BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN
PRESENTEERT:

BIG BROTHER AWARDS

EDITIE
2013

PROGRAMMA / INHOUD

WELKOM OP DE BIG BROTHER AWARDS 2013.

Net als in voorgaande edities zijn de Big Brother Awards dé gelegenheid om de grofste privacyschenders van het afgelopen jaar in de schijnwerpers te zetten. Maar daarnaast zijn ze ook een gelegenheid om aandacht te vragen voor privacy in het algemeen. Om stil te staan bij de staat van privacy in Nederland anno 2013.

Want de winnaars en genomineerden die vanavond centraal staan, staan niet op zichzelf. De privacyschendingen waar we vanavond aandacht voor vragen zijn geen incidenten. Ze passen structureel in een context van brede maatschappelijke en politieke ontwikkelingen.

Daarom willen we vanavond naast de schendingen zelf, ook het grotere geheel belichten. De technologische ontwikkelingen, het politieke klimaat, de maatschappelijke normen en de commerciële belangen die de jaarlijkse golf aan Big Brother Awards-kandidaten voortbrengen. Dat doen we in deze publicatie en ook met de bijdrages van de sprekers en gasten van vanavond.

We willen laten zien dat deze ontwikkelingen ook kunnen inspireren tot een positieve bijdrage aan het privacydebat: informatief onderzoek, inspirerende kunst, innovatieve software en intressante projecten. Deze bijdrages bieden we vanavond een podium. Want één ding is duidelijk: privacy leeft meer dan ooit.

Veel plezier vanavond!

OVER DE BIG BROTHER AWARDS

DE NAAM

De award ontleent zijn naam aan de totalitaire, alziende leider 'Big Brother' uit het boek 1984 van George Orwell. Tot nu toe werden de Big Brother Awards genoemd naar het jaar waarover de prijzen werden uitgereikt: in 2012 was er 'editie 2011'. Vanaf dit jaar worden de awards genoemd naar het jaar waarin ze worden gehouden. Dit jaar is het dus editie 2013.

DE AWARDS

De Big Brother Awards 2013 worden uitgereikt in twee categorieën: de Publieksprijs en de Expertprijs. Voor de Publieksprijs kon iedereen personen, bedrijven of overheden nomineren die in het afgelopen jaar de privacy geschonden hebben. Op basis van het aantal nominaties is er vervolgens een top-3 gemaakt waar iedereen op kon stemmen. De genomineerde met de meeste stemmen mag de Publieksprijs mee naar huis nemen. In aanvulling op de Publieksprijs heeft Bits of Freedom een aantal experts gevraagd om kandidaten aan te dragen die in het afgelopen jaar minder (media)aandacht hebben gekregen, maar die zeker een plek in de schijnwerpers verdienen. Op basis van deze suggesties zijn er drie genomineerden en vervolgens de winnaar van de Expertprijs gekozen.

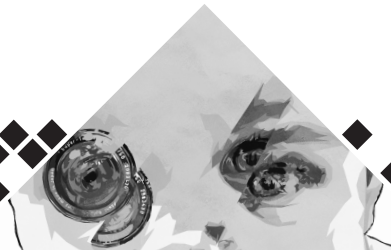
DE ORGANISATIE

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 2013 MEDE MOGELIJK GEMAAKT

De negende editie van de Big Brother Awards Nederland, op 29 augustus 2013, is mede mogelijk gemaakt door de hulp van talloze vrijwilligers, Pakhuis de Zwijger, ontwerpbureaus Merged Visible en Structure & Narrative, visueel collectief WERC, crossmedia-productiebedrijf Engage! en Onno Warns. Bits of Freedom wil hen hiervoor hartelijk bedanken.

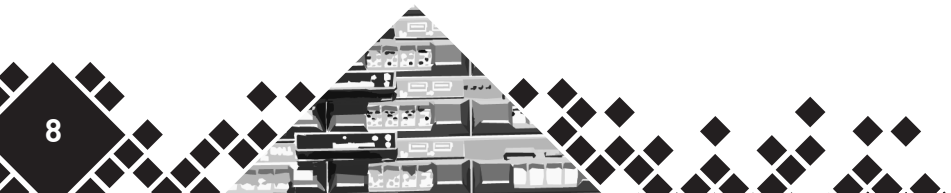
Amsterdam, 29 augustus 2013



DE STAAT VAN PRIVACY

SENSORS & SURVEILLANCE

De afgelopen jaren zijn sensors steeds kleiner geworden, steeds meer gaan registreren en alomtegenwoordig geworden. Camera's kleiner dan je oog filmen de auto's op de Nederlandse snelwegen. GPS-trackers zitten in je telefoon. Microfoons luisteren mee naar gesprekken op pleintjes. En al die gegevens worden opgeslagen, voor steeds langere duur. We zijn de eerste generatie wiens leven wordt vastgelegd met wijdverspreide, kleine sensors. En de komende jaren zal deze trend alleen maar doorzetten. Het internet verhuisde van je desktop naar de smartphone in je broekzak, en nu naar ontelbaar veel apparaten in je privéomgeving en de publieke ruimte. Je kenteken, gezichtskenmerken, bewegingen en reisgedrag worden geregistreerd. Sociale media verleiden je tot het delen van de meest intieme details en gebeurtenissen.



FEITEN:

Drones van Defensie worden meer dan twee keer per week ingezet.

Landen waarvan we weten dat ze internetverkeer op grote schaal tappen: Zweden, Verenigd Koninkrijk, Duitsland, Amerika, Frankrijk.

Aantal opvragingen van abonneegegevens van landelijke telecomdatabase CIOT in 2012: 2.758.435 keer.

"Items of interest will be located, identified, monitored, and remotely controlled through technologies such as radio-frequency identification, sensor networks, tiny embedded servers, and energy harvesters — all connected to the next-generation internet using abundant, low-cost, and high-power computing," aldus David Petraeus, ex-baas van de CIA over Internet of Things.

Afmetingen kleine spionagedrone: 16 gram, 12 cm rotorbreedte.

Feit: theoretische afluistercapaciteit van Engelse transatlantische kabelafluisterprogramma Tempora: 21 petabytes per dag, oftewel 23.643.898.043.698.436 bytes.

DATABESITAS / YOUR DATA EVERYWHERE

Door die groei van het aantal sensors en surveillance, laten we onbedoeld meer sporen na dan ooit. Internetten, een iPhone vol Apps en ons reisgedrag, doktersbezoek en energieverbruik leveren samen een digitale voetafdruk op die ons persoonlijke leven griezelig accuraat weergeeft. Tegelijkertijd wordt de bescherming van al deze gegevens juist minder. Bedrijven pleiten voor softere regels terwijl ze ondertussen databases aan elkaar knopen, dataminen en profielen opstellen van burgers. Big Data verbindt gegevens met elkaar op een manier die we een paar jaar geleden nog voor ondenkbaar hielden. Al die gegevens over ons worden door slimme analyse omgezet in informatie. Het is die informatie die de basis vormt voor beslissingen van overheden en bedrijven over jou.

FEITEN:

Je smartphone is een privacy hazard: veertig procent van de populairste apps heeft geen privacybeleid. Daarnaast voldoen heel veel apps niet aan de privacywetgeving: ze slaan gevoelige informatie op zonder toestemming, verzamelen veel meer gegevens dan nodig of geven informatie door aan derden.

Eind 2013 zullen er ongeveer een half miljoen “slimme” energiemeters zijn geplaatst. Deze meters zijn slecht beveiligd en verraden veel over het energiegebruik en daarmee het gedrag van mensen. De uitrol gaat gewoon door ondanks privacybezwaren.

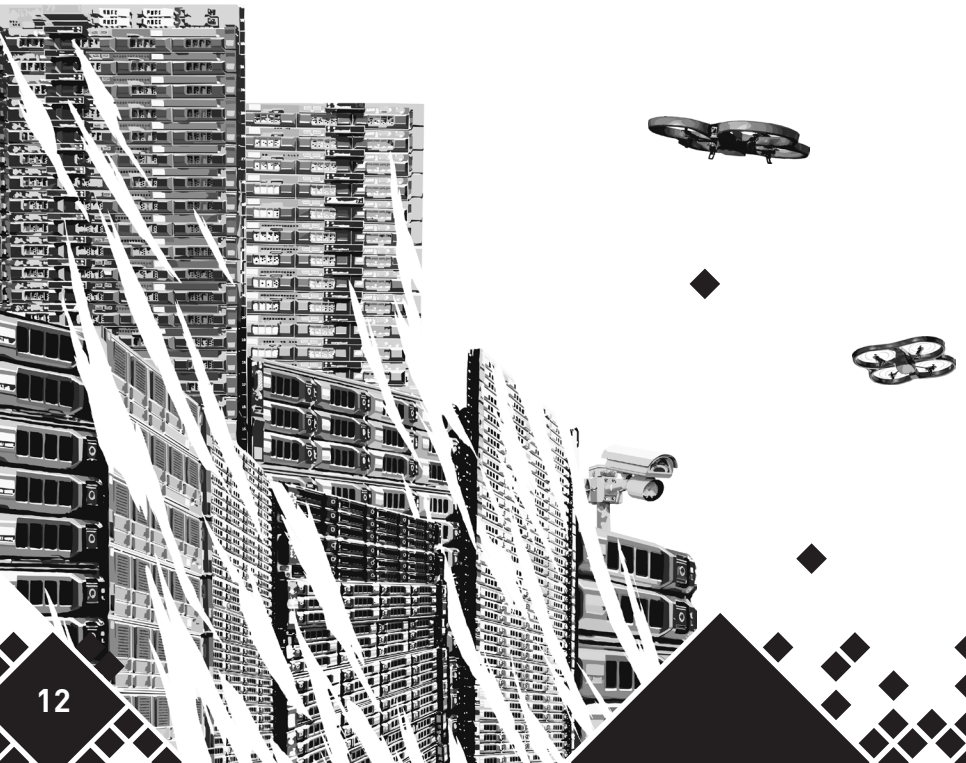
In de VS gebeurt het al jaren, maar ook in Nederland overwegen supermarkten Jumbo en Polare wifi-tracking. Je locatie en gedrag wordt dan offline gedetailleerd in kaart gebracht en bijgehouden.

Equens, de partij die pinbetalingen verwerkt zit op een goudmijn aan informatie en wil daarom alle pingegevens van klanten verkopen. Alleen vanwege ‘grote maatschappelijke onrust’ is dit plan tijdelijk (!) geparkeerd.

Ook de Nederlandse overheid lijdt aan databesitas. Profiling en datamining zijn technieken die steeds meer worden ingezet, ondermeer voor het maken van nieuw beleid. Tegelijkertijd is onduidelijk welke gegevens overheden verzamelen en op welke basis beslissingen over burgers worden genomen.

PRIVACY GEHACKT

Steeds vaker wordt op systemen van burgers, bedrijven én de overheid ingebroken en gevoelige informatie buit gemaakt. Niet alleen door criminelen overigens. Ook de overheid wil toegang tot alles waarin een computer is verwerkt: je laptop, je gehoorapparaat en je auto. Criminelen breken in om geld te verdienen en overheden om criminelen te vinden of kritieke infrastructuur van andere landen te saboteren. En dat terwijl je die computers altijd en overal bij je draagt, ze je meest intieme informatie bevatten en onderdeel zijn van het apparaat waarmee je je met 130 km/uur verplaatst. Jouw data - en daarmee jijzelf - vallen dus aan criminelen en de overheid ten prooi, terwijl maatregelen om je daartegen te beschermen grotendeels afwezig zijn.



FEITEN:

150.000 computers in ons land zijn besmet geweest met het Citadel-virus. 750 GB aan computerbestanden van onder andere energieproducenten, ministeries, ziekenhuizen, waterleiding- en luchtvaartmaatschappijen kwamen in handen van criminelen.

Alle politiekorpsen overtreden de wet waarin geregeld is hoe zij met gevoelige gegevens om moeten gaan. Geen van de korpsen voldeed aan alle normen.

De Duitse overheid maakte gebruik van spyware om verdachten te bespioneren. De politie kon de software naar eigen inzicht uitbreiden met extra functionaliteit. Ook werd de informatie onvoldoende versleuteld naar een Amerikaanse server verzonden. Criminelen konden bovendien inbreken op de verbinding en de besturing van de spyware overnemen.

De Belastingdienst heeft alle parkeergegevens over 2012 opgevraagd van mensen die bij een parkeerautomaat op kenteken parkeerden.

De rechter stak een stokje voor het gebruik van taps door het Autoriteit Consument & Markt (ACM). Uit niets bleek dat de officier van justitie heeft getoetst of de verstrekking voldoet aan de beginselen van proportionaliteit en subsidiariteit.

Als gebruiker is het nog steeds bijzonder lastig om inzage te krijgen in alle gegevens die door bedrijven en de overheid over je worden opgeslagen - zoals je belgedrag - terwijl je daar wel recht op hebt.

SPREKERS

JACOB APPELBAUM

On anonymity and global surveillance

De Amerikaanse hacker, onderzoeker en activist Jacob Appelbaum is vooral bekend als het publieke gezicht van het Tor-project. Hij vliegt de wereld over om zowel activisten als overheden te overtuigen van het belang van online anonimiteit. In 2010 sprak hij namens WikiLeaks op een hackerconferentie in New York en sindsdien is hij het doelwit van aanhoudende surveillance en regelmatige aanhoudingen door de Amerikaanse autoriteiten.

Eerder dit jaar interviewde Appelbaum de - toen nog anonieme - klokkenluider Edward Snowden. Het past in zijn missie om surveillance wereldwijd te openbaren en ter discussie te stellen. Op de Big Brother Awards zal hij verder ingaan op de massale surveillance door overheden en hoe we daar tegen kunnen strijden.

SEBASTIAN

Hoe vergroten hackerspaces de bewustwording van veiligheid en privacy bij internetters?

Met een achtergrond in de ICT en rondhangen in kelders met andere mensen met een tech-interesse, raakte Sebastian aan het begin van het millennium betrokken bij de hackerscene door deelname aan de CCC en Nederlandse hacker-events. Tegelijkertijd sloot hij zich aan bij hacklabs/internetwerkplaatsen ASCII & PUSCII en jaren later Technologia Incognita en LAG. Deze culturele omgeving legde de basis voor zijn professionele ontwikkeling en zorgde voor tal van interessante banen bij zowel publieke als private organisaties, van de gezondheidszorg en de financiële sector tot idealistische NGO's.

Binnen deze hackerspaces en -labs heeft Sebastian diverse workshops en evenementen georganiseerd, kennis gemaakt met diverse onderwerpen en genoten van de vele discussies die ontstonden. Omdat deze omgeving een grote invloed heeft gehad op zijn persoonlijke denkbeelden, zal hij op de Big Brother Awards vertellen welke rol hackerspaces spelen in het vergroten van bewustwording van veiligheid en privacy van internetters.

MIRIYAM AOURAGH

Wat kunnen we hier leren van de surveillancepraktijken in de Arabische wereld?

Op haar blog omschrijft Miriyam Aouragh zichzelf als antropoloog, internetonderzoeker en activist. In 2008 promoveerde ze aan de UvA met haar onderzoek naar internetactivisme in Palestina, Jordanië en Libanon. Tegenwoordig is ze Leverhulme Fellow aan CAMRI, University of Webminster, voor een project rond internet en 'counter-revolutions' in het Midden-Oosten en Noord-Afrika.

Door haar onderzoek weet Aouragh als geen ander welke rol technologie speelt in zowel het ontstaan als het onderdrukken van revoluties in het Midden-Oosten. Ze zal op de Big Brother Awards vertellen over wat we kunnen leren van overheidssurveillance in de Arabische wereld.

CLAUDIO GUARNIERI

The commercialization of surveillance

Claudio Guarnieri werkt als security researcher voor Rapid7. Daarnaast is hij lid van de Shadowserver Foundation: een collectief van security professionals dat strijdt tegen malware en cybercrime. Hij heeft diverse antimalware tools ontwikkeld en is een fel voorvechter van open source software in de beveiligingsindustrie.

Voor Citizenlab werkte Guarnieri mee aan een onderzoek naar de verspreiding van de commerciële spyware FinFisher. Op de Big Brother Awards zal hij vertellen over de vercommercialisering van digitale spionage.

AXEL ARNBAK

In hoeverre hebben geheime diensten toegang tot onze gegevens in de cloud?

Als promovendus aan het Instituut voor Informatierecht (IVIR) doet Axel Arnbak onderzoek naar de regulering van cybersecurity. In 2009 won hij met zijn masterscriptie over dataretentie de Internet Scriptieprijs. Daarna werkte hij een tijd voor Bits of Freedom op onderwerpen als netneutraliteit en datalekken.

Bij het IVIR heeft hij onder andere publicaties geschreven over de Patriot Act en de toegang van Amerikaanse geheime diensten tot informatie in de cloud -een onderwerp dat sinds de onthullingen van Edward Snowden extra in de belangstelling staat. Op de Big Brother Awards zal hij verder ingaan op wat deze onthullingen betekenen voor de veiligheid van onze gegevens.

KUNSTENAARS

FRONT404

FRONT404 is een kunstenaarsduo uit Utrecht bestaande uit Thomas voor 't Hekke en Bas van Oerle. Na samengewerkt te hebben aan een afstudeeropdracht voor de Hogeschool voor de Kunsten in Utrecht besloten ze onder de naam FRONT404 verder te werken aan verdere projecten, met name interactieve installaties. Privacy is een terugkerend thema in hun werk.

Hun werk **Sphere** omschrijven ze als een 'curious creature that likes to keep an eye on things'. Wat er gebeurt als er even niets te zien is kun je zelf ervaren.

CONSTANT DULLAERT

Constant Dullaart studeerde aan de Rietveld Academie en aan de Rijksakademie voor beeldende kunsten, waar hij later 'artist in residence' was. Zijn werkt richt zich op het visualiseren van de taal van het internet, met oog voor politiek en de invloed van het bedrijfsleven. Zijn werk is zowel digitaal als in print verschenen en geëxposeerd in diverse internationale galerieën en musea.

In de video **Terms of Service** (2012) leest de vriendelijke interface van Google de complexe gebruikersvoorwaarden voor - een document dat veel vertelt over het bedrijf achter de zoekmachine.

MODDR_

Het Rotterdamse moddr_ is een ‘media/hacker/co-working space voor artgeeks’. Opgericht door oud studenten Media Design van het Piet Zwart instituut, richt moddr_ zich op het modificeren (modding) van technologie op een artistieke manier.

Commidy.us is een platform met als doel mensen meer controle over hun data te geven. “They make money from your data, why shouldn’t you?”

DATA DEALER

De browsergame Data Dealer is ontstaan uit een samenwerking van game designers en hacktivisten uit Oostenrijk, Duitsland en de VS. De makers typeren het spel als een soort Farmville, maar dan met het oogsten van persoonsgegevens in plaats van radijsjes.

Wolfie Christl, één van de bedenkers van het spel, denkt dat door ‘gamification’ van privacy het bewustzijn bij een grote groep mensen zal groeien. Door jezelf in de schoenen van een dataverzamelaar te plaatsen leer je spelenderwijs wat er allemaal met je privé-gegevens gebeurt.

NOMINATIES PUBLIEKSPRIJS

Voor de Publieksprijs kon iedereen personen, bedrijven of overheden nomineren die in het afgelopen jaar de privacy geschonden hebben. Op basis van het aantal nominaties is er vervolgens een top-3 gemaakt waar iedereen op kon stemmen. De genomineerde met de meeste stemmen mag de Publieksprijs mee naar huis nemen.

IVO OPSTELTEN

Opstelten holt stug door in zijn poging digitale ontwikkelingen naar zijn hand te zetten

Als winnaar van de BBA 2010 en erkend aanhanger van 'law and order' heeft Minister Opstelten zich ook dit jaar hard ingezet voor het afbreken van onze digitale rechten. Van het opslaan, bewaren en scannen van alle kentekens via ANPR-technologie tot zijn wetsvoorstel om computers te kunnen hacken: Ivo Opstelten laat geen kans onbenut om de surveillancestaat tot stand te brengen. Privacy is voor hem niets meer dan een onnodige kostenpost op de begroting.

Dit jaar is hij zijn belofte voor nieuwe wetgeving nagekomen. Begin mei is de Wet Computercriminaliteit III ter consultatie op internet aangeboden. Hierin zal niet alleen het hacken van computers - of alles waarmee contact met internet gemaakt kan worden - aan het opsporingspalet van politie worden toegevoegd, maar ook het kunnen blokkeren en filteren van websites en het kunnen sanctioneren van het niet nakomen van een decryptiebevel door de verdachte.

Daarnaast is het steeds eenvoudiger geworden om auto's op wegen in de gaten te houden. Een reden voor Opstelten om de ANPR-technologie landelijk in te zetten en de kentekens in een database te zetten – je weet immers nooit waar het goed voor is. En de verzamelde gegevens worden eveneens overgedragen aan de Belastingdienst.

Geld is sowieso belangrijk voor Opstelten. Zo merkt hij naar aanleiding van een onderzoek naar de kosten behorende tot nieuwe Europese regelgeving voor bescherming van persoonsgegevens op, dat het hem zorgen baart hoe hoog deze zijn. Jouw privacy kost geld – en dat is niet de bedoeling.

MEER INFORMATIE:

Wet computercriminaliteit III
http://www.ad.nl/ad/nl/1012/Nederland/article/detail/3332144/2012/10/15/Opstelten-politie-moet-computer-mogen-hacken.dhtml

Inzet ANPR-technologie om getuigen te vinden
http://webwereld.nl/beveiliging/59624-kentekendatabase-mogelijk-ook-voor-vinden-getuigen

De zorgen van minister Opstelten over de hoge kosten van privacybescherming:
http://www.nu.nl/economie/3494256/bedrijven-miljard-kwijt-europese-regel.html

NSA & AIVD

NSA & AIVD surveilleren van wieg tot graf met hun digitale navelstreng

Veiligheidsdiensten horen in essentie onze vrijheid – en onze grondrechten – te beschermen. Dit jaar heeft Edward Snowden ons laten zien dat de veiligheidsdiensten hiervoor geen middel schuwen. Ook als dit betekent dat al onze vertrouwelijke communicatie tot op het bot gefileerd wordt. Je beroepen op je recht op privacy is voor de NSA en de AIVD een reden om aan te nemen dat je iets te verbergen hebt.

Op 6 juni onthulde The Guardian dat de NSA gebruik maakt van Prism, een programma dat gebruikt wordt om informatie te verzamelen uit gegevens van (Amerikaanse) communicatie-aanbieders, waaronder Microsoft, Facebook en Google. Later bleek deze onthulling gelekt te zijn door klokkenluider Edward Snowden, die naar Hongkong gevlucht was en vervolgens naar Rusland vertrok.

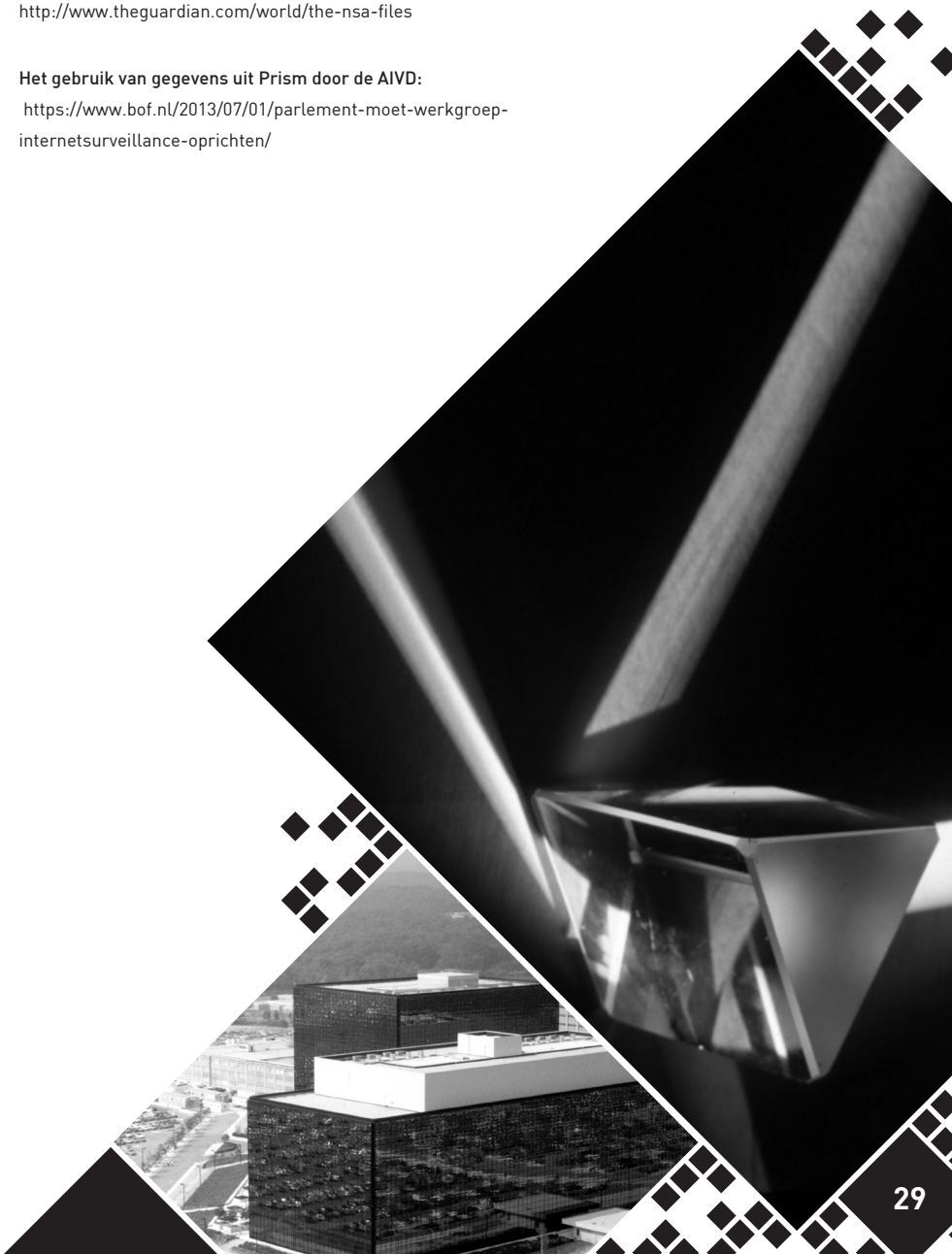
Na de eerste eerste onthulling volgde een reeks van openbaringen over de werkzaamheden van veiligheidsdiensten. Zo verzamelt de NSA al het internetverkeer, evenals sms-verkeer van en naar de Verenigde Staten. De Engelse geheime dienst, GCHQ, tapt transatlantische kabels af die via het Verenigd Koninkrijk lopen en ook Nederland maakt gebruik van gegevens die via deze systemen verzameld worden.

De kritiek die ontstond doet de NSA vrij weinig – vooral omdat het gaat om gegevens van niet-Amerikanen. De Nederlandse regering stelt zich vervolgens op het standpunt dat het niet aan de AIVD of Nederland is om te controleren op welke wijze de gegevens die zij ontvangen van andere geheime diensten verzameld is. En dat was dan dat. Genoeg reden voor een nominatie dus.

MEER INFORMATIE:

De onthullingen rond massale surveillance door de NSA:
http://www.theguardian.com/world/the-nsa-files

Het gebruik van gegevens uit Prism door de AIVD:
https://www.bof.nl/2013/07/01/parlement-moet-werkgroep-internetsurveillance-oprichten/



EQUENS

Equens zoekt andere manieren om de rekening te betalen

Arm Equens. De taak van dit bedrijf is om betalingsgegevens te verwerken. Helaas blijkt het verdienmodel minder riant dan beoogd want Equens besloot dit jaar uit een ander vaatje te tappen. Het leek ze een goed idee om je transactiegegevens te verkopen aan winkels – en hun concurrenten – waar je iets gekocht hebt. Handig toch? Na massale kritiek is dit plan ''tijdelijk'' in de koelkast gezet.

Equens is één van de grootste Europese verwerkers van betalingsverkeer. Ondanks een jaarlijkse 10.4 miljard transacties en 4.4 miljard toonbankbetalingen en geldopnames, is de marge die hierop verdiend wordt voor Equens te klein.

Dus tijd voor een ander plan: het verkopen van pintransactiegegevens. Deze gegevens zouden geanonimiseerd worden, waarbij ze niet te herleiden zouden zijn tot een persoon maar wel tot de wijk waarin die persoon woont.

Kritiek volgde: van privacyorganisaties, banken en de politiek. Ineens vond Equens het geen goed plan meer. Niet omdat de gegevens uiteindelijk toch wel herleidbaar zouden zijn of omdat het plan op zichzelf slecht is, maar vanwege de maatschappelijke onrust die door het plan ontstond.

Nu gaat Equens in overleg met banken en andere partijen om alsnog draagvlak te creëren. Wordt dus ongetwijfeld vervolgd.

MEER INFORMATIE:

De plannen van Equens om pingegevens van klanten door te verkopen:
http://nos.nl/video/510043-equens-wil-pingegevens-verkopen.html

Equens verkoopt voorlopig geen pintransacties:
http://www.nrc.nl/nieuws/2013/05/24/equens-ziet-voorlopig-af-van-doorverkopen-gegevens-pintransacties/

NOMINATIES EXPERTPRIJS

In aanvulling op de Publieksprijs heeft Bits of Freedom een aantal experts gevraagd om kandidaten aan te dragen die in het afgelopen jaar minder (media)aandacht hebben gekregen, maar die zeker een plek in de schijnwerpers verdienen. Op basis van deze suggesties zijn er drie genomineerden en vervolgens de winnaar van de Expertprijs gekozen.

RONALD PLASTERK

Terwijl iedereen wijst naar de VS, bouwt Plasterk verder aan een Nederlandse Prism.

Het leek zo mooi: een wijziging van de grondwet om het briefgeheim uit te breiden naar alle vormen van privécommunicatie. Maar toen het voorstel voor het nieuwe communicatiegeheim er eindelijk was, bleek minister Plasterk er een enorme achterdeur in te hebben gebouwd. Alle privécommunicatie tussen burgers is geheim - tenzij de regering daar anders over denkt.

Volgens het nieuwe voorstel mag er namelijk inbreuk worden gemaakt op het communicatiegeheim na machtiging van een minister of in het kader van de nationale veiligheid. Rechterlijke toetsing komt er dan niet aan te pas. En dat komt de regering mooi uit, aangezien we later dit jaar een wetswijziging kunnen verwachten die inlichtingendiensten de bevoegdheid geeft om massaal internetverkeer af te tappen.

Terwijl alle ogen dus gericht zijn op de Amerikaanse NSA, bouwt Plasterk verder aan de Nederlandse variant van Prism. De minister leek sowieso niet onder de indruk van de onthullingen van Edward Snowden. 'De AIVD gebruikt Prism niet', bracht hij naar buiten. Dat wisten we al, waar het om gaat is of de AIVD informatie gebruikt die via Prism is verkregen. En dat laat Plasterk in het midden: "De wijze waarop specifieke gegevens zijn verkregen wordt in beginsel niet gedeeld."

"Er is veel kritiek op hoe de Amerikaanse overheid burgers volgt, maar we vergeten onszelf een spiegel voor te houden," zegt Nico van Eijk, professor aan het Instituut voor Informatierecht. "Het conceptvoorstel voor het communicatiegeheim laat zien dat het in Nederland niet beter gesteld is."

BRONNEN:

De reactie van Bits of Freedom op het conceptvoorstel voor de wijziging van Artikel 13 van de Grondwet:
https://www.bof.nl/2013/01/17/voorstel-modernisering-communicatiegeheim-onvoldoende/

De reactie van minster Plasterk op de onthullingen over Prism en aftappen door de AIVD:
http://www.rijksoverheid.nl/regering/nieuws/2013/06/21/geen-onbelemmerde-toegang-tot-internet-en-telefoon-voor-aivd-en-mivd.html

HET EUROPEES PARLEMENT

Na elke stap richting meer privacybescherming zetten ze weer twee stappen terug.

De bonte lappendeken die we het Europees Parlement noemen, levert op zijn minst tegenstrijdige resultaten als het om privacy gaat. Soms gaan we er dankzij het EP een stap op vooruit, maar veel vaker zetten we helaas twee stappen terug.

Vorig voorjaar stemde het Parlement er mee in om de Amerikaanse overheid toegang te geven tot de gegevens van Europese vliegtuigpassagiers. Daarbij vond het Parlement het niet nodig om eerst het Europese Hof van Justitie te laten beoordelen of dit wel door de beugel kon.

Na dit dieptepunt ging het Parlement verder met het vormgeven van nieuwe Europese privacyregels. Veel parlementsleden hebben daarbij vooral goed geluisterd naar lobbyisten van de IT- industrie. Daarom ligt er nu - na een jaar van stemmen en praten - een voorstel met duizenden amendementen, die voor het grootste deel slecht nieuws zijn voor burgers. De definitieve stemming volgt nog maar het stemt niet optimistisch.

Recenter stelde het Parlement zich merkwaardig laks op in relatie tot het Prism-schandaal. In plaats van woede en verontwaardiging volgde er een matige resolutie. Gevolg: de onderhandelingen met de Verenigde Staten over een nieuw handelsverdrag gaan gewoon door. Tijdens deze onderhandelingen zal ook de doorgifte van persoonsgegevens door bedrijven naar de Verenigde Staten worden besproken.

We hopen het natuurlijk van harte, maar het lijkt onwaarschijnlijk dat het Parlement haar ruggengraat terugvindt voordat ze opnieuw gaat stemmen en onderhandelen over onze privacy. Gelukkig is het binnenkort onze beurt om te stemmen: in mei 2014 kiezen we een nieuw Europees Parlement. U bent gewaarschuwd.

BRONNEN:

Europees Parlement stemt in met Passenger Name Record overeenkomst:
http://www.europarl.europa.eu/news/en/pressroomcontent/20120419IPR43404/html/Parliament-gives-green-light-to-air-passenger-data-deal-with-the-US

Europees Parlement dreigt privacyregelgeving te verzwakken:
http://www.edri.org/edrigram/number11.11/weaker-data-protection-regulation%3F

TAFTA onderhandelingen vinden doorgang ondanks Prism:
https://www.bof.nl/2013/07/05/tafta-europees-parlement-mist-kans-om-amerikaanse-spionage-te-bestrijden/

DE BELASTINGDIENST

Al rijdt de leaserijder nog zo snel, onze ‘geheelde’ database achterhaalt hem wel.

De Belastingdienst heeft, in een poging om de schatkist enigszins op peil te houden, de jacht geopend op de automobilist. Dit doen ze door het opvragen van gegevens van parkeerinstanties en snelwegcamera’s. Gegevens die verwijderd hadden moeten worden. Desondanks wordt er gegraven in deze berg gegevens, net zolang tot ze de allerlaatste overtreder gevonden hebben. Ondertussen is dat wel een enorme inbreuk op de privacy van iedereen die niets heeft misdaan.

De Belastingdienst gebruikt wel erg graag informatie van anderen. Zo heeft ze een convenant gesloten met de Landelijke Eenheid (de voormalige KLPD) om informatie van ANPR-camera’s te verkrijgen. Deze informatie wordt verwerkt, met name om leaserijders te kunnen controleren. Maar daarmee verzamelt de Belastingdienst dus automatisch alle gegevens van iedereen die over de Nederlandse snelwegen rijdt. Dat is een onacceptabele privacyschending. Daar komt nog bij dat de Belastingdienst gebruik maakt van kentekengegevens die de politie al zou hebben moeten verwijderen. Kortom, de wet wordt gehandhaafd op grond van gegevens die niet voorhanden mogen zijn, en toch worden gebruikt. Vreemd.

Daarbovenop vraagt de Belastingdienst informatie op over parkeerders bij parkeerinstantie SHPV. De SHPV zou deze gegevens na acht weken moeten verwijderen, maar blijkbaar worden ze na die periode versleuteld en alsnog bewaard. Dat komt de Belastingdienst mooi uit, want daardoor kunnen zij deze informatie opvragen. Wederom op oneigenlijke grond dus.

De Belastingdienst komt weg met deze ‘heling’ van gegevens omdat mogelijk inkomstenverlies door frauderende leaserijders boven jouw privacy wordt gesteld. Dat is een nominatie meer dan waard.

BRONNEN:

http://computerworld.nl/cloud/78687-fiscus-buiten-schot-bij-privacyschending
http://www.nrc.nl/nieuws/2013/08/06/politie-schendt-wet-door-opslag-alle-kentekens/
http://webwereld.nl/overheid/78677-belastingdienst-vraagt--gewiste--parkeerdata-op

MEER INFORMATIE:

http://computerworld.nl/cloud/78687-fiscus-buiten-schot-bij-privacyschending
http://www.nrc.nl/nieuws/2013/08/06/politie-schendt-wet-door-opslag-alle-kentekens/
http://webwereld.nl/overheid/78677-belastingdienst-vraagt--gewiste--parkeerdata-op

FOTO CREDITS

Portret Jacob Appelbaum: Joi Ito
Portret Miryam Aouragho: Institute of Network Cultures
Portret Axel Arnbak: Maarten Tromp
Prism logo: Adam Hart-Davis (Natural Science)
Foto Europees Parlement: Europees Parlament
Portretten Ivo Opstelten & Ronald Plasterk: rijksoverheid.nl
Foto moddr: Daniil Vasiliev

ORGANISATIE

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

OPMAAK

Structure & Narrative:
www.structurenarrative.com