Manipulatie, Verlies en Bedrog van Data

Buro Jansen & Janssen

Observant 67, augustus 2015

Inhoudsopgave Observant #67

Mocht je een interessant artikel hebben over je confrontatie met politie en justitie, een nieuwe wetgeving, onderzoek of scriptie mail het ons: info@burojansen.nl

Manipulatie, Verlies en Bedrog van Data Observant 67, augustus 2015
http://respubca.home.xs4all.nl/pdf/Observant67BJJaug2015.pdf

Big Data is hét *buzzword* van de afgelopen jaren. Alles wordt anders, gemakkelijker of complexer, zo moeten wij geloven, maar of dat nu werkelijk zo is, blijft de vraag. Als het om straatnamen, huisnummers, Kadaster of Kamer van Koophandel gegevens gaat, is het duidelijk dat vooral de openbare toegang tot die data allerlei toepassingen mogelijk maakt.

Is dat echter Big Data die belangrijk is, en gaat het dan niet vooral om gemak en toegang in plaats van serieuze Big Data? De media verdwijnen langzaam achter een betaalmuur, dus díe Big Data zijn we aan het verliezen. De wetenschap lijkt zich langzaam wel op te maken voor meer toegang, al is er nog een lange weg te gaan. De overheid is qua transparantie een gesloten fort dus Big Data vanuit die hoek is voorlopig niet toegankelijk.

Jansen & Janssen probeert aangaande het laatste voorbeeld al vele jaren verandering in aan te brengen. Sinds twee jaar is daar een nieuw archief aan toegevoegd, het Nationaal Veiligheidsarchief dat probeert de

archieven van de inlichtingendiensten te ontsluiten. In deze nieuwsbrief lees je meer over de meer dan 3.500 pdf’s en 50.000 geheime documenten. Ook data betreffende preventief fouilleren in Amsterdam komt aan de orde en wat die data zichtbaar maakt met betrekking tot het beleid ten aanzien van de rechten van haar burgers.

Big Data kan ook zomaar je vrijwilligersbaan kosten, en als je data verdwijnt, is je sociale netwerk weg. Data betreffende identificatieplicht maakt duidelijk waarom de overheid niet transparant wil zijn. En tot slot is het natuurlijk van essentieel belang om te weten waar je data geparkeerd staat en hoe veilig dat is.

Wilt u dat Jansen & Janssen de komende jaren onderzoek blijft doen naar politie, justitie en inlichtingendiensten, steun ons dan. Wordt donateur of vraag familie, vrienden en bekenden donateur te worden. Bankrekening N56 INGB 0000 6039 04 (ING 603904 BIC: INGBNL2A) ten name van Stichting Res Publica, Postbus 11556, 1001 GN Amsterdam. Res Publica is de stichting van Buro Jansen & Janssen.

Al dertig jaar diepgravend, kritisch en doortastend burgerrechten onderzoek. Buro Jansen & Janssen, gewoon inhoud.

Overheid blijft verdienen aan ID-controles

Er zijn in tien jaar tijd maar liefst 277.726 ID-boetes uitgeschreven. Van alle boetes zijn er uiteindelijk 135.188 betaald hetgeen de overheid rond de 6 miljoen euro heeft opgeleverd.

In het najaar van 2007 publiceerde Buro Jansen & Janssen een informatiekrant over de toepassing van de Wet op de Uitgebreide Identificatieplicht (WUID) die 1 januari 2005 werd ingevoerd. In de publicatie kwamen uiteenlopende verhalen aan bod van burgers waaruit duidelijk werd dat de WUID op grove wijze door de politie wordt ingezet. Sommige dagbladen kopten naar aanleiding van de J&J-krant dat de overheid miljoenen binnensleept aan opgelegde boetes vanwege het niet dragen/tonen van de ID-kaart. Zo zou op basis van de cijfers over 2005 de overheid 1,3 miljoen euro hebben verdiend aan ID-boetes.

Door de discussie over de hoeveelheid geld en de bonnenquota, sneeuwde de uitvoering van de WUID zelf onder. Die uitvoering was en is nu juist in tegenspraak met de oorspronkelijke bedoeling van de wet, de identiteit vaststellen van iemand die een overtreding heeft begaan en niet om extra boetes uit te delen vanwege het niet dragen/tonen van de ID-kaart. We zijn inmiddels tien jaar verder en Jansen & Janssen heeft opnieuw cijfers opgevraagd. Zo kan de balans worden opgemaakt over het gebruik van de legitimatieplicht door de overheid.

Er zijn in tien jaar tijd, van 1 januari 2005 tot en met 31 december 2014 om precies te zijn, maar liefst 277.726 ID-boetes uitgeschreven. Het betrof hier 68.431 dubbele boetes (37 procent, ID + overtreding) en 169.808 enkelvoudige boetes n.a.v. identiteitscontroles (63 procent). Van alle boetes zijn er uiteindelijk 135.188 betaald hetgeen de overheid rond de 6 miljoen euro heeft opgeleverd (uitgaande van overwegend meerderjarige boetes van 50 euro), terwijl er 10.966 ID-boetes werden ingetrokken. Hoeveel mensen er geprocedeerd hebben tegen hun bekeuring is niet duidelijk, ook niet of de rechter in een meerderheid van de gevallen de burger steunde dan wel de overheid.

Dubbele boete

Uit de cijfers blijkt dat er sprake is van twee soorten ID-boetes. Ten eerste de dubbele boete. Je rijdt door rood licht, bent aan het wildplassen, je bevindt je in 'kennelijke staat van dronkenschap op de openbare weg', of je rijdt zonder voor of achterlicht. Dit zijn voorbeelden van 'feitcodes' die onderdeel uitmaken van de top-10 overtredingen in combinatie met een ID-boete. Voor dergelijke overtredingen wordt je op

de bon geslingerd maar je bent niet in staat om jezelf daarbij te identificeren waarna je een tweede boete krijgt opgelegd, kassa voor de overheid.

Een dubbele boete dus maar vaak onterecht, want zowel de wetgever als het College van procureurs-generaal [landelijke leiding van Openbaar Ministerie, red.] hebben aangegeven dat burgers zich op andere wijze mogen legitimeren (andere pasjes bijvoorbeeld) of een identificatiebewijs langs kunnen laten brengen op het politiebureau. Bij de dubbele boetes is onduidelijk of de politiefunctionaris de overtreder ook die mogelijkheid heeft geboden. Het aantal dubbele boetes komt in tien jaar tijd neer op ongeveer 37 procent van het totale aantal ID-boetes.

Als iemand alleen voor openbare dronkenschap wordt geboekt registreert het Centraal Justitieel Incassobureau (CJIB), uitvoeringsorganisatie van het ministerie van Veiligheid en Justitie, niet of die persoon al dan niet zijn identiteitsbewijs heeft laten zien. Er is namelijk sprake van één proces-verbaal, dronkenschap, en niet voor een boete voor het zich niet kunnen legitimeren.

In 2012 werden er bijvoorbeeld 12.049 boetes uitgeschreven voor het met 'aangebroken flessen, blikjes en dergelijke met alcoholhoudende drank bij zich hebben op een weg', waarbij 313 burgers ook nog eens een tweede boete opgelegd kregen voor het niet tonen van een ID-bewijs. In die andere 11.736 gevallen is onduidelijk of naar een ID-bewijs is gevraagd, of die ook is getoond en of iemand zich op een andere manier heeft gelegitimeerd. Een enkelvoudige boete dus voor een overtreding, ID lijkt bijzaak, de burger wordt niet dubbel gestraft.

Rechtsongelijkheid

Of er sprake is van rechtsongelijkheid is op basis van de cijfers van het CJIB niet vast te stellen. Er is ook sprake van enkelvoudige ID-boetes die niet duiden op een strafbaar feit, maar slechts op een identiteitscontrole. Je loopt op straat en je wordt staande gehouden door een agent die naar jouw ID-bewijs vraagt. Als je deze niet kunt of wilt tonen, krijg je een bekeuring.

In 2007 kwam Buro Jansen & Janssen tot de conclusie dat ruim 40.000 WUID-boetes enkelvoudige boetes waren die duiden op een identiteitscontrole. In 2009 meldt J&J op basis van de door de overheid uitgevoerde evaluatie van de WUID: 'Volgens de onderzoekers van Significant klopt dat cijfer (van Jansen & Janssen 40.000) niet en zijn het maar 20.000 boetes. Zij komen tot die conclusie door te wijzen op het

'veld voor 'opmerkingen van de verbalisant'' van het proces-verbaal.' In plaats van ongeveer 40 procent identiteitscontroles zou het gaan om 20 procent, nog steeds een fors aantal.

Bij de vaststelling van die 20 procent beweren de onderzoekers van de overheid dat zij 500 ID processen-verbaal hebben doorgekeken om te constateren wat agenten als opmerking hadden genoteerd bij het uitdelen van een ID-boete. Of dit een wetenschappelijke steekproef was, hoe deze steekproef tot stand is gekomen, wat de bedoeling was van de steekproef; de minister maakte dit niet duidelijk.

J&J heeft vervolgens de totale selectie van processen-verbaal 447e Sr (feitcode D517) van 2005 tot en met 2007 opgevraagd. Het gaat om 138.719 processen-verbaal aan de hand waarvan duidelijk wordt dat opmerkingen niet eenduidig zijn. Een van de eersten is een persoon in een auto die geen geldig legitimatiebewijs in bezit had, maar het proces-verbaal geeft aan dat op het brondocument geen verklaring is vermeld. Iemand anders geeft aan wél een bankpas bij zich te hebben, maar geen ID-bewijs. Weer een ander zegt dat hij liever niet met zijn paspoort op zak wenst rond te lopen; waarom hij is aangehouden is onduidelijk. Diverse processen-verbaal bevatten geen verklaring.

Wie de lijst doorneemt, komt tot de conclusie dat het allemaal nogal willekeurig overkomt, rechtsongelijkheid dus. J&J in 2009: 'Buro Jansen & Janssen was nog voorzichtig in haar conclusies in 2007. Recente registratie van het CJIB die door het bureau is opgevraagd met betrekking tot de enkele bekeuringen laten een stabiel beeld zien van identiteitscontroles in Nederland van rond de 65 procent (64,2 procent in 2005, 61,2 procent in 2006, 65 procent in 2007 en 66,6 procent in 2008). Controles waarbij alleen om een identiteitsbewijs is gevraagd en geen andere overtreding of strafbaar feit is gepleegd.'

Stijging aantal sepots

De constante lijn van inzet van de WUID-maatregel door de politie is ook aan de hand van de cijfers over tien jaar te zien. Het aantal door politie uitgevoerde identiteitscontroles komt neer op 169.808 (63 procent van het totaal van 277.726 uitgeschreven ID-boetes). Het betreft staande aanhoudingen zonder duidelijke wettelijke grondslag. Opvallend is dat het aantal sepots, boetes die naderhand door de overheid worden ingetrokken, de laatste jaren weer toeneemt: in 2014 vonden er 2.844 sepots plaats, terwijl het aantal na 2006 juist aan het dalen was.

Een ander opvallend verschijnsel is dat over het algemeen maar de helft van de ID-boetes wordt betaald. In ongeveer 50 procent van de gevallen

laten mensen hun zaak voorkomen bij een onafhankelijke rechter, worden boetes vernietigd of kan of wil iemand niet betalen. Dit constateerde Buro Jansen & Janssen ook in 2009 nadat in een evaluatierapport van het ministerie van Veiligheid en Justitie werd geconcludeerd dat er geen verzet was tegen de WUID-wet, maar dat wel veel meer burgers dan bij andere wetgeving ervoor naar de rechter stapten.

De evaluatie van het ministerie werd uitgevoerd door een commercieel bureau, Significant, die daarvoor uitsluitend politieagenten had geïnterviewd. De functionarissen waren allen blij met de nieuwe bevoegdheid. Toenmalig minister Hirsch Ballin, tevens hoogleraar Rechten van de Mens aan de UvA sinds 2011, concludeerde op basis van de evaluatie dat er niets aan de hand was met de WUID. De wet werd goed toegepast en het verschijnsel van dubbele boetes en identiteitscontroles bestonden eigenlijk niet, al ondervonden de onderzoekers wel de nodige problemen om de cijfers op een rijtje te houden.

J&J: 'In de evaluatie wordt op verschillende plekken geprobeerd de situatie van de enkele boetes uit te leggen door het aantal dubbele boetes te berekenen. De eerste keer komt het aantal Trias-boetes (wildplassen) en Mulder-boetes (geen licht op je fiets) op 40 procent. Iets verder op pg.13 is dat aantal gestegen naar 61 procent. Op pg.81 is het aantal plotseling 36 procent van alle WUID-boetes en een pagina later weer 40 procent.'

Ook rond die analyse waren cijfers van het CJIB opgevraagd en luidde de conclusie: 'De cijfers die Buro Jansen & Janssen op grond van de WOB bij het CJIB heeft opgevraagd over 2005 tot en met 2008 laten een lichte daling zien van 35,8 procent in 2005 naar 33,4 procent in 2008. Er is volgens het CJIB geen sprake van andere dubbele boetes. De kolom 'geen combinatie gevonden' is erg helder en gedurende de afgelopen vier jaar licht gestegen.'

Stabilisatie ID-boetes

Na tien jaar lijkt het uitschrijven van ID-boetes gestabiliseerd rond de 20.000. Dit aantal werd al bereikt in 2008 en zet zich tot en met 2014 voort. Of de grote hoeveelheid identiteitscontroles (rond de 60 procent van het totaal, 169.808 in tien jaar tijd) ook een constant beeld laten zien van het discriminatoir optreden van de politie is niet duidelijk. Wel is de kans aanwezig dat machtsmisbruik van politiefunctionarissen gepaard gaat met discriminatoir optreden.

'In de evaluatie uit 2009 wordt geconcludeerd dat op basis van de steekproef uit het bedrijfsprocessensystemen (BPS) van de politie dat 'iets minder dan de helft van de zaken betrekking heeft op personen met een niet-Nederlandse achtergrond.' Iets minder dan de helft, heeft volgens de onderzoekers te maken met de 'normale' 'mate waarin deze groepen voorkomen in de registratie van de politie', analyseerde Jansen & Janssen in 2009.

Eigenlijk is er in de laatste jaren niets veranderd, al roepen recente vragen over de kwaliteit van het politiewerk, over etnisch profileren en andere elementen van het discriminatoir optreden van de politie twijfels op over omvang en aard van identiteitscontroles via de Wet op de Uitgebreide Identificatieplicht. In 2009 wees Jansen & Janssen naar hangjongeren, zowel blanke Nederlanders als bijvoorbeeld Marokkaanse Nederlanders die niet in overtreding zijn, maar wel regelmatig om hun identiteitsbewijs worden gevraagd en ook op de bon worden geslingerd.

Volgens de overheid heeft dit allemaal te maken met civielrechtelijk optreden tegen overlast en openbare orde verstoringen. In hoeverre de WUID eigenlijk discriminatoir optreden van diezelfde overheid faciliteert, is en wordt niet onderzocht. Bij alles moet worden aangetekend dat cijfers van de overheid in het algemeen niet heel nauwkeurig zijn, dus moet er rekening worden gehouden met allerlei marges. Tevens worden de cijfers niet automatisch door de overheid openbaar gemaakt en moeten burgers daarom vragen.

Buro Jansen & Janssen, augustus 2015

Wob stukken en overzichten
http://openbaarheid.nl/wob-resultaten/uitgebreide-identificatieplicht-20092014-2015/

Terug naar de inhoudsopgave

identificatieplicht en dubbele boetes en identiteitscontrole						
					dubbele boete	identiteitscontrole
	instroom	ID en Trias	ID en Mulder	ID en Trias en Mulder	totaal Trias/Mulder	geen combinatie
2005	56241					
2006	38396					
2005/2006	94637	24722	14765		39487 (42%)	55150 (58%)
2007	31584	7666	2760	524	10950 (35%)	20634 (65%)
2008	21339	4958	1790	374	7122 (33%)	14217 (67%)
2009	24434	348	1945	5683	7976 (33%)	16458 (67%)
2010	24639				9526 (39%)	15113 (61%)
2011	21694				8861 (41%)	12833 (59%)
2012	18675				7458 (40%)	11217 (60%)
2013	20100				8179 (41%)	11921 (59%)
2014	20624				8359 (41%)	12265 (59%)
	277726				107918 (39%)	169808 (61%)
totaal zonder2005/2006	183089				68431 (37%)	114658 (63%)

	instroom	weg/extra?	verwerkt	naar parket	betaald	ingetrokken	vernietigd	dubbele zaak	overige?	vonnis	overlijden
2005	56241	-509	**56750**	**29576**	**26461**	**703**			**10**		
2006	38396	-1461	**40857**	**21228**	**17573**	**2049**			**7**		
2007	31584	-2734	**34318**	**17629**	**15383**	**1306**					
2008	21339	-710	**22049**	**11449**	**10195**	**404**			**1**		
2009	24434	295	**24139**	**12489**	**11369**	**281**					
2010	24639	175	**24464**	**13198**	**11039**	**227**					
2011	21694	6082	**15612**	**5995**	**9408**	**196**	**1**				**12**
2012	18675	7364	**11311**	**4**	**9802**	**1328**	**53**			**94**	**30**
2013	20100	7165	**12935**	**18**	**10419**	**1628**	**273**			**571**	**26**
2014	20624	2801	**17823**		**13539**	**2844**	**290**	**279**		**836**	**35**
totaal	**277726**		**260258**	**111586**	**135188**	**10966**	**617**		**18**	**1501**	**103**

Jouw data is zelden veilig bij een beheerder

Het parkeren van data in de vorm van een website, e-mails of in de *cloud* is niet van risico's gevrijwaard. Jouw data staat altijd ergens anders op een computer geparkeerd, of die nu in beheer is van een commercieel bedrijf of een kleine activistische provider.

De meeste mensen vertrouwen erop dat bedrijven of personen die hun data op het internet beheren dit netjes doen. Tot een paar jaar geleden was er nog nauwelijks besef over die vertrouwelijkheid en de beveiliging van data. Recente discussies over privacy, maar ook datalekken en hackers, hebben bijgedragen aan een iets groter bewustzijn. Daarnaast zijn de afgelopen tijd in binnen- en buitenland diverse servers en data van activisten in beslag genomen.

Het is logisch dat de discussie over de veiligheid van opslag moeizaam verloopt, data op het internet is ongrijpbaar. De ontwikkelingen gaan snel, men is schijnbaar afhankelijk en de online services van Google, Yahoo, Hotmail en Facebook lijken niets te kosten. Over grote bedrijven wordt echter veel vaker bericht zodra er sprake is van veiligheidslekken, privacyschendingen of andere zaken. Ook voeren individuen actie tegen privacyschendingen door internetgiganten, zoals het vergeetrecht van Google en persoonsdata van Facebook.

De actievoerder online

Inlichtingendiensten beleven hoogtijdagen met '*big data*', zo maakte klokkenluider Edward Snowden de wereld duidelijk aan de hand van gelekte overheidsdocumenten van de Amerikaanse datastofzuiger NSA (National Security Agency). Activisten daarentegen zijn massaal overgestapt op het voeren van online-campagnes en mobilisatie voor protest via Twitter, Facebook en Google. Traditionele actiemethoden, zoals het verspreiden van papieren pamfletten, kranten en brochures, zijn veelal op de achtergrond geraakt.

Met de digitale oplossingen hebben zij vaak hun autonome informatiestructuur losgelaten en uitbesteed aan dominante technologische bedrijven. Het is kostenbesparend en het bereik zou groter zijn, maar het zicht op de data zelf en de gegevensverwerking van gebruikers, ondersteuners en sympathisanten van de campagne is volledig verdwenen. Veel van de commerciële internetbedrijven nemen het namelijk niet zo nauw met zowel de veiligheid als de privacy van haar gebruikers. Daarnaast hebben deze digitale multinationals nauwe contacten met overheden, zoals Snowden met zijn gelekte documenten

heeft aangetoond. Kleinere internetbedrijven verschillen meestal nauwelijks van de grote jongens.

In de artikelen 'Met de billen bloot op Facebook' en 'FB inlichtingendienst' uit *Observant #65* wordt dieper ingegaan op de werking van sociale media en de wijze waarop Facebook met data van haar gebruikers omgaat. Daarin wordt niet alleen gewaarschuwd voor de werkwijze van de multinationals, ook de gebruikers, waaronder activisten, dienen in deze hun verantwoordelijkheid te nemen. Zij delen zoveel informatie op sociale media en nodigen anderen uit dit ook te doen, waardoor er in wezen organogrammen van actiegroepen, campagnes of netwerken kunnen worden samengesteld.

Dat is ideaal voor zowel bedrijven die geld willen verdienen aan advertenties en data op internet, als voor inlichtingen- en veiligheidsdiensten. De internetgiganten bieden om die reden steeds meer gratis toepassingen aan, zodat gebruikers naast sociale media ook hun e-mails, foto’s, chats, documentenopslag kunnen overhevelen naar de computers van deze bedrijven. De vraag of die data daar veilig geparkeerd staat, is meestal van ondergeschikt belang. 'Het zal wel goed geregeld zijn', is de doorsnee gedachte.

Een enkele keer haalt de in beslagname van een server of data de media. Microsoft wil bijvoorbeeld bepaalde data niet overhandigen aan de Amerikaanse FBI omdat deze data in Ierland geparkeerd staat en de Amerikanen daar geen jurisdictie hebben. Zulke berichten zijn echter spaarzaam. De meeste bedrijven willen dit niet aan de grote klok hangen, omdat gebruikers zich dan zullen afvragen of die gratis diensten niet ten koste gaan van allerlei rechten. Of dat je documenten van je opleiding niet in een datacentrum in Nederland, maar elders in de wereld geparkeerd blijken te staan.

Veiligheid essentieel

Voor activisten is veiligheid van data eigenlijk essentieel wanneer je acties, campagnes, etc. voorbereid. Misschien willen donateurs of activisten anoniem blijven, wil je niet dat bekend wordt dat een bepaald e-mailadres aan jou als persoon is gekoppeld, of dat je woonadres te traceren valt. Data is meestal een goudmijn voor de overheid en een in beslag genomen server of dataset kan veel onthullen, niet alleen over een persoon, maar ook over groepen, netwerken, campagnes etc.

De afgelopen tijd zijn er enkele acties van overheden geweest waarbij servers en data van activisten in beslag zijn genomen. In 2011 werd in Nederland een dataset in beslag genomen bij *Animal Rights Media*, een

zelf beheerde server voor dierenrechtenactivisten. In de zomer van 2014 werd de server van de linkse DIY-website *Indymedia Bristol* in beslag genomen door de Engelse politie. Ook vorig jaar werd een server van de Amerikaanse links-radicale groep Mayfirst door de FBI in beslag genomen op last van de Griekse overheid.

In alle gevallen bleef het in eerste instantie onduidelijk wat er precies aan de hand was. De beheerders van de websites en servers traden niet meteen naar buiten met het nieuws. Bij het Engelse en Nederlandse voorbeeld kun je je afvragen waarom er niet direct een verklaring is uitgegaan van de beheerders. De Amerikanen van Mayfirst mochten niets naar buiten brengen, er gold een *Gag Order.* Zij moesten van de politie zwijgen over de zaak, anders zouden ze zelf vervolgd worden.

Het Nederlandse voorbeeld draait om *Animal Rights Media* (ARM). Enige jaren geleden beheerde een groep activisten vanuit Nederland een server in Denemarken waarop verschillende dierenrechtengroepen hun websites lieten draaien met eigen e-mailadressen. Het achterliggende idee was dat je met servers in eigen beheer zelf zicht kon houden op de content en kon reageren op eventueel ingrijpen door de overheid. Het onderhoud van de oorspronkelijke ARM-server was goed geregeld.

De Amerikaanse FBI echter zette de provider waar de server zich bevond onder druk bij een politieoperatie tegen de Amerikaanse actiegroep LAKills.net. Wat er precies met de data is gebeurd, is onduidelijk. Ook Animal Rights Media kreeg een brief, maar deelde die niet met de activistische achterban. De mensen die de server beheerden, hebben geen verklaring doen uitgaan, ook niet toen zij de server verplaatsten naar Nederland.

Er is door de groep nog wel onderzoek gedaan om een nieuwe server in een ander land op te zetten, maar dat bleek niet haalbaar. Enerzijds was dat het gevolg van een financieel verhaal, anderzijds hielden de technische mensen die de server onderhielden ermee op.

'Activepaulus'

Dit betekende echter niet het einde van Animal Rights Media. De Nederlander Paul alias 'activepaulus', een van de personen van de oorspronkelijke groep, ging in z'n eentje verder met een nieuwe server. Hij bood hosting en e-maildiensten aan en verschillende Nederlandse groepen en personen, zoals de organisatie van het jaarlijkse anarchistische actiekamp PinksterLanddagen en activiste Joke Kaviaar, maar ook buitenlandse groepen, maakten gebruik van zijn diensten. Paul presenteerde zich uitdrukkelijk als een activistische hoster met kennis

van zaken. Slechts een enkele gebruiker heeft Paul ooit gevraagd hoe het met de veiligheid van de server zat, of iemand anders benaderd om naar de server te kijken.

De website van Joke werd lange tijd door Paul gehost. Zij is gevraagd naar haar ervaringen met hem: 'Tot 7 december 2011 werd mijn website en daaraan gekoppelde e-mailadres gehost door Paul, ofwel Animal Rights Media. Paul heeft me dit in 2004 aangeboden. Hij presenteerde zich als *reseller*, dat wil zeggen: hij huurde een server bij een groot hostingbedrijf, Flexwebhosting. Ook deed hij het voorkomen alsof hij wist wat hij deed. Voor mij als leek was hij een 'techie'. Het zou veilig zijn, beweerde hij, de overheid ofwel justitie zou er niet bij kunnen.'

Niet alle gebruikers van ARM wisten dat Paul zelf geen server bezat, hij had niet de beschikking over een fysieke machine. De server waar hij gebruik van maakte, draaide in de *cloud.* Het was misschien een virtuele server, maar eerder *cloud* waar hij een aantal websites op kon draaien. Een *cloud* is zeg maar een term die wordt gebruikt indien je een server laat draaien op een harde schijf van een computer van iemand anders. Over de hardware had Paul dus niets te zeggen. Flexwebhosting schrijft op haar website bij *reseller*: 'Zelf uw hostingdiensten verzorgen: Met *reseller* hosting van Flexwebhosting kunt u zelf eenvoudig hostingpakketten voor u zelf of voor uw klanten samenstellen.'

Een ingevoerde in de technische status van de service die Paul aanbood zegt hierover: 'Paul gebruikte een VServer of OpenVZ opstelling als 'prefab' server. Bij een virtuele server wordt een gehele machine (computer) gesimuleerd bij het bedrijf waar je internetruimte huurt. Je moet het zo zien dat een OpenVZ/VServer geen eigen dienst is. De bestanden staan als het ware niet op je eigen machine maar in een map op de *host*. Hierdoor is het dus veel moeilijker om je gevoelige data te beschermen tegen toegang van het hostingbedrijf.'

In antwoord op vragen van Jansen & Janssen zegt Paul dat 'de servers nooit slecht hebben gefunctioneerd. Waar dat verhaal vandaan komt vind ik zeer bijzonder, er zijn altijd geschoolde IT'ers bij betrokken geweest.' Hij presenteert zichzelf als IT-specialist in zijn contacten met mensen en zijn cv op zijn persoonlijke website. In antwoord op vragen geeft hij aan dat hij bij 'een gerenommeerd ICT-bedrijf werkt dat gespecialiseerd is in cloud-servers.' Hij zou daar Senior Network Programmer zijn. In zijn cv staat dat het enige ICT-bedrijf waar hij nu nog werkt 'W. K. Computerhulp' is (de naam van de persoon is geanonimiseerd). Of zijn verhaal over zijn kennis ten aanzien van serveronderhoud klopt, is niet vast te stellen. Toch zijn er grote vraagtekens te zetten bij de veiligheid van de service die hij aanbood.

DDoS-aanvallen

Joke Kaviaar wist dat Paul niet zelf een server beheerde, maar die huurde bij Flexwebhosting. 'Door de jaren heen waren er wel eens problemen. Zo is er menig DDoS-aanval geweest waardoor mijn site offline raakte en hij de boel moest resetten', schrijft zij. Paul verzekerde haar echter dat hij wist wat hij deed en dat haar data, website en e-mail veilig bij hem waren.

Paul kon dat echter nooit met zekerheid beweren. De fysieke server was eigendom van Flexwebhosting waardoor derden in ieder geval eenvoudig bij de server konden komen en, indien nodig, ook naar de virtuele server van Paul konden kijken. In het geval van Joke bleken die derden politie en justitie te zijn. Haar data werd door de overheid in beslag genomen.

Paul zelf beweert dat hij een server draaide met 'CentOS en als webbeheer een *customized* versie van Direct Admin. Deze *customized* versie hebben we zelf aangepast om alle vormen van beveiligingslekken dicht te gooien.' Joke, en waarschijnlijk ook anderen, waren geïmponeerd door deze termen en zullen niet verder hebben doorgevraagd.

Iemand die heel lang met Paul heeft gewerkt schrijft ons: 'Hij heeft zich in onze tijd nooit echt bezig gehouden met de technische zaken aangaande de server. Eigenlijk is het zo dat, als ik erover terugdenk, hij alleen dingen via een webpanel kon instellen.' Specifiek over de DDoS-aanvallen op de server van Animal Rights Media stelt deze bron: 'Van DDOS-aanvallen weet ik niets af via de Deense server. Ik heb het idee dat dat verhaal met een korrel zout moet worden genomen.'

Aanhouding Joke K.

De onveiligheid van de server van Paul hadden grote gevolgen voor Joke. 'Op 13 september 2011 vielen rechercheurs van de Nationale Recherche mijn woning binnen. Er werd vanwege een viertal teksten die ik geschreven en gepubliceerd had huiszoeking gedaan waarbij ik tevens werd aangehouden wegens opruiing '*met terroristisch oogmerk*'. Ze hebben me drie dagen in Zwolle in volledige beperking vastgehouden. Het heeft nog tot voorjaar 2012 geduurd voor ik erachter kwam dat er nog veel meer schade was aangericht door de onveilige server van Paul. Ik kreeg toen het procesdossier van de zaak in handen, door de Nationale Recherche 'Gulkana' genoemd.'

In de drie dagen dat Joke in volledige beperkingen in Zwolle gevangen

werd gehouden, zat de overheid niet stil. 'Justitie had een '*vordering bevriezing van gegevens*' en een '*vordering verstrekking historische gegevens*' ingediend bij Flexwebhosting, de host waar Paul de server huurde. Uit het dossier blijkt dat ze meer dan 4700 e-mails in handen hebben gekregen. Flexwebhosting had met de '*vordering verstrekking historische gegevens*' eveneens het bevel gekregen '*geheimhouding in acht te nemen omtrent al hetgeen u terzake van de vordering bekend is*'. De host had dus zwijgplicht en voldeed aan bevriezing en verstrekking.'

Omdat Paul niet zelf over de fysieke server beschikte, maar harde schijfruimte huurde van een extern bedrijf, had hij niets te zeggen over de data en kon tevens geen enkele veiligheid garanderen. 'Paul heeft niets van de acties van justitie en de medewerking van Flexwebhosting gemerkt. Het is gebeurd zonder dat er bij hem alarmbellen afgingen. Een aantal e-mails met daarin opgenomen de gewraakte 'opruiende' teksten zijn in het procesdossier terechtgekomen en maakte deel uit van de bewijsvoering', stelt Joke.

Paul zelf over de acties van politie en justitie: 'Die ochtend heeft justitie contact opgenomen met Flexwebhosting en deze ertoe aangezet enkel de website van Joke Kaviaar plat te leggen. Flexwebhosting heeft geen enkel contact met ons daarover opgenomen. Tevens was het een verzoek en dus niet een gerechtelijk bevel. We hebben hier contact over opgenomen met Flexwebhosting. Deze was, hoewel zij altijd op de hoogte waren van de inhoud van de websites, ineens van mening veranderd omdat dit criminele activiteiten zouden zijn.'

Op vragen waarom zijn verhaal over zijn contacten met FLexwebhosting en het nauwe contact met Joke over de zaak in tegenspraak zijn met de verhalen van anderen, waaronder dat van Joke zelf, wil Paul niets zeggen. 'Wij hebben daarna de hele server uitgepluisd en geconstateerd dat er geen data van andere websites was meegenomen.' Hoe Paul dit heeft kunnen constateren, kan hij niet duidelijk maken.

Bristol Indymedia

De constructie die Paul gebruikte voor zijn server werd ook toegepast door Bristol Indymedia (BIM), een alternatief mediaproject dat in 2001 online ging. Ook deze club had een virtuele server gehuurd bij een commercieel bedrijf. Op de website konden mensen zelf hun bijdragen posten, zoals bij Indymedia Nederland.

Augustus 2014 ging de website van BIM offline. Een week lang was er sprake van onrust vanwege de onduidelijkheid wat er aan de hand was. Op 27 augustus 2014 bracht BIM een verklaring uit: *'Last week we heard*

from our web hosts that the police had a court order to access the Bristol Indymedia server. […] We consider this server to be compromised, users should assume that from this point on the Police have access to the IP address of anyone accessing this site.'

Wederom bleek naderhand dat de fysieke server niet in bezit was van de beheerders van BIM, maar elders werd afgenomen van een Engelse hostingpartij. Bristol Indymedia stelt: '*We don't know for sure, but assume that our web hosts have complied with the order and given the police this access*.' Hoe het met de IP-loggegevens van de gebruikers van de site was gesteld, bleef onduidelijk. Indymedia UK: '*The false claim is that IP logs were kept for the last 16 months. As the site only launched, with a brand new CMS, on March 21st, 2014, this clearly cannot be true.*'

Iemand reageert op libcom.org: '*It sounds like Bristol Indymedia weren't storing IP addresses, so previous users should be okay, I think. In general it'd be good practice to hide your IP using a proxy or VPN if you really must post online about something illegal (or don't post at all, preferably).*' Het team van BIM heeft echter zelf verwarring gezaaid door in haar verklaring te stellen dat '*users should assume that from this point on the Police have access to the IP address of anyone accessing this site*.'

Naast kritiek op het beleid aangaande het bewaren van historische gegevens, volgde er een discussie over het lekken van IP-adressen door de DIY-website. Indymedia UK meldde dat Bristol Indymedia werd gehost op een 'Bytemark Debian virtual server.' Vanaf maart 2014 draait de website op het gebruiksvriendelijke gratis Wordpress publicatie platform. Een van de gebruikers stelde na de inbeslagname door de politie de vraag of het gebruik van Wordpress wel zo'n veilige optie was. Omdat Indymedia ook reacties van gebruikers toelaat, is de vraag gerechtvaardigd waarom de website niet voldoende beveiligd wordt door bijvoorbeeld een versleutelde verbinding (https).

Hoe lang en wat er van de gebruikers is vastgelegd, blijft onduidelijk, maar Bristol Indymedia had in ieder geval de moed om te verklaren wat er gebeurd was. Mede omdat het bedrijf waar zij hosten hen had ingelicht. Paul van Animal Rights Media meed elke verantwoordelijkheid, of hij nu wel of niet wist wat er plaatsgevonden had.

Nieuwe dreiging

Joke over de dagen voordat haar website offline ging: 'Mijn arrestatie werd pas na mijn vrijlating bekend toen justitie het met een persbericht,

voorzien van citaten uit mijn teksten, de wereld in slingerde. Ik heb Paul ook zelf gebeld en gemaild, de teksten stonden immers op zijn server. Binnen een week na mijn vrijlating begon justitie te dreigen mij opnieuw te zullen arresteren omdat de teksten waarover het ging nog op mijn site stonden. Ik heb geweigerd die te verwijderen en stelde Paul op de hoogte van deze ontwikkeling.'

Of Paul de kennis en vaardigheden bezat om het hoofd te bieden aan de complexe technische en juridische situatie, is onduidelijk. Joke was echter verbaasd over het offline gaan van haar website. 'Op 7 december 2011 belde iemand mij dat justitie mijn site ontoegankelijk had laten maken. Ik was verbaasd, want wist van niks. Ik belde als eerste Paul om te vragen of het klopte en zo ja, hoe dat dan kon. Hij zei dat hij kon zien dat de rechten anders waren gezet door onbekenden en zei dat ie dat kon fiksen. Even later belde hij dat het probleem was opgelost.'

Paul bleek echter niet lang in staat om de website online te houden. Joke belde hem daarover en kreeg de indruk dat hij niet wist wat er aan de hand was. 'Hij reageerde alsof hij er niks van begreep en zei dat hij het niet kon oplossen.' Wat iedereen had kunnen weten, was dat omdat Paul niet over een eigen fysieke server beschikte en slechts prefab serverruimte huurde bij een internetbedrijf en weinig zeggenschap had over het beheer van die server. Daarnaast wist hij eigenlijk niet wat hij deed, bleek de ‘achterkant’ van de server lek en kon Flexwebhosting op last van justitie de website van Joke Kaviaar offline halen.

Paul zelf zegt over het offline gaan van de website: 'Het bleek dat de website wel op de server bleef staan, maar dat de rechten waren veranderd waardoor de *public map* steeds op privé werd omgezet. We hebben dit eerst handmatig aangepast, met als resultaat dat de website enkele minuten weer online was. Echter na enige tijd klapte deze weer uit. We zijn toen op onderzoek uit gegaan waarna bleek dat Flexwebhosting een proces had geïmplementeerd om dit automatisch weer aan te passen.'

Paul zegt dat hij juist wel veel verstand van zaken heeft en tevens veel contact met Flexwebhosting. 'Toen wij dit proces eruit haalden, volgde het eerste telefonische contact met Flexwebhosting (hiervoor hadden we per mail wisselende communicatie). De provider dreigde de complete server er helemaal uit te trekken. Om onze andere klanten niet te duperen, hebben we dit aan Joke uitgelegd en de opties besproken.' Hoe Paul bij dat 'proces' kon komen, maakt hij niet duidelijk. Joke beweert echter dat Paul reageerde alsof hij er niks van begreep en dat hij het niet kon oplossen. Waarom Paul niet aan de bel heeft getrokken is onduidelijk, alsmede waarom hij geen persverklaring heeft verspreid.

Veiligheidsrisico

In tegenstelling tot Bristol Indymedia en ook Mayfirst hebben Paul en Animal Rights Media nooit iets geschreven over wat er gebeurd is met de e-mails en de website van Joke Kaviaar. Dat is kwalijk, want niet alleen die data werd op zijn server gehost, ook die van andere groepen uit binnen- en buitenland, zoals de Pinksterlanddagen. Die liepen eveneens gevaar omdat de server van Paul een veiligheidsrisico was. Joke schrijft hierover dat 'Paul wat lacherig gereageerd heeft, alsof het hem niets kon schelen.'

Omdat de diensten die Paul aanbood onveilig waren, besloten enkele mensen de server onschadelijk te maken. Dit werd overigens niet meteen gedaan. Een jaar lang is geprobeerd Paul meer te laten doen aan de veiligheidsaspecten van zijn diensten. Een van de betrokken mensen: 'De server van Animal Rights media is neergehaald omdat deze een paar keer het middelpunt vormde van een justitieel onderzoek naar activisten. Met het onder ogen krijgen van het strafdossier van Joke Kaviaar bleek (en later in de rechtszaak) dat de VPS/Server lek was en via de achterkant benaderbaar voor inlichtingendiensten en justitie.'

Paul is door diverse mensen benaderd om zijn server beter te beveiligen of om internetdiensten aan andere organisaties over te dragen en in ieder geval mensen te waarschuwen. Eén van de betrokkenen: 'Paul was nooit benaderbaar. Hij gaf aan dit onnodig te vinden. Bij activisten bakte hij zoete broodjes en liet hen geloven dat zijn server goed beveiligd was.' De situatie was onhoudbaar, al helemaal nadat bleek dat justitie mogelijk ook tegen anderen juridische stappen zou ondernemen. 'Wij waren nog in volledige voorbereiding toen het nieuws kwam dat er weer een actiegroep in het vizier lag bij justitie vanwege de server', stelt een van de betrokkenen.

Helaas kon niemand van de gebruikers worden ingelicht. Volgens een betrokkene was daar geen tijd voor. 'De server en Paul stonden waarschijnlijk onder observatie vanwege Joke Kaviaar en 'anonymous' die haar website weer overeind hielp. Het van tevoren waarschuwen van mensen konden we niet doen, omdat we niet wisten of iemand in paniek zou raken waardoor ons de toegang tot de server afgesneden kon worden.' Er was dus geen tijd om mensen en groepen te waarschuwen die eigenlijk al lang op de hoogte waren van het feit dat er iets mis was met de diensten die Paul aanbood. Zij hadden zelf geen stappen gezet om zowel hun eigen data als de data van hun gebruikers veilig te stellen.

In het geval van Paul met zijn Animal Rights Media server was er zoveel

mis dat het voor de overheid en de commerciële partij erg gemakkelijk was om van zijn onwetendheid gebruik te maken. Bij Bristol Indymedia kun je achteraf ook vraagtekens zetten over de in acht genomen veiligheid ten aanzien van haar gebruikers. BIM valt misschien te verwijten dat zij niet helder communiceerden over het loggen van gegevens en het ontbreken van enige versleuteling bij het communiceren op de nieuwssite.

Aan de andere kant plaatste BIM zo snel mogelijk informatie over de in beslag genomen server en werd er gecommuniceerd over mogelijke data van gebruikers die in het bezit waren gekomen van de overheid. Paul daarentegen heeft totaal niet gecommuniceerd met allerlei gevolgen voor zeker één individu, Joke Kaviaar, maar misschien ook voor anderen. Naast de onveiligheid van de server, het niet inschakelen van mensen met kennis om de beveiliging te verbeteren, is hem aan te rekenen dat hij niet heeft gecommuniceerd over wat er plaats gevonden heeft.

Mayfirst

Een andere groep die niet met de buitenwereld communiceerde nadat het offline ging is Mayfirst, maar in tegenstelling tot Paul wisten zij wél waar ze mee bezig waren en was het hen door de Amerikaanse autoriteiten verboden te communiceren over het voorval. Mayfirst bezit haar eigen fysieke infrastructuur. Kort na de in beslagname van de Bristol Indymedia server werd in Amerika ook een server uit een serverkast getild. De zaken hebben echter niets met elkaar te maken. Deze server was van het internetcollectief Mayfirst/People Link. Mayfirst host veel NGO’s in Amerika, maar ook daarbuiten, zoals van groepen in Griekenland.

Aan het einde van de zomer van 2014 was het plots niet meer mogelijk te mailen en mail te ontvangen via de Mayfirst server. De groep staat echter bekend om haar open karakter en publiceert altijd als er problemen zijn met een server. Dit keer gebeurde dat niet en dat was erg vreemd. Mayfirst gaf geen enkele verklaring tot eind vorig jaar toen de 67-jarige activist Alfredo Lopez meldde dat hij drie maanden lang gedwongen was door de Amerikaanse overheid om te zwijgen over de inbeslagname van de server.

Mayfirst werd onderworpen aan een *Gag Order*, een verbod om over een juridische zaak te spreken in de openbaarheid. Pas eind 2014 werd duidelijk wat er aan de hand was nadat de zwijgplicht was opgeheven. Alfredo maakte bekend dat MayFirst het internationale bekende Indymedia Athene host. Op verzoek van de Griekse overheid was de server waarop IMC Athene draaide door de FBI uit een serverkast getild.

Het gevolg was dat niet alleen Indymedia Athene offline werd gehaald, maar ook allerlei andere websites en e-mail accounts.

Hoewel het om IMC Athene ging, waren andere gebruikers ook de klos. Of Mayfirst dit had kunnen voorkomen, is niet geheel duidelijk. Mensen die hun website of e-mail bij Mayfirst draaiden, hadden ook zelf een back-up kunnen maken van zowel hun website als hun e-mail. Dat is uiteraard niet alleen de verantwoordelijkheid van de aanbieder, hoewel die ook helder moet communiceren over wat er aangeboden wordt en of er een back-up is die, als een server in beslag wordt genomen, nog toegankelijk is voor de klanten.

Daarnaast heeft een aanbieder, commercieel of activistisch, ook de verantwoordelijkheid te communiceren over het optreden van de overheid tegen servers of websites. Mayfirst wilde dat wel, maar mocht het niet. De groep maakte na drie maanden duidelijk wat er was gebeurd en gaf daarbij aan dat de server van Mayfirst geen loggegevens bijhield zodat de politie niet wist wie en wanneer een website bezocht werd. E-mails waren wel in beslag genomen.

Conclusie

Bristol Indymedia maakte de inbeslagname van de server na een aantal dagen openbaar en attendeerde de gebruikers op de risico's. Hoewel BIM daar misschien niet heel helder over communiceerde, was het voor gebruikers direct duidelijk dat mogelijk hun loggegevens in bezit waren gekomen van de politie. Paul van Animal Rights Media had alle mogelijkheid om te communiceren, maar deed dat niet. Zelfs niet om aan te geven dat hij niet wist wat er aan de hand was.

Door de strafzaak van Joke K. is inmiddels bekend dat alle 4700 e-mails van haar in handen van justitie terecht zijn gekomen. Of er loggegevens van bezoekers van haar website door de overheid zijn bemachtigd, is niet duidelijk. Naar alle waarschijnlijkheid wel, want Paul gebruikte veel standaard-instellingen. Daarnaast draaiden er veel meer websites op de server van Paul en hadden ook veel meer mensen een e-mail account bij hem afgesloten. Hoewel de server van Paul niet in beslag is genomen, is duidelijk dat een ieder die gebruik maakte van zijn diensten gevaar liep. Dat was minder het geval bij Mayfirst en Bristol Indymedia.

Deze drie voorbeelden maken duidelijk dat het parkeren van data in de vorm van een website, e-mails of in de *cloud* niet van risico's is gevrijwaard. Jouw data staat altijd ergens op een computer geparkeerd van iemand, of die nu in beheer is van een commercieel bedrijf of een kleine activistische provider. Facebook kan ook je profiel plotseling op

slot doen of verwijderen. Dan ben je als actiegroep niet alleen je website, data en tijdlijn maar ook je contacten kwijt. Joke dacht dat zij goed zat bij Paul, maar raakte uiteindelijk haar website en haar e-mails kwijt doordat hij zijn zaken niet goed op orde had en daarover niet communiceerde.

Buro Jansen & Janssen, augustus 2015

Terug naar de inhoudsopgave

Statement on Federal Gag Order Against MF/PL
https://linksunten.indymedia.org/node/130060

'Gagged' by the Government: a Police State Story
http://thiscantbehappening.net/gagged?page=2

Statement on Justice Department Subpoena of Athens
https://mayfirst.org/athens-imc-subpoena

A National Security Gag Order
http://bubbamuntzer.blogspot.nl/2015/02/a-national-security-gag-order.html

Security is Not a Crime—Unless You're an Anarchist
https://www.eff.org/deeplinks/2015/01/security-not-crime-unless-youre-anarchist

Anarchist website Bristol Indymedia to close following police raid
http://www.bristolpost.co.uk/Anarchist-website-Bristol-Indymedia-close/story-22848036-detail/story.html

Police serve Bytemark with production order for Bristol Indymedia information
http://indymedia.org.uk/en/2014/09/517868.html

Police action against Bristol Indymedia
https://www.indymedia.org.uk/en/2014/08/517810.html?c=on#comments

Police investigating the incendiary anarchist minority raid Bristol IMC, who shut down their project (UK)
http://325.nostate.net/?tag=indymedia-bristol

https://libcom.org/blog/sources-police-raid-bristol-indymedia-290820141

Hoe zit het eigenlijk met mijn data?

Het is onmogelijk om 100 procent grip te hebben op je data en/of persoonsgegevens op het internet. Dagelijks gaan jouw persoonlijke gegevens honderden keren door databases van de overheid. Je kan er wel rationeler en doelbewuster mee omgaan. Dit houdt in dat je jezelf een aantal vragen stelt.

1. Waar staat mijn website of heb ik mijn e-mailadres geparkeerd? Ook ik bezoek wel eens Indymedia of een ander links-activistisch forum, wordt mijn bezoek gelogd?

2. Hoe is het met de backups gregeld? Maak ik zelf regelmatig backups?

3. Wie kan er bij mijn data?

4. Vertrouw ik de mensen die de computers beheren waar mijn data (website, e-mail, cloud) op staat? De cloud is een buzzword voor opslagruimte die online benaderbaar is. Jij kunt zelf de ‘cloud’ beheren of het door een bedrijf laten doen. Gegevens worden altijd op fysieke harde schijven van computers opgeslagen.

5. Ken ik die beheerders überhaupt? Zullen zij niet zomaar de data overhandigen aan de overheid?

6. Hoe zit het met de beveiliging van de diensten, wordt dit door anderen gecontroleerd (audit door onafhankelijke derden)?

7. Weet ik waar de data is opgeslagen (geografisch, Nederland of elders)?

8. Wat betekent die geografische locatie voor de veiligheid van mijn data?

9. Worden er loggegevens van de webserver, mailserver of andere servers bewaard? Loggegevens zijn als het ware de sporen die je als gebruikers achter laat. En wie kunnen die logfiles bekijken?

10. Is het noodzakelijk dat ik mijn data bij die beheerder parkeer? Voorbeeld: Kan ik in plaats van mijn kalender elk half uur te synchroniseren met Google dat verplaatsen naar een hoster die ik ken, is het internet wel nodig voor mijn agenda?

Mocht je nu gemotiveerd zijn geraakt om je e-mail, website of andere data te verhuizen naar mensen die zich wel bekommeren om jouw data, dan kan je op de website https://help.riseup.net/en/security/resources/radical-servers een hostingspartij uitzoeken. Sommige internetcollectieven vragen een kleine vergoeding en sommigen bieden een beperkt aanbod van mogelijkheden.

Buro Jansen & Janssen, augustus 2015

Terug naar de inhoudsopgave

Het COA stuurde vrijwilliger weg vanwege diens geëngageerdheid

Jan Kees diende in 2013 zijn werkzaamheden als yogaleraar bij het AZC in Leersum te beëindigen. Het Centraal Orgaan opvang asielzoekers vond zijn politieke opvattingen niet stroken met de vereiste neutraliteit. De Nationale ombudsman boog zich over de kwestie.

Jan Kees maakt, naast portret- en kunstfoto's, ook foto's van acties en demonstraties. Daarnaast heeft hij een ruime ervaring in de zorg en was langdurig werkzaam bij het asielzoekerscentrum (AZC) in Leersum. Door bezuinigingen in de zorg, maar ook op de afdeling voorzieningen voor vluchtelingen, raakte Jan Kees zijn werk op het AZC kwijt. Enkele asielzoekers verzochten hem zijn yogalessen in het centrum voort te zetten. Hij stemde daarmee in en moest een contract ondertekenen als vrijwilliger van het Centraal Orgaan opvang asielzoekers (COA).

Na enkele maanden vrijwilligerswerk verricht te hebben, werd Jan Kees in 2013 door het COA de wacht aangezegd. Hij had jarenlang beroepsmatig als verpleegkundige op het centrum gewerkt. Hij zou zich namelijk nogal kritisch hebben uitgelaten over de politie. Wat was het geval? Jan Kees had foto’s van een vluchtelingendemonstratie op zijn 'gesloten' Facebook-pagina geplaatst, alleen te bekijken door vrienden en bekenden van hem. Het COA echter zou spontaan op zijn pagina zijn gestuit en eiste beëindiging van zijn activiteiten als fotograaf bij politieke manifestaties.

Klachtenprocedure

De bewuste fotoserie over uitgeprocedeerde vluchtelingen die in Amsterdam demonstreerden, plus de op Facebook vermelde kritische teksten van Jan Kees aangaande het Nederlandse asielbeleid, zou in de ogen van de locatiemanager en de vrijwilligerscoördinator van het AZC Leersum niet stroken met de uitgangspunten zoals die worden omschreven in het vrijwilligerscontract. Zowel van medewerkers als vrijwilligers van het COA wordt geëist dat zij zich politiek neutraal opstellen op het internet.

'Daaronder vallen blijkbaar ook foto's van vluchtelingendemonstraties', vertelt Jan Kees. 'Ik kreeg van de locatiemanager de keuze voorgelegd: doorgaan met vrijwilligerswerk en dan stoppen met het doen van politieke uitlatingen en plaatsen van foto’s van demonstraties op het internet, of stoppen met mijn vrijwilligerswerk. Deze keuze heb ik als intimiderend en vrijheid beperkend ervaren.' Jan Kees diende daarop zijn

vrijwilligerswerk te beëindigen.

Aangezien de fotoserie enkel op Facebook toegankelijk was voor vrienden, was Jan Kees zeer verbaasd over het feit dat het COA deze had weten in te zien. 'De locatiemanager vertelde mij dat het COA een extern bureau heeft dat onderzoek doet naar het privéleven van haar medewerkers, vrijwilligers en stagiaires.' Jan Kees beschouwde de eis van het COA om geen foto’s van demonstraties te plaatsen op internet als een vorm van censuur en startte in datzelfde jaar, 2013, een klachtenprocedure binnen het COA.

Zijn klachten bestonden er onder meer uit dat het COA zonder mijn medeweten inbreuk had gemaakt op zijn persoonlijke levenssfeer en dat daarvoor een extern bureau was ingeschakeld. Tevens beklaagde hij zich erover dat hij door het COA in zijn werkzaamheden als fotograaf werd beperkt, terwijl hij slechts één uur per week yogales gaf.

Tijdens een hoorzitting heeft Jan Kees benadrukt dat het fotograferen van demonstraties een journalistieke en dus een politiek neutrale activiteit is. Afdeling Juridische Zaken zou van deze hoorzitting een conceptverslag maken, maar dat is niet gebeurd. Zijn klachten werden ongegrond verklaard nadat het COA plotseling beweerde geen extern bureau te hebben ingeschakeld. In de klachtafwikkeling werd in het geheel niet ingegaan op zijn punt dat journalistieke fotografie een politiek neutrale activiteit is.

Ombudsman

Jan Kees liet het hier niet bij zitten en diende een klacht in bij de Nationale ombudsman. Deze heeft uitgebreid onderzoek gedaan, waarbij het COA met nieuwe argumenten en bevindingen kwam die nog niet eerder naar voren waren gebracht. Het COA bleef stug volhouden dat zij de bewuste foto's op zijn openbare Facebook-profiel hadden gezien en niet op zijn afgeschermde pagina's.

Ook werd duidelijk dat de vrijwilligerscoördinator van het COA, na te hebben vernomen dat Jan Kees tevens kunstenaar is, in 2013 op internet op zoek is gegaan naar werk van hem. Hij stuitte daarbij op naaktfotografie en heeft dit vervolgens gemeld aan de locatiemanager. Deze heeft vervolgens advies ingewonnen bij een beleidsadviseur van de Unit uitvoeringsprocessen van het COA, binnen de organisatie 'bureau veiligheid' genoemd.

De beleidsadviseur en de locatiemanager hebben vervolgens de openbare Facebook-pagina van Jan Kees bekeken en troffen naast

naaktfoto's ook fotomateriaal aan over de ontruiming van een tentenkamp van uitgeprocedeerde asielzoekers plus reacties van Jan Kees met uitgesproken kritiek op het overheidsbeleid. 'Het doelbewust zoeken naar fotografie van mijn hand staat haaks op de bewering dat de coördinator bij toeval mijn foto's was tegengekomen. Daarnaast klopt hun bewering over de naaktfoto's niet aangezien Facebook hieromtrent een zeer streng beleid voert.'

Het COA volhardde erin de vraag van Jan Kees omtrent het politiek-neutrale karakter van journalistieke fotografie onbeantwoord te laten. Na diverse vragen van de Nationale ombudsman hieromtrent aan hun adres, betreffende fotomateriaal van de ontruiming van een tentenkamp waar personen verbleven die geen opvang meer hadden bij het COA, antwoordde het COA dat het bij het publiceren van beeldmateriaal gaat om 'de mogelijke schending van de privacy van een kwetsbare doelgroep.'

Jan Kees: 'Ook dit antwoord sloeg nergens op, aangezien een groep vluchtelingen die demonstreert voor een eerlijke opvang en een humaan asielbeleid zich niet voor niets manifesteert en dus juist de publiciteit zoekt voor hun zaak. Daarnaast heeft het COA niets meer met deze groep te maken, omdat zij niet langer onder de opvang van het COA valt.'

Vervolgens verklaarde de locatiemanager in de loop van het verdere onderzoek dat het CAO aan de hand van de foto's van tentenkampen er niet op kon vertrouwen dat Jan Kees zich in de contacten met bewoners van het AZC politiek neutraal zou opstellen. Hierbij denkt het COA aan het actief aanbieden van hulp aan bewoners van het AZC om bijvoorbeeld een toekomstige uitzetting te voorkomen. Jan Kees: 'Dat punt is in het eerste gesprek en de klachtenafhandeling nooit naar voren gekomen en kwam volledig uit de lucht vallen.'

Vrije meningsuiting

De Nationale ombudsman heeft Jan Kees aangaande zijn fundamentele kritiekpunt – het verbod van het COA om foto's van demonstraties op internet te plaatsen in combinatie van het geven van yogalessen op vrijwillige basis binnen het AZC – gelijk gegeven: 'Door verzoeker voor te houden dat als hij wilde doorgaan met het geven van yogales op het AZC, hij moest stoppen met het publiceren van foto's, heeft het COA verzoekers recht op een vrije meningsuiting niet gerespecteerd. De onderzochte gedraging is niet behoorlijk.'

Terugkijkend blijft Jan Kees zich verbazen en irriteren dat het COA om de

hete brij heen is blijven draaien. 'Hoe toevallig is het dat de vrijwilligerscoördinator onderzoek doet naar mijn kunstzinnige fotografie juist op het moment als ik even daarvoor een demonstratie van uitgeprocedeerde asielzoekers heb gefotografeerd. Vervolgens werden allerlei redenen naar voren gebracht om maar niet in te hoeven gaan op mijn klacht dat het COA mijn journalistieke fotografie wilde censureren. Het COA wist natuurlijk ook zelf wel dat zij zich op glad ijs bevond.'

Jan Kees neemt het het COA bijzonder kwalijk dat de overheidsorganisatie niet transparant opereert, medewerkers en vrijwilligers controleert op wat zij in hun vrije tijd doen en dat dit er uiteindelijk toe heeft geleid dat er geen yogalessen meer worden gegeven binnen het AZC Leersum. 'Wonen in een AZC is gedwongen ledigheid. Er zijn minimale middelen voor ontspanning en activiteiten. Het leven is er zwaar als gevolg van stress en veel mensen in een beperkte ruimte. Yoga biedt ontspanning.'

Buro Jansen & Janssen, augustus 2015

Het volledige onderzoek van de Nationale ombudsman is hier te lezen. https://www.nationaleombudsman.nl/rapporten/2014/%20206#volledige_tekst

Terug naar de inhoudsopgave

Dubieus onderzoek van VU en NSCR naar cybercriminaliteit

Medewerkers van de Vrije Universiteit en het NSCR hebben in samenwerking met het Openbaar Ministerie ruim 2.000 personen geënquêteerd voor een onderzoek naar cybercriminaliteit. De respondenten is niet verteld dat zij benaderd zijn omdat zij als veroordeelden of verdachten te boek staan.

In juni dit jaar zijn allerlei mensen benaderd voor een onderzoek van de Vrije Universiteit (VU) in Amsterdam en het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR). Het betreft personen die door het ministerie van Veiligheid en Justitie ervan worden verdacht zich in het verleden schuldig te hebben gemaakt aan enigerlei vorm van cybercriminaliteit, of daarvoor zijn veroordeeld. Dat wordt echter niet vermeld in de brief die is gedateerd van 15 juni 2015 en ondertekend door prof.dr. Wim Bernasco (VU Amsterdam/NSCR) en Marleen Weulen Kranenbarg, MSc (NSCR).

Het NSCR maakt deel uit van de NWO, de Nederlandse Organisatie voor Wetenschappelijk Onderzoek. Op haar website stelt de NSCR dat zij 'zich toelegt op fundamenteel wetenschappelijk onderzoek naar criminaliteit en rechtshandhaving.' Het instituut werd in 1992 opgezet door het toenmalige Ministerie van Justitie en de Universiteit van Leiden. Op dit moment wordt het NSCR mede gefinancierd door het Ministerie van Veiligheid en Justitie en de Vrije Universiteit.

Het onderwerp van de uitnodigingsbrief betreft 'Onderzoek *NL-ONLINE-OFFLINE*' waaraan respondenten kunnen deelnemen middels een *online survey*. Op de gerelateerde website wordt gesproken van een onderzoek onder dezelfde naam. Het lijkt allemaal volstrekt onschuldig aangezien er gesproken wordt over de 'kennis van computers en het internet en over uw ervaringen met online en offline veiligheid.' Respondenten wordt voorgehouden dat zij een tegoedbon van Bol.com, VVV of Zalando ontvangen ter waarde 50 euro (vet gedrukt!). Daarnaast wordt expliciet vermeld dat de mening van respondenten voor de onderzoekers van groot belang is.

CyberCOP

In werkelijkheid wordt het onderzoek niet *NL-ONLINE-OFFLINE* genoemd maar '*Cyber Crime Offender Profiling (CyberCOP): the human factor examined.*' Oftewel, onderzoek naar het profiel van de cybercrimineel, want de menselijke factor moet natuurlijk een beeld/profiel scheppen van de persoon van de 'crimineel' ten behoeve van de opsporing door

het ministerie van Veiligheid en Justitie en haar diensten. Het onderzoek richt zich dus op verdachten en plegers van cybercriminaliteit en niet zomaar op kennis en ervaringen met computers, internet en veiligheid. Een medewerkster van het Openbaar Ministerie (OM) laat weten dat de uitnodigingsbrief zo is opgesteld dat 'niet op te maken is dat de respondent zelf verdachte is geweest van een delict.'

Uit het besluit van het Agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR), de dienst waarvan onderzoekers de adressen van de respondenten gekregen heeft, blijkt in het geheel niet dat het uitsluitend om verdachten of veroordeelden gaat. 'In het verzoek van 10 juni 2014, 2014-0000658731, heeft het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving verzocht om autorisatie voor de systematische verstrekking van gegevens uit de basisregistratie personen in verband met het uitvoeren van het onderzoek *CyberCrime Offender Profiling (CyberCOP): the human factor examined*.'

Artikel 2 lid 1 van het besluit luidt: 'Aan de onderzoeksinstelling wordt op zijn verzoek een gegeven verstrekt dat is vermeld op de persoonslijst van een ingeschrevene, indien het een gegeven betreft dat is opgenomen in bijlage II bij dit besluit.' Het BPR heeft op 26 februari 2015 toestemming verleend voor het verstrekken van gegevens. Uit bijlage 1 van het besluit blijkt duidelijk dat het om daders gaat. Of het ook gaat om verdachten maakt het besluit niet duidelijk. 'Het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving is recentelijk begonnen aan een meerjarig onderzoeksproject naar de plegers van *cybercrime*.' Bij navraag blijkt dat het onderzoek ook gericht is op daders: “Voor dit onderzoek zijn zowel personen benaderd die ooit verdacht zijn geweest van het plegen van een online delict als personen die ooit verdacht zijn geweest van het plegen van een offline delict.”

Als een van de respondenten de onderzoekers van het NSCR benaderd, wordt gesteld dat ook slachtoffers benaderd zijn. Het BPR maakt echter helemaal geen melding van slachtoffers in het besluit. Er is dus geen toestemming verleend voor het verkrijgen van gegevens over slachtoffers van cybercriminaliteit. Slachtoffers zijn dus niet benaderd. Bijlage 1 stelt dat het bij 'centraal doel/probleemstelling van het onderzoek' gaat om 'het zicht krijgen op (verschillende typen) cybercriminelen, hoog-risico groepen te identificeren en effectievere en beter gerichte interventies en sancties ontwikkelen.' De onderzoekers schrijven in een email bericht met vragen over het onderzoek dat zij “niet alleen geïnteresseerd zijn in offline en online daderschap, maar ook in de vraag of deze mensen wel eens slachtoffer worden. Vandaar de keuze voor deze meer algemene naam en beschrijving.”

Daders en verdachten

Het onderzoek is duidelijk gericht op daders en verdachten van cybercriminaliteit. De medewerkers van het NSCR stellen dat het onderzoek dat uitgevoerd wordt op basis van de gegevensverstrekking uit de BRP zich richt op 'bekende plegers van cybercriminaliteit (op basis van door het Openbaar Ministerie aan ons verschafte verdachten-registraties).'

Er is een selectie gemaakt bestaande uit 1.050 verdachten van *cybercrime*-delicten en 1.050 verdachten van overige delicten, in totaal 2.100 personen. 'Zij worden bevraagd over hun achtergronden, motieven, persoonlijkheid en sociale netwerken.' De steekproef is volgens de medewerkster van het OM uitgevoerd middels een 'abstractie van registers'. Daarvoor zijn twee selectiecriteria gebruikt. Een daarvan houdt in dat de pleger zijn delict in de periode tussen 2000 en 2014 moet hebben gepleegd. Het lijkt dus te gaan om mensen die veroordeeld zijn, maar een medewerkster gaf ook dat het ook om verdachten gaat.

De vragenlijst voor de respondenten is opmerkelijk omdat het vragen oproept waarvoor de verstrekte antwoorden zullen worden gebruikt. De respondenten worden uitgedaagd om hun kunde te tonen en er worden technische vragen gesteld. Een van de respondenten heeft de indruk dat de onderzoekers de respondenten proberen te stimuleren om zich te bewijzen om aan een van de stereotyperingen van cybercriminelen te voldoen.

In het onderzoek wordt om zeer specifieke daderkennis gevraagd, maar daarnaast ook kennis die voor opsporingsdiensten van groot belang kan zijn, zoals bijnamen van kennissen, delicten die recent zijn begaan en de contacten van de respondent. Het wordt duidelijk dat de vragen zijn gericht op wat het onderzoek zegt te te bestuderen: 'de typische persoonlijkheidskenmerken van cybercriminelen, hun sociale (criminele) netwerken, hun primaire motivaties en hun criminele carrière.' De onderzoekers stellen in de bijlage van het BPR besluit dat het onderzoek zich richt op de gelijkenis tussen 'cybercriminelen' en 'criminelen uit de offline wereld', hun persoonlijkheid en of 'ze deel uit maken van criminele organisaties.'

Wetenschappelijk onderzoek is noodzakelijk, maar waarom wordt de respondenten niet verteld dat het in dit geval niet over computers, internet en veiligheid gaat? Het onderzoek lijkt onafhankelijk, maar er is op allerlei fronten samenwerking met het openbaar ministerie en de

respondenten wordt dat niet gemeld. Het is duidelijk dat de onderzoekers bang zijn dat als de geadresseerden dat weten ze niet meedoen. De respondenten worden dus als een soort geblinddoekt proefdier behandeld voor een onderzoek dat niet het echte onderzoek is wat uitgevoerd wordt. Waarom wordt de werkelijke naam van het onderzoek niet aan de geadresseerden gegeven? Waarom wordt de bijlage van het besluit van Agentschap BPR niet aan de geselecteerden toegestuurd? Waarom staat in de aanvraag bij BPR niet de naam van het NL-ONLINE-OFFLINE onderzoek?

In antwoord op vragen over het onderzoek, wordt geen antwoord gegeven op de vraag waarom niet de werkelijke naam van het onderzoek aan de proefpersonen is vermeld. Wel schrijven de onderzoekers: "In de brief vermelden wij expliciet niet dat er in dit onderzoek personen zijn aangeschreven die ooit verdacht zijn geweest van een strafbaar feit. De reden hiervoor betreft het waarborgen van de privacy omdat het altijd mogelijk is dat iemand anders dan de aangeschreven persoon de brief open maakt."

De onderzoekers stellen dat zij: "Bij al onze onderzoeken hanteren wij een uitgebreide en zorgvuldige toetsingsprocedure voordat deze worden uitgevoerd. Hierbij wordt de opzet van het onderzoek en de benaderingswijze van de respondenten getoetst door zowel het College van Procureurs Generaal van het Openbaar Ministerie en tevens voorgelegd aan de commissie Ethiek Rechtswetenschappelijk & Criminologisch Onderzoek van de Rechtenfaculteit van de Vrije Universiteit Amsterdam. Daarnaast wordt er een melding gedaan bij het College Bescherming Persoonsgegevens. In deze procedure wordt de meest zorgvuldige benaderingsmethode bepaald. Dit is ook gebeurd voor het NL-ONLINE-OFFLINE onderzoek."

Middels de Wet Openbaarheid van Bestuur zijn bij het ministerie van Veiligheid en Justitie en het College van Procureurs Generaal stukken opgevraagd over het NL-ONLINE-OFFLINE onderzoek. Beide bestuursorganen stellen dat zij geen stukken met betrekking tot dit onderzoek hebben. In een presentatie over het onderzoek '*Cyber Crime Offender Profiling (CyberCOP): the human factor examined'* worden de volgende partners van VU en NSCR genoemd: "Team High Tech Crime, Nationale Politie Landelijk Parket, Openbaar Ministerie en Reclassering Nederland."

Vermanende woorden

NL-ONLINE-OFFLINE is een profielonderzoek van de overheid over cybercriminelen. Het heet geen *NL-ONLINE-OFFLINE* maar '*Cyber Crime*

Offender Profiling (CyberCOP): the human factor examined.' Hierbij gaat het vooral om mogelijke interventies en sancties. Aan het einde van de enquête wordt het de respondenten nog eens benadrukt hoe belangrijk het wel niet is dat zij de vragen serieus hebben ingevuld. Hiervoor wordt hen een vraag voorgelegd om te controleren of ze wel écht de vragen goed hebben gelezen en beantwoord. Want als dat niet het geval is, lopen zij de beloning van 50 euro mis.

Na deze vermanende woorden wordt de respondent het volgende voorgelegd: 'Voor wetenschappelijk onderzoek is het relevant om de gegevens die u zojuist heeft verstrekt te koppelen aan gegevens die over u bekend zijn in lokale of landelijke registers (zoals het Sociaal Statistisch Bestand en het Justitieel Documentatie Systeem). Dit zal alleen gebeuren als u hiervoor toestemming geeft. Uiteraard zullen ook die gegevens uitsluitend worden gebruikt voor wetenschappelijke doeleinden en volstrekt vertrouwelijk behandeld, anoniem verwerkt en veilig bewaard worden.'

Nu hebben de onderzoekers in Bijlage 1 van het besluit van het Agentschap BPR aangegeven dat 'de gegevens uit de BRP worden gebruikt om een vragenlijst op te sturen naar de persoon.' Er wordt tevens vermeld dat 'op geen enkel moment tijdens het onderzoek een persoon herleidbaar wordt gerapporteerd.' Dit zal mogelijk betrekking hebben op het doorgeven van mogelijke strafbare feiten die de respondenten in de enquête hebben ingevuld.

Er wordt in de bijlage echter niet vermeld dat de verstrekte gegevens van de ondervraagde worden gekoppeld aan de data van justitie: 'koppelen aan gegevens die over u bekend zijn in lokale of landelijke registers.' In principe hoeft dat natuurlijk niet omdat die gegevens niet in het bezit zijn van het Agentschap BPR, maar het roept wel vragen op over de mate van 'eerlijkheid' van de onderzoekers en het openbaar ministerie.

Volgens de onderzoekers wordt “geen van de verzamelde gegevens gedeeld met derden, ook niet met het OM. Er zal nooit zonder expliciete toestemming van de respondent koppeling plaatsvinden met data van het OM. Het OM heeft ons enkel geholpen met het verzenden van de brieven. Het OM en het BPR helpen echter niet alleen bij de mailing aan de proefpersonen, ook bij het koppelen aan ‘gegevens die over u bekend zijn in lokale of landelijke registers (zoals het Sociaal Statistisch Bestand en het Justitieel Documentatie Systeem)’. Dit zou anoniem zijn, maar dat kan niet bij koppeling aan die bestanden, daarnaast krijgt iedere proefpersoon een persoonlijke deelnamecode, die maar een keer is te gebruiken.

Lok-onderzoek?

Het VU/NSCR-onderzoek is gericht op *cyber profiling.* Daarvoor worden personen benaderd die zelf niet weten dat ze benaderd zijn als veroordeelde of verdachte. Zij krijgen een vragenlijst voorgelegd waarmee ze uit de tent worden gelokt om daderkennis te presenteren. Maar dat niet alleen, ook info over mogelijke mededaders en andere gegevens over strafbare feiten waarvoor zij veroordeeld zijn, en/of mogelijke strafbare feiten die zij recentelijk zouden hebben gepleegd en waarvoor zij niet veroordeeld zijn. Dit laatste over de connecties van de respondent is natuurlijk gericht op het in kaart brengen van criminele netwerken.

Verdachten worden ook op deze wijze benaderd, dus het zou net zo goed een lok-onderzoek kunnen zijn. Vraag is of de respondenten op hun rechten ten aanzien van de gegevens die zij mogelijk prijsgeven, zijn gewezen? Waarom spelen de onderzoekers geen open kaart omtrent het werkelijke doel van het onderzoek? Vanwaar die omslachtigheid en vaagheid? Is dit een wetenschappelijk onderzoek waarbij geënquêteerden worden ingelicht over de ware doelstelling, of is hier soms sprake van een *phishing* expeditie van een instituut dat gefinancierd wordt door het Ministerie van Veiligheid en Justitie en direct samenwerkt met het OM?

Respondenten zijn reeds strafrechtelijk vervolgd of niet verdachten meer omdat er geen bewijs werd gevonden voor hun schuld. Toch worden zij verleid om aan te geven met wie, waar, wanneer en waarom zij mogelijke strafbare feiten hebben begaan. Los van het *profiling* en *phishing* gedeelte van het onderzoek, roept de aanpak vragen op over de wetenschappelijke verantwoording ervan. Want welke serieuze data levert het op om de stoere veroordeelde en/of verdachte cyber criminelen uit de tent te lokken om hun kunde te tonen en met wie ze contact hebben. Het enige waar het onderzoek op gericht lijkt te zijn is de bevestiging van bestaande stereotypering over de cyber criminelen. Dat is zowel voor de wetenschap als voor de opsporing weinig vruchtbaar.

Buro Jansen & Janssen, augustus 2015

Terug naar de inhoudsopgave

Brief aan respondenten
http://respubca.home.xs4all.nl/pdf/briefvanvunscraanproefpersonen.pdf

besluit agentschap BPR
http://respubca.home.xs4all.nl/pdf/besluitBPRinzakeonderzoek.pdf
Welkomstekst bij onderzoek NL-Online-Offline
http://respubca.home.xs4all.nl/pdf/Welkomnlonlineoffline.pdf

presentatie over het onderzoek Cyber Crime Offender Profiling (CyberCOP): the human factor examined
http://respubca.home.xs4all.nl/pdf/NWOCyberCrimemetTeamHighTechCrimeetc.pdf

Solidarity with imprisoned activists with or without Facebook

On the 23rd of June 2014, I opened Facebook and found news that two friends had been arrested after participating in protests on the other side of the world. Natalie Lowrey is an Australian environmental activist who was arrested in Malaysia on 22 June during a peaceful action against Australian-owned Lynas Corporation's rare earth plant in Malaysia. Yara Sallam is an Egyptian feminist activist who was arrested in Egypt on 21 June during a peaceful demonstration against the country's anti-protest law. These two women human rights defenders (WHRDs) and friends who I had met at different moments in my activist life were now in jail, and I was alarmed and worried.

I immediately re-posted the two news items with messages that said "Sending strength and cheer to Natalie (Nat) while in detention after a protest in Malaysia" and "Sending strength and cheer to Yara during her detention in Egypt." I found it odd that I was not able to tag Yara like I had tagged Nat, but I didn't give it much thought.

For three weeks, I engaged in a frenzied exchange of testimonies, pictures, news items, and calls to action about my two friends who were in jail. There was a lot of traffic on my newsfeed regarding Natalie's situation and the background of the fight against Lynas, and also about Yara's situation along with other WHRDs arrested during the 21 June demonstration. Another WHRD arrested along with Yara is Sanaa Seif, a young woman I do not know personally but whose stories I am learning about through the campaign demanding their release. My sole contact was through Facebook, and the two intertwined experiences of Nat and Yara raise questions for me about my own use of Facebook, and how as a movement we can be conscious of the benefits and the threats involved.

At first, Nat was posting directly to Facebook – a video from the protest, a short note saying she was fine and expected to be deported back to Australia soon. Later, Nat's friend Tully began posting on her behalf – reporting that she had visited Nat in jail, that Nat was being treated well, that she was in good spirits although concerned by the delay in her case. The other 15 activists arrested at the protest, all Malaysian, had been released within hours but Nat was held overnight, and then longer. Friends of the Earth created an Avaaz petition demanding Nat's release, several calls to action started circulating, and friends used Nat's Facebook wall to give updates and share news regarding her detention.

On 26 June, The Guardian published an article stating the case may not

be straight-forward, and that the police were considering charges that carry a 2 year jail term. Luckily, on 27 June Nat was released on bail and she was able to return to Australia. She immediately continued her activism, giving interviewsabout her experience in jail where she focused on the campaign against Lynas, delivering an eviction notice to Lynas in Sydney, and to organizing solidarity for the Malaysian activists who were now being charged for the 22 June protest. Nat has expressed that the solidarity messages she received on Facebook and through other channels helped to keep her strong throughout the campaign. I'm glad that Facebook served as a platform for us to know what was going on with Nat and for her to know that she was not alone.

Contrast this to Yara, who I was unable to tag in my initial posting about her arrest. Several organizations quickly became active on Facebook to support Yara, Sanaa, and all the WHRDs jailed since 21 June. The hashtag FreeYara was the first item I saw, followed by a statement from the African Women's Development Fund, a press release by Human Rights Watch, and an action alert from Front Line Defenders. I posted a picture of Yara from the Bring Back Our Girls campaign, pointing out Yara's acts of solidarity and that it's time to stand in solidarity with her.

On 27 June, The Feminist Wire re-published an interview with Yara, including this beautiful quote from her: *"Solidarity is not only important in terms of having a collective feeling of support that we are all fighting for the same cause, to end patriarchy, but also because we all know different tools and have different skills."* On 30 June I saw an update pass through my newsfeed that the court had decided to postpone the case until 13 September 2014, effectively keeping Yara in prison until further notice. AWID organized a petition and the Women Human Rights Defenders International Coalition circulated a statement with a photograph of the WHRDs in jail. On 7 July, I was moved to tears by a post by Mona Seif, describing her sister Sanaa's strong spirit. On 15 July, someone circulated through Facebook a blog post from A Paper Bird gathering support for Yara and all human rights defenders in Egypt. On that same day, I was inspired reading a newsitem stating that hundreds of people had come out in Cairo to demonstrate in solidarity with Palestine, in defiance of the anti-protest law. At that point, my Facebook newsfeed was starting to be filled with Palestine and the atrocities that Israel is committing in Gaza.

The possibility that Yara's Facebook profile has been removed continues to nag at me, a low murmur among the distress I feel about her prolonged detention. I checked my inbox in Facebook and the message thread I had with Yara has been interrupted. All of her messages were replaced by this: "This message is no longer available because it was

identified as abusive or marked as spam." Instead of her name, I see "Facebook User." At the bottom it reads, "You cannot reply to this message." All that remains is a monologue from me to her last January, when we connected on Facebook.

I asked some friends (on Facebook, of course) if they had also noticed that Yara's profile was down. This elicited a brief exchange about the dangers of Facebook in relation to privacy and surveillance, and a couple of resources were posted and shared. Digital security is a huge concern for WHRDs whose accounts are surveilled and hacked, whose whereabouts can be mapped through social media creating potential online and physical risks. It's important for all of us to pay attention to these issues, for our own protection and to make sure we don't put others at risk by tagging or posting about people who are vulnerable to threats and attacks – or who simply don't want to be tagged.

The truth is, I don't know what happened to Yara's profile. All I know is that she and I connected on Facebook last January, I saw her posts regularly on my newsfeed, and when I tried to tag her on 23 June, her profile was gone. Did I accidentally delete her from my contacts? If so, I should still be able to search for her on Facebook, right? One explanation for Yara's sudden disappearance from Facebook is that her profile was disabled by Yara or her friends as a digital security strategy since she is under arrest and likely does not have access to the Internet. If that is the case, why would I see a notice saying that her messages were removed because they were marked as abusive? It seems more likely (to me) that some people in power in Egypt made use of the complaint mechanism in Facebook to denounce Yara as abusive and got Facebook to take down her profile.

And this is the issue that concerns me: what are our rights regarding our Facebook accounts, and how did Yara lose her right to have her account? What happened to all the information in her account? Her status updates from reading Chimamanda Adichie's Americanah, her photographs of her vacation, her posts about the situation in Egypt, the messages that she wrote to me? These questions are slightly rhetorical, as this incident mostly serves as a reminder that Facebook owns everything, and we own nothing. Our profiles, accounts, and everything we post of Facebook are the property of a corporation that does with it what it pleases, including deleting us altogether. When we conceptualize Internet rights, how can we articulate the right to our digital identity, including ownership and control of our Facebook profiles? At minimum, Facebook should provide an explanation to what happened to Yara's profile. Was it shut down because someone complained? What were the complaints? I think it should also explain what happened to Yara's archive, where is it? Who

has access to it?

I know it sounds naïve, we know Facebook is a corporate entity and if we don't want to play by their rules then we can always opt out. But in this globalized interconnected world, I feel it's much more complex than that. On one hand, there is the recognized power of social media as a tool to mobilize, share information, and counter mainstream media propaganda. But there is also an aspect that is more to do with personal connections, and the relationship-building required for movement-building. Yara and I lost touch after I left my job at AWID. We reconnected on Facebook a year later, and by then she had also changed jobs. We met through our work, and didn't have each other's personal email addresses. I appreciate that Facebook provides a platform where activists can connect and communicate beyond our organizational affiliations. I think that helps us build a stronger movement. (More on this issue about unaffiliated activists, and how we build relationships and movements that transcend our jobs and organizational representations some other time.)

Through Facebook I've also stayed in touch with Nat, who I met in 2009 when I worked at Friends of the Earth International. A few months ago, Nat posted an interview where she recounts her experience with burnout and her strategies to stay healthy. This was a bridge between my environmental activism and my work in support of WHRDs, where I was promoting the importance of self-care. I have seen these unexpected bridges pop up regularly on my Facebook account, with 900+ contacts ("friends", if you will) that I collected from my 20+ years of activism and NGO employment, studies, and family. There is the scary part of Facebook that this corporation can map your life and relationships – sell it to advertisers and also give it to whomever is surveilling you. But also the amazing side of this same coin: seeing for myself how disperse bits of my life come together, the global trajectory that brought me to where I am in the here-and-now.

So, I'm not ready to give up on Facebook. I need to be mindful about how I use it and ensure that I am not over-relying on it. Immediately, I need to get better at taking conversations off Facebook and onto email, as well as keeping track of my friends' email addresses. (And I'll hold the questions about Gmail for another time as well… let's just say I'll be looking to change email service soon.) But I still count on Facebook to stay updated on what is happening to Yara and the other Egyptian WHRDs who are in jail today, to learn about the struggle against Lynas that landed Nat in a Malaysian jail for some days, and to continue finding connection and common purpose with my sisters and brothers all around the world.

Yara has been in jail for six weeks and counting. We are invited to write letters to her and other human rights defenders jailed in Egypt, like this one published by Amina Doherty on the Feminist Wire. I re-posted a beautiful photo-montage made by Mona Seif to keep Yara in our hearts and minds: *"Since Yara's profile seems to have gone missing, let's populate Facebook with her smile and continue support actions to free Yara and all defenders jailed for protesting against the anti-protest law."* It's one small contribution to make sure that Yara doesn't vanish along with her Facebook profile.

Analia Penchaszadeh 6 August, 2014

Original published on http://www.genderit.org/es/node/4077

Update on the article on 16 June 2015

Update about Yara: In October 2014, Yara and the other 23 people arrested in June 2014 were sentenced to three years in prison, to an additional three years of police surveillance, to a 10,000 EGP fine (1,000 euros), and to repayment for property damages they allegedly caused, in relation to their alleged participation in a protest on June 21, 2014. In December 2014, an appeals court reduced the sentence to 2 years' imprisonment and 2 years' police surveillance. In a few days, they will have been in prison for one year.

Update about Yara's Facebook profile: While Yara's Facebook page has not been re-established, someone created a Wikipedia page about Yara that does appear on Facebook when I searched for Yara's name. Meanwhile, the original message thread that I had with Yara now appears with this statement (in Spanish, translation mine): "This message has been temporarily eliminated until we are able to verify the sender's account." Curiously, when I change my settings to English, I just have a thread that only shows the messages I wrote, no other explanation.

Terug naar de inhoudsopgave

Exposed on Facebook

As is widely warned, your social life can easily be mapped if you are active on Facebook. This article shows how it happens. It is translated from the original in Dutch posted at Bureau Jansen & Jansen. [http://www.burojansen.nl/artikelen_item.php?id=523**]**

You leave metadata traces when you communicate over the internet and telephone. These are mostly individualised tracks, information about yourself and the direct contacts that you maintain with other people. Of course the results can give a picture of your social world but for that, the data must be gathered for a long time.

Individual data is hard data about where, at what time and with whom you spoke. This data can be used by investigative agencies to profile you as a suspect, a witness or an unknown participant in an event. Whether you've been around when other people said stuff, you've called someone, you've sent a whatsapp message or you received an SMS you didn't even respond to , everything gets collected for the investigation.

Metadata Collection

Data is important for prosecution in a criminal case, for the intelligence services less so. They will undoubtedly collect a lot of data but that is the nature of intelligence ('At a meeting with his British counterparts in 2008, Keith Alexander, then head of the National Security Agency (NSA) reportedly asked, "Why can't we collect all the signals, all the time?" *Washington Post* 13-05-14). This data only really has intelligence value when you follow someone's digital steps for a long time. In order to prevent attacks, data is often not that useful. It might indicate patterns, but it does not predict future actions.

On December 20, 2013 NBC News opened with: "NSA program stopped no terror attacks, says White House panel member". The *Guardian* (14-01-14) underlines this claim by stating that according to the Senate Judiciary Committee, the collection of bulk phone data has played a limited role in preventing terrorism.

The *Guardian* based its assertion on a study by the New America Foundation, which concluded that the NSA has not managed to foil any attacks. The attack on the Boston Marathon on April 15, 2013 supports that conclusion. Multiple agencies (including FBI, CIA and NSA) had monitored the suspects, but they were able still to carry out the attacks.

Two cases in the Netherlands show the same thing. The intelligence services failed to prevent the murders of Pim Fortuyn and Theo van Gogh. **(These two assassinations rocked Dutch society: Fortuyn, a controversial right-wing politician was shot by Volkert van der Graaf in May 2002 during the elections; van Gogh was a film-maker killed in November 2004 by Mohammed Bouyeri)**. The AIVD **[Dutch acronym for the General Intelligence and Security Service, ie the Dutch secret service]** was already aware of most members of the Hofstad group, to which Mohammed Bouyeri belonged. It was also known that they met in the home of Bouyeri and his address book was copied for the intelligence services by Amsterdam police. The AIVD has indicated that it hacked web forums and in addition the service most likely made wiretaps and internet taps on the Hofstad group. Yet Theo van Gogh was murdered despite this data collection by the secret service.

Open Book

This indicates that the prevention of attacks is not the most important objective of the intelligence services. They want to keep an eye on 'subversives' and the 'counterculture.' Specific information may be useful to be able to zoom in on a group but that data (metadata) is itself only partially interesting.

Take Margriet and Barbara, the two women described later in this story. Through their social media, we can see that they communicate with each other a lot, for example, most days at 4pm for about two minutes. Margriet lives in the east of Amsterdam, Barbara in the west. There is also one location posted on their social media that is shared by the two women. Laurence (the man who is also described in this story) rarely communicates with either woman, only with Barbara at certain times. The three never have group discussions.

But we have now lost the 'bigger picture' because we are zooming in directly on the individual. We've lost the 'helicopter' perspective, we're not above the person, but actually right next to him/her. For the police this is important for tracing suspects of crime, since you can precisely fix someone's life in retrospect. For the intelligence services, this data is meaningless, you're always too late, as shown by the murder of Van Gogh.

Nowadays everyone leaves a trail of data, as shown by the Snowden revelation. The government has a great passion for collecting information and that is where the 'guilt' lies in this case. This has actually been known for many years, but many seemed not to care. The discussion

about the data that people themselves generate on the internet with their own 'private' communications has faded into the background.

Information about my presence in Tesco is communicated both in a concealed manner through metadata and out in the open through our active broadcasts, like Twitter and Instagram. . If you take your smartphone on an action - for example, overturning storage shelves as a protest against the power of supermarkets - you not only have your metadata collected (without making a phone call you reveal your location), but also through twitter if you use your phone to take pictures and post them online.

That the government collects data then becomes an afterthought. Actually many people share details of their whole lives every second of the day, not only through metadata but also through 'real' data, which is easily visible on Facebook. We took three people (Margriet, Barbara and Laurence) who are politically active in alternative circles in the Netherlands and asked them if we could analyse their Facebook data. We then produced graphic images.

Who's who

Imagine you are vaguely friends with Margriet. You've never met her friends and are invited to her thirtieth birthday party. She organizes a celebration and all her family and friends come over. Even occasional friends or acquaintances are there.

If you take a photograph of the room where the party takes place, you get roughly an outline of Margriet's Facebook page. Her family is looking at each other, people from the NGO where she works do the same, squatters share the latest gossip, participants from her dance group greet one another, and others hang out in little groups. A few loners who don't really know anyone roam around.

In the course of the evening, the dance floor is the centre of the party, you can also see groups forming there. You can see on the Facebook page of Margriet that at the beginning of the evening, friends will seek each other out. This happens not just on her thirtieth birthday, but every day.

Generally, most people appear on Facebook with their full name (first and last). Also NGOs, action groups, bands, squats and alternative nightlife have a complete profile on social media. Thus it becomes obvious pretty quickly what someone has sympathy for, where he or she goes out, which squats the person knows and what actions they

supported.

It is remarkable that all these actions and NGOs are put together on the same page. There are no big companies like Coca Cola, Monsanto and Shell. The three activists clearly demonstrate their political views through their Facebook pages. Of course, Margaret, Barbara and Laurence are known to Bureau Jansen & Jansen, but even with unfamiliar activists it would be easy to draw conclusions as to their political affiliations, friends, family, employment and social network.

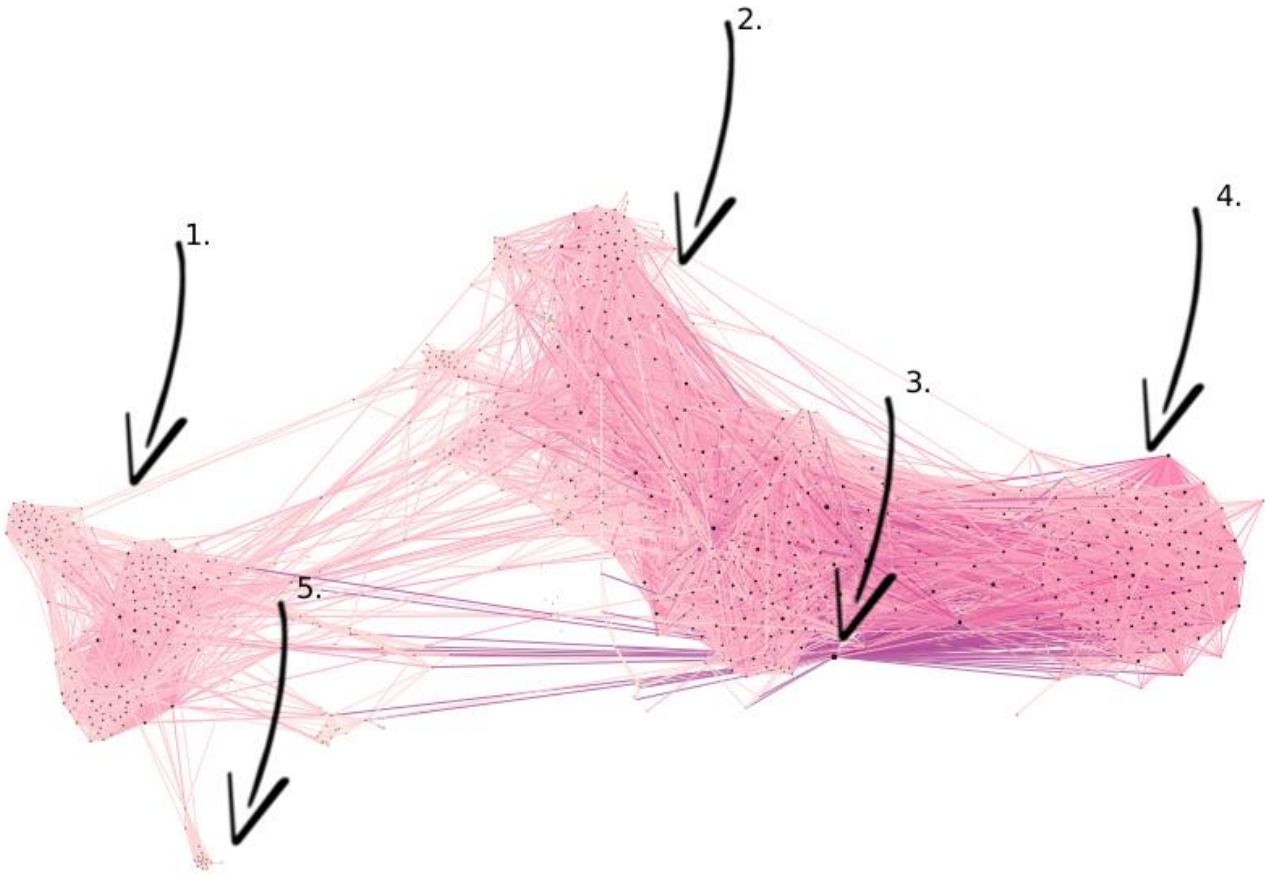
A squatting symbol on Facebook, for example, is something totally different than a squat symbol on a T-shirt you're wearing today. That T-shirt you wear is most probably anonymous, with no name or personal information. Using your Facebook page, the T-shirt is linked to your name, your social network, your environment. It is not anonymous and it even goes beyond your personal identification.

Not perfect

Of course, the picture is not perfect and should take into account a number of incongruities, but the graphical representation of the three people creates a picture of their lives. Upon seeing her graph, it struck Margriet that her "social network is very visible." She also noticed easily that the image is not perfect: "Funny that there are a band and a person caught here who now barely active." The picture is not precise, which leads to some comments on the interpretations.

Many communications, such as "likes" on Facebook do not mean everything. In the images the various individuals and groups are marked with different colours. Dark red is a sign of great activity, but in this analysis we do go deeper into this matter. A lot of activity itself is easy to define in this superficial analysis. It is clear, though, that a more sophisticated analysis about activities could be made. The level of activity should not in itself lead automatically to conclusions about leadership and hierarchy**.**

Also, communication on Facebook is not everything. People who are very active on the Internet, may be actually very shy in reality. People with a big mouth who act tough on the Internet, do not necessarily fulfil an important role within a group and / or social network. And, of course, not everyone is present on Facebook. There are still people who do not have a Facebook page, who are not visible on the network. However, it must be said that even with these caveats, Laurence admitted that his life is portrayed quite accurately.



Facebook graph of Barbara
Arrow 1: Old friends and contacts through third parties with no strong links
Arrow 2: Colleagues and NGOs related to the work of Barbara
Arrow 3: Strong relationship with Barbara, stands out in the network (her boyfriend Evert)
Arrow 4: Colleagues and nightlife related to Evert
Arrow 5: Old friends and contacts through family group with no strong ties
Between 1 and 5: Family swarm
Between 2 and 4: Individuals, squats and alternative entertainment.

Family swarm

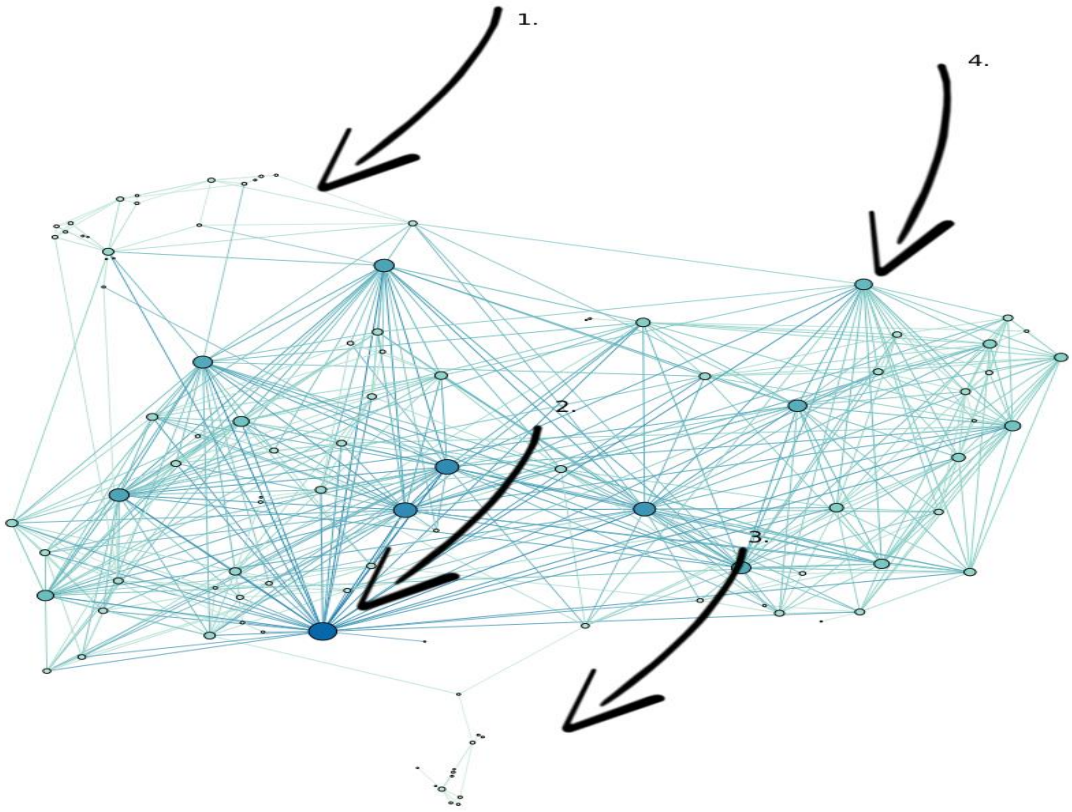
The Facebook graph of Margriet consists of a large swarm (arrow 1 of her picture), a small cloud at the bottom (arrow 3), two clouds together (arrow 4) and a few isolated individuals at the top. The image of Barbara shows on its left side a small cloud with a group below (arrow 1 and 5), and on the right a big swarm in an arc from top to bottom (arrows 2, 3 and 4). Laurence has a large cloud in the centre (arrow 2 and 4) and two groups, one at the top (arrow 1) and one at the bottom (arrow 3).

In all three images, the family groups are obvious. Margriet has a small family (arrow 3) which makes up its "own" cloud. Barbara has a large cloud to the left of the central swarm. That's her family and probably old friends in the country where she comes from. Laurence has a small cloud

below the main cloud, which gathers his family and some old friends.

All three activists have some 'distance' from their family. Whereas for Barbara this has something to do with physical distance, for Laurence and Margaret it could say something about their respective degrees of attachment. With Barbara it is noticeable that away from the central cloud there are two small clouds (arrow 1 and 5) in addition to the 'family' swarm (between arrow 1 and arrow 5). The explanation of this cloud: a group of friends or acquaintances in the country where Barbara comes from. Arrow 1 shows a small network that is connected with some clouds in the central swarm. It is not directly connected (arrow 3) to the large cloud. Probably this is a group from the past with which for various reasons fewer relationships are now maintained.

How can the specific family-swarms be distinguished from others? Actually that's quite simple, since the activists are on Facebook with their surnames. In the 'family' clouds a particular name is common. Of course this is making an assumption about names, but when asked, Margriet indicates that it is "correct about where the family is." Laurence also says that arrow 3 shows a "surprisingly loose network, a network composed of old friends and family. I have little contact with them and the Facebook graph shows that.” In any case, the family swarm is not included in the central cloud of all three of the activists.



Facebook picture of Laurence
Arrow 1: Cloud of friends or colleagues who are involved in NGOs
Arrow 2: Activist swarm around squat in Amsterdam (groups, individuals, squats etc.)
Arrow 3: Family swarm and some old friends
Arrow 4: Activist swarm in The Hague (groups, individuals, squats etc.)

Activist swarm

For all three subjects of analysis, the activist swarm consists of a set of groups, squats, alternative entertainment and people. For Margriet, it is a cloud (arrow 1) of different parts. Top left is a collection of people, bands and groups around some nightlife and squats like OCCII on Amstelveenseweg in Amsterdam West and the Valreep squat in Amsterdam East.

At the bottom left of the central cloud the word 'Anarchist' pops up frequently, for example Anarchist Group Friesland and Anarchist Collective Utrecht. These groups and people hang out around at Doorbraak, a leftist organisation. On the right below are individuals in the swarm working for various NGOs. Given the work of Margriet, it is logical that she connects with this group of people. **Only a few groups are in front, these are special people.**

Finally for Margriet, on the upper right is a group of people and bands that are grouped between the alternative nightlife and squats (top left) and to the right of the activists swarm. Top right is a sort of bridge between the two dancing groups right of the central cloud.

Laurence’s activist swarm (arrows 2 and 4) divides sharply. On the right below, there is a specific group of squatters / activists who have the same hobbies. On the right above, there is a group of people and organisations around the Autonomous Centre Den Haag (arrow 4). Bottom left is people connected to the Valreep squat in Amsterdam East, like with Margriet. It is striking how the Valreep (arrow 2) acts for Laurence as a kind of spider web, making lots of connections with people and groups.

There are the activists and squatters from Amsterdam. The central axis of Laurence's activist swarm is formed between the Valreep in Amsterdam and the Autonomous Centre in The Hague. Top left are a few people present who provide the link between the Amsterdam squat scene and the cloud above the activists swarm. This little cloud has broken loose from the central cloud and is made up by people who are

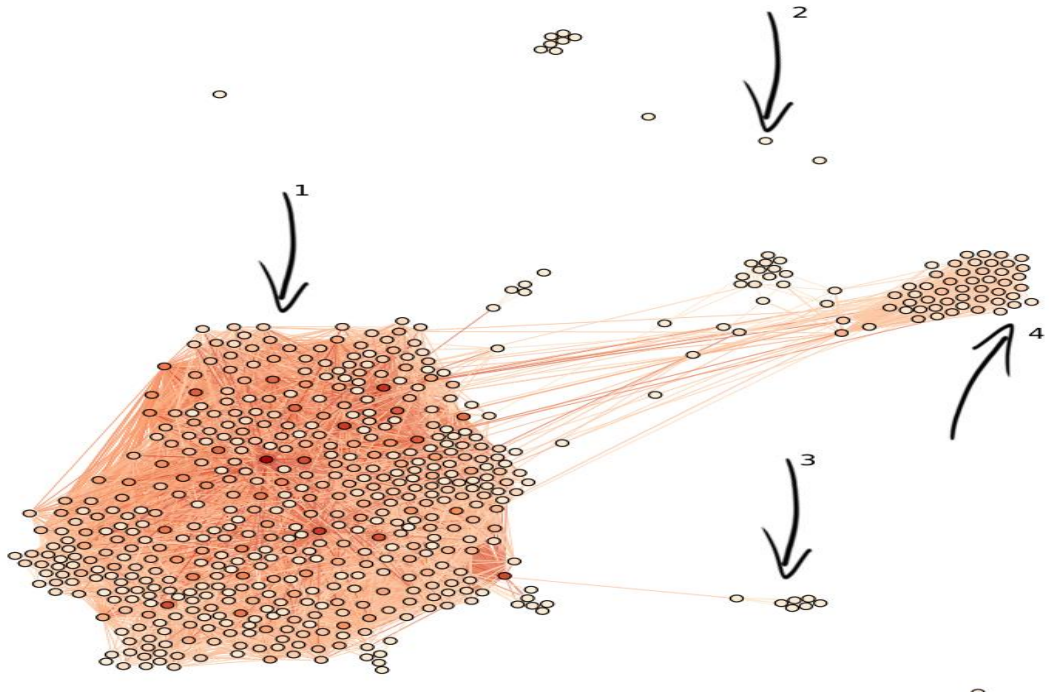
involved in an NGO.

The 'Valreep - Autonomous Centre' axis in Laurence's activist swarm is not directly visible as it is with Margriet’s swarm. Some individuals play a central role in the 'big cloud.' Margriet says "in the large cloud (arrow 1) there are a couple of people who are apparently very active on Facebook as Albert and Astrid." These two people were active in the past (1990s and early 2000s), but no longer play an important role in the activist scene. Not only groups can play a unifying factor but also individuals, as in the swarms around Albert and Astrid. They hold Margriet’s cloud together.

In Barbara's graph something similar is going on. The underside of the large cloud (arrows 2, 3 and 4) is held together by a single person (arrow 3). This is someone who has a lot of connections with Barbara, her boyfriend Evert. Even without knowledge of the relationship between Barbara and Evert, it is possible to see he has a very active position within her network. It is clear that Evert is very close to Barbara. This can be concluded from the fact that Evert has many contacts with the family swarm (between arrows 1 and 5).

On the right-side of Evert is the part of the cloud (arrow 4) occupied by colleagues and groups around the venue where he works. In the middle are mostly the alternative nightlife and squats (around arrow 3). Halfway along the top there is a slight break in the visible cloud. The upper part therefore seems to be separated from the lower half (arrow 2).

The top is occupied by Barbara's colleagues in the workplace, an NGO which has some contacts with the activist scene. From the top there are some individuals who stand aside from the main cloud in two small bursts and also maintain contact with the 'other side', the swarm of family and old friends. These are people who have connections with the country where Barbara comes from, something which can be discerned from the names of the people.



Facebook graph of Margriet
Arrow 1: activists swarm with groups, individuals, squats and alternative entertainment.
Arrow 2: Loose individuals, mostly old classmates from high school
Arrow 3: Family swarm
Arrow 4: Leisure cloud: a large (where the arrow is pointing) and small dance (to the left of the big cloud)

Leisure cloud

For Margriet it is striking that there are two separate clouds to the right of the activist swarm (arrow 4 and next to arrow 4). Central to these two clouds are the names of people in a dance group. The individuals around it are likely to be members or supporters, such as in the activists swarm. Barbara and Laurence do not indicate their hobbies clearly, which may mean that they do business with people who do not use Facebook or who are not visible in a swarm.

Various conclusions could be made with regard to who is and is not visible in the groups. Yet the clusters around work, connections around an NGO, around a squat or a venue, are very clear. A more logical explanation is that the activity is clear if it is embedded in an existing structure, such as the two dance groups where Margriet is a member. For Margriet, this seems to be the case regarding her old classmates: "The group at the very top is former classmates from my high school with a few isolated contacts", says Margriet about her own Facebook graph.

Barbara’s graph shows two clear clouds . One is a swarm of family and friends flanked by two separate clouds of old friends or acquaintances with whom less contact is maintained. This cloud is independent of her life in the Netherlands, but is similar to the dance club clouds of Margriet in that it is a separate world with few connections to the rest. Like with the cloud for Barbara's work (above) and the work of Evert (below), the centre is occupied by entertainment, personal contacts and some activism and squats. Barbara does not have a clearly separate group for sports, culture or nature within her network. Barbara and Margriet are linked in the centre which is occupied by entertainment, personal contacts and some activism and squats. Margriet and Barbara are also part of the network of Laurence.

Social network capture

After seeing his Facebook graph Laurence wonders how he is going to change his behaviour on Facebook. "It gives a clear insight into my social life," he observes. He notes that an analysis of Facebook data makes it clear where the weak links in his life are. "That's pretty scary, strange to find out this way," he adds.

Margriet was also amazed at how sharply her social life can be mapped on Facebook: "If you know what topics swarms or clouds are interested in, you have a wealth of information. And by using a combination of individuals and groups it can be easily found out. However, you do not only know what the central issues are, but it also shows how certain information can be disseminated within those specific networks. You know who is active, who plays a central role, who has a lot of connections, so. And that is not only useful for advertisers."

Facebook arranges your social life, but it does much more than that alone. People give this internet company their personal data. This information may be harmless if you look only at the raw elements, but whoever puts the data in context can make a detailed picture of the guests at Margriet’s thirtieth birthday. This picture reflects her social life, not only on that day. It puts people into groups, shows their political affiliations and provides insight into relationships.

Whoever makes a graphic image of all the groups and individuals from Margriet’s Facebook page can draw a specific social history of her (and of course the same goes for Barbara and Laurence). This would include her youth, school, college, and employment history, as well as her leisure, activism and political preferences. Maybe the information is not perfect, but Facebook has access to so much data that the ability to profile will

only get better in the coming years.

Ultimately, the question is whether you want to have your entire social life visible to all or whether you want to keep control of it. That is a personal choice which is a separate issue to privacy concerns. 'What information do I want to share with a company and thus indirectly with the world?' is the primary question we must all be asking ourselves in this new digital age.

Maikel van Leeuwen

Facebook pictures, pictures of your Facebook page or a social graph

The attached images are a visualisation of the Facebook pages of Margaret, Barbara and Laurence. The links in the network, the lines between the circles are called "edges." A connection can be a "like" or a comment.

A node, a circle in the graphs, is a person and / or organisation within the network. Nodes and edges form a social picture, a Facebook graph. The size of a node is determined by the 'popularity' in the network. How popular a node is can be determined with all sorts of calculations. The popularity is determined by the number of likes, but also by the sending or receiving of messages.

Terug naar de inhoudsopgave

Amsterdam Oost paste ten onrechte preventief fouilleren toe

In Amsterdam Oost vonden te weinig geweldsincidenten plaats om preventief fouilleren op straat toe te mogen passen. Het was de reden dat de gemeente het middel in 2014 niet langer inzette.

In 2009 concludeerde Buro Jansen & Janssen dat de overheid op zijn minst jongleert met cijfers als het gaat om preventief fouilleren in Amsterdam. Eigenlijk kun je stellen dat de onderbouwing van een zwaar ingrijpend middel als preventief fouilleren faalt en op zijn minst leugenachtig is. De Amsterdamse gemeenteraad heeft zelf als criterium gesteld dat er minimaal één incident per hectare moet plaatsvinden voordat de overheid over kan gaan tot preventief fouilleren.

In 2014 wordt het gebrek aan onderbouwing voor preventieve fouillering maar weer eens opnieuw onderstreept. Peter van de Wijngaart, kritisch GroenLinks-lid in Amsterdam Oost, schrijft op zijn blog: 'Dit heldere en goed toetsbare criterium is waar preventief fouilleren in Amsterdam Oost al jarenlang niet aan heeft kunnen voldoen. Er zijn in Amsterdam Oost te weinig incidenten om een zwaar middel als preventief fouilleren toe te mogen passen. Door creatief rekenwerk wist de gemeente kunstmatig het incidentcijfer nog net op 1,01 te houden.'

COT en slecht onderzoek

In 2009 schreef Buro Jansen & Janssen naar aanleiding van de analyse van rapportages over preventief fouilleren van het onderzoeksinstituut voor Veiligheids- en Crisismanagement (COT) een artikel. Bij het COT werkte toentertijd Hoogleraar Veiligheid en Recht Erwin Muller, nu lid van de onderzoeksraad voor veiligheid en ook hoogleraar bestuurskunde aan de Universiteit van Leiden Uri Rosenthal (voormalig minister van Buitenlandse Zaken).

J&J: 'Als je de evaluaties afzonderlijk bekijkt, dan lijken zij solide. Bij het naast elkaar plaatsen van de diverse rapportage ontstaat echter een ander beeld. Men claimt dat de maatregel effectief is, maar de cijfers geven volstrekt geen eenduidig beeld. Het jongleren met cijfers lijkt als doel te hebben het nut van preventief fouilleren te ondersteunen, maar daarmee wordt de onschuldpresumptie aangetast zonder dat er een steekhoudend argument is.'

'De gepresenteerde cijfers', zo vervolgt J&J, 'geven slechts ruimte aan één conclusie, namelijk dat er niets te zeggen valt over de effectiviteit. De cijfers zijn niet eenduidig, er worden feiten en gegevens op een hoop

gegooid waardoor een schroevendraaier een vuurwapen wordt en in de loop der jaren worden niet dezelfde gegevens bijgehouden.'

'Preventief fouilleren is vergelijkbaar met de wet op de uitgebreide identificatieplicht. De overheid wil haar gezag herstellen door aanwezig te zijn op straat en de burger aan te spreken. Bij ons onderzoek naar de uitvoering van de Wet op de uitgebreide identificatieplicht (WUID) hebben wij al aangetoond dat dit leidt tot willekeurige identiteitscontroles. In 2005 en 2006 was er in 40 procent van de WUID-boetes geen sprake van een andere overtreding of strafbaar feit. Deze controles waren gewone identiteitscontroles.'

'Bij preventief fouilleren in Amsterdam leidt het tot een inbreuk op de onschuldpresumptie van de burger zonder dat deze daarvoor iets terugkrijgt. Dit noemt men in Amsterdam dan eufemistisch Respectvol Fouilleren. Criminaliteitsbestrijding is gebaat bij goed onderzoek en transparante evaluaties, niet bij Oostblok-achtige positieve rapportages', zo schreef Buro Jansen & Janssen in 2009 aan het COT.

Handdoek in de ring

In 2014 schrijft Van de Wijngaart op zijn blog: 'Na een jaar lang touwtrekken tussen de gemeente en Peter van de Wijngaart van Wij Verdienen Beter [titel blog - red.] gooide de burgemeester op de handdoek in de ring. Preventief fouilleren in Amsterdam Oost werd met onmiddellijke ingang beëindigd. Preventief fouilleren is een heel zwaar handhavingsmiddel waarvoor we in Nederland strikte criteria hanteren. Aan deze criteria werd eenvoudigweg niet voldaan.'

'Enerzijds', zo vervolgt Van de Wijngaart, 'geeft de wet aan dat er een verstoring dient te zijn van de openbare orde. Anderzijds zijn er de criteria van de gemeenteraad waarvan de kern is dat er minimaal één wapenincident per hectare dient te zijn in een gebied waar preventief wordt gefouilleerd. Dit heldere en goed toetsbare criterium is waar preventief fouilleren in Amsterdam Oost al jarenlang niet aan heeft kunnen voldoen. Er zijn in Amsterdam Oost te weinig incidenten om een zwaar middel als preventief fouilleren toe te mogen passen.'

'Door creatief rekenwerk wist de gemeente kunstmatig het incidentcijfer nog net op 1,01 te houden. Op 8 november 2013 gaf de burgemeester echter toe dat deze manier van berekenen niet correct was en paste hij het gebied in Amsterdam Oost aan. Amsterdam Oost werd door het besluit uiteraard niet crimineler, dus ook op dat besluit was nog het nodige aan te merken.'

'Als niet wordt voldaan aan de criteria van de raad mag de burgemeester bij hoge uitzondering toch een gebied aanwijzen voor preventief fouilleren. Van deze uitzondering maakte de burgemeester gebruik om het Amstelstation aan te wijzen. Uit cijfers van de politie bleek echter dat er op het Amstelstation in het geheel geen wapenincidenten zijn. Bij afwezigheid van incidenten kan uiteraard ook niet gesproken worden van een verstoring van de openbare orde', besluit Van de Wijngaart.

Aangezien de overheid zelf zelden documenten openbaar maakt, heeft Jansen & Janssen dat gedaan op de website openbaarheid.nl. Big Data uit de archieven van de overheid.

Buro Jansen & Janssen, augustus 2015

Originele posting van Peter van de Wijngaart
http://www.wijverdienenbeter.nl/artikelen/einde_fouilleren.html

artikel van Buro Jansen & Janssen
http://www.burojansen.nl/artikelen_item.php?id=413

stukken door van de Wijngaart verkregen
http://openbaarheid.nl/wob-resultaten/preventief-fouilleren-amsterdam-oost-2014/

Terug naar de inhoudsopgave

Veiligheidsarchief, daar hebben we de AIVD niet voor nodig

Twee jaar geleden werd het Veiligheidsarchief opgericht. Doel is het blootleggen van theorie, praktijk, effectiviteit en rechtmatigheid omtrent het functioneren van inlichtingen- en veiligheidsdiensten in Nederland.

Op de officiële internetpagina van de archieven van de Algemene Inlichtingen en Veiligheidsdienst (AIVD) worden op dit moment drie inzageverzoeken weer gegeven. Het gaat om het verzoek over het Interkerkelijk Vredesberaad (IKV) vanaf 1977 tot 1988 rond de 'campagne tegen kernwapens' (sinds maart 2015 online), de FNV in de jaren ’70 en ’80 (sinds juni 2014 online) en Stichting Opstand (sinds mei 2014 online).

Dit is het online-archief van de inlichtingendienst. Telegraaf-journalist Bart Olmer wijdde in maart 2015 een tweet aan de publicatie van het inzageverzoek IKV nadat de AIVD er eerst zelf op Twitter gewag van had gemaakt. Sinds de de publicatie van het IKV-archief is er geen nieuw inzageverzoek online gezet. Het Nationaal Veiligheidsarchief neemt deze taak over door zelf geheime overheidsinformatie openbaar te maken.

Veiligheidsarchief

Het Veiligheidsarchief is een project van Stichting Argus in samenwerking met Buro Jansen & Janssen en bestaat sinds de zomer van 2013. Doel van het archief is het blootleggen van theorie, praktijk, effectiviteit, rechtmatigheid (zowel ten aanzien van nationale als internationale wetgeving en verdragen) van het werk van inlichtingen- en veiligheidsdiensten in Nederland. Dit onderzoek wordt op verschillende manieren uitgevoerd.

Ten eerste door het bevragen van inlichtingendiensten, ministeries en andere overheidsorganen (bestuursorganen) om documenten openbaar te krijgen. Hiertoe worden ook allerlei juridische procedures gevoerd. Ten tweede door het analyseren van de verkregen overheidsdocumenten, het ter beschikking stellen aan het publiek en het leggen van verbanden binnen en tussen verschillende dossiers. Daarbij gaat het niet alleen om casussen uit het verleden, ook het verbinden van verleden, heden en toekomst is een van de uitgangspunten. Ten derde door onderzoek te stimuleren naar het beleid en de praktijk van inlichtingen- en veiligheidsdiensten.

Bij het onderzoek gaat het om verschillende aspecten van het werk van

inlichtingen- en veiligheidsdiensten. Het gaat om transparantie en verantwoording over zowel effectiviteit, als over de rechtmatigheid van gebruikte methoden en interventies. Ook de balans tussen het democratische proces en de interventies van inlichtingen- en veiligheidsdiensten, zoals bij activiteiten van geheime diensten in politieke partijen, is onderwerp van onderzoek. De balans tussen het buitenparlementaire protest en de interventies van inlichtingen- en veiligheidsdiensten in het leven van betrokkenen en organisaties die dit protest vormgeven, krijgt eveneens de nodige aandacht.

Veel van het onderzoek zal gaan over de verhouding tussen de praktijk van de inlichtingen- en veiligheidsdiensten en de waarborgen die grondwettelijke, burgerrechtelijke, mensenrechtelijke wetten, verdragen, afspraken etc. (zowel nationaal als internationaal) voorstaan ten aanzien van de vrijheid van meningsuiting en het recht op vrijheid van meningsvorming, het recht op manifestaties en openbaar protest, het recht om samen te komen, het gebruik van de publieke ruimte, het recht op vrije keuzes in een rechtsstaat die als uitgangspunt heeft dat iedereen onschuldig is tenzij het tegendeel is bewezen, en andere burgerrechtelijke en mensenrechtelijke aspecten (zowel nationaal als internationaal) van het maatschappelijke leven.

Website

U kunt bijdragen aan dit project door ons te steunen, inzageverzoeken in te dienen, documenten te analyseren, onderzoek te promoten en/of zelf onderzoek te doen. Voor vragen, opmerkingen en aanvullingen kunt u contact opnemen met Hans van Drunen en/of Buro Jansen & Janssen. Voor inzageverzoeken en het opvragen van uw politiedossier kunt u ook de website www.openheid.nl raadplegen.

Op dit moment staan er ruim 3.500 pdf's op deze website met rond de 50.000 aparte documenten die een omvang hebben van meer dan tienduizenden pagina's, merendeel documenten die niet eerder openbaar waren. Het archief is qua vorm en toelichting volop in ontwikkeling. U kunt bijdragen door aan te geven hoe zaken beter kunnen worden georganiseerd.

Buro Jansen & Janssen, augustus 2015

Het Nationaal Veiligheidsarchief
http://hetnationaalveiligheidsarchief.nl

Terug naar de inhoudsopgave

Nieuw blog over justitie- en veiligheidsbeleid

Het weblog justitieenveiligheid.nl is een initiatief van Buro Jansen & Janssen. Een blog met reacties op gedane uitingen van politie-, justitie- en inlichtingendiensten over het Nederlandse en Europese beleid en praktijk. Daarnaast wordt er bericht over de wijze waarop de media zich op dit terrein bezighouden.

Verwacht geen diepgravend en onderbouwd onderzoekwerk. Op basis van de reeds voor handen zijnde kennis wordt uit de losse pols gereageerd. Soms wat over de top, soms humoristisch, soms opgefokt, maar altijd met reden om je druk te maken. Mocht u een interessante bijdrage hebben en dit met ons en anderen wilt delen, stuur het dan op, misschien dat wij het plaatsen.

Buro Jansen & Janssen, augustus 2015

Nieuw blog over justitie- en veiligheidsbeleid
http://justitieenveiligheid.nl

Terug naar de inhoudsopgave

Onderzoek naar politieoptreden Haaglanden

Al enkele jaren staat het politieoptreden in sommige buurten van Den Haag ter discussie. De overheid (gemeente, politie, openbaar ministerie en anderen) spreken van incidenten en niet van structureel buitenproportioneel optreden. Terwijl slachtoffers, verschillende organisaties en zelfs ex-agenten wel degelijk spreken van een structureel probleem, blijven burgemeester en politie dit ontkennen en bagatelliseren.

Na de dood van Mitch Henriquez op 27 juni 2015 als gevolg van politieoptreden, zijn veel mensen uit woede de straat op gegaan. Zij eisten verandering. De vraag is of dit ook daadwerkelijk gaat gebeuren, want het is diezelfde overheid die al jaren niet bijster veel heeft gedaan aan de groeiende onvrede. Het is daarom tijd voor een onderzoek naar de wijze waarop de politie optreedt in Den Haag.

Met dit onderzoek willen wij een beeld schetsen van wat er de afgelopen jaren is gebeurd in de Haagse wijken. We verzamelen verhalen van mensen die in aanraking zijn gekomen met de politie en die van mening zijn dat de agenten buitenproportioneel hebben opgetreden. Dit kunnen zowel verhalen zijn van wat jezelf is overkomen, maar ook over wat je gezien hebt.

Onderdeel van dit onderzoek is tevens de wijze waarop de overheid met de protesten sinds de dood van Mitch Henriquez is omgegaan. Mensen die de straat op gingen, werden van van alles beschuldigd. Wij willen van hen horen wat er is gebeurd.

Tot slot doen wij onderzoek naar de wijze waarop de overheid nu ingrijpt in bijvoorbeeld de Schilderswijk. Wordt er daadwerkelijk iets gedaan aan het politieoptreden of is het optreden van de overheid er vooral op gericht om de boel te sussen, het protest te ondermijnen en eventueel verzet uit elkaar te spelen?

Het onderzoek naar het politieoptreden bestaat uit drie delen:

1. Onderzoek naar politieoptreden gedurende de afgelopen vijf jaar in Den Haag waarbij de nadruk ligt op verhalen van mensen die hiervan het slachtoffer zijn geworden. (Denk aan buitensporig geweld, etnisch profileren, onnodige ID-controles etc.)

2. Onderzoek naar het optreden van de politie bij de demonstraties na de dood van Mitch Henriquez. Wat gebeurde er volgens u, de mensen die de straat opgingen om hun stem te laten horen.

3. Onderzoek naar wat de gemeente daadwerkelijk doet in de vooral de Schilderswijk en Transvaal. Wordt er daadwerkelijk iets gedaan aan het politieoptreden, of is het optreden van de overheid er vooral op gericht om de boel te sussen, protest te ondermijnen en eventueel verzet uit elkaar te spelen?

Melding doen van politieoptreden kan hier. (Natuurlijk is het mogelijk om anoniem je verhaal te vertellen of een melding te doen.)

Onderzoek naar politieoptreden Haaglanden
http://onderzoekpolitieoptreden.nl

Terug naar de inhoudsopgave

Voorzichtig: De vijand heeft grote oren

Dit stuk zal gaan over benaderingen door de politie in Utrecht. Aanleiding voor ons om ons hier mee bezig te houden waren enkele benaderingen de laatste tijd van mensen in Utrecht in een nogal korte periode.
We vinden het van belang om het verhaal over de benaderingen naar buiten te brengen. Belangrijk voor zowel de benaderden als voor andere mensen in de axiescene. Belangrijk voor de benaderen omdat ze zo laten zien dat zij zich niet laten intimideren door de wouten. Dat zij, ondanks de schok en angst die vaak samengaan met deze benaderingen, met hun verhaal komen en daarmee een mogelijkheid geven om de werkwijze van de p.i.d. in de openbaarheid te brengen.
Het is ook van belang voor mensen in de scene omdat de benaderingen laten zien dat het geen enkele zin heeft om erop in te gaan met als idee dat je zo informatie over de kit zult krijgen. Ze zullen nooit jets loslaten (bijvoorbeeld wat ze nou precies van je weten, hetgeen waar je zelf zo benieuwd naar bent). En Uberhaupt, voordat een p.i.d.'er je vertrouwt (wat hi' overigens nooit zal doen) zul je toch met echt goede informatie moeten komen, omdat ze alle verkregen informatie natrekken. Het spelletje meespelen met succes kun je daarom beter nooit doen.
Verder is het noodzakelijk als je benaderd bent om dat te vertellen aan mensen die je dat verhaal toevertrouwd. Dit kan het wantrouwen, wat helaas soms het gevolg is van benaderingen, aanzienlijk voorkomen.
Verder kan dan worden nagegaan of er iemand gevaar loopt, want de reden van de benadering is niet alleen de 'belangstelling' voor je eigen aktiviteiten, maar juist ook de 'be-- langstelling' voor de aktiviteiten en ideeen van andere mensen of groepen. Tevens kunnen we aan de hand van de verhalen laten zien wat de achterliggende bedoelingen zijn van het benaderen.
De tot nu toe bekende benaderingen zijn in het algemeen zeer stereotiep. De handelswijze en opstelling van de wout is vaak hetzelfde.

Voorzichtig de vijand heeft grote oren, benaderingen in Utrecht
http://respubca.home.xs4all.nl/pdf/voorzichtigdevijandheeftgroteoren.pdf

utreg(s)ters tegen ongewenste politie intimidaties, 1989

Terug naar de inhoudsopgave

Tips om veiliger te e-mailen

Stel, je maakt gebruik van Gmail. Google, het bedrijf achter Gmail, kijkt met je mee zodra je aan het mailen bent. Gmail is weliswaar gratis, maar Google wil in ruil wel graag jouw data inzien waarmee het onder meer gericht en op persoonlijke maat adverteerders kan binnenhalen. Voor Google betekent gratis dus niet voor niets. Google heeft een betaalde versie van gmail waarbij het bedrijf zegt dat het de e-mails niet scant.

http://www.theguardian.com/technology/2014/apr/15/gmail-scans-all-emails-new-google-terms-clarify
http://digiwonk.wonderhowto.com/how-to/you-cant-stop-gmail-from-scanning-your-emails-but-you-can-limit-their-ad-targeting-0154412/

Je kunt echter ook veiliger mailen waarmee je de kans dat jouw data commercieel geëxploiteerd wordt verkleint. De mogelijkheden daartoe die in het onderstaande geboden worden zijn natuurlijk niet 100 procent waterdicht. Live communiceren zonder gebruik te maken van digitale middelen is natuurlijk altijd veiliger. Wil je veiliger mailen dan heb je verschillende opties.

1. Maak gebruik van e-mail van het bedrijf dat het internet bij je thuis verzorgt, bijvoorbeeld xs4all, Ziggo, KPN, UPC of een ander bedrijf, ook wel aangeduid als provider.

Kijk in het contract met de internetprovider of je ook een eigen e-mailadres hebt en maak er gebruik van. Van Gmail is bekend dat zij de e-mails van haar gebruikers doorzoekt. De meeste providers doen dat niet, althans dat zeggen ze in hun privacyverklaringen. Tot nu toe zijn er ook geen gevallen bekend van bedrijven, los van Google, die actief de inhoud van e-mails doorzoeken. De providers bewaren wél de verkeersgegevens, meestal voor het berekenen van de kosten, verbetering van de diensten en sommige gegevens in verband met de bewaarplicht. Die bewaarplicht is wel van tafel op dit moment.

http://tweakers.net/nieuws/101909/alle-grote-providers-zijn-gestopt-met-de-bewaarplicht.html
http://fd.nl/economie-politiek/1096172/rechter-zet-streep-door-bewaarplicht-van-providers

2. Vertrouw je het bedrijf dat jouw internetaansluiting aanbiedt onvoldoende of niet, of heb je geen eigen aansluiting, dan kan je ook kiezen voor een alternatieve organisatie die e-mail verzorgt en zich meer inzet voor de veiligheid van haar gebruikers. Dit zijn

onder andere riseup, autistici. Bij sommige van deze bedrijven/organisaties moet je betalen.

Stap 1: Bezoek de website van deze organisaties/bedrijven en vraag een e-mailadres aan.
Hier vind je een lijst,
https://help.riseup.net/en/security/resources/radical-servers

https://nadir.org represents politics by undogmatic leftists in the internet, including electronic services such as mail-providing and web-hosting.

Some random descriptions of https://aktivix.org from the aktivix description generator: Aktivix is a donation-funded herd of sweaty techies who desire to enable computer-users to disrupt capitalism in a fluffily non-hierarchical manner. Aktivix is a donation-funded co-operative of fluffy hacktivists who wish to empower collectives to challenge authority in an entirely sustainable manner. Aktivix is a consensus-based network of tired activists who wish to facilitate community-groups to communicate in a open and non-hierarchical manner.

3. Vertrouw je optie 2 ook niet, dan kun je altijd nog je e-mails 'beveiligen'/'versleutelen' in plaats van ze openlijk over het internet te versturen. Beveiligen is het versleutelen op het internet, weer wat veiliger.

Stap 1: Je hebt voor versleuteling twee programma's nodig. Op de eerste plaats het e-mailprogramma Mozilla Thunderbird. Hiermee download je je e-mails op je eigen computer. Je bent zelf verantwoordelijk voor een backup. Download dit programma en installeer het op je computer, laptop, tablet.

https://support.mozilla.org/en-US/kb/installing-thunderbird-windows

Ten tweede maak je gebruik van het versleutelprogramma GPG4Win voor het verpakken van je e-mails. Download dit programma en installeer het op je computer, laptop, tablet. Hier iets meer over GPG en verpakken/versleutelen van mails.

http://gpg4win.org/download.html
http://gpg4win.de/handbuecher/novices_5.html
http://www.reddit.com/r/DarkNetMarkets/comments/1qdzl8/guide_pgp_4_n00bz/

Stap 2: Nu moet je de twee programma’s aan elkaar koppelen, even lastig maar is zo gebeurd.
Stap 3: Maak twee sleutels. Een 'publieke' sleutel voor anderen waarmee ze een e-mail gericht aan jou kunnen verpakken en een 'private' sleutel die je met niemand deelt. Maak eerst de publieke sleutel en dan de private sleutel.

https://www.bestvpn.com/blog/7063/secure-your-email-with-gpg4win-part-1-introduction-and-installation/
https://www.bestvpn.com/blog/7117/secure-your-email-with-gpg4win-part-2-use-gpg4win-with-mozilla-thunderbird/

Terug naar de inhoudsopgave

Buro Jansen & Janssen heeft geld nodig

Sympathie voor het werk van Buro Jansen & Janssen? Wordt dan nu donateur.
Wordt donateur of vraag familie, vrienden en bekenden donateur te worden. Bankrekening NL56 INGB 0000 6039 04 (ING 603904 BIC: INGBNL2A) ten name van Stichting Res Publica, Postbus 11556, 1001 GN Amsterdam. Res Publica is de stichting van Jansen & Janssen.
Buro Jansen & Janssen is aangemerkt als ANBI (Algemeen Nut Beogende Instellingen) instelling. Dit betekent voor mensen die ons willen steunen het volgende:
- Als een instelling door de Belastingdienst is aangewezen als een ANBI, kan een donateur giften van de inkomsten- of vennootschapsbelasting aftrekken (uiteraard binnen de daarvoor geldende regels).
Voor Buro Jansen & Janssen betekent dit:
- Een ANBI hoeft geen successierecht of schenkingsrecht te betalen over erfenissen en schenkingen die de ANBI ontvangt in het kader van het algemeen belang.
- Uitkeringen die een ANBI doet in het algemene belang zijn vrijgesteld voor het recht van schenking.

Terug naar de inhoudsopgave

2;3;6 Afscherming

[redacted]

Lessen in veiligheid

[redacted]

62 IDEOLOGISCHE MISDAAD - CRIMINALITEITSBEELDANALYSE 2007

openbaar!

Amsterdam, 27 april 2014

Aan Ministerie van Veiligheid en Justitie
Minister [redacted]
[redacted] Den Haag

Onderwerp: bezwaar informatieverzoek ideologische misdaad

Geachte [redacted]

We leven in een tijdperk waarin de overheid intensieve aandacht heeft voor alle data en de zelfredzaamheid van burgers. Burgers zijn zowel verdachte van een mogelijke misstap in de wereld van Big Data, als potentiële werknemers van de BV [redacted]

De pijlers van deze welzijnsstaat [redacted] worden getroffen door privatisering, bezuinigingen, schandalen, disfunctioneren en [redacted] van instanties en het ontspoorde toezicht. [redacted]. Wij moeten meewerken om de bezuinigingen op allerlei fundamentele voorzieningen mogelijk te maken. Tegelijkertijd wordt geprobeerd die voorzieningen om te vormen tot winstgevende bedrijven.

Als bewoners van Nederland moeten participeren, zal de staat haar informatie en zeggenschap moeten delen. Openbaarheid, medezeggenschap in beleid en transparantie zijn dan logische zaken. Voor een goede controle op de democratische besluitvorming en overheidshandelen is openbaarheid van essentieel belang. [redacted] rapport met de titel "Criminaliteitsbeeld Analyse Ideologische Misdaad" geschreven door [redacted] Het kapitalisme wordt door de Nederlandse politie niet gezien als ideologie.

Zonder deze openbaarheid is controle door de burger niet uitvoerbaar. De transparantie in het huidige Nederland faalt. Burgers mogen hun buren verzorgen, maar niet toezichthouder van de overheid zijn en kunnen het beleid niet mede vormgeven. Na privatisering van een voorziening staat de burger helemaal met lege handen. Buro [redacted] vecht al dertig jaar voor een meer transparante overheid die rekenschap aflegt niet alleen [redacted] binnen de politieke arena, maar vooral direct aan haar burgers. Dit doet zij vooral op het terrein van he veiligheidsbeleid, maar meer en meer ook op andere beleidsterreinen. Openbaarheid als uitgangspunt voor een interactieve samenleving, pas dan kan echte participatie plaats vinden.

Buro [redacted]
[redacted] Amsterdam
www.burojansen.nl
www.openbaarheid.nl
www.hetnationaalveiligheidsarchief.nl