BIG BROTHER AWARDS

JURYRAPPORT 2011

BIG BROTHER AWARDS

JURYRAPPORT 2011

ORGANISATIE

De Big Brother Awards worden georganiseerd door Bits of Freedom:
www.bigbrotherawards.nl
www.bof.nl

OPMAAK

Verzorgd door Largetosti:
www.largetosti.com

INHOUDSOPGAVE

De shortlist met genomineerden voor de Big Brother Awards 2011 zijn vastgesteld door de onafhankelijke expertjury.

OVER DE BIG BROTHER AWARDS

Met de Big Brother Awards worden elk jaar de grofste privacyschenders te kijk gezet. Personen, bedrijven en overheden die het afgelopen jaar bij uitstek controle op burgers en inbreuken op privacy hebben bevorderd staan op 7 maart 2012 extra in de schijnwerpers.

DE NAAM

De award ontleent zijn 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 Bits of Freedom, een onafhankelijke burgerrechtenbeweging die opkomt voor communicatievrijheid en privacy op internet. Deze grondrechten zijn onmisbaar voor ieders sociale en persoonlijke vrijheid, voor maatschappelijke innovatie en voor een democratische rechtstaat. Maar die internetvrijheid is niet vanzelfsprekend. Persoonlijke gegevens worden opgeslagen en geanalyseerd. Het verkeer van internetgebruikers wordt geanalyseerd, afgeknepen en geblokkeerd. De kracht van Bits of Freedom ligt in de combinatie van inhoudelijke expertise, een constructieve bijdrage aan beleid 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

EDITIE 2011 MEDE MOGELIJK GEMAAKT

De achtste editie van de Big Brother Awards Nederland, op 7 maart 2012, is mede mogelijk gemaakt door de hulp van talloze vrijwilligers, Pakhuis de Zwijger, ontwerpbureau Largetosti, visueel collectief WERC en crossmedia productiebedrijf Engage! Bits of Freedom wil hen hiervoor hartelijk bedanken

Amsterdam, 24 februari 2012

OVER DIT RAPPORT

Voor u ligt het juryrapport waarin de nominaties voor de Big Brother Awards 2011 worden toegelicht. De winnaars van de Awards worden, net als de winnaar van de Publieksprijs, bekend gemaakt op 7 maart 2012 tijdens een feestelijke prijsuitreiking in Pakhuis de Zwijger.

SINDS 22 DECEMBER 2011

kon het publiek kandidaten voordragen in drie categorieën: Overheid, Personen en Bedrijven. In tegenstelling tot vorig jaar is gekozen om de categorie Voorstellen te laten vallen. Ondanks het schrappen van deze categorie ontvingen we dit jaar nog meer inzendingen dan vorig jaar. De jury wil alle inzenders hartelijk bedanken: velen van u kwamen met goede en nauwkeurige bronvermeldingen.

DAARNA KON DE JURY AAN DE SLAG

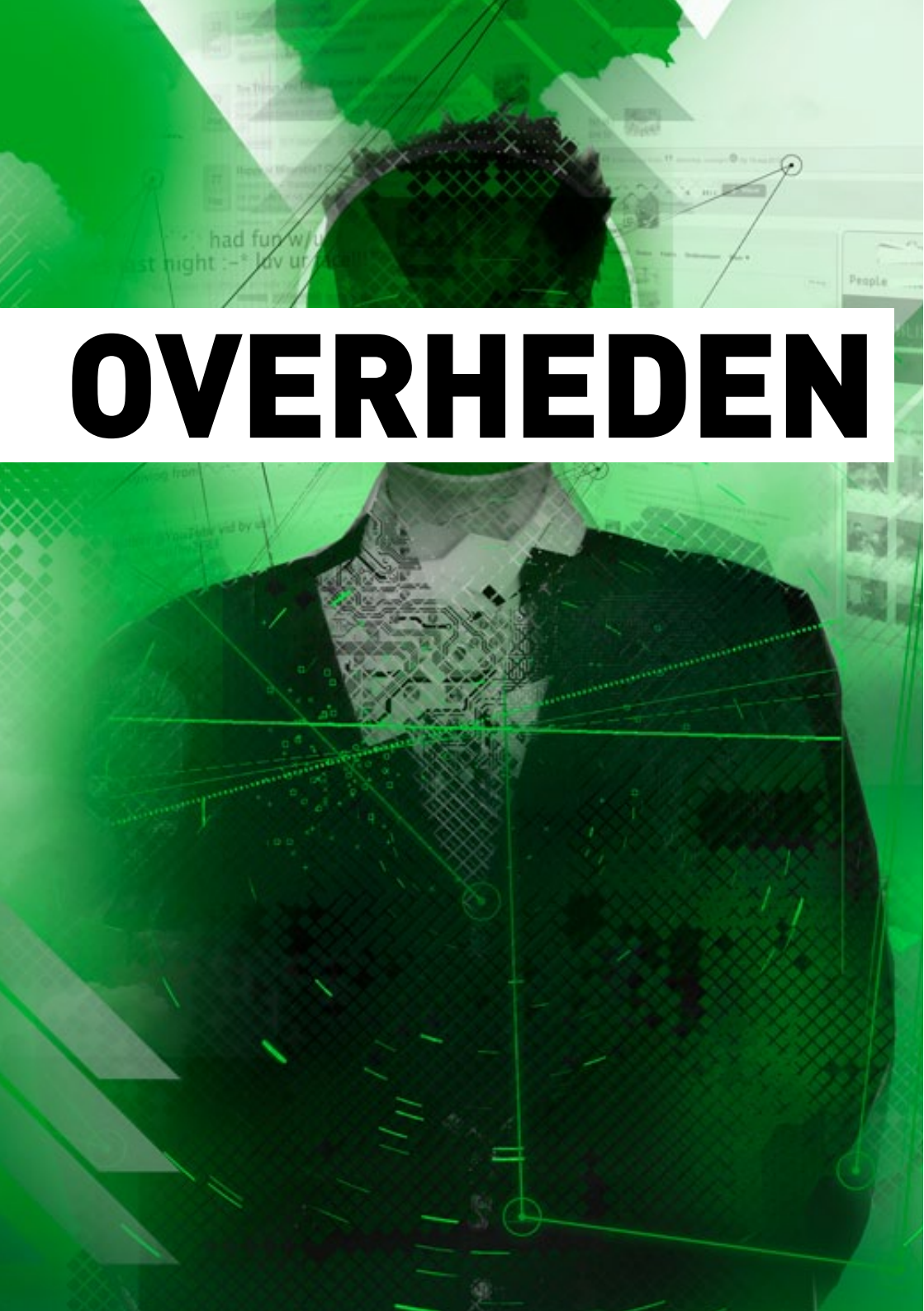
De jury is samengesteld uit experts op het gebied van privacybescherming, informatierecht, consumentenproblematiek en internet. De jury heeft tijdens de beraadslagingen in volle onafhankelijkheid geopereerd. Bits of Freedom noch andere personen of organisaties hebben op enigerlei wijze invloed uitgeoefend op het oordeel van de jury.

DIT JAAR

De categorie bedrijven telt vier nominaties. Een vermelding is postuum: het desbetreffende bedrijf is inmiddels failliet. De jury vond de nominatie echter zo zwaar wegen, dat zij er een bijzondere vermelding voor in het leven heeft geroepen.

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

OVERHEDEN



DE GEMEENTE RHENEN: KONINGINNEDAG IN HET HUIS VAN BEWARING

Omdat ze preventieve huiszoekingen wil doen voor Koninginnedag

De gemeente Rhenen wil er zeker van zijn dat het bezoek van Koningin Beatrix op 30 april 2012 een groot feest wordt. Daarvoor moeten argeloze inwoners wel thuis onbekend bezoek toelaten, anders mogen ze uit logeren – op kosten van de staat. Een middel dat zijn doel volledig mist.

In januari 2012 maakte de gemeente Rhenen bekend bij de voorbereidingen van Koninginnedag 2012 preventieve huiszoekingen te zullen inzetten. Volgens burgemeester Joost van Oostrum is dit nodig om de veiligheid van Koningin Beatrix te kunnen garanderen. Mensen die niet meewerken aan deze huiszoekingen kunnen worden gearresteerd, aldus van Oostrum: “Ik snap uw emotie maar ik zou u echt willen aanraden om zich daar niet tegen te verzetten. Want als u dat doet, dan denk ik dat u op 30 april niet in Rhenen bent maar in het arrestantencomplex van de politie Utrecht te Houten,” waarschuwde de burgemeester tijdens een informatiebijeenkomst na vragen van een verontruste inwoner. Een dag na de bekendmaking van de huiszoekingsmaatregel schreef hij op Twitter: “Het is een gevoel van eerst schrikken en daarna het FEESTgevoel weer oppakken. Zo ging het gisterenavond gelukkig ook.”

Huizen doorzoeken zuiver omdat de Koningin ergens een feestje geeft, is een verstrekkende maatregel. Een huiszoeking is een hoogst ingrijpend en intimiderend middel. De maatregel wordt verdedigd met een verwijzing naar de aanslag in Apeldoorn op Koninginnedag 2009. Maar lokale huiszoekingen hadden die aanslag nooit kunnen voorkomen: de dader woonde in een heel andere gemeente.

Dat de burgemeester van Rhenen het begrijpelijke verzet van zijn gewone, onverdachte burgers meteen beantwoordde met de opmerking dat iedereen die niet meewerkt in hechtenis zou worden genomen, toont zijn minachting voor het klassieke huisrecht.

MEER INFORMATIE:

RTV Utrecht, 'Huizen Rhenenaren mogelijk doorzocht op 30 april' (27.01.12)
http://www.rtvutrecht.nl/nieuws/416686/huizen-rhenenaren-mogelijk-doorzocht-op-30-april
Gemeente Rhenen, presentatie informatiebijeenkomst Koninginnedag 2012 (01.2012)
http://www.koninginnedag2012.nl/library/uploads/documenten/Presentatie-rhenen.pdf
Twitter, Burgemeester Rhenen over het feestgevoel (27.01.12)
https://twitter.com/#!/JoostvOostrum/status/162782162653941760
Twitter, Burgemeester Rhenen over de criteria voor huiszoekingen (27.01.12)
https://twitter.com/#!/JoostvOostrum/status/162969200736997376

HET KORPS LANDELIJKE POLITIEDIENSTEN: OPNIEUW INBREKEN TELT NIET

Vanwege het gebruik van spyware en het opnieuw hacken van hacking-slachtoffers

Het KLPD heeft nieuwe technische speeltjes ontdekt: met spyware kan de dienst op afstand verdachten bespioneren en zelfs onschuldigen zijn niet veilig voor haar hacktools. De wetgever werkt nog niet mee en ook de gevolgen zijn nog niet te overzien. Maar wat niet weet wat niet deert, toch?

In een brief aan de Tweede Kamer bevestigde minister Opstelten (Veiligheid en Justitie) in december 2011 dat het Korps Landelijke Politiediensten (KLPD) gebruik maakt van spyware voor opsporingsdoeleinden. Deze software kan op afstand en zonder medeweten van mensen op hun computer worden geïnstalleerd. Hierna is het mogelijk om hun computer op afstand te besturen en gegevens op die computer in te zien.

Het Duitse Hooggerechtshof oordeelde eerder over dit programma dat toepassing ervan als opsporingsmiddel in strijd was met de Duitse grondwet. Uit een spraakmakende analyse van een Duitse vereniging van ethische hackers bleek verder dat de software in kwestie veel meer kan dan alleen communicatie vastleggen. Het spywareprogramma kan op elk moment uitgebreid worden met extra functies. De vastgelegde gegevens worden na opslag verzonden naar

een server in de Verenigde Staten, en de beveiliging was zo slecht dat iemand anders het programma kon kapen. Het KLPD gebruikt juist dit soort spyware.

Niet alleen bij verdachten maar ook bij onschuldige slachtoffers brak het KLPD in. Het gebruikte het criminele computernetwerk Bredolab om berichten naar door datzelfde netwerk geïnfecteerde computers te sturen. In een pop-up kon de computergebruiker vervolgens lezen dat zijn computer besmet was. Het is zeer de vraag of hiervoor een wettelijke bevoegdheid bestaat. In ieder geval heeft het parlement niet gedebatteerd over de inzet van deze technische mogelijkheden.

Het oprollen van een crimineel netwerk is belangrijk en het KLPD verdient daarvoor lof. Maar in haar streven om computercriminaliteit aan te pakken, zoekt het KLPD doelbewust de grenzen van de wet op. Spyware is hoogst omstreden software die diepgaand ingrijpt in de persoonlijke levenssfeer: hiermee kan een computer worden overgenomen. De wettelijke bevoegdheid om spyware ten behoeve van misdaadbestrijding in te zetten en op afstand te installeren is niet vastgelegd. Ook het hacken van computers van slachtoffers is zonder precedent. Bij het inzetten van dergelijke verstrekkende en omstreden middelen moet in een publiek debat onderzoek worden gedaan naar noodzaak en proportionaliteit. Alleen machtigingen afgeven is in dergelijke gevallen onvoldoende: de wettelijke bevoegdheden moeten zonder twijfel aanwezig zijn, en zulke grootschalige operaties moeten worden bewaakt door een rechter-commissaris.

MEER INFORMATIE:

Kamervragen en -antwoorden over het gebruik van spysoftware (13.12.11)
https://zoek.officielebekendmakingen.nl/ah-tk-20112012-1374.html
Bundesverfassungsgericht, 'Leitsätze zum Urteil des Ersten Senats vom 27. Februar 2008' (27.02.08)
http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html
Chaos Computer Club, 'Chaos Computer Club analysiert aktuelle Version des Staatstrojaners' (26.10.11)
http://ccc.de/de/updates/2011/analysiert-aktueller-staatstrojaner
Merel Koning, 'Conclusie Bredolab botnet studie' (09.2011)
http://www.bredolab.nl/scriptie/conclusie/
Security.nl, 'Nederlandse politie kocht Duitse spionagesoftware' (11.10.11)
http://www.security.nl/artikel/38803/1/Nederlandse_politie_kocht_Duitse_spionagesoftware.html
Webwereld, 'Politie ontkent terughacken Bredolab-bots' (01.11.10)
http://webwereld.nl/nieuws/67649/politie-ontkent-terughacken-bredolab-bots.html

DE POLITIE- EN OPSPORINGSDIENSTEN: WIJ CONTROLEREN ANDEREN, NIET ONSZELF

Omdat ze hun eigen verplichte privacycontrole niet naleven

De nieuwe Wet Politiegegevens biedt de politiediensten meer mogelijkheden dan voorheen om persoonsgegevens te gebruiken voor hun handhavings- en opsporingstaken. Ze kunnen hierdoor misstanden beter aanpakken en overtreders makkelijker traceren. Helaas vergeten ze daarbij zelf om zich aan de regels te houden.

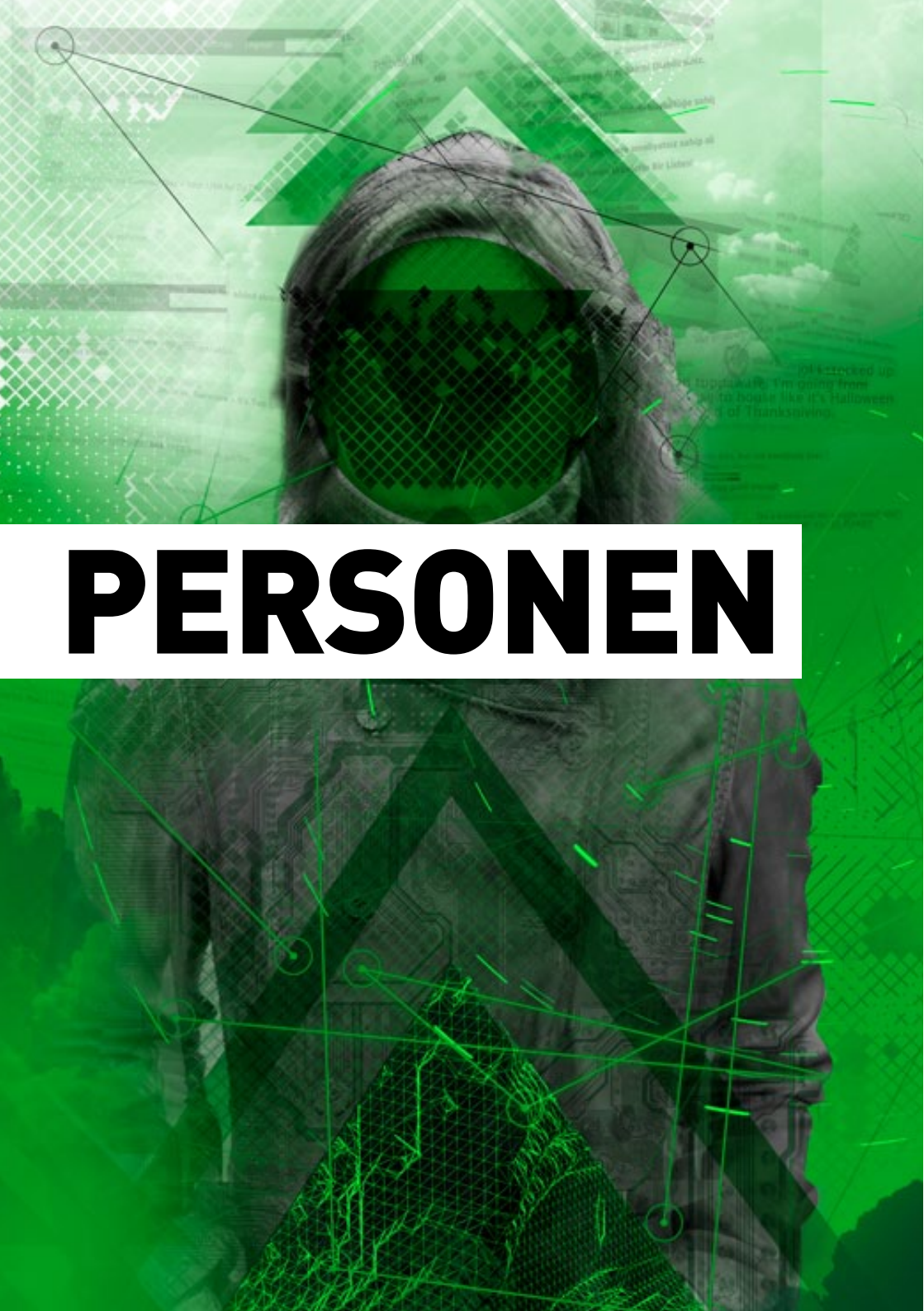
De politiediensten (25 regiokorpsen en 7 opsporingsdiensten, waaronder het KLPD en de FIOD) hebben een uitbreiding van hun bevoegdheden gekregen middels de Wet Politiegegevens (Wpg). Deze wet biedt hen ruimere mogelijkheden dan voorheen voor het verzamelen, bewaren en verstrekken aan derden van persoonsgegevens, ook van mensen die nog niet als verdachte zijn aangemerkt. Daarbij gold als voorwaarde dat zij twee jaar na inwerkingtreding van de wet (en daarna elke vier jaar) een controle op hun privacybeleid en -praktijk zouden uitvoeren; dit om te waarborgen dat de ruimere bevoegdheden zorgvuldig zouden worden toegepast. Politie- en opsporingsgegevens bevatten tenslotte uiterst gevoelige informatie.

De deadline voor de eerste verplichte controle was 1 januari 2011. Geen van de diensten voerde echter een dergelijk onderzoek uit: zo gaf het politiekorps Flevoland doodleuk aan dat het afronden van de audit pas voor 28 oktober 2011 op de rol stond. De Fiscale Inlichtingen- en Opsporingsdienst (FIOD) verklaarde de verplichte controle 'uit het oog verloren' te zijn. En de Koninklijke Marechaussee betoogde dat de uitkomsten van de audit 'op voorhand vaststonden'. Het College Bescherming Persoonsgegevens was coulant en stelde haar handhaving uit tot 1 mei 2011. Maar in juli 2011 moest de privacywaakhond constateren dat alle partijen behalve de FIOD en het korps Zeeland de privacyregels nog steeds overtraden.

Het is nooit leuk om je eigen beleid te moeten controleren. Maar bij handhavingsmacht en verregaande bevoegdheden hoort nu eenmaal grote verantwoordelijkheid. En juist politie- of opsporingsdiensten – die immers de handhavers van de wet zijn – mogen zich nooit aan haar eigen verplichtingen jegens controlerende instanties onttrekken.

MEER INFORMATIE:

College Bescherming Persoonsgegevens, 'Politie en opsporingsdiensten verzuimen privacyaudit uit te voeren' (19.07.11)
http://www.cbpweb.nl/Pages/rap_2011_privacyaudit_politie_bod.aspx
College Bescherming Persoonsgegevens, 'Definitieve bevindingen naar aanleiding van het onderzoek naar de externe privacy-audit Wpg' (19.07.11)
http://www.cbpweb.nl/pages/rap_2011_privacyaudit_politie_bod_rapporten.aspx
Memorie van toelichting Regels inzake de verwerking van politiegegevens (Wet politiegegevens) (24.10.05)
https://zoek.officielebekendmakingen.nl/kst-30327-3.html?zoekcriteria=%3Fzkt%3DEenvoudig%26pst%3D%26vrt%3D30327%26zkd%3DInDeGeheleText%26dpr%3DAfgelopenDag%26spd%3D20100517%26epd%3D20100518%26sdt%3DDatumBrief%26ap%3D%26pnr%3D1%26rpp%3D10%26_page%3D2%26sorttype%3D1%26sortorder%3D4&resultIndex=14&sorttype=1&sortorder=4


PERSONEN

AFKE SCHAART: RUPSJE NOOITGENOEG VAN PRIVACYSCHENDINGEN

Vanwege haar privacy-onvriendelijk stemgedrag

De fractiewoordvoerster ICT en innovatie van de VVD stemt systematisch voor elke maatregel die privacy inperkt en tegen plannen die privacy juist beschermen. Haar achterban mort. Onze privacy kreunt.

Tweede Kamerlid Afke Schaart (VVD) heeft in 2011 een opmerkelijke staat van dienst opgebouwd. Ze bracht haar stem uit tegen een voorstel dat internetgebruikers moet beschermen tegen het volgen en bewaren van hun surfgedrag door adverteerders. Ook diende ze een voorstel in dat telecombedrijven zou toestaan om gratis alternatieven voor hun bel- en smsdiensten – denk aan WhatsApp en Skype – van een prijskaartje te voorzien. Het probleem is dat die bedrijven voor dit 'filteren op inhoud' uiteraard wel de gegevens over internet- en belgedrag van hun klanten moeten kunnen analyseren. Bijvoorbeeld met de controversiële techniek Deep Packet Inspection. Een voorstel om het gebruik van die techniek aan banden te leggen, kon niet op haar stem rekenen.

Dit alles kwam de nummer 31 van de VVD-kandidatenlijst voor de Tweede Kamer op kritiek van te staan, ook van VVD-sympathisanten. Haar stemgedrag en voorstellen maken inbreuk op privacy, zijn slecht voor innovatie en schaden het liberale imago van haar partij.

Het stemadvies van een fractiewoordvoerder is zwaarwegend: in het merendeel van de gevallen vertrouwt een partijfractie bij stemmingen op dit oordeel. Afke Schaart heeft zich het afgelopen jaar steevast tegen privacybescherming gekeerd, zonder oog voor privacyvriendelijke alternatieven. Juist voor een Kamerlid dat vrijheid en democratie voorstaat is dat een hoogst zorgelijke opstelling.

MEER INFORMATIE:

Handelingen Tweede Kamer der Staten-Generaal, 'stemmingen in verband met het wetsvoorstel Wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen'(21.06.11)
https://zoek.officielebekendmakingen.nl/dossier/32549/h-tk-20102011-95-9?resultIndex=24&sorttype=1&sortorder=4
Afke Schaart, 'Amendement Schaart over netneutraliteit' (01.06.11)
http://afkeschaart.vvd.nl/actueel_16181/37744/
Teldersstichting, 'De wenselijkheid van een wet op netneutraliteit' (28.06.11)
http://teldersstichting.vvd.nl/nieuws/241/column-de-wenselijkheid-van-een-wet-op-netneutraliteit
VVD.nl, 'Gebruikers mobiel internet moeten porno en spam kunnen blijven weren' (08.06.11)
http://www.vvd.nl/actueel/1380/gebruikers-mobiel-internet-moeten-porno-en-spam-kunnen-blijven-weren#related_reactions
VVD.nl, 'VVD in de bres voor betaalbaar internet' (01.06.11):
http://www.vvd.nl/actueel/1368/vvd-in-de-bres-voor-betaalbaar-internet#related_reactions
Volkskrant, 'Kamer debatteert over aparte tarieven voor Skype en WhatsApp' (08.06.11)
http://www.volkskrant.nl/vk/nl/2694/Internet-Media/article/detail/2443117/2011/06/08/Kamer-debatteert-over-aparte-tarieven-voor-Skype-en-WhatsApp.dhtml

EDITH SCHIPPERS: GEFUNDEERD STOPBORD? DOORDENDEREN!

Omdat zij het omstreden Electronisch Patiëntendossier een private doorstart gaf

Het parlement had serieuze bedenkingen over het Elektronisch Patiëntendossier en trok vervolgens hard aan de noodrem. Maar minister Edith Schippers liet zich niet op een doodlopend spoor zetten. Met alle privacyrisico's van dien.

"Het wetsvoorstel is zó belangrijk voor de verbetering van de veiligheid en de privacy voor de patiënt dat ik het de moeite waard vond om het toch door te zetten ondanks de moeilijkheden die ik in de Eerste Kamer verwachtte." Dat zei minister Edith Schippers (Volksgezondheid, Welzijn en Sport) over het Elektronisch Patiëntendossier (EPD), vlak voor de stemming in de Eerste Kamer. Via het EPD kunnen zorgverleners digitaal informatie opslaan en uitwisselen over patiënten en hun medicijngebruik. Ten tijde van Schippers' uitspraak maakten ICT-professionals zich al langer ernstige zorgen over beveiligingsrisico's rondom het EPD project. Het project was volgens hen ondoordacht en slecht beveiligd. De vrees van de bewindsvrouw werd bewaarheid: unaniem schoot de Senaat het landelijk EPD af, juist vanwége de gebrekkige privacy en veiligheid rondom dit tien jaar lopende project.

Een paar maanden nadat de plannen voor een landelijk EPD in de Eerste Kamer waren gestrand, gooide Schippers het EPD echter over de heg bij Zorgverzekeraars Nederland. Ze stak eenmalig ruim twee miljoen euro in de private doorstart van de landelijke gegevensuitwisseling.

Met deze zet ligt het beheer van het EPD ineens volledig bij de private sector, zonder parlementaire controle of inspraak voor de burger. Daarnaast kunnen de zorgverzekeraars, door geen contracten aan te gaan met huisartsen of klinieken die niet 'mee' willen, het hele zorgveld dwingen tot een EPD. Een EPD dat ook onder veel zorgverleners absoluut niet gewenst was: het percentage artsen dat heeft aangegeven dat zijzelf niet in het EPD willen worden opgenomen, is meer dan het tienvoudige van het gemiddelde.

De jury ziet Schippers' manoeuvre als een kwalijke manier van uitbesteden: wat het parlement gemotiveerd afkeurt, doet ze alsnog door het aan private partijen over te laten. Met risico's voor de privacy van Nederlanders. Wat nu gebeurt met de gegevens van die Nederlanders in het EPD is door dit outsourcen moeilijker te controleren. En patiëntengegevens onder de hoede van zorgverzekeraars brengen is hoogst discutabel: juist verzekeraars willen bitter graag weten welke klanten 'profijtelijk' zijn en welke niet. Bovendien hebben de verzekeraars geen belang bij het (laten) ontwikkelen van privacy-vriendelijke systemen om gegevens uit te wisselen op een wél veilige manier. Zelfs patiënten die een EPD wíllen, maar dan veilig, trekken aan het kortste eind.

MEER INFORMATIE:

Eerste Kamer, 'Eerste Kamer verwerpt unaniem voorstel landelijk EPD' (05.04.11)
http://www.eerstekamer.nl/nieuws/20110405/eerste_kamer_verwerpt_unaniem
NOS, 'Eerste Kamer blokkeert EPD' (30.03.11)
http://nos.nl/video/229468-eerste-kamer-blokkeert-epd.html
Webwereld, 'Toch miljoenen van minister voor privaat EPD' (09.12.11)
http://webwereld.nl/nieuws/108838/toch-miljoenen-van-minister-voor-privaat-epd.html
NRC, 'Schippers orkestreert iedereen over de elektronische snelweg' (17.12.11)
http://weblogs.nrc.nl/opklaringen/2011/12/17/schippers-orkestreert-iedereen-over-de-elektronische-snelweg/
AutomatiseringGids, 'ICT'ers sceptisch over Elektronisch Patiëntendossier' (29.03.11)
http://www.automatiseringgids.nl/nieuws/2011/13/icters-sceptisch-over-elektronisch-patientendossier
Medisch Contact, 'Artsen dienen massaal bezwaar in tegen EPD' (05.2009)
http://medischcontact.artsennet.nl/Nieuwsartikel/59071/Artsen-dienen-massaal-bezwaar-in-tegen-EPD.htm

FRED TEEVEN: CRIMEFIGHTER KLEEDT PRIVACY STEEDS VERDER UIT

Persoonsgegevens niet veilig bij staatssecretaris van Veiligheid en Justitie

Fred Teeven zet in op steeds zwakkere privacywetgeving. Medische dossiers zijn niet meer heilig en camerabeelden zijn voor hem vooral handig om frustraties te verminderen. Wat hem betreft is het einde van de afkalving van ons recht op privacy nog lang niet in zicht.

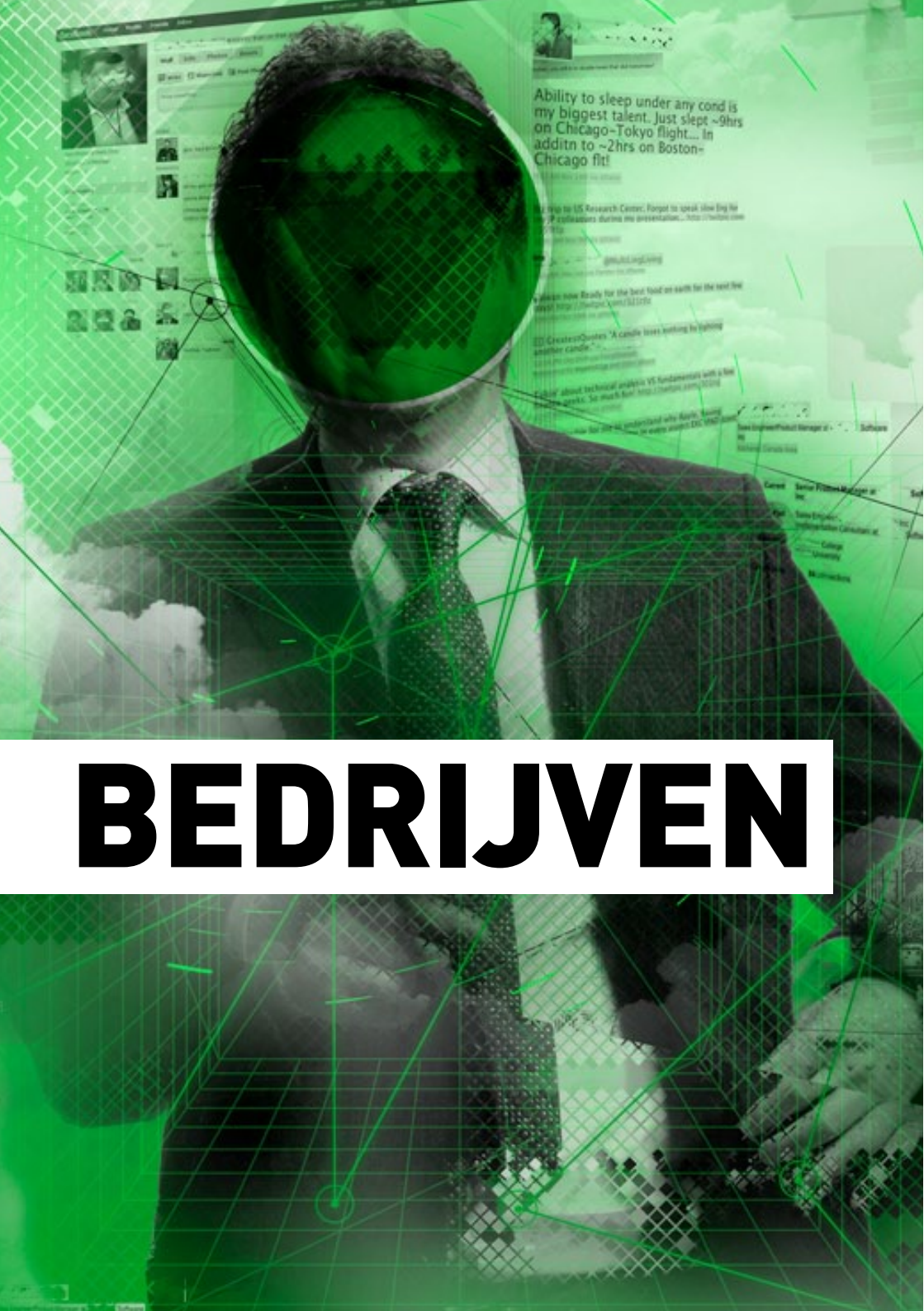
Op dit moment kunnen verdachten niet gedwongen worden om inzage te geven in hun medisch dossier ten behoeve van een TBS-oplegging. In februari 2011 schreef Staatssecretaris Fred Teeven (Veiligheid en Justitie) echter in een brief aan de Tweede Kamer dat hij politie en justitie toegang wil geven tot bepaalde medische dossiers. Rechters kunnen dan, ook als verdachten niet meewerken, op basis van hun medisch dossier toch tot een TBS-oplegging besluiten. Hiermee komt de vertrouwensrelatie van zorgverleners met hun patiënten op de tocht te staan. Immers: wie is nog eerlijk tegen zijn psycholoog wanneer alles wat hij daar zegt, tegen hem gebruikt kan worden?

Daarnaast lanceerde Teeven in december 2011 het plan om burgers en bedrijven de mogelijkheid te geven zelf beelden van daders van strafbare feiten op internet te zetten. De oud-officier van justitie verdedigde de noodzaak voor deze wetswijziging niet met een grotere pakkans voor daders, maar betoogde: "Wanneer echter niet alle mogelijkheden om de beelden optimaal te gebruiken worden benut, dan leidt dat gevoelens van frustratie en teleurstelling bij de slachtoffers en mogelijk ook tot het verminderen van het vertrouwen in opsporing en vervolging." Blijkbaar is het verminderde vertrouwen in de rechtstaat en de afschaffing van de onschuldpresumptie voor de jurist Teeven geen bezwaar.

Fred Teeven blijft zich ieder jaar inzetten om privacy in te perken. Enkele privacyregels zijn inmiddels al tot op het bot uitgekleed. De jury kan alleen maar concluderen dat deze bewindvoerder zijn burgers liefst helemaal naakt ziet.

MEER INFORMATIE:

NRC, "Verscherping tbs-beleid kabinet betekent privacyschending' (17.02.11)
http://www.nrc.nl/nieuws/2011/02/17/kabinet-ontlopen-tbs-straf-wordt-onmogelijk/
Kamerstukken, Memorie van toelichting bij de wijziging van de Wet Bescherming Persoonsgegevens (12.2011)
http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2011/12/20/memorie-van-toelichting-wijziging-van-de-wet-bescherming-persoonsgegevens/c-documents-and-settings-nsenff-ad-000-desktop-camera-pers-5641b-mvt-versie-consultatie-en-advies-dec-11.pdf
Automatisering Gids, 'Teeven: 'Zwak privacywet af' (21.12.11)
http://www.automatiseringgids.nl/nieuws/2011/51/teeven-zwak-privacywet-af
Artikel 88 Wet op de Beroepen in de Individuele Gezondheidszorg:
http://lexius.nl/wet-op-de-beroepen-in-de-individuele-gezondheidszorg/artikel88


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

CONNEXXION: NEEMT ZWARTRIJDEN WEL HEEL LETTERLIJK

Vanwege het aangeven van hun eigen passagiers

Vervoersbedrijf Connexxion biedt reizigers naast snoepautomaten in de bus nog een extra service. Agenten in burger, ijverige kaartcontroleurs en de Vreemdelingenpolitie waken op haar buslijnen over u en ons. Heeft u de pech om met het verkeerde uiterlijk in de verkeerde zone te zitten, dan riskeert u dat uw buschauffeur u aangeeft.

Eind 2011 werd bekend dat vervoersbedrijf Connexxion sinds 2010 actief heeft geholpen bij het opsporen en uitzetten van mensen zonder geldige verblijfsvergunning. De vreemdelingenpolitie hield deze mensen op grond van hun uiterlijke kenmerken aan en controleerde hun verblijfsstatus. De Raad van State beoordeelde deze gang van zaken als onrechtmatig. Maar toen waren al twaalf personen als gevolg van de tips van Connexxion het land uitgezet.

Uit de uitspraak van de Raad van State blijkt dat buschauffeurs van Connexxion het maar raar vonden dat 'negroïde' vrouwen uit Amsterdam geregeld naar welgestelde gemeenten zoals Heemstede en Bloemendaal reisden. Het vervoersbedrijf tipte de Vreemdelingenpolitie. Deze vrouwen werden daarna gevolgd: de politie postte bij buslijnen, in samenwerking met controleurs van de busmaatschappij, en volgde ze stiekem tot aan hun werkadres, waar ze werden aangehouden. Het verweer van Connexxion: "Als iemand geen geldig plaatsbewijs heeft en zich niet wil legitimeren, moeten wij de politie inschakelen.

Het vervult de jury met afschuw dat er bedrijven zijn die op basis van oppervlakkige aannames hun eigen klanten op een zo schandalige manier verklikken.

MEER INFORMATIE:

Haarlems Dagblad, 'Klopjacht op illegalen in villawijken' (23.02.11)
http://www.haarlemsdagblad.nl/nieuws/regionaal/haarlemeo/article6548801.ece/Klopjacht-op-illegalen-in-villawijken-
Volkskrant, 'Connexxion werkte samen met politie' (24.02.11)
http://www.volkskrant.nl/vk/nl/2844/Archief/archief/article/detail/1851492/2011/02/24/Connexxion-werkte-samen-met-politie.dhtml
Volkskrant, 'Twaalf illegale werkster lang uitgezet. opgepakt wegens negroïde uiterlijk' (16.12.11)
http://www.volkskrant.nl/vk/nl/2686/Binnenland/article/detail/3078913/2011/12/16/Twaalf-illegale-werksters-land-uitgezet.dhtml
Uitspraak Raad van State (13.07.11)
http://zoeken.rechtspraak.nl/detailpage.aspx?ljn=BR2059
OVPro.nl, 'Connexxion: 'Wij helpen geen illegalen oppakken' (23.12.11)
http://www.ovpro.nl/management/2011/12/23/connexxion-wij-helpen-geen-illegalen-oppakken/

FACEBOOK: BEURSGANG MET U, MAAR ZONDER UW INSTEMMING

Omdat het met de gegevens van haar gebruikers naar de beurs gaat

Facebook heeft een twijfelachtige reputatie op het gebied van privacy en krijgt steeds vaker de wind van voren. Maar niets weerhoudt haar: het bedrijf maakt nu haar eigen feestje door middel van een beursgang. Aandeelhouders willen daarna natuurlijk profiteren van de waarde van onze persoonlijke gegevens. En dat kunnen wij ook onszelf aanrekenen.

Facebook ligt regelmatig onder vuur vanwege privacyschendingen. Zowel in de Verenigde Staten (door de Federal Trade Commission) als in Europa is onderzoek gedaan naar het privacybeleid van de tech-gigant uit Californië.

Een greep uit de keur aan klachten en onderzoeksresultaten:
1. Facebook heeft toegegeven de internetactiviteit van haar gebruikers bij te houden, ook wanneer deze zich buiten Facebook.com bevinden. Bovendien bleek het bedrijf gegevens van niet-Facebook-gebruikers te verzamelen.
2. Facebook beloofde dat het de persoonlijke gegevens van haar gebruikers niet deelt met adverteerders, maar doet dat wel degelijk. Daarnaast krijgen apps toegang tot bijna alle persoonlijke data van gebruikers.
3. Facebook vertelde gebruikers dat zij toegang tot hun informatie konden beperken, bijvoorbeeld tot hun vrienden. Niettemin werd die data dan ook gedeeld met de apps van die vrienden .
4. Facebook is begonnen een Real Name Policy af te dwingen. Alleen onder een zogenaamde 'echte naam' mag men een account gebruiken. Iedereen die een artiestennaam heeft of een alias, moet er rekening mee houden dat zijn of haar gehele account opgeheven wordt. Dat terwijl er veel situaties denkbaar zijn waarin het gebruik van een alias nodige bescherming biedt, bijvoorbeeld voor bloggers in weinig democratische regimes.
5. Sinds 2011 bouwt Facebook in Europa een databank met gezichtsgegevens van gebruikers via de tags die aan foto's worden toegevoegd. Gebruikers is daarvoor nooit om toestemming gevraagd, noch konden ze eenmaal opgeslagen gegevens laten verwijderen. Pas op last van de Ierse Data Protection Commissioner (DPC) pastte Facebook dit enigszins aan.

Facebook maakt zichzelf rijk met de informatie die wij met onze vrienden en kennissen delen: met mensen die we vertrouwen. Nu het bedrijf naar de beurs gaat en alle aandeelhouders nadien winst uit hun investering willen halen, zal het pas echt werk maken van het uitbaten van onze persoonlijke data.
De jury wil met de nominatie voor Facebook ook onderstrepen dat wijzelf niet vrij van blaam zijn. We werken hartelijk mee aan onze eigen privacyschendingen.

MEER INFORMATIE:

Wall Street Journal, 'Facebook Sets Historic IPO' (02.02.12)
http://online.wsj.com/article/SB10001424052970204879004577110780078310366.html
Federal trade Commission, 'Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises' (29.11.11)
http://ftc.gov/opa/2011/11/privacysettlement.shtm
www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf
Facebook.com, 'Our Commitment to the Facebook Community' (29.11.11)
https://blog.facebook.com/blog.php?post=10150378701937131
Facebook v Europe, 'Legal procedure against"Facebook Ireland Limited"' (18.08.11)
http://www.europe-v-facebook.org/EN/Complaints/complaints.html
Ierse Data Protection Commissioner, 'Facebook Ireland Ltd. Report of Audit' (21.12.11)
http://www.dataprotection.ie/documents/facebook report/final report/report.pdf
Bloomberg, 'Facebook sued for tracking users after log-off; class-action status sought' (01.10.11)
http://www.bloomberg.com/news/2011-09-30/facebook-may-face-group-privacy-suit-over-web-tracking-after-users-log-off.html
The Guardian, 'Facebook's 'real name' policy attacked by Chinese blogger' (09.03.11)
http://www.guardian.co.uk/world/2011/mar/09/chinese-blogger-mark-zuckerberg-dog
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, 'Gesichtserkennungsfunktion von Facebook verstößt gegen europäisches und deutsches Datenschutzrecht. Löschung biometrischer Daten bei Facebook gefordert' (02.08.11)
http://www.datenschutz-hamburg.de/news/detail/article/gesichtserkennungsfunktion-von-facebook-verstoesst-gegen-europaeisches-und-deutsches-datenschutzrech.html?tx_ttnews[backPid]=1&cHash=e5aa3f2d234135e37c41c8e747295317
Eurobarometer, 'Attitudes on Data Protection and Electronic Identity in the European Union' (06.11)
http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

KPN: TROTS OP VOLGEN VAN HAAR EIGEN GEBRUIKERS

Vanwege het gebruiken van Deep Packet Inspection

Telecombedrijf KPN dacht een nieuwe manier te hebben gevonden om haar aandeelhouders tevreden te stellen met goede winstcijfers. Kon het bedrijf nagaan welke gratis internetdiensten hun klanten gebruikten waarvoor ze bij KPN wél moesten betalen? Voor dat doel werd een onnodig en zeer omstreden middel ingezet, dat trots werd geclaimd als primeur.

In mei 2011 ontstond ophef nadat bekend werd dat KPN gebruik maakte van Deep Packet Inspection (DPI) bij haar klanten. De mobiele telefonieaanbieder gebruikte deze techniek om op detailniveau te bekijken wat hun klanten precies op internet deden, met name om te achterhalen hoeveel klanten WhatsApp gebruikten, een dienst waarmee je – anders dan via KPN zelf – gratis kan sms'en. Vol trots claimde KPN topman Marco Visser dat zijn werkgever als eerste telecomleverancier ter wereld DPI inzette om haar bedrijfsvoering te optimaliseren. De verkregen informatie bleek het bedrijf voorts zonder toestemming van haar klanten te gebruiken voor interne marketingdoeleinden.

De onafhankelijke telecommunicatie autoriteit OPTA stelde vast dat, ook zonder daadwerkelijk rond te neuzen in e-mails of foto's, via DPI "aanbieders kennis nemen van meer informatie dan alleen de informatie die is bestemd voor de afhandeling van het berichtenverkeer". Reden voor de autoriteit om het College Bescherming Persoonsgegevens in te schakelen.

KPN beweerde dat DPI nodig was om te weten welk volume aan verkeer allerlei toepassingen gebruikten. Maar verkeersstromen bestuderen kan uitstekend zonder elk datapakketje van je abonnees inhoudelijk onder de loep te leggen. Dat KPN zich van geen kwaad bewust lijkt te zijn en zelfs prat ging op haar handelen gaat het voorstellingsvermogen van de jury volledig te boven.

MEER INFORMATIE:

KPN presentatie, 'KPN Investor Day: Group Strategy' (10.05.11)
http://pulse.companywebcast.nl/playerv1_0/default.aspx?id=12193&bb=true&swf=true (vanaf 3u 33min)
NOS, 'Consumentenbond: snel onderzoek naar gebruik DPI' (13.05.11)
http://nos.nl/video/240270-consumentenbond-snel-onderzoek-naar-gebruik-dpi.html
Webwereld, 'OPTA: spionage van KPN vergaand en overbodig - Update' (13.05.11)
http://webwereld.nl/nieuws/106670/opta--spionage-van-kpn-vergaand-en-overbodig---update.html
OPTA, 'Voorlopige bevindingen OPTA over gebruik van Deep Packet Inspection door aanbieders van mobiele telefonienetwerken' (30.06.11)
http://www.opta.nl/nl/download/publicatie/?id=3439

BIJZONDERE VERMELDING:

DIGINOTAR, DE KONINKLIJKE NOTARIËLE BEROEPSORGANISATIE EN DE KONINKLIJKE BEROEPSORGANISATIE VAN GERECHTSDEURWAARDERS: CERTIFICAAT VAN ONVERMOGEN

Omdat ze de betrouwbaarheid van communicatie van Iraanse en Nederlandse burgers in gevaar hebben gebracht

Een Nederlands bedrijf haalde door laksheid de wereldpers en anderen betaalden de rekening. Derden probeerden tegen beter weten in hun eigen hachje te redden. Ze vergaten daarbij dat de veiligheid van anderen op het spel stond.

In september 2011 moesten de ministers Donner en Opstelten, in navolging van de meest gebruikte internetbrowsers, het vertrouwen in DigiNotar opzeggen. Dit Nederlandse bedrijf garandeerde via certificaten de veiligheid van communicatie op internet. Maar de website van DigiNotar bleek, vanuit Iran, al weken eerder te zijn gehackt. Hierdoor dachten (Iraanse) internetgebruikers ten onrechte dat ze veilig communiceerden via bijvoorbeeld Gmail, terwijl ze in werkelijkheid werden afgetapt. DigiNotar gaf ook echtheidscertificaten af voor overheidswebsites zoals DigiD en de Belastingdienst. Deze waren door de hack niet meer betrouwbaar en moesten uiteindelijk preventief op slot.

DigiNotar bleek al langere tijd het slachtoffer van hackers. Het bedrijf merkte niet dat ongeveer 300.000 Iraanse computers bij hen valse certificaten ophaalden. Zelfs nadat ze een inbraak had gedetecteerd, deed DigiNotar zelf geen enkel onderzoek. Daar begon het bedrijf pas een maand later mee, en verzweeg daarna nog ruim een maand dat er iets aan de hand was.

De regering verklaarde noodgedwongen alle uitgeleverde DigiD-certificaten ongeldig. Maar wat deden de Koninklijke Notariële Beroepsorganisatie en de Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders, de instanties die DigiNotar hadden opgezet? Ze spanden een kort geding aan en wilden een langere termijn om te kunnen blijven werken met de gehackte – en dus onveilige - certificaten.

De communicatie van honderdduizenden Iraniërs is door de laksheid van DigiNotar gecompromitteerd. Hun communicatie kon worden afgeluisterd. De Nederlandse overheid moest met een grootschalige operatie haar beveiliging up to date brengen, waardoor onder meer DigiD tijdelijk niet bereikbaar was. Allemaal bewijzen van groot onvermogen van een laks bedrijf dat hierdoor de privacy van veel mensen enorm veel schade heeft toegebracht.

Voor DigiNotar komt deze vermelding postuum: het bedrijf is inmiddels failliet. Maar wellicht kan dit de Beroepsverenigingen der Notarissen en Gerechtsdeurwaarders er in de toekomst van weerhouden om hun bedrijfsgerelateerde belangen te plaatsen boven de privacy en veiligheid van anderen.

MEER INFORMATIE:

Persbericht ministerie van Binnenlandse Zaken en Overheidsrelaties, 'Overheid zegt vertrouwen in de certificaten van Diginotar op' (03.09.11)
http://www.rijksoverheid.nl/nieuws/2011/09/03/overheid-zegt-vertrouwen-in-de-certificaten-van-diginotar-op.html
Kamerbrief ministerie van Binnenlandse Zaken en Overheidsrelaties, 'Digitale Inbraak DigiNotar' (05.09.11)
http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2011/09/05/digitale-inbraak-diginotar/kamerbrief-digitale-inbraak-diginotar.pdf
NOS.nl, 'Veiligheid overheidssites niet gegarandeerd' (03.09.11)
http://nos.nl/artikel/269586-veiligheid-overheidssites-niet-gegarandeerd.html
NRC.nl, 'Browsers zeggen definitief vertrouwen in Diginotar op' (03.09.11)
http://www.nrc.nl/nieuws/2011/09/03/browsers-zeggen-vertrouwen-in-diginotar-op/
Rapport Fox-IT, 'DigiNotar Certificate Authority breach' (05.09.11)
http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf
Webwereld, 'DigiNotar.nl staat al jaren open voor hackers' (30.08.11)
http://webwereld.nl/nieuws/107756/diginotar-nl-staat-al-jaren-open-voor-hackers.html
Nu.nl, 'Chronologie DigiNotar' (20.09.11)
http://www.nu.nl/diginotar/2620512/chronologie-diginotar.html
Uitspraak Rechtbank Den Haag in zaak Koninklijke Notariële Beroepsorganisatie en de Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders LJN: BT6349 (27.09.11)
http://www.rechtspraak.nl/Organisatie/Rechtbanken/Haarlem/Nieuws/Pages/**FaillissementDiginotarBV.aspx**
http://zoeken.rechtspraak.nl/detailpage.aspx?ljn=BT6781
Uitspraak faillissement DigiNotar (20.09.11)
http://www.rechtspraak.nl/Organisatie/Rechtbanken/Haarlem/Nieuws/Pages/FaillissementDiginotarBV.aspx

OVER DE JURY

KARIN SPAINK (JURYVOORZITTER)

is columniste en schrijfster. Ze schrijft onder meer voor Het Parool, werkt momenteel aan een boek over de invalidenwagen Canta en is hoofdredacteur van de serie The Next Ten Years over maatschappelijke veranderingen die het internet teweeg brengt. Van 1999 tot 2006 was zij voorzitter van Bits of Freedom.

ANTOINETTE HERTSENBERG

is programmamaakster en presentatrice van consumentenprogramma's TROS Radar en Opgelicht?! Zij is in 2009 door vaktijdschrift Villamedia benoemd tot 'Journalist van het Jaar'. In 2010 heeft Opzij haar uitgeroepen tot 'machtigste mediavrouw van Nederland'.

NICO VAN EIJK

is hoogleraar Media- en Telecommunicatierecht aan de Universiteit van Amsterdam, en directeur van het Instituut voor Informatierecht (IViR). Tevens is hij voorzitter van de Vereniging voor Media- en Communicatierecht (VMC), lid van de Raad van Toezicht van de Nederlandse Publieke Omroep (NPO) en voorzitter van twee commissies van de Sociaal Economische Raad (SER).

TYPHOON

Glenn de Randamie, beter bekend als Typhoon, won op jonge leeftijd de Grote Prijs (2004), één van de meest begeerde talentprijzen van Nederland. Talloze optredens volgden, net zoals zijn debuutalbum 'Tussen Licht en Lucht'. Privacy is een onderwerp waar hij zich sinds lang mee bezig houdt en dat, naast het werken aan zijn nieuwe plaat, een belangrijke plek in z'n leven inneemt.

EDO ROOS LINDGREEN

is partner bij KPMG Advisory. Daarnaast is hij part-time professor in IT en Auditing aan de Universiteit van Amsterdam en programma directeur van Amsterdam IT Audit Programme (AITAP). Ook is hij mede-oprichter van het Amsterdam Platform for Privacy Research (APPR). Daar werken onderzoekers van verschillende faculteiten samen om het privacy-vraagstuk multidisciplinair te benaderen.

MEDE MOGELIJK GEMAAKT DOOR:

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

BIG BROTHER AWARDS

OBJECTOSTI

WEBCAST BY engage
WWW.ENGAGETV.COM

WERC

PAKHUIS DE ZWIJGER*

De genomineerden voor de Big Brother Awards 2011 zijn vastgesteld door de onafhankelijke expertjury. Deze organisaties hebben geen invloed gehad op het oordeel van de jury.