daarnaast ongevoelig voor kritiek. Ondanks een vernietigend vonnis van de rechter en aanhoudende kritiek in de media weigert minister Ter Horst haar excuses aan te bieden over het onwettig aftappen van Telegraafjournalisten waartoe zij opdracht gaf. En naar aanleiding van de kritiek over de ongerichte kentekenopslag bij Zwolle zei ze: 'Als je criminelen wilt vangen, moet je soms onorthodoxe methoden gebruiken.' Ze gaat er daarbij aan voorbij dat de kentekenopslag voor alle langsrijdende

auto's geldt. Ook stelde zij onlangs fier 'van de stroming veiligheid boven privacy' te zijn. Deze dooddoener komt haar op een bijzondere vermelding te staan.

Met haar rigide standpunten simplificeert Ter Horst het debat over privacy. Ze polariseert door te suggereren dat wie niets te verbergen heeft, ook niets hoeft te vrezen, en te stellen dat veiligheid altijd boven privacy gaat. Volgens de Jury kunnen die twee in werkelijkheid niet zonder elkaar, en kan de categorie Personen niet zonder een nominatie voor minister Ter Horst.

Meer informatie

Nederlands Juristen Blog, 'Wachten op de kraak' (21.09.09)
http://njblog.nl/2009/09/21/wachten-op-de-kraak/
Digitaal bestuur, 'Nog veel vragen rond het Burgerservicenummer' (10.11.06)
http://digitaalbestuur.nl/nieuws/nog-veel-vragen-rond-burgerservicenummer
NRC Handelsblad, 'Bodyscanner ingezet op alle vluchten naar VS' (30.12.09)
http://www.nrc.nl/binnenland/article2448157.ece/Bodyscanner_ingezet_op_alle_vluchten_naar_VS
Vrij Nederland, 'Guusje ter Horst: "Een opstand van de elite is hard nodig"' (07.07.09)
http://www.vn.nl/Standaard-media-pagina/GuusjeTerHorstEenOpstandVanDeEliteIsHardNodig.htm
Digitaal bestuur, 'Verzet tegen databank met DNA van agenten' (24.11.08)
http://digitaalbestuur.nl/nieuws/verzet-tegen-databank-met-dna-van-agenten
Volkskrant, 'AIVD moet afluisteren Telegraaf staken' (23.07.09)
http://www.volkskrant.nl/binnenland/article1265441.ece/AIVD_moet_afluisteren_Telegraaf_staken

Ab Klink, minister van Volksgezondheid, Welzijn en Sport

'Eigenlijk gaan we ervan uit dat iedereen wil meedoen'

Ab Klink heeft in 2009 veel Nederlanders onaangenaam verrast met een premature brief over de opname van hun medische gegevens in het Elektronisch Patiëntendossier (EPD). In de bijbehorende folder verzweeg de minister ten onrechte de nadelen van zo'n gekoppeld patiëntendossier. Ook de wijze waarop toestemming werd gevraagd, was bepaald onorthodox: wie zweeg stemde toe, wie van deelname aan het EPD verschoond wilde blijven, moest zich expliciet afmelden. Dat juist de nee-zeggers vervolgens kopieën van hun paspoort moesten inleveren om hun weigering gestand te doen, maakte de zaak er niet fraaier op. Desondanks hebben honderdduizenden Nederlanders bezwaar gemaakt tegen opname van hun gegevens in het EPD. Onder artsen en specialisten is het verzet nog groter. Blijkens een enquête van Medisch Contact wil een ruime meerderheid van hen zelf niet opgenomen worden in het EPD. Dat zou een helder signaal voor deze minister moeten zijn, die te lichtzinnig omgegaan is met de kritiek op, en de bezwaren tegen het EPD.

Voorts heeft Klink, ondanks beloftes van zijn voorganger, het medisch beroepsgeheim nog steeds niet herzien en

geactualiseerd. Met de invoering van elektronische patiëntendossiers zijn er tal van nieuwe beroepsgroepen bijgekomen die door hun werk met grote hoeveelheden medische gegevens te maken krijgen, maar voor wie het medisch geheim niet geldt: systeembeheerders, software-ontwikkelaars, datatypistes, etcetera. Je kunt niet enerzijds automatisering afdwingen, en anderzijds doen alsof alles bij het oude blijft. Neem daarbij het recente gegeven, dat minister Klink nog steeds vasthoudt aan DigiD voor de authenticatie van patiënten tot hun EPD – ondanks alle bezwaren tegen deze onveilige methode van toegangsbeveiliging. Terwijl de minister aan de Kamer het hoogst haalbare beveiligingsniveau had belooft. Het risico op het lekken van gevoelige medische gegevens is zodoende groot.

Daarnaast hekelt de jury Klinks opstelling over de diagnosebehandelcombinaties (DBC). Het DBC-systeem is een financieringssystematiek in de zorg, waarbij gedetailleerde informatie over de diagnose en behandeling van een patiënt bij de zorgverzekeraars gestuurd moet worden. Het bezwaar daarvan is – buiten dat verzekeraars deze gevoelige informatie kunnen misbruiken om aan risicoselectie te doen – dat deze systematiek artsen verplicht het medisch beroepsgeheim systematisch te schenden. In de geestelijke gezondheidszorg hebben ettelijke psychiaters en psychologen aangegeven hierdoor in grote verlegenheid te zijn gebracht. Ook de vrij gevestigde psychiaters, die helemaal geen vergoeding van de overheid of de zorgverzekeraars krijgen, werden verplicht het DBC-systeem te gebruiken. Diverse psychiaters hebben om die reden hun praktijk gesloten. Klink wil van geen probleem weten. 'Het systeem is leidend', zegt de minister.

De jury erkent dat de minister zich, in tegenstelling tot enkele van zijn collega's, bezig houdt met de privacy van patiënten en de beveiliging van het systeem. Zijn woorden zijn echter onvoldoende in daden omgezet. De Jury wil het signaal van de

burger kracht bijzetten met een nominatie in de categorie Personen: het is tijd dat de privacykwesties niet alleen benoemd worden, maar centraal staan bij de invoering van het EPD en de DBC's.

Meer informatie

Informatiefolder 'Het elektronisch patiëntendossier (EPD)' (PDF) (05.09.08)
http://www.minvws.nl/includes/dl/openbestand.asp?File=/images/meva-2875251b-_tcm19-171660.pdf
AD, 'Woede om EPD-brief Klink' (03.11.08)
http://www.ad.nl/ad/nl/1012/Binnenland/article/detail/326684/2008/11/03/Woede-om-EPD-brief-Klink.dhtml
Medisch Contact, 'Te vroeg voor landelijk EPD', enquête onder artsen over deelname EPD (14.05.09)
http://medischcontact.artsennet.nl/blad/Tijdschriftartikel/Te-vroeg-voor-landelijk-EPD.htm
Webwereld, 'VVD fileert Klink over beveiliging EPD' (15.01.10)
http://webwereld.nl/nieuws/64866/vvd-fileert-klink-over-beveiliging-epd.html

Frans Heeres, korpschef van de politie Midden- en West-Brabant

'Ach, met Google Earth gebeurt al hetzelfde'

Korpschef Frans Heeres hoopt tijdens de eerstvolgende Tilburgse kermis onbemande spionagevliegtuigen (drones) van het leger te kunnen inzetten om de orde te handhaven. 'Het is een goed middel als je de mensen op zo'n groot kermisterrein in de gaten wilt houden. Voor voetbalwedstrijden lijkt het me ook een uitstekend middel', meldde Heeres in het Brabants Dagblad. Het gebruik van drones is misschien wel makkelijk, maar is het ook menselijk?

Uit niets is gebleken dat de inzet van zo'n ingrijpend surveillancemiddel noodzakelijk is voor de handhaving van de openbare orde tijdens een kermis. De jury stoort zich in het bijzonder aan de redenering die Heeres aan de dag legt. In dezelfde krant zegt hij: 'Ach, met Google Earth gebeurt al hetzelfde.' De korpschef beseft blijkbaar niet dat Google Earth een collectie is van oude satellietfoto's en mensen dus helemaal niet live in de gaten houdt. En al zóu dat het geval zijn: dat de ene instelling de fout in gaat en de privacy schendt, kan nooit betekenen dat de overheid dat dan 'dus' ook mag doen.

De jury heeft de maatschappelijke positie van Heeres laten meewegen in haar oordeel. Zijn opmerkingen getuigen van een zeer gebrekkige kennis van techniek, wat niet past bij een

korpschef. Daarbij vindt de jury de inzet van militaire middelen bij civiele ordehandhaving buitenproportioneel, en een akelig voorbeeld van function creep. Genoeg redenen om de korpschef te nomineren voor een Big Brother Award in de categorie Personen, en hem te verwijzen naar http://earth.google.com/intl/nl/ zodat hij kan leren wat de dienst precies inhoudt.

Meer informatie

Brabants Dagblad, 'Spionagevliegtuigjes ook boven de kermis' (11.01.10)
http://www.brabantsdagblad.nl/regios/tilburg/6072387/Spionagevliegtuigjes-ook-boven-de-kermis.ece
Tweakers, 'Defensie zet onbemande cameravliegtuigen in tijdens jaarwisseling' (28.12.09)
http://tweakers.mobi/nieuws/64585
Ministerie van Defensie, 'Vliegende nachtkijkers ingezet tijdens jaarwisseling' (Video) (01.01.10)
http://www.defensie.nl/actueel/nieuws/2010/01/01/46142977/Vliegende_nachtkijkers_ingezet_tijdens_jaarwisseling_video

Over de Jury

Karin Spaink (voorzitter) is een Nederlands activiste, en publiciste. Ze schrijft onder meer voor Het Parool (1992 tot heden) en haar blog spaink.net. Verder is ze lid van de programmacommissie van HAR. Van 1999 tot 2006 was zij voorzitter van Bits of Freedom.

Prof. dr. Bart Jacobs is hoogleraar beveiliging en correctheid van programmatuur aan de Radboud Universiteit Nijmegen, en Design and Verification of Secure Software Systems aan de Technische Universiteit Eindhoven. Daarnaast is hij bestuurslid bij de Oophaga Foundation.

Prof. dr. 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.

Dr. Bart Schermer is als universitair docent verbonden de Universiteit Leiden. Verder is hij partner bij Considerati, redacteur van het Tijdschrift voor Internetrecht en interim-voorzitter van de United Nations CEFACT Legal Group.

Prof. dr. Valerie Frissen werkt als senior strateeg bij TNO Informatie- en Communicatie Technologie en is namens TNO als hoogleraar ICT & Sociale Verandering verbonden aan de Erasmus Universiteit Rotterdam. Verder is zij lid van de raad van toezicht van de Nederlandse Publieke Omroep.

Bart de Koning schrijft over politiek, economie en recht. In 2008 schreef hij het boek “Alles onder controle?”, waarin hij uitlegt waarom de overheid de burger tegenwoordig niet meer vertrouwt.

De Big Brother Awards
wordt mede mogelijk
gemaakt door

De genomineerden voor de Big Brother Awards 2009 zijn vastgesteld door een onafhankelijke expertjury. Deze organisaties hebben geen invloed gehad op het oordeel van de jury.