Social Media Surveillance In Nederland

Buro Jansen & Janssen

Observant #70, oktober 2017

Inhoudsopgave Observant #70 / oktober 2017

Social Media Surveillance in Nederland

1. Social media surveillance in Nederland

2. Dagelijks een structurele monitor;
Social media surveillance door de Nederlandse politie

3. Reputatie management bedrijven, de nieuwe private inlichtingendiensten

4. De burger als dreigingsscore;
Social media surveillance in de Verenigde Staten

5. Overgeleverd aan de grillen van social media multinationals;
Facebook en Twitter en de Nederlandse social media surveillance

6. Maak het werk van Buro Jansen & Janssen mogelijk, word donateur

Gehele Observant #70 social media surveillance in Nederland (pdf)

De Nederlandse politie houdt zich in toenemende mate bezig met social media surveillance. Uit documenten die door Buro Jansen & Janssen via een beroep op de Wet Openbaarheid Bestuur zijn verkregen blijkt dat de Nederlandse politie hiertoe samenwerkt met de social media monitoring bedrijven Coosto, OBI4wan en HowAboutYou. Ook de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) maakt gebruik van de diensten van in ieder geval Coosto. Buro Jansen & Janssen heeft de reputatiemanagement bedrijven Coosto en OBI4wan zelf ook gevraagd naar hun samenwerking met de politie en de NCTV en hun betrokkenheid bij social media surveillance. Tot slot zijn ook verschillende social media platformen benaderd door Buro Jansen & Janssen over surveillance met als gevolg dat Facebook Coosto heeft benaderd over het gebruik van Facebook data voor social media surveillance.

Een maatschappelijk debat in Nederland ontbreekt vooralsnog. Dit is verontrustend, aangezien social media surveillance op gespannen voet met staat met grondrechten zoals de vrijheid van meningsuiting, het recht tot manifestatie, de vrijheid van vergadering en de bescherming van persoonsgegevens in het geding is.

Social media surveillance in Nederland is een inleidend artikel en kan tevens gelezen worden als een samenvatting van de overige vier, uitgebreidere, artikelen.

Dagelijks een structurele monitor; Social media surveillance door de Nederlandse politie beschrijft de ontwikkeling van social media surveillance in Nederland. Buro Jansen & Janssen heeft door middel van een aantal Wob verzoeken inzicht proberen te verkrijgen in social media surveillance door de Nederlandse politie. De Nederlandse overheid is niet transparant en heeft slechts een beperkt aantal documenten openbaar gemaakt, maar uit de documenten blijkt dat de Nederlandse politie zich de afgelopen jaren in toenemende mate bezig houdt met social media surveillance.

Reputatie management bedrijven, de nieuwe private inlichtingendiensten gaat in op de rol van de bedrijven Coosto, OBI4wan, HowAboutYou en Buzzcapture. Social media monitoring bedrijven vormen een geaccepteerde bedrijfstak, maar zijn eigenlijk vergelijkbaar met de meer obscure private inlichtingendiensten uit het verleden. Bovengenoemde bedrijven geven in antwoord op vragen van Buro Jansen & Janssen geen duidelijkheid over hun samenwerking met de Nederlandse politie en hun standpunt ten aanzien van social media surveillance.

De burger als dreigingsscore; Social media surveillance in de Verenigde Staten beschrijft het maatschappelijk debat in de Verenigde Staten over social media surveillance. Dit debat kwam op gang na onderzoek van de Amerikaanse burgerrechtenbeweging ACLU (American Civil Liberties Union), die in 2016 via een beroep op de Freedom of Information Act informatie (Amerikaanse Wob) informatie over social media surveillance boven tafel kreeg, vooral over de rol van bedrijven als Geofeedia en Intrado. Het Amerikaanse debat is tevens relevant voor Nederland.

Overgeleverd aan de grillen van social media multinationals; Facebook en Twitter en de Nederlandse social media surveillance gaat over de rol van social media platformen zoals Facebook en Twitter. Deze hebben geen actief en transparant beleid om het gebruik van social media data voor surveillance doeleinden tegen te gaan. Dit wordt tevens duidelijk uit hun beantwoording hierover van vragen van Buro Jansen & Janssen.

Maak het werk van Buro Jansen & Janssen mogelijk, word donateur. Wilt u dat Buro Jansen & Janssen de komende jaren onderzoek blijft doen naar politie, justitie en inlichtingendiensten, overheidsoptreden in het algemeen, bedrijven die meewerken aan repressief overheidsbeleid en/of zelf ook repressief of diep ingrijpen in het leven van burgers in Nederland en Europa steun ons dan.
Word donateur of vraag familie, vrienden en bekenden donateur te worden. Bankrekening NL56 INGB 0000 6039 04 ten name van Stichting Res Publica, Postbus 11556, 1001 GN Amsterdam.

Een ode aan Jeremy Hammond die een gevangenisstraf uitzet voor het openbaar maken van documenten over Stratfor

Naar inhoudsopgave Observant #70

Social Media Surveillance in Nederland

De Nederlandse politie doet aan social media surveillance en werkt hierbij in ieder geval samen met de social media monitoring bedrijven Coosto, OBI4wan en HowAboutYou. Dit blijkt uit documenten die door Buro Jansen & Janssen via een beroep op de Wet Openbaarheid Bestuur Wob) zijn verkregen. Ook de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) huurt de diensten van Coosto in voor surveillance-doeleinden.

Grootschalige surveillance op internet door inlichtingendiensten kreeg bekendheid door de onthullingen van Edward Snowden in 2013 over het '*sleepnet'* van de Amerikaanse inlichtingendienst National Security Agency (NSA). De NSA verzamelt zoveel mogelijk informatie van social media. Het opsporen van mogelijke terroristen vormt de legitimatie voor deze praktijken. De effectiviteit van het 'sleepnet' is nooit bewezen. Social media surveillance vindt echter niet alleen plaats door inlichtingendiensten, maar ook door de politie.

Social media surveillance door de politie is in Nederland echter nauwelijks onderwerp van debat, in tegenstelling tot in de Verenigde Staten. De burgerrechtenbeweging ACLU (American Civil Liberties Union) onthulde in 2016 de samenwerking tussen de Amerikaanse politie en de bedrijven Intrado en Geofeedia. Geofeedia verzamelt en indexeert data van social media platformen, die vervolgens worden gebruikt voor surveillance en opsporingsdoeleinden. Intrado verkoopt de politie een zogenaamde Facebook Threat score. In de Verenigde Staten hebben Facebook en Twitter Geofeedia, en enkele vergelijkbare bedrijven zoals Media Sonar en Snaptrends de toegang tot hun platformen ontzegd.

Dagelijks een structurele monitor

Het verzamelen van inlichtingen door de overheid over burgers is van alle tijden, ook in Nederland. Deze surveillance was traditioneel

het terrein van de inlichtingendiensten. Nieuw is dat ook de Nederlandse politie zich de afgelopen jaren op het terrein van online en social media surveillance begeeft. Buro Jansen & Janssen heeft door middel van een aantal Wob-verzoeken inzicht proberen te verkrijgen in social media surveillance in Nederland. De Nederlandse overheid is niet transparant en heeft slechts een beperkt aantal documenten openbaar gemaakt. Hieruit wordt echter duidelijk dat de Nederlandse politie zich de afgelopen jaren in toenemende mate bezig houdt met social media surveillance.

Belangrijk bij de ontwikkeling van social media surveillance is het ontstaan van Real Time Intelligence Centers (RTICs). Een RTIC is een uitgebreide meldkamer waarin data uit politieregisters, andere gegevens (zoals bijvoorbeeld van de Kamer van Koophandel) en persoonsgegevens van social media platformen zoals Facebook en Twitter samenkomen. Social media data zijn een belangrijke bron van OSINT (Open Source INTelligence), van oudsher een typisch 'product' van inlichtingendiensten. De politie wil OSINT nu echter inzetten binnen de gehele organisatie.

Politiekorpsen experimenteren al een aantal jaren met social media monitoring, niet alleen ten behoeve van communicatie en webcare, maar ook voor surveillance en opsporingsdoeleinden. Sinds ongeveer 2013 ontwikkelt de politie een meer gecentraliseerde aanpak. In het startdocument *Project Initiatie Document (PID), Politie in operationele politieprocessen van 2013* spreekt de Nederlandse politie de ambitie uit om social media surveillance een vast onderdeel van het dagelijkse politiewerk te laten worden. "Door de informatieorganisatie in de eenheden wordt er dagelijks online een structurele monitor gedraaid", aldus het document. Twee jaar later in 2015, wordt het belang van OSINT veelvuldig benadrukt in het adviesrapport *IM Adviesrapport Tools Informatieorganisatie Evaluatie en advies*. De politie wil OSINT inzetten voor het "versterken van de (realtime- en righttime) informatiepositie van de politie, verbeteren van de interpretatie (duiding) van informatie, kansen bieden voor verhoging van de heterdaadkracht." De politie voert ondertussen dag en nacht online en social media surveillance uit, zo blijkt uit het rapport.

Social media surveillance is een publiek private samenwerking. De politie probeert weliswaar haar eigen tool iColumbo/IRN, dat werd

ontwikkeld voor de opsporing, om te bouwen voor social media surveillance, maar huurt nu al jaren commerciële tools in bij private bedrijven. Uit via de Wob openbaar gemaakte documenten blijkt dat de politie sinds tenminste 2012 gebruik maakt van de diensten en tools van Coosto, en sinds 2013 samenwerkt met OBI4wan en HowAboutYou. Ook de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) maakt sinds 2011 gebruik van de tools van Coosto.

Zo schrijft de politie in het openbaar gemaakte rapport *Online media monitoring: tool en proces (2) ervaringen en inzichten naar aanleiding van operationele ervaring bij de politie-eenheid Zeeland - West-Brabant*: "De gegenereerde resultaten van OBI4wan zijn niet zo volledig als bij de andere gebruikte online media monitor op het RTIC (Coosto). Vooral bij de bronnen Facebook, YouTube en Instagram zijn de resultaten bij het gebruik van dezelfde zoekopdrachten van Coosto vollediger."

De technologie van Coosto en OBI4Wan wordt niet alleen ingezet voor communicatiedoeleinden, maar ook bij het verwerken van meldingen en aangiften en in Real Time Intelligence Centers, bij de opsporing en in het algemeen voor social media surveillance. Voor zover bekend gebruikt de Nationale Politie de tools van Buzzcapture alleen voor communicatiedoeleinden.

De social media monitoring industrie

Coosto, OBI4wan, HowAboutYou en Buzzcapture zijn reputatiemanagement bedrijven. Zij bieden monitoring tools aan op het terrein van reputatiemanagement of webcare. (HowAboutYou heeft overigens geen eigen technologie en gebruikt exclusief de tools van OBI4wan). Deze worden afgenomen door bedrijven en overheidsorganen die negatieve publiciteit willen tegengaan. Essentieel onderdeel van het reputatiemanagement is de sentiment-analyse. Bedrijven verzamelen data die worden voorzien van een label goed/positief, slecht/negatief en neutraal. De labels dienen om de publiciteit over een product of dienst te volgen. Daarbij gaat het natuurlijk vooral om negatieve berichtgeving, waar een producent snel op wil reageren.

Reputatiemanagement is dus risicomanagement. Om risico's te vermijden worden zoveel mogelijk gegevens van online en social media verzameld. Coosto, OBI4wan en Buzzcapture verzamelen data met zoekmachines die het internet afspeuren. De gegevens komen in principe van open bronnen: informatie die door bedrijven en individuen op het internet wordt gedeeld. Zij bewaren die data in archieven in Nederland. Enkele van deze bedrijven hebben een archief van internetdata dat terug gaat tot 2007 of 2009. In deze databanken bewaren bedrijven alle door hen verzamelde informatie, ook informatie die mensen inmiddels van hun social media account hebben verwijderd. De reputatiemanagement bedrijven hebben van deze online en social media data handelswaar gemaakt.
Coosto, OBI4wan, HowAboutYou en Buzzcapture borduren eigenlijk voort op de traditie van private inlichtingendiensten. Deze schimmige bedrijven werden sinds het eind van de vorige eeuw met name ingehuurd door multinationals om actiegroepen die campagnes tegen die bedrijven voerden in de gaten te houden. Een bekend voorbeeld is ABC (Algemene Beveiligings Consultancy) van Peter Siebelt, dat in de jaren 90 in het nieuws kwam door het inzamelen van oud papier en het inzetten van informanten, om de verzamelde informatie vervolgens door te verkopen aan media en multinationals. Het verschil met de private inlichtingendiensten is echter dat social media monitoring een geaccepteerde bedrijfstak vormt. De klantenkring is breed en bestaat naast commerciële bedrijven ook uit non-gouvernementele organisaties zoals Greenpeace en de Consumentenbond, en inmiddels dus ook de politie.

Op gespannen voet met grondrechten

Social media surveillance staat op gespannen voet met de vrijheid van meningsuiting en de vrijheid van vergadering en betoging. In de Verenigde Staten kwam de afgelopen jaren aan het licht dat leden van de Black Lives Matters beweging met behulp van technologie van de Amerikaanse reputatie management bedrijven Geofeedia, Snaptrends en Intrado, en het Canadese bedrijf Media Sonar in de gaten worden gehouden. Dit was onder meer het geval rond de

demonstraties in Ferguson, naar aanleiding van het doodschieten van Mike Brown door de politie.

Ook in Nederland wordt social media surveillance ingezet om kritische burgers en protestgroepen in de gaten te houden. Uit het rapport *Online media monitoring: tool en proces (2) ervaringen en inzichten naar aanleiding van operationele ervaring bij de politie-eenheid Zeeland - West-Brabant* blijkt dat de politie onder meer een pro-Gaza demonstratie op social media monitort.

Het taalgebruik in de via de WOB openbaar gemaakte interne beleidsdocumenten is wollig. Zo spreekt de politie over social media surveillance in het kader van de "opvolging van meldingen RTIC, een verzoek van de operatie, ter ondersteuning van probleemgerichte aanpak en creëren veiligheidsbeelden, bij het opsporingsproces, internetmonitoring niet-thematisch, gerichte monitoring op thema's, gerichte monitoring in het kader van preparatie van evenementen en het onderbouwing van dreigingsmeldingen en inschattingen." Ook gebruikt de politie termen als "niet-thematische internetmonitoring" (dat wil zeggen: structurele dan wel permanente social media monitoring) en "gerichte monitoring op thema´s", die gericht kan zijn op evenementen, vooral demonstraties (zoals de pro-Gaza demonstraties of protesten tijdens de NSS - Nuclear Security Summit), maar ook op voetbalwedstrijden, feesten, of feesten van motorclubs in het bijzonder.

Het gaat dus om permanente social media monitoring en surveillance die gericht is op demonstraties, andere manifestaties, maar ook op voetbalwedstrijden, en gewone feesten, feesten van een motorclubs.

De Nederlandse politie lijkt zich niet bezig te houden met de vraag hoe social media surveillance zich verhoudt tot de grondrechten van burgers. In de via de Wob openbaar gemaakte documenten wordt niet ingegaan op de consequenties voor de vrijheid van meningsuiting en de vrijheid van vergadering en betoging. Juridische kaders ontbreken volledig in de documenten. Veelzeggend is de passage in het adviesrapport van 2015 (*IM Adviesrapport Tools Informatieorganisatie Evaluatie en advies*) dat vermeldt "dat de

juridische kaders voor de gebruikers van de tools nog moeten worden opgesteld".

Bescherming van persoonsgegevens

De politie mag niet ongelimiteerd persoonsgegevens verzamelen, verwerken en bewaren. Haar beleid ten aanzien van opslag en verwerking van persoonsgegevens is wettelijk geregeld. Er vinden jaarlijkse audits plaats en er zijn maximum bewaartermijnen. Door gebruik te maken van de diensten van Coosto, OBI4wan/HowAboutYou en Buzzcapture omzeilt de politie deze wettelijke beperkingen.

De online en social media gegevens die Coosto, OBI4wan/HowAboutYou en Buzzcapture verzamelen zijn persoonsgegevens, hetgeen door de bedrijven ook wordt bevestigd in hun privacy verklaringen. Ook de Autoriteit Persoonsgegevens (AP) beschouwt de door bedrijven verzamelde data als persoonsgegevens. Aan het bewaren en het verwerken van persoonsgegevens worden wettelijke voorwaarden gesteld. In de 'Beleidsregels publicatie van persoonsgegevens op internet uit 2007' zijn weliswaar geen expliciete bewaartermijnen opgenomen, maar staat wel dat "gegevens niet langer mogen verwijzen naar identificeerbare personen dan strikt noodzakelijk en de gegevens moeten juist zijn en ter zake dienend." In antwoord op vragen van Buro Jansen & Janssen antwoordt de AP: "Het feit dat persoonsgegevens op internet staan, betekent niet dat ze zomaar opnieuw gebruikt mogen worden in een andere context, voor een ander doeleinde. … Zelfs als het nieuwe doel verenigbaar is met het oude doel, kan de verwerking onrechtmatig zijn."

Hoewel de Autoriteit Persoonsgegevens aangeeft geen zelfstandig onderzoek te hebben gedaan, stelt men wel dat: "bedrijven die de persoonsgegevens verzamelen van sociale media, een zelfstandige grondslag dienen te hebben voor de (verdere) verwerking, en er zorg voor moeten dragen dat de gegevens niet verouderd en niet onjuist zijn. Dat betekent ook dat deze bedrijven de gegevens niet langer mogen bewaren dan noodzakelijk voor het behalen van de gerechtvaardigde doeleinden die zij nastreven."

Geen van de reputatiemanagement bedrijven heeft de verwerken van persoonsgegevens gemeld bij de Autoriteit Persoonsgegevens (of haar voorganger het College Bescherming Persoonsgegevens). Tevens worden de bedrijven al tien jaar niet gecontroleerd door de AP. Als antwoord aan Buro Jansen & Janssen geeft de AP aan het niet als haar prioriteit te zien om hier tegen op te treden. "De Autoriteit Persoonsgegevens beschouwt uw brief als een belangrijk signaal," aldus de AP, maar "de Autoriteit Persoonsgegevens ontvangt jaarlijks duizenden tips en meldingen en moet daarom een selectie maken welke zij nader onderzoekt." De AP maakt niet duidelijk of zij nader onderzoek zal instellen naar de bedrijven.

De bescherming van persoonsgegevens is ook anderszins in het geding. Social media monitoring is big business, de data en archieven van bedrijven zijn commercieel interessant. In de Verenigde Staten werken verschillende social media monitoring bedrijven samen met, of zijn overgenomen door, grote multinationals. In Nederland speelt dit vooralsnog op bescheidener schaal, maar Coosto en OBI4wan breiden wel uit en hebben internationale ambities. Coosto heeft ondertussen vestigingen in België, het Verenigd Koninkrijk en Spanje. OBI4wan heeft begin 2017 Buzzcapture overgenomen en een vestiging in Duitsland geopend, hetgeen gefinancierd is door Main Capital Partners B.V., een Nederlandse investeerder in de IT-industrie. Gezien deze ontwikkelingen is het dan ook reëel dat archieven met persoonsgegevens van de Nederlandse social monitoring bedrijven in de toekomst in buitenlandse handen terecht komen.

Sentiment-analyse

Alle social media monitoring bedrijven doen aan sentiment-analyse. De tools die de politie inhuurt voor social media surveillance gebruiken sentiment-analyse als functionaliteit om de data te 'ordenen' en te 'analyseren'. De sentiment-analyse geeft berichten een positief, negatief of neutraal label en aan de hand van de gelabelde berichten kunnen personen worden geprofileerd.

Bedrijven zoals Coosto, OBI4wan, HowAboutYou en Buzzcapture presenteren de sentiment-analyse doorgaans als een wetenschappelijke methode. Er wordt gesproken over analyse met behulp van machine learning, of het toepassen van een set regels, automatisch en handmatig. Het lijken indrukwekkende concepten, maar het is veelal een verkooppraatje. Hoe effectief het meten van sentimenten is, is namelijk ongewis. Er is geen wetenschappelijke onderbouwing van de kwaliteit, nauwkeurigheid en totstandkoming van de analyses.

Buro Jansen & Janssen heeft Coosto, OBI4wan en Buzzcapture ook gevraagd naar de onderbouwing van de door hen gehanteerde sentiment analyse. OBI4Wan is het enige bedrijf dat deze vraag beantwoordt, maar het is weinig verhelderend. Op de vraag "In uw tool maakt u gebruik van een zogenaamde sentiment-analyse, maken de politie en de NCTV ook gebruik van die sentiment-analyse? Hoe nauwkeurig is die? Is er wetenschappelijk onderzoek dat die nauwkeurigheid bevestigd? Is dat openbaar?" antwoordt het bedrijf namelijk: "niet van toepassing."

De politie zelf rept in de via de WOB openbaar gemaakte documenten met geen woord over de betrouwbaarheid en nauwkeurigheid van de sentiment analyse. De politie gebruikt de tools voor social media surveillance zonder kennis te hebben van de werking van de tools, de broncode en de werking van de sentiment-analyse. Een bijkomend probleem is dat de politie niet op de hoogte is van de algoritmes die aan de sentiment-analyse ten grondslag liggen.

Dit is verontrustend. Zo is in de Verenigde Staten wel de nodige discussie ontstaan over de beperkingen en gevaren van de social media surveillance met behulp van sentiment-analyse. Met name het gebruik door de Amerikaanse politie van de tool Beware van Intrado, dat burgers en adressen een gevarenscore geeft, zorgde voor ophef. De Amerikaanse burgerrechtenbeweging ACLU wees er op dat de effectiviteit van de methode niet wetenschappelijk is onderzocht is, dat data onnauwkeurig zijn en dat de methode tot etnisch profileren kan leiden. Naar aanleiding van de ontstane maatschappelijke ophef zagen enkele Amerikaanse politiediensten af van het verdere gebruik van Beware. Bovengenoemde risico's zijn ook in de Nederlandse context relevant. Het gebrek aan kennis en

interesse van de Nederlandse politie op dit gebied is dan ook verontrustend.

Gebrek aan transparantie en verantwoording

Er vallen dus veel vraagtekens te plaatsen bij social media surveillance. Een serieus maatschappelijk debat is op zijn plaats en noodzakelijk. De Nederlandse overheid is echter weinig transparant. Buro Jansen & Janssen heeft in 2016 en 2017 verschillende Wob-verzoeken ingediend bij de politie en andere bestuursorganen. Hierop zijn enkele documenten openbaar gemaakt, waaruit blijkt dat de politie in ieder geval de tools van Coosto en OBI4wan/HowAboutYou gebruikt voor social media surveillance en opsporing. Illustratief voor de houding van de Nederlandse overheid is echter dat de passages in documenten die over opsporing gaan, veelal zwart zijn gemaakt. Daarnaast is het Buro Jansen & Janssen bekend dat, er naast de openbaar gemaakte documenten, nog vele andere documenten bestaan. De overheid heeft deze documenten echter nog niet openbaar gemaakt.

Niet alleen de overheid is weinig transparant, dit geldt ook voor social media platformen en social media monitoring bedrijven. Zij maken social media surveillance immers mogelijk; de meeste data die door social media monitoring bedrijven worden verzameld en geanalyseerd zijn afkomstig van social media platformen.

Social media platformen: geen actief en transparant beleid

Social media platformen hebben geen actief en transparant beleid om te voorkomen dat social media data worden gebruikt voor surveillancedoelen. In de Verenigde Staten hebben Facebook en Twitter de afgelopen jaren weliswaar enkele bedrijven, waaronder Geofeedia, Snaptrends en Media Sonar, de toegang tot hun gebruikersdata ontzegd nadat bekend werd dat deze bedrijven de data doorverkochten voor surveillance doeleinden. Dit gebeurde echter pas na maatschappelijke ophef, en niet uit eigen initiatief. Bovendien vormen bovengenoemde bedrijven slechts het topje van

de social media surveillance ijsberg, aangezien er vele andere social media monitoring bedrijven actief zijn en het onbekend is of deze ook de toegang zijn ontzegd.

Om te onderzoeken hoe de situatie in Nederland is heeft Buro Jansen & Janssen verschillende social media platformen gevraagd naar hun beleid om te voorkomen dat social media data worden gebruikt voor surveillance doeleinden, en naar hun relatie met de bedrijven Coosto, OBI4Wan en Buzzcapture. De meeste platformen (Twitter, LinkedIn, Google, Reddit, 4chan, Pinterest) hebben niet geantwoord en zijn dus niet bereid om enige verantwoording af te leggen. Alleen Facebook doet een poging om de vragen te beantwoorden.

Facebook heeft in maart 2017 haar Platform Policy aangepast en expliciet opgenomen dat data niet gebruikt mogen worden voor surveillance doeleinden. Ook Facebook heeft echter geen actief en transparant beleid om te voorkomen dat social media data worden gebruikt voor social media surveillance. Facebook gaat niet actief op zoek naar bedrijven die social media data verzamelen en doorverkopen voor surveillance doeleinden. Facebook stelt in antwoord op vragen van Buro Jansen & Janssen weliswaar dat er mechanismen zijn en dat het snel tot actie overgaat als bedrijven de platformvoorwaarden overtreden, maar in de praktijk blijkt dit niet het geval te zijn. Zo sprak Facebook Coosto pas aan na vragen van Buro Jansen & Janssen over de samenwerking tussen Coosto en Nederlandse politie. Facebook maakt niet duidelijk of het ook OBI4wan heeft aangesproken.

Bedrijven: tegenstrijdig, ontwijkend en verhullend

Buro Jansen & Janssen heeft ook de bedrijven Coosto, OBI4wan en Buzzcapture aangeschreven over hun betrokkenheid bij social media surveillance. Hierbij werd de bedrijven onder meer gevraagd naar hun samenwerking met politie en de NCTV en hun standpunt ten aanzien van social media surveillance. De antwoorden van de bedrijven zijn tegenstrijdig, ontwijkend en verhullend.

Geen van de bedrijven spreekt zich expliciet uit tegen social media surveillance. Zo stelt OBI4wan dat hun reputatie management en webcare tools "niet bedoeld zijn voor surveillance van individuen en daar ook niet voor gebruikt mogen worden." Het bedrijf zegt dat het geen uitspraak mag doen over het al dan niet samenwerken met de Nationale Politie. OBI4wan laat onduidelijk of hun tools door de politie voor social media surveillance doeleinden worden gebruikt. Op de vraag of de tool van het bedrijf wordt ingezet bij het RTIC en de opsporing en of het bedrijf deze overheidsactiviteiten ziet als surveillance van burgers, antwoordt OBI4wan dat zij daar "geen uitspraak over doen."

Ook Coosto geeft ontwijkende en verhullende antwoorden op vragen over haar medewerking aan social media surveillance. Coosto zegt dat het zich sinds kort aan de platformvoorwaarden van Facebook houdt, volgens welke sinds maart 2017 platformdata niet gebruikt mogen worden voor surveillance doeleinden. Coosto geeft echter geen expliciet antwoord op de vraag of het samenwerkt met de politie of de NCTV. Het bedrijf beëindigt haar beantwoording aan Buro Jansen & Janssen dat het "de voorwaarden van onze partners (zoals Facebook en Twitter etc.) volgt, in combinatie met ons moreel kompas en regelgeving".

De trein van social media surveillance rijdt voort

De Nederlandse politie doet de afgelopen jaren steeds meer aan social media surveillance. Deze ontwikkeling zal zich in de toekomst waarschijnlijk blijven voortzetten. Bedrijven als Coosto, OBI4Wan, HowAboutYou en Buzzcapture vormen een geaccepteerde bedrijfstak, waarover geen kritische vragen worden gesteld.

Dit is verontrustend, zeker daar social media surveillance veel vragen oproept. Social media surveillance staat op gespannen voet met grondrechten, zoals de vrijheid van meningsuiting en de vrijheid van vergadering en betoging. De bescherming van persoonsgegevens is in het geding. De door de bedrijven gebruikte methode van sentiment analyse is discutabel en riskant.

De trein van social media surveillance rijdt voort, zonder dat er sprake is van een politiek of maatschappelijk debat over de wenselijkheid en risico's hiervan. De overheid, social media platforms en social monitoring bedrijven zijn niet transparant en frustreren hiermee een maatschappelijk debat.

Social Media Surveillance in Nederland (pdf)

Gehele Observant #70 social media surveillance in Nederland (pdf)

Andere artikelen

Dagelijkse en structurele monitoring; De Nederlandse politie en social media surveillance

Reputatie management bedrijven, de nieuwe private inlichtingendiensten

De burger als dreigingsscore; Social media surveillance in de Verenigde Staten

Overgeleverd aan de grillen van social media multinationals; Facebook en Twitter en de Nederlandse social media surveillance

Bijlagen

Politie

presentatie Inge Hoogstad RTIC (pdf)

politie besluit OBI4wan HowAboutYou (pdf)

politie besluit OBI4wan online media monitoring tool en proces (pdf)

PID social media in de operationele politie processen (pdf)

politie besluit IM adviesrapport tools informatieorganisatie (pdf)

politie besluit Buzzcapture (pdf)

politie besluit nep accounts presentatie (pdf)

Ministerie van Veiligheid en Justitie

besluit ministerie van V en J Coosto Buzzcapture primair (pdf)

besluit ministerie van V en J Coosto Buzzcapture bij bezwaar (pdf)

Autoriteit Persoonsgegevens

persoonsgegevens_op_internet_2007 (pdf)

brief aan Autoriteit Persoonsgegevens (pdf)

aanvullende brief aan Autoriteit Persoonsgegevens (pdf)

Autoriteit Persoonsgegevens antwoord (pdf)

Coosto

Product Changes Coosto 29 juni 2017 (pdf)

vragen aan Coosto (pdf)

antwoorden coosto (pdf)

vragen aan Wiseguys (pdf)

factsheet Coosto november 2014 (pdf)

Coosto Open facsheet NL 2014 (pdf)

OBI4wan

vragen aan OBI4wan (pdf)

antwoorden OBI4wan (pdf)

vragen aan Sitedata (pdf)

factsheet OBI4wan november 2014 (pdf)

Buzzcapture

vragen aan Buzzcapture (pdf)

antwoorden van Buzzcapture (pdf)

factsheet Buzzcapture november 2014 (pdf)

Reputatiemanagement bedrijven

reputatiemanagenment bedrijven factscheets 2014 (pdf)

reputatiemanagenment bedrijven 2012 (pdf)

Montoring webcare tools 2012 (pdf)

Facebook

letter to Facebook (pdf)

eerste e-mail van Facebook (pdf)

tweede e-mail van Facebook (pdf)

derde e-mail van Facebook (pdf)

vierde e-mail van Facebook (pdf)

Twitter

letter to twitter (pdf)

eerste e-mail van Twitter (pdf)

tweede e-mail van Twitter (pdf)

Google

letter to Google (pdf)

eerste e-mail van Google (pdf)

tweede e-mail van Google (pdf)

LinkedIn

letter to LinkedIn (pdf)

eerste e-mail van LinkedIn (pdf)

tweede e-mail van LinkedIn (pdf)

4chan

letter to 4chan (pdf)

Pinterest

letter to Pinterest (pdf)

Reddit

letter to Reddit (pdf)

Naar inhoudsopgave Observant #70

Dagelijkse en structurele monitoring

Social Media Surveillance door de Nederlandse politie

Over grootschalige surveillance door inlichtingendiensten op internet ontstond in 2013 veel discussie door de onthullingen van Edward Snowden. Bij die onthullingen ging het in eerste instantie om de activiteiten van de Amerikaanse inlichtingendienst NSA, National Security Agency. De NSA verzamelt zoveel mogelijk informatie van bronnen op het internet met het doel om mogelijke terroristen op te sporen.

Dat inlichtingendiensten over iedereen informatie verzamelen met het idee daar verdachten van staatsgevaarlijke activiteiten uit te distilleren is op zich niet nieuw. Tijdens de Koude Oorlog werden veel mensen met vermeende linkse sympathieën in de gaten gehouden. Zij zouden misschien wel communist zijn of voor de Sovjet-Unie werken. In Nederland werden om die reden niet alleen mensen van de Communistische Partij Nederland, maar tal van maatschappelijke organisaties zoals de Nederlandse Vrouwen Bond, in de gaten gehouden.

Massale surveillance door inlichtingendiensten zorgt voor ophef in de Verenigde Staten en grote delen van de wereld, maar wordt tegelijkertijd als een noodzakelijk kwaad gezien in de strijd tegen terrorisme. Het gaat dan meer om surveillance door inlichtingendiensten, die iedereen in de gaten houden, dan om afluisteren door opsporingsdiensten. In Nederland werd dit jaar een wijziging van de Wet op de inlichtingen- en veiligheidsdiensten, die de AIVD en MIVD grotere bevoegdheden geeft, soepel door de Kamer geloodst. Bij deze wijziging is er sprake van sleepnetwetgeving, vergelijkbaar met de uitgebreide bevoegdheden van de NSA.

Grootschalige surveillance door de politie roept meer weerstand op. Dit zou betekenen dat de overheid constant meekijkt, een politiestaat, waarbij burgers bang zijn zich openlijk te uiten. Vaak

wordt dan verwezen naar de praktijken van de Stasi in het voormalige Oost-Duitsland. Bijna dertig jaar na de val van de Muur in 1989, de digitale revolutie en verschillende aanslagen in de Westerse wereld, rukt echter de wens van overheden op om massaal hun burgers te bespioneren. Hiervoor worden niet alleen inlichtingendiensten ingezet, ook de politie begeeft zich op het terrein van online en social media surveillance.

Reputatiemanagement is eigenlijk risicomanagement

Voor die surveillance huurt de politie bedrijven in die zich bezig houden met social media monitoring en daarvoor online en bij de social media persoonsgegevens verzamelen. Deze bedrijven, Coosto en OBI4wan verzamelen al jaren dit soort gegevens en slaan die op. Buzzcapture wordt ingehuurd voor communicatiedoeleinden door de Nationale Politie. Er is echter geen bewijs dat Buzzcapture voor social media surveillance wordt ingezet. De reputatiemanagement bedrijven spreken in 2014 van 400.000 bronnen (Coosto) en 400.000 Nederlandstalige bronnen (OBI4wan). Onder bronnen verstaan de bedrijven social media platforms als Facebook en Twitter, websites zoals nu.nl en tweakers.net, maar ook Wordpress sites en internetfora.

De bedrijven presenteren zich als reputatiemanagement bedrijven. De informatie is primair bedoeld om de communicatie tussen producent en consument of overheid en burger te verbeteren. De social media monitoring bedrijven verzamelen data, indexeren die, maken die doorzoekbaar en voorzien ze van een sentiment analyse, een functionaliteit die bepaald of een bericht positief, negatief of neutraal is. De bedrijven beheren grote historische archieven die teruggaan tot 2009 (Coosto en Obi4wan) en 2007 (Buzzcapture). Vervolgens verkopen zij die data door, zodat merken als Shell of Unilever de risico´s die ze lopen bij een online mediastorm kunnen beperken. Reputatiemanagement is in feite risicomanagement. Niet alleen bedrijven gebruiken de monitoring tools, ook maatschappelijke organisaties en overheidsdiensten, waaronder de politie. De politie gebruikt de tools niet alleen voor communicatie, maar ook voor social media surveillance en opsporing. Buro Jansen

& Janssen heeft verschillend Wob-verzoeken ingediend om social media surveillance door de politie in beeld te brengen.

Real Time Crime Center RTCC

Het toenemende gebruik van social media surveillance door de politie hangt samen met de ontwikkeling van Real Time Intelligence Centers (RTIC). De RTIC is een uitgebreide meldkamer, een inlichtingenmeldkamer, maar geen vervanging van de klassieke meldkamer. In de Verenigde Staten zijn deze aan het begin van deze eeuw opgezet als crime centers om moord en doodslag aan te pakken, maar uiteindelijk doorontwikkeld als surveillance centra. In Nederland zijn de RTIC'S vanaf 2010 ontwikkeld. In zulke Intelligence Centers komen *harde* en *zachte* data, waaronder online en social media gegevens samen. Met behulp van een sentiment analyse worden die data geanalyseerd en kunnen daarmee het politiewerk sturen.

De RTIC is gemodelleerd naar de Amerikaanse RTCC, Real Time Crime Center. De eerste RTCC's werden rond 2005 opgezet. Bij deze centra ging het vooral om het samenbrengen van lokale en federale politie-informatie, zoals posities van politieagenten en auto´s, gegevens uit politieregisters over overtredingen, strafbare feiten en gevangenisstraffen; en publieke informatie als gegevens van het bevolkingsregister, kadaster, kamer van koophandel en andere overheidsdatabestanden; maar ook om cameratoezicht, kaarten en beelden van helikopters. Online media of social media gegevens speelden nog geen rol van betekenis in de beginfase van de RTCC's.

Bij de inlichtingenmeldkamers in de VS werd al snel duidelijk dat er sprake was van een verschuiving in de doelstellingen. Bij de start van de New Yorkse RTCC zou het centrum alleen moord, doodslag en schietincidenten behandelen. De risico´s van massale surveillance op basis van zowel politieregisters als openbare data werden door de politie onderkend. Van die aanvankelijke beperkte doelstelling is echter weinig over. De RTCC's zijn ingezet om demonstranten te bespioneren, zoals die van de Black Lives Matter beweging. Onderzoek van de American Civil Liberties Union (ACLU) in 2016 toonde aan dat de politie Facebook, Instagram, Twitter,

YouTube en andere sociale media rond de klok monitorde en leden van actiegroepen in de gaten hield.

De kop boven het artikel in De Leeuwarder Courant uit december 2012 over de opening van het RTIC (Real Time Intelligence Center) in Drachten is dan ook niet misplaatst. *Politiespionnen zoeken verdachten op internet* klinkt als een inlichtingendienst die mensen in de gaten houdt. De techniek heeft die surveillance mede mogelijk gemaakt. Mensen delen hun persoonlijk leven op internet. Soms met gebruikmaking van de privacy settings die berichten afschermen van het brede publiek, maar meestal niet. Berichten, foto´s, meningen en fantasieën worden gedeeld met iedereen. Daarnaast hebben de lage kosten van opslag van data en het voor handen zijn van allerlei simpele programma's die het verzamelen van data op het internet vergemakkelijken, bijgedragen aan de ontwikkeling.

Real Time Intelligence Center, RTIC in Nederland

De Nederlandse RTIC´s gingen in 2012 van start. Doel van de RTIC's is om de politie beter voorbereid op een melding te laten reageren. Bij de RTIC´s komen naast de gebruikelijke politieregisters en NAW (naam, adres en woonplaats) gegevens ook cameratoezicht en informatie vanuit internet en social media binnen. Daarnaast wordt ook informatie van burger apps zoals Burgernet, informatie van beveiligingsbedrijven en van sensoren voor bewegings- en geluidsdetectie aan de inlichtingen van de RTIC´s toegevoegd.

Inge Hoogstad van de politie-eenheid Rotterdam geeft in een presentatie uit februari 2016 over de Dienst Regionaal Operationeel Centrum (DROC) aan, wat voor informatie er bij het RTIC samenkomt. Bij de DROC zijn de meldkamer Rotterdam en de RTIC van de politie-eenheid Rotterdam samengebracht. Volgens de presentatie gaat het om gegevens uit Blueview (processen verbaal, verhoren, aangiftes, gegevens van verdachten en bijvoorbeeld openstaande boetes), Verona (wapenvergunningen), SKDB (strafrechtsketendatabank) en de Kamer van Koophandel. Deze

gegevens behoren tot de *hardere* informatie die de politie raadpleegt zowel bij meldingen als onderzoek.

Zachte informatie

Naast deze gegevens worden in de presentatie ook social media platforms zoals Google, Facebook en Twitter genoemd. Deze *zachte* informatie staat in de presentatie van Hoogstad in dezelfde lijst als de informatie uit politieregisters. De *harde* politie en overheidsdata komen samen met de *zachte* data die afkomstig is uit online en social media. Informatie die mensen zelf, al dan niet publiekelijk, delen op social media is ook *zachte* informatie die de inlichtingeneenheden van de Nederlandse politie, Teams Criminele Inlichtingen (TCI), de voormalig Criminele Inlichtingen Eenheden (CIE´s) en de Regionale Inlichtingen Diensten (RID), verzamelen. Het TCI richt zich voornamelijk op criminaliteit, de RID op de handhaving van de openbare orde en het in de gaten houden van politieke (buitenparlementaire) activiteiten.

Het TCI en de RID gebruiken voor hun informatie inwinning traditionele media, het internet en social media, maar ook gesprekken met verdachten die vastzitten om hen onder druk informatie te ontfutselen, en de inzet van informanten en infiltranten. Dit kan een bezoek zijn van een agent aan een café, een flat of moskee, maar ook het inzetten van infiltranten of informanten bij acties, demonstraties of vermeende criminele activiteiten. Het gaat onder meer om inlichtingen over mogelijke criminele activiteiten, relaties tussen verdachten, politieke activiteiten, actiegroepen en acties van voetbalsupporters. Informatie van het TCI en de RID wordt *zachte* informatie genoemd, omdat het vaak om informatie gaat die is gebaseerd op geruchten of roddels. Informanten kunnen bijvoorbeeld niet zomaar vertrouwd worden, maar kunnen ook door een criminele organisatie zijn ingehuurd om onjuiste informatie te verspreiden of concurrenten een hak te zetten. Ook anonieme tips zijn in principe zachte informatie.

Zachte informatie kan aanleiding zijn om nadere inlichtingen in te winnen, een huis binnen te treden en te doorzoeken, extra politie in te zetten bij een demonstratie of een manifestatie te verbieden.

Slechts een enkele keer rukt de politie naar aanleiding van zachte informatie groot uit. Dit heeft onder meer te maken met de omstandigheden, de betrouwbaarheid van de tip of de informant, en informatie uit de *harde* gegevens waar de politie over beschikt. Bij terrorismedreiging gebeurt het soms, zoals bij de melding over IKEA in maart 2009 (zie *Meer dan 200.000 professionals doen maar wat tegen terrorisme*, Buro Jansen & Janssen).

De RTIC's van de Nationale Politie maken geen gebruik van dezelfde zachte informatie als het TCI en de RID, zoals uit de presentatie van Inge Hoogstad van de politie eenheid Rotterdam blijkt. Dit kan informanten in gevaar brengen en bronnen van de diensten onthullen. De zachte informatie van de RTIC bestaat uit openbare bronnen van traditionele media, zowel fysiek als digitaal, en andere nieuwsorganen, fora, blogs en social media.

PID Social Media in operationele politieprocessen

De RTIC´s ontwikkelden zich in de periode dat de politieregio´s opgingen in de Nationale Politie. Allerlei regionale politiesystemen moesten bij de vorming van de Nationale Politie opgaan in een landelijk systeem. Het systeem Blueview bijvoorbeeld, een soort zoekmachine die in 2007 werd ingevoerd, maakt het mogelijk dat medewerkers van verschillende politieregio's in elkaars systemen kunnen kijken. De overgang naar de Nationale Politie ging gepaard met het opzetten van meldkamers en RTIC´s per eenheid, die echter wel een nationale verbinding hebben.

De Nationale Politie is op 1 januari 2013 gestart, maar veel ontwikkelingen waren daarvoor al in de afzonderlijke politieregio´s ingezet, zo ook het denken over RTIC´s en de inzet van risico- of reputatiemanagement tools. In 2013 werd een voorstel gedaan om te onderzoeken wat de mogelijkheden waren voor het gebruik van social media door de politie. Als startpunt gebruikt de Nationale Politie het document *Project Initiatie Document (PID) Social Media in operationele politie processen*. Volgens het PID document is één van de doelen voor fase 0 van het project Social Media in operationele Politie Processen (SMPP) "een ruwe inventarisatie van wat er in de eenheden reeds is gerealiseerd: de nulmeting (peildatum 1 maart

2013).” Voor deze ruwe inventarisatie is gebruik gemaakt van “de bevindingen uit praktijkervaringen m.b.t. social media in elke politie eenheid (2009-2013)”.

In het PID wordt opgesomd wanneer de politie social media bruikbaar acht. Het document noemt “actieve wederkerigheid (tweerichtingsverkeer), crisis watch, webcare, crowdcontrol, event watch, realtime intelligence tool, operationele opsporingstool en kennisdeler”. De terreinen waarbij de politie social media wil inzetten, lopen sterk uiteen. Het gaat om communicatie met burgers over aangiften, meldingen, maar ook om de eigen communicatie van de politie over haar werk. Daarnaast noemt het document de inzet van social media door de politie bij evenementen en crowd control. Dan is er de inzet als inlichtingenbron bij dezelfde meldingen en communicatie met politieagenten in de wijk of op locatie. Daarnaast formuleert het document als ambitie dat “de eenheden dagelijks online een structurele monitor draaien” en als laatste zou social media ook voor de opsporing een belangrijk middel kunnen zijn. De Nationale Politie wil hier kennelijk weinig ruchtbaarheid aan geven. De passages over opsporing zijn in de, naar aanleiding van de Wob-verzoeken van Buro Jansen & Janssen, openbaar gemaakte documenten namelijk zwart gemaakt.

Van communicatie naar permanente surveillance

De Nationale Politie huurt dus reputatiemanagement bedrijven als Coosto, Obi4wan/HowAboutYou en Buzzcapture in. De politie gebruikt de diensten van de bedrijven niet alleen voor haar eigen communicatiebeleid (Buzzcapture) en de contacten met burgers, maar ook voor meldingen, aangiften, handhaving, Real Time Intelligence Center en opsporing (Coosto, OBI4wan en HowAboutYou).

De politie verstrekt geen documenten over Coosto. Uit het document *Online media monitoring: tool en proces (2), Ervaringen en inzichten naar aanleiding van operationele ervaring bij de politie-eenheid Zeeland - West-Brabant* blijkt echter dat Coosto op dezelfde wijze wordt ingezet als OBI4wan. Zo staat in het document dat Coosto meer data van Facebook boven tafel krijgt dan OBI4wan. “De

gegenereerde resultaten van OBI4wan zijn niet zo volledig als bij de andere gebruikte online media monitor op het RTIC (Coosto). Vooral bij de bronnen Facebook, YouTube en Instagram zijn de resultaten bij het gebruik van dezelfde zoekopdrachten van Coosto vollediger." De reden voor het verschil wordt niet in het rapport vermeld. Het kan een aanwijzing zijn voor het gebruik van nep- of schaduwaccounts of andere manieren waarop in Facebook vriendengroepen wordt binnengedrongen.
Het PID document stelt in 2013 vast, dat de politie vaak geen strategie heeft op het gebied van social media surveillance. "Tijdens crisissituaties en evenementen hebben eenheden als zodanig geen vastgesteld beleid over de inzet van social media. In een aantal grote steden is dit wel het geval." Aan de andere kant spreekt het document over "een divers beeld" en over social media in "verschillende operationele processen en op verschillende organisatieniveaus".

Eigenlijk zijn de verschillende regiokorpsen al lang voor de aanvang van de Nationale Politie begonnen met online en social media surveillance. Het PID document concludeert: "In de huidige situatie wordt binnen de eenheden verschillend omgegaan met het monitoren van social media. Ook zijn er veel verschillende software tools en diverse soorten ICT-hardware in gebruik (groot/klein, freeware/licentie, etc). Voor de aanschaf van tools is er geen landelijke standaard."

In het PID document passeren mogelijke strategieën de revue: van online opschalen in geval van crisis en evenementen, tot aan twitterende agenten, monitoring en opsporing. In grote lijnen zijn er twee strategieën. De incidentele benadering waarbij social media pas worden geraadpleegd wanneer iemand een feestje op Facebook aankondigt en wanneer er camerabeelden van een mishandeling worden gedeeld, als een vorm van crisisbeheersing of opschaling vanuit de social media surveillance. En de surveillance zelf, waarbij social media data zijn opgenomen in de informatie organisatie van de politie. Van RTIC tot de inlichtingentak van de politie-organisatie met lokale onderdelen (Districtelijk Informatie Knooppunt), regionale RIK (Regionaal Informatie Knooppunt), het landelijke team OSINT (Open Source INTelligence), Opsporing en SGBO, wordt social media gebruikt. "Door de informatieorganisatie in de eenheden wordt er dagelijks online een structurele monitor

gedraaid", is het doel dat het PID document van 2013 voor social media surveillance formuleert.

Open Source Intelligence OSINT

OSINT (Open Source INTelligence) heeft altijd een belangrijke rol gespeeld bij de politie, maar vooral bij de inlichtingendiensten van de politie, het TCI en de RID. Naast de klassieke inlichtingen elementen HUMINT (de menselijke bronnen zoals informanten) en SIGINT (Signal Intelligence, het tappen van communicatie) is OSINT voor de politie de belangrijkste informatiebron. OSINT kan bestaan uit de verhalen die de wijkagent opvangt om zicht te houden op de wijk, of de rechercheur die geruchten hoort tijdens een onderzoek naar een overval. Naast die informatie verzamelen het TCI en de RID andere *zachte* informatie, zoals berichten, verhalen, geruchten en folders.

Met de ontwikkeling van online en social media is OSINT voor de gehele politie van groot belang geworden, Dit wordt onderstreept door de oprichting van het *landelijke Team OSINT* in 2011 dat open bronnen op internet monitort. In navolging zijn de Real Time Intelligence Centers per 1 januari 2014 met social media surveillance begonnen. Vanaf dat moment voeren de RTIC's de klok rond social media surveillance uit met het doel om de social media te monitoren, analyseren en vervolgens te interveniëren.

Twee jaar na het verschijnen van het PID document, in 2015, wordt het belang van OSINT veelvuldig benadrukt in het adviesrapport *IM Adviesrapport Tools Informatieorganisatie Evaluatie en advies*. De politie wil OSINT inzetten voor het "versterken van de (realtime- en righttime) informatiepositie van de politie, verbeteren van de interpretatie (duiding) van informatie, kansen bieden voor verhoging van de heterdaadkracht". De politie voert ondertussen rond de klok online en social media surveillance uit, blijkt uit het rapport.

Het adviesrapport van 2015 spreekt over de *mindset* van politiefunctionarissen, over de inrichting van de Nationale Politie en het opleiden van medewerkers in het gebruik van social media monitoring tools. Er wordt gesproken over de RTIC en de OSINT

taak van de politie en een evaluatie van de tools. “Juridische kaders voor de gebruikers van de tools” moeten nog worden opgesteld, staat in het document. Of alle politie eenheden dezelfde social media monitoring tools gebruiken voor communicatie, RTIC, opsporing, ofwel social media surveillance, zoals de wens was in het PID document van 2013 blijkt niet uit het rapport.

Project X

Het PID document van 2013 is nog enigszins terughoudend als het gaat om real time surveillance, hoewel het de wens uitspreekt om “dagelijks online een structurele monitor te draaien”. In het advies rapport in 2015 wordt het belang van OSINT en social media surveillance onderstreept, al wordt de laatste term niet gebruikt. De omslag hangt samen met twee incidenten. De politie verwijst altijd naar *Project X* dat op 21 september 2012 in Haren plaatsvond en een mishandeling in Eindhoven op 4 januari 2013 waarbij de verdachten op social media werden omschreven als de Eindhovense kopschoppers. Bij het *Project X* feest werd een uitnodiging voor een verjaardagsfeest massaal rondgestuurd en kwamen er uiteindelijk heel veel mensen opdraven. Bij de mishandeling in Eindhoven ontstond naar aanleiding van camerabeelden op social media een klopjacht om de verdachten te vinden. Bij *Project X* werden uiteindelijk ook social media ingezet om verdachten van vernielingen en plundering op te sporen.

Het PID document van 2013 refereert aan beide incidenten: “Social media zijn niet meer weg te denken uit onze maatschappij. Mensen gebruiken social media om elkaar te betrekken, te informeren en te beïnvloeden met in hun kielzog de reguliere media. De gevolgen hiervan kunnen groot zijn: voor bestuurders, politie, het Openbaar Ministerie, maar ook voor de burger zelf. Recente voorbeelden zijn de publieke verontwaardiging over de verdachten van uitgaansgeweld in Eindhoven (camerabeelden) en een ogenschijnlijk onschuldige Facebook-uitnodiging die leidde tot grote ongeregeldheden in Haren (*Project X*).”

In het adviesrapport van 2015 wordt verder ingegaan op de redenen van het starten van het project Social Media in operationele Politie

Processen (SMPP). Daar wordt alleen verwezen naar *Project X*: "Het klein bedoelde feest groeide uit tot een ware hype", aldus het rapport. Social media worden afgeschilderd als een kanaal dat onbeheersbare gevolgen kan hebben. "Mensen gebruiken social media om elkaar te betrekken, te informeren en te beïnvloeden. De gevolgen hiervan kunnen voor bestuurders, politie, het Openbaar Ministerie … groot zijn."

De overheid gebruikt *Project X* als legitimatie om grootschalige surveillance op het internet te gaan organiseren. "De politie is toegerust om te acteren in de publieke ruimte. Surveilleren en handhaven op het internet en in de social media staan echter nog in de kinderschoenen", aldus het PID document. In het rapport wordt regelmatig verwezen naar de commissie *Project X* Haren (onder leiding van Job Cohen), die stelt dat "social media mogelijkheden bieden om verbinding te maken in de haarvaten van de maatschappij". Het rapport gebruikt die mogelijkheden om te stellen dat "in alle politieprocessen de social media een cruciale rol spelen. Denk daarbij onder andere aan handhaven, het verzamelen van informatie, het duiden ervan en het eventueel interveniëren".

Project X en de Eindhovense mishandeling zijn door de politie duidelijk gebruikt om het proces van de integratie van online en social media surveillance binnen de politie te versnellen en uit te breiden. Of social media bij die incidenten al dan niet daadwerkelijk een grote rol hebben gespeeld, is voor de politie van minder belang. Het uit de hand gelopen feest in Haren roept namelijk naast bestuurlijke en operationele vragen ook vragen op over de normale Open Source INTelligence en de toen gebruikte social media monitoring tools.

Project X werd misschien wel geïnitieerd op social media, maar het lijkt erop dat de aandacht van reguliere media, vooral radio 3FM, er uiteindelijk voor zorgde dat de uitnodiging voor het verjaardagfeest door veel jongeren werd opgepakt. Zelfs zonder social media monitoring tools had de politie kunnen voorspellen dat er op 21 september 2012 iets ging gebeuren in Haren. De hoeveelheid feestgangers was van tevoren niet te voorspellen, ook niet naar aanleiding van het aantal hypothetische bezoekers op Facebook. Monitoring tools hadden hooguit kunnen vaststellen dat *Project X* veel reacties opleverde op social media, maar het feit dat het de

reguliere media haalde was daar ook al een aanwijzing voor. Bij de Eindhovense *kopschoppers* speelde social media in eerste instantie geen rol van betekenis. Pas nadat de politie zelf de publiciteit had gezocht om de verdachten te vinden, werd op social media naar de verdachten gezocht.

Demonstraties, voetbal en feestjes als surveillancedoel

De ambities van de politie op het gebied van OSINT zijn uiteenlopend. Volgens het evaluatierapport van 2015 (IM Adviesrapport Tools Informatieorganisatie Evaluatie en advies) gaat het om het gebruiken ervan in het kader van de "opvolging van meldingen (MK) RTIC, een verzoek van de operatie (gepland en ad hoc, o.b.v. acties/instappen etc.), ter ondersteuning van probleemgerichte aanpak en creëren veiligheidsbeelden, bij het opsporingsproces (incl. veiligstellen bewijslast), internetmonitoring niet-thematisch, gerichte monitoring op thema's, gerichte monitoring in het kader van preparatie van evenementen en het onderbouwing van dreigingsmeldingen en inschattingen".

In het rapport wordt onderscheid gemaakt tussen "internetmonitoring niet-thematisch" en "gerichte monitoring op thema's (thematische informatie coördinatie)". Het gaat dus om respectievelijk monitoring rond de klok van het internet en om specifieke surveillance. Uit de via de Wob openbaar geworden documenten blijkt waar die gerichte monitoring op thema's op gericht is. Het gaat om evenementen zoals demonstraties (pro-Gaza demonstratie, protest tijdens de Nuclear Security Summit NSS), picket lines en andere manifestaties, maar ook voetbalwedstrijden, en gewone feesten, feesten van een motorclubs. Mensen die politiek actief zijn, supporter zijn van een voetbalvereniging of vermeend lid van een motorclub worden in de gaten gehouden op social media. De voorbeelden die de politie opsomt lopen uiteen van incidenten (ongeval, televisie uitzending, vermissing, terrorismemelding), mogelijke problemen met de openbare orde (*Project X* feest, motorclubfeest en voetbalwedstrijd) of demonstraties en manifestaties.

De vrijheid van meningsuiting, het recht op manifestatie en de vrijheid van vergadering komen hiermee evident in het geding. Social media surveillance staat op gespannen voet met de rechtstaat. Geen van de geopenbaarde documenten maken gewag van dit spanningsveld. Voor de politie bestaat er geen onderscheid meer tussen een demonstratie, een feest, een vermissing of een ongeval. In de documenten is er maar één juridisch kader: "Juridische kaders t.b.v. de operationele politieprocessen: actief wederkerige inzet, crisis en evenementen, big data, realtime intelligence, opsporen, veilig onderzoek doen en veiligstellen en gebruik politie+ (een soort politie Twitter)." Voor de politie is een "vermissing van een minderjarig meisje, een ongeval bij een treinstation, het uitzenden van een mogelijk maatschappelijke onrust veroorzakend televisieprogramma, een feest van een motorclub, een mogelijk *Project X*-achtig feest, terrorisme-gerelateerde melding, RKC – Feijenoord en een pro-Gaza demonstratie" eenzelfde crisissituatie.

Publiek-Private Samenwerking

Bij de ontwikkeling van de RTIC's en de ontsluiting van online en social media voor surveillance doeleinden wordt de samenwerking tussen opsporingsdiensten en private partijen zichtbaar. In de Verenigde Staten is die ontwikkeling door de Freedom of Information Requests van de American Civil Liberties Union (ACLU) duidelijk aan te wijzen. In Nederland is de Nationale politie weinig transparant over deze publiek-private samenwerking. De politie en de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) hebben geen documenten openbaar gemaakt die aangeven hoe de diensten zijn uitgekomen bij private partijen als Coosto, Obi4wan, HowAboutYou en Buzzcapture. Het ministerie van Veiligheid en Justitie heeft bijvoorbeeld geen aanbesteding uitgeschreven voor een social media monitoring tool voor de NCTV.

Wat uit de openbaar gemaakte documenten wel duidelijk wordt is dat in tegenstelling tot de Amerikaanse tool Beware, van het bedrijft Intrado, de door de Nederlandse politie gebruikte reputatiemanagement tools van private bedrijven als Coosto tot op heden nog geen actief gebruik maken van politie-informatie. Zij

gebruiken alleen online en social media informatie. *Harde* informatie van de politie is nog gescheiden van online en sociale media inlichtingen.

Sentiment analyse, Positief - Negatief

De politie verzamelt niet zelf die data van het internet. Hiervoor huurt zij reputatiemanagement bedrijven in. Bedrijven zoals Coosto, OBI4wan en Buzzcapture bieden de politie een archief met historische data en real time monitoring van uiteenlopende social media platforms (zoals Facebook, Twitter), blogs en websites (zoals Nu.nl, Tweakers).

De bedrijven hebben een archief opgebouwd dat vele jaren teruggaat, Buzzcapture tot 2007 en Coosto en OBI4wan tot 2009. Van sommige platformen en websites worden nieuwe data elke 5 minuten verzameld. Om de data voor hun klanten inzichtelijk te maken wordt er op de berichten een sentiment analyse uitgevoerd. De politie krijgt ook de beschikking over deze sentiment analyse.

De sentiment analyse is een extra functionaliteit binnen de tool van de reputatiemanagement bedrijven, die bepaalt of een bericht goed/positief of slecht/negatief is. Er is meestal ook een derde optie toegevoegd: neutraal of sentiment onbekend. Met de gelabelde berichten van een persoon kan een profiel van een persoon worden samengesteld.

Voor producenten die een nieuw product op de markt brengen kan een sentiment analyse van belang zijn om de marketing op aan te passen. Een worst is lekker of vies, of de consument heeft geen mening. De meeste mensen zullen echter geen heel uitgesproken mening hebben over een product, dus blijft de vraag wat een sentiment analyse nu precies zegt. Is een opmerking van een klant dat de worst wel lekker is, maar dat de structuur van de worst niet bevalt, een positief of negatief sentiment? Voor de producent is het van belang dat de consument gewoon de worst gaat kopen.

Coosto, Buzzcapture en OBI4wan gebruiken een sentiment analyse met de labels positief, negatief en neutraal. Clipit, een ander

reputatiemanagement bedrijf, schrijft bij haar product dat “het sentiment wordt weergegeven niet alleen aan de hand van vijf niveaus met ook met verschillende kleuren”. Donkergroen is dan heel positief en donkerrood heel negatief. Het verloop van groen via geel naar rood is de schaal van positief naar negatief.

Deze kleurschakering wordt ook gebruikt in het programma Beware van het Amerikaanse bedrijf Intrado Inc. bij het vaststellen van een gevarenscore, waarbij burgers en adressen een gevarenscore/risicoscore (Facebook Threat Score) krijgen op grond van een berekening door het programma. Beware geeft een score aan met groen (goed), geel (enigszins een gevaar) of rood (gevaarlijk).

Het systeem van de gevarenscores van Beware is nooit wetenschappelijk onderzocht. De Amerikaanse burgerrechtenorganisatie ACLU stelt dat effectiviteit en nauwkeurigheid van Beware niet gemeten is. Tevens ontbreekt het aan controle, transparantie en onafhankelijk onderzoek naar het gebruik van Beware. En tot slot wijst de burgerrechtenbeweging op het gevaar van profilering als gevolg van het gebruik van Beware. De technologie zou bijdragen aan etnisch profileren.

Sentiment analyse is analyse van de taal van een bericht. Hoofd ontwikkelaar van Buzzcapture Eike Dehling legt in 2014 in het artikel *How does sentiment analysis work?* uit hoe de analyse werkt. Hij stelt dat er verschillende mogelijkheden zijn voor het vaststellen van een sentiment. De aanwezigheid of afwezigheid van bepaalde woorden, groepen of samenstelling van woorden, type woorden zoals scheldwoorden, ontkenning of bevestiging en ten slotte emoticons, symbolen die een emotie zouden weergeven.

Als voorbeeld van een bericht met een positief sentiment schrijft de ontwikkelaar dat iemand een goed weekend heeft gehad. Een negatief sentiment is een bericht over de stomme reactie van een bank op een vraag over een hypotheek. De meeste risicomanagement bedrijven gebruiken een automatisch label mechanisme om een Facebook bericht, tweet, blogpost of iets anders van een stempel of score te voorzien. Dehling schrijft op de website van Buzzcapture dat die automatische stempelmachine

zelflerend is. Hij gaat er dus vanuit dat de nauwkeurigheid en de kwaliteit van de sentiment analyse in de loop der jaren beter wordt.

Koningssentiment

Natuurlijk zijn de reputatiemanagement bedrijven erg enthousiast over de sentiment analyse die zij aanbieden. OBI4wan schrijft dat zij "100% nauwkeurigheid nastreeft." Op de website staat echter dat "de nauwkeurigheid van het sentiment, maximaal 75% – 79% is". Wat deze waarden precies betekenen blijft onduidelijk, want er wordt niet ingegaan op de nulwaarde: 75% – 79% ten opzichte van wat? Daarnaast stelt het bedrijf dat "over het algemeen het sentiment 80% neutraal is."

OBI4wan garandeert haar klanten echter dat "de correctheid van het sentiment daadwerkelijk rond de 98% is". Of dit echt zo is, valt te betwijfelen. OBI4wan komt niet voor in de top vier bedrijven die volgens Emerce in 2016 het sentiment rond het Koningshuis goed hebben gemeten. Uit die test komt Buzzcapture als winnaar naar voren met 89% "correct beoordeeld sentiment". Daarna volgen SentiOne (75%), Clipit (74%) en Meltwater (36%).

De vraag is of het sentiment rond het Koningshuis wel eenduidig te meten valt. Sentiment analyse is geen exacte wetenschap en bevat tal van complexe elementen, zoals door bedrijven ook wordt onderkend. Zo schrijft OBI4wan in een artikel *meten is weten, maar weet ook wat je meet* dat "sarcasme en cynisme het lastig maken om hier écht een sluitend beeld te geven".

Natuurlijk zijn er uitgesproken meningen van Oranjegezinden en Republikeinen, maar het is de vraag of het merendeel van de Nederlanders ook zo´n scherpe mening heeft. Als 89% (64.629) van de geanalyseerde 72.617 berichten, wordt bestempeld als neutrale berichten over het Koningshuis, wat zegt dat dan? Zijn dat daadwerkelijk kleurloze meningen of zitten daar juist belangrijke

nuanceringen in? Volgens Emerce waren 89% van de geanalyseerde berichten nieuwsberichten en zijn deze daarom als neutraal beoordeeld.

Sentiment-industrie

Reputatiemanagement bedrijven proberen zich door middel van de sentiment analyse te onderscheiden. Een grote berg online en social media gegevens aanbieden is niet heel ingewikkeld, maar om die databerg inzichtelijk te maken voor de klant is lastiger. De sentiment analyse is voor bedrijven een mogelijkheid zich te onderscheiden en daarom benadrukken zij hoe succesvol hun methode zou zijn.

Zo stelt Amit Moran, data analist van het Amerikaanse bedrijf Crosswise, dat je met sentiment analyse de echte kracht van social media kan gebruiken. Door de hoeveelheid data kan volgens hem met behulp van sentiment analyse van individuele tweets de veranderende mening van gebruikers door de tijd worden vastgesteld. Anderzijds is Moran minder stellig over de toepasbaarheid van analyses voor alle onderwerpen. Hij stelt dat een sentiment analyse ten aanzien van bijvoorbeeld een worst niet automatisch kan worden gebruikt voor bijvoorbeeld het Koningshuis. “The phrases and patterns used to express sentiment varies across domains and need to be adapted when switching between domains.”

Moran geeft aan dat sentimenten over een specifiek onderwerp niet noodzakelijkerwijs gebruikt kunnen worden op een ander terrein. Dit heeft natuurlijk alles te maken met taal en het taalbegrip. Hoe taal wordt gebruikt, en of online woordgebruik wel overeenkomt met offline taalgebruik, zijn vragen die sentiment analyse compliceren en bemoeilijken. Dominick Soar, content manager bij het bedrijf Brandwatch, schrijft in 2011 dat sentiment analyse is gebaseerd op taal, maar dat niet altijd kan worden vastgesteld welk sentiment de social media gebruikers uiten. Volgens de manager gebruiken mensen op sociale media geen normale of standaardtaal. Hij noemt het dialecten, slang of andere manieren om hun gevoelens te uiten. Brandwatch heeft hiervoor natuurlijk een oplossing, want volgens

Soar zou het bedrijf door machine learning de oplossing voor het taalprobleem hebben gevonden.

Naast de bovenstaande problemen is er ook nog het probleem van spelling en spelfouten. Frank Scheelen, ontwikkelaar bij Coosto zegt in een artikel op Recruitment Matters dat "15% van alle tweets spelfouten bevatten". Scheelen noemt naast de taalfouten ook andere aspecten die ervoor zorgen dat "sentiment analyse nooit perfect zal kunnen zijn". Zoals het feit dat cynisme en sarcasme niet kunnen worden vastgesteld door de systemen en dat gemengde gevoelens en de context waarin bepaalde opmerkingen worden gemaakt niet door analyses worden opgepikt.

Algoritmen

De reputatiemanagement bedrijven presenteren de sentiment analyse als een wetenschappelijke methode, maar de analyse is een verkooppraatje. Er wordt gesproken over analyse met behulp van machine learning, of slechts het automatisch en handmatig toepassen van een set regels. Hoe effectief het meten van sentimenten is blijft ongewis. Er is geen wetenschappelijke onderbouwing van de kwaliteit, nauwkeurigheid en totstandkoming van de analyses.

Sentiment analyse is gebaseerd op algoritmen: formele regels, vastgelegd door computertechnici, die een voorspelling maken over het sentiment van een bericht op basis van historische regels en patronen. Voor die voorspellingen, regels en patronen zijn wel historische data nodig. Daarom verzamelen de reputatiemanagement bedrijven veel data.

Coosto spreekt bijvoorbeeld over drie miljoen berichten die dagelijks worden verzameld en voorzien van een sentiment. Coosto en OBI4wan doen de sentiment analyse automatisch. Buzzcapture claimt dat het naast automatisch labelen ook nog aan het handmatig vaststellen van het sentiment, door medewerkers van het bedrijf doet. Het bedrijf stelt dat halverwege 2014 6,5 miljoen berichten in haar database zaten die handmatig waren gelabeld. Van een archief

dat sinds 2007 is aangelegd met miljoenen berichten die dagelijks worden verzameld is dat slechts een fractie.

Cathy O'Neil, Amerikaanse wiskundige en schrijfster van het boek Weapons of Math Destruction, trekt een parallel tussen het social media archief van de reputatiemanagement bedrijven en de historische data over algoritmen in het algemeen. Die historische data over algoritmen roepen vragen op over het succes van die algoritmen.

In het artikel *How can we stop algorithms telling lies?* In *The Guardian* van juli 2017 verwijst zij naar de financiële crisis van 2007/2008 en het enthousiasme over het gebruik van algoritmen in de financiële sector dat aan de crisis voorafging. "Financial risk models also use historical market changes to predict cataclysmic events in a more global sense, so not for an individual stock but rather for an entire market. The risk model for mortgage-backed securities was famously bad – intentionally so – and the trust in those models can be blamed for much of the scale and subsequent damage wrought by the 2008 financial crisis."

Politie-algoritmen

De vragen die O'Neil oproept zijn legitiem. Hoe werken de algoritmen en kunnen we ze vertrouwen? Begrijpen de bedrijven die sentiment analyse aanbieden de algoritmen zelf nog wel? Deze vraag is mede relevant omdat sommige bedrijven de technologie verhuren aan andere bedrijven. HowAboutYou huurt OBI4wan in. Buzzcapture huurt de technologie in van Coosto en TextKernel in. Vervolgens huurt de Nederlandse politie HowAboutYou en Buzzcapture weer in.

Het is duidelijk dat de politie samenwerkt met reputatiemanagement bedrijven. Uit de openbaar geworden documenten blijkt tevens dat de politie sentiment analyse gebruikt voor social media surveillance. In het rapport van de politie-eenheid Zeeland-West-Brabant van 18 februari 2015 over de ervaring met het gebruik van OBI4wan staan in "bijlage 1 eisen aan de online media monitor" bij "rapportages maken" dat de tool ingericht kan worden naar de wensen van de

politie. Volgens het rapport gaat het om allerlei aspecten waaronder "analyses van afzenders, locatie (kaartje), wanneer er over de zoekopdracht veel gesproken wordt, volumes, webcare status, gebruikers, bronsoorten, afhandelsnelheid, invloed van afzenders, sentiment".

Sentiment analyse is opgenomen in de tool en kan ook handmatig worden aangepast. Het rapport stelt tevens dat bij de social media monitoring de "metadata die beschikbaar zijn, worden opgeslagen bij het originele bericht". Het rapport vervolgt: "Daarnaast verrijken wij het bericht met metadata uit eigen analyses, zoals de belangrijkste woorden in een bericht, het sentiment, locatiegegevens en gegevens over de afzender."

De afdeling persvoorlichting van de politie eenheid Zeeland-West-Brabant ziet gescoord sentiment als een relevante functionaliteit. "Visualisaties van volumes, gerelateerde topics, sentiment, influencers en gesprekslocaties vertellen het online verhaal" staat in de paragraaf basisfuncties van de tool. Bij aanvullende werkafspraken wordt het belang van sentiment analyse opnieuw onderstreept: "Tijdens het monitoren blijft het relevant en noodzakelijk om toch alle berichten te scannen op inhoud, relevantie en sentiment." In het rapport blijkt dat naast de persvoorlichters, de politie-infodesk, het RTIC en de opsporing de sentiment analyse gebruiken.

"De Infodesk is servicepunt voor informatieverzoeken van verschillende afdelingen binnen de politie-eenheid Zeeland - West-Brabant", is de eerste zin van hoofdstuk 5 van het rapport van de politie eenheid Zeeland-West-Brabant. "De monitor gebruiken collega's vooral voor openbare orde, handhaving en strafrechtelijke onderzoeken (evenementen/demonstraties, opsporingsvragen, dreigingsinschatting, mensenhandel, enzovoort). Zaken waarbij online media voor de Infodesk van toegevoegde waarde is, zijn onder andere: Inzicht krijgen in netwerken van personen, kennisbron voor interesses, bewegingen en sentimenten rond personen voor omgevingsbeelden bij een incident; regie voeren op thema's (motorclubs, overvallen, inbraken, enzovoort)."

Hoeveel inzicht heeft de politie in de zoektechnologie en de sentiment analyse en daarmee de profilering van de bedrijven? Kan

de politie de zoekopdracht, de sentiment analyse van berichten en de profilering middels die gelabelde berichten nabootsen om te achterhalen waarom iemand als verdachte of potentieel gevaar wordt aangemerkt? In de openbaar gemaakte documenten naar aanleiding van de Wob verzoeken van Buro Jansen & Janssen staat niets over de aanwezigheid van deze kennis bij de politie of de Nationaal Coördinator Terrorisme en Veiligheid (NCTV).

Voor de sentiment analyse worden veel data door social media monitoring bedrijven verzameld. De bedrijven hebben daartoe grote databanken aangelegd met veel historisch materiaal. De politie gebruikt die historische gegevens, blijkt uit de openbaar gemaakte documenten. Dit staat op gespannen voet met wetgeving ten aanzien van de bescherming van persoonsgegevens.

Databanken vol Nederlanders en geen controle

Gebruikers van online media en social media weten niet dat hun berichten, meningen en opinies worden verzameld door deze social media surveillance bedrijven. Het gaat ook om persoonlijke informatie over woon- en verblijfplaats, werk, familieomstandigheden en allerlei andere tot de persoon herleidbare gegevens die gebruikers op het internet delen.

De gegevens die Coosto, OBI4wan, HowAboutYou en Buzzcapture verzamelen zijn persoonsgegevens. De bedrijven bevestigen dit in hun privacy verklaringen. Ook de Autoriteit Persoonsgegevens gaat er vanuit dat de online en social media gegevens die worden verzameld persoonsgegevens zijn. “De AP heeft geen onderzoek gedaan naar deze bedrijven, maar gaat er in algemene zin van uit dat gegevens die van sociale media worden verzameld in veel gevallen persoonsgegevens zijn als bedoeld in artikel 1, onder a, van de Wet bescherming persoonsgegevens (Wbp). Dit omdat de gegevens direct of indirect herleidbaar zijn naar natuurlijke personen, ofwel rechtstreeks via hun sociale media-account, of indirect, via de verantwoordelijken voor deze sociale netwerksites. Voorzover de door u genoemde bedrijven de inhoud van berichten verzamelen, al dan niet in combinatie met locaties, connecties en

persoonlijke interesses, hebben de gegevens betrekking op natuurlijke personen."

Aan het bewaren en het verwerken van persoonsgegevens worden wettelijke voorwaarden gesteld. De Autoriteit Persoonsgegevens verwijst naar *Beleidsregels publicatie van persoonsgegevens op internet uit 2007*. Hierin staan geen expliciete bewaartermijnen, maar wel staat vermeld dat "gegevens niet langer mogen verwijzen naar identificeerbare personen dan strikt noodzakelijk en de gegevens moeten juist zijn en ter zake dienend". In antwoord op vragen van Buro Jansen & Janssen over de archieven van de social media monitoring bedrijven antwoordt de Autoriteit Persoonsgegevens: "Het feit dat persoonsgegevens op internet staan, betekent niet dat ze zomaar opnieuw gebruikt mogen worden in een andere context, voor een ander doeleinde. … Zelfs als het nieuwe doel verenigbaar is met het oude doel, kan de verwerking onrechtmatig zijn."

Hoewel de Autoriteit Persoonsgegevens aangeeft geen zelfstandig onderzoek te hebben gedaan, stelt men wel dat: "bedrijven die de persoonsgegevens verzamelen van sociale media, een zelfstandige grondslag dienen te hebben voor de (verdere) verwerking, en er zorg voor moeten dragen dat de gegevens niet verouderd en niet onjuist zijn. Dat betekent ook dat deze bedrijven de gegevens niet langer mogen bewaren dan noodzakelijk voor het behalen van de gerechtvaardigde doeleinden die zij nastreven."

Geen van de reputatiemanagement bedrijven heeft het verwerken van persoonsgegevens gemeld bij de Autoriteit Persoonsgegevens (en haar voorganger het College Bescherming Persoonsgegevens). Tevens worden de bedrijven al tien jaar niet gecontroleerd door de bevoegde instantie, de Autoriteit Persoonsgegevens over bijvoorbeeld de verwerking van persoonsgegevens, de duur van het bewaren van de gegevens en de sentiment analyse.

OBI4wan stelt op vragen van Buro Jansen & Janssen dat zij recentelijk haar "privacy verklaring heeft aangepast op de nieuwe wetgeving" en dat "wij voldoen of gaan wij voldoen aan toekomstige wetgeving". Het bedrijf spreekt ook over "interne en externe audits" in haar privacyverklaring. Coosto spreekt in haar privacyverklaring over "toegangsbeveiliging, encryptie, monitoring en auditing,

periodieke penetratietests, scans op potentiële kwetsbaarheden en certificeringen". In de privacy verklaring van Buzzcapture staat hier niets over. De privacy verklaringen vermelden niet of de controles betrekking hebben op het verwerken van persoonsgegevens, de bewaarduur, de samenwerking met de overheid of de sentiment analyse.

De Autoriteit Persoonsgegevens ziet het niet als haar prioriteit om op te treden, geeft zij in haar antwoord aan Buro Jansen & Janssen aan. "De Autoriteit Persoonsgegevens beschouwt uw brief als een belangrijk signaal", schrijft het bestuursorgaan, maar "de Autoriteit Persoonsgegevens ontvangt jaarlijks duizenden tips en meldingen en moet daarom een selectie maken welke zij nader onderzoekt". De Autoriteit Persoonsgegevens maakt niet duidelijk of zij de genoemde bedrijven zal aanschrijven.

Dat controle op databanken noodzakelijk is blijkt uit een rapport van het College bescherming persoonsgegevens (de voorganger van Autoriteit Persoonsgegevens) van juni 2012. Het College deed onderzoek naar databanken van de Criminele Inlichtingen Eenheden (CIE's) van de politie. Die databanken zitten vol met gegevens, waaronder gegevens verkregen via informanten en infiltranten, geruchten en OSINT. Het is niet duidelijk of deze inlichtingen betrouwbaar zijn. Het gaat om informatie over vermeende criminele activiteiten, dus om burgers die nog niet verdacht zijn, maar dat op basis van de informatie wel kunnen worden. Onbetrouwbare informatie kan grote gevolgen hebben voor deze mensen.

Het CBP was van mening dat de CIE's van de regionale politiekorpsen Flevoland en Brabant Zuid-Oost "onvoldoende maatregelen hebben getroffen om de wettelijke eisen omtrent bewaartermijnen van politiegegevens na te leven. Daarmee handelen zij in strijd met de wet". De kritiek richtte zich op zowel het gebrek aan een jaarlijkse controle of de gegevens nog relevant zijn en bewaard dienen te blijven, als op het overschrijden van de maximale bewaartermijn van vijf jaar. De kritiek op de korpsen leidde eind 2013 tot het opleggen van een dwangsom door het CBP

omdat de politie de aanbevelingen van het College nog niet had opgevolgd.

ARBIT

De politie mag dus niet ongelimiteerd persoonsgegevens verzamelen, verwerken en bewaren. Haar beleid ten aanzien van opslag en verwerking van persoonsgegevens is wettelijk geregeld. Er vinden jaarlijkse audits plaats en er zijn maximum bewaartermijnen. Door gebruik te maken van de diensten van Coosto, OBI4wan, HowAboutYou en Buzzcapture omzeilt de politie deze wettelijke beperkingen. Zelfs door gebruikers verwijderde berichten op social media zijn gewoon terug te vinden in de databases van de social media monitoring bedrijven. Samenwerking met private IT-bedrijven is echter ook gebonden aan wet- en regelgeving, ook bij inhuur door de politie en de NCTV.

Van Coosto is bekend dat zij voor het werk voor de NCTV de standaard Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT) heeft ondertekend. De politie heeft deze ARBIT overeenkomsten die ze zou moeten sluiten met Coosto, OBI4wan, HowAboutYOU en Buzzcapture niet openbaar gemaakt. De verwerking van de persoonsgegevens en de veiligheid van de archieven wordt volgens de overheid geregeld door de ARBIT, Algemene Rijksvoorwaarden bij IT-overeenkomsten, die een kader scheppen voor de digitale veiligheid van de persoonsgegevens.

In artikel 18 komt de verwerking van persoonsgegevens aan bod. Deze moet op “behoorlijke en zorgvuldige wijze en in overeenstemming met de toepasselijke wet- en regelgeving” gebeuren. Tevens is in de ARBIT opgenomen dat er geen “onnodige verzameling en verdere verwerking van persoonsgegevens” plaatsvindt. Dit laatste artikel verwijst naar de *Beleidsregels publicatie van persoonsgegevens op internet uit 2007* van de Autoriteit Persoonsgegevens, die aangeeft dat gegevens niet “zomaar opnieuw mogen worden gebruikt”, dat er een “zelfstandige grondslag” moet zijn voor verwerking en gegevens “niet verouderd en onjuist” zijn. Uit de via de Wob openbaar gemaakte documenten

blijkt niet dat politie en de NCTV de bedrijven op deze aspecten hebben gecontroleerd.

Gebrek aan transparantie

Buro Jansen & Janssen heeft geprobeerd meer helderheid te krijgen over social media surveillance door politie en de NCTV. In 2016 vroeg Buro Jansen & Janssen via Wob-verzoeken documenten op over de bedrijven Coosto, Buzzcapture, OBI4wan en HowAboutYou, en over "nep account of schaduw accounts op sociale media of het internet in het algemeen", "het programma SMPP", het "Advies rapport ten aanzien van de evaluatie van het operationele gebruik van diverse social media monitoring tools op diverse afdelingen" en "de namen of bedrijven van diverse social media monitoring tools of online media monitoring tools (of vergelijkbare namen) waarmee de politie op diverse afdelingen de afgelopen jaren heeft geëxperimenteerd".

De politie maakte een rapport over het gebruik van OBI4wan door de politie-eenheid Zeeland-West- Brabant openbaar (*Online media monitoring: tool en proces (2)*). Ook werden enkele losse documenten over een proef met het gebruik van de tools van OBI4wan/ HowAboutYou bij de landelijke eenheid, de eenheid Zeeland-West- Brabant en de eenheid Den Haag verstrekt. HowAboutYou wordt in verschillende documenten als verantwoordelijke en contactpersoon voor de proef met OBI4wan genoemd. In 2017, ruim een half jaar na de verzoeken, maakte de politie documenten over Buzzcapture (een offerte aanvraag en offertes) en twee algemene documenten, het *Project Initiatie Document (PID)* en het *IM Adviesrapport* openbaar. De politie weigert documenten over Coosto openbaar te maken.

In 2017 diende Buro Jansen & Janssen vervolgens nieuwe verzoeken in over de relatie tussen de Nederlandse politie en de Amerikaanse social media monitoring bedrijven SnapTrends en Geofeedia, de Canadese bedrijven Media Sonar en Hootsuite en de Nederlandse bedrijven Meltwater, iMonitoring, Teezir en Tracebuzz. Tevens is Buro Jansen & Janssen bekend met het bestaan van andere documenten. Daar is in 2017 ook naar gevraagd. Het gaat om

Project Initiatie Document OSINT 2011 Open source intelligence mei 2011, Toepassingsdocument social media 2013-2015, Position paper OSINT in de Informatieorganisatie, Nationale Politie (PIO, SMPP), Nederland 2015, Open bronnen tools inwinning: Troonswisseling Nationale Politie Eenheid Amsterdam (CIO, DRI) Nederland 2013 / Referentiemodel Bedrijfsprocessen Politie (RBP2012), Verbeteren van Politie Processen (VVP), Online media monitoring: tool én proces, Nationale Politie Eenheid Zeeland West-Brabant, Nederland, 2014 / RTIC medewerkers (evaluaties), Nationale Politie, diverse eenheden, Nederland, 2014 en 2015, OSINT medewerkers (evaluaties), Nationale Politie, diverse eenheden, Nederland, 2014 en 2015 en Internetrechercheurs (evaluaties), Nationale Politie, diverse eenheden, Nederland, 2015. Deze documenten zijn nog niet openbaar gemaakt.

Verontrustend en opmerkelijk

Ondanks de weinig transparante houding van de overheid is aan de hand van allerlei bronnen en via de Wob openbaar gemaakte documenten, die via de Wob zijn verkregen, de social media surveillance in beeld gebracht. De politie werkt met verschillende reputatiemanagement bedrijven samen. De bedrijven Coosto, Obi4wan en HowAboutYou worden ingehuurd door de politie voor zowel communicatie als Real Time Intelligence Centers en opsporing. Buzzcapture is voor zover bekend alleen voor communicatie voor de Nationale Politie ingehuurd.

In het verleden werkte de politie aan een eigen tool die specifiek gericht was op de opsporing. Uit de openbaar gemaakte documenten blijkt dat de politie deze tool, iColumbo/IRN, wil ombouwen voor online en social media surveillance, dus niet meer exclusief voor de opsporing. Uit de openbaar gemaakte documenten blijkt niet of de ontwikkeling van die eigen tool wordt voortgezet. De commerciële tools kunnen dus worden ingehuurd in afwachting van de oplevering van de eigen tool, iColumbo/IRN, of vanwege de grote hoeveelheid historische data waarover de bedrijven beschikken en de toegevoegde waarde van de sentiment analyse.

In zowel het PID document project SMPP van 2013 als het evaluatiedocument van 2015 die via Wob-verzoeken van Buro Jansen & Janssen openbaar zijn geworden, wordt met geen woord gesproken over de consequenties van het inhuren van private bedrijven. Vragen met betrekking tot de grote historische archieven van de bedrijven, de kennis over de werking van de tools, de broncode, sentiment analyse en algoritmen komen in geen van de documenten aan bod. Ook in de stukken die openbaar zijn gemaakt door het ministerie van Veiligheid en Justitie over het gebruik van Coosto komen deze aspecten niet aan de orde.

De politie huurt private partijen in die informatie aanbieden voor surveillance, opsporing en het scoren van burgers, maar controle op de bewaartermijnen van de persoonsgegevens, de verwerking van die gegevens en audits van de kwaliteit en nauwkeurigheid van de databanken zijn niet beschikbaar. De bedrijven hebben de verwerking van de persoonsgegevens nooit aangemeld bij bevoegde instanties.

Het is opmerkelijk dat de politie en de NCTV geen informatie hebben over de consequenties van het inhuren van private partijen voor social media surveillance. Daarnaast is het verontrustend dat in de documenten met geen woord wordt gesproken over de mogelijke schendingen van grondrechten zoals de vrijheid van meningsuiting, het recht op manifestatie en de vrijheid van vergadering. De politie en de NCTV gaat rechtsstatelijke vragen uit de weg terwijl social media surveillance op gespannen voet staat met de rechtstaat.

Dagelijkse en structurele monitoring
De Nederlandse politie en social media surveillance (pdf)

Gehele Observant #70 social media surveillance in Nederland (pdf)

Andere artikelen

Social Media Surveillance in Nederland

Reputatie management bedrijven, de nieuwe private inlichtingendiensten

De burger als dreigingsscore; Social media surveillance in de Verenigde Staten

Overgeleverd aan de grillen van social media multinationals; Facebook en Twitter en de Nederlandse social media surveillance

Verder lezen

Meer dan 200.000 professionals doen maar wat tegen terrorisme

Bijlagen

Politie

presentatie Inge Hoogstad RTIC (pdf)

politie besluit OBI4wan HowAboutYou (pdf)

politie besluit OBI4wan online media monitoring tool en proces (pdf)

PID social media in de operationele politie processen (pdf)

politie besluit IM adviesrapport tools informatieorganisatie (pdf)

politie besluit Buzzcapture (pdf)

politie besluit nep accounts presentatie (pdf)

Ministerie van Veiligheid en Justitie

besluit ministerie van V en J Coosto Buzzcapture primair (pdf)

besluit ministerie van V en J Coosto Buzzcapture bij bezwaar (pdf)

Autoriteit Persoonsgegevens

persoonsgegevens_op_internet_2007 (pdf)

brief aan Autoriteit Persoonsgegevens (pdf)

aanvullende brief aan Autoriteit Persoonsgegevens (pdf)

Autoriteit Persoonsgegevens antwoord (pdf)

Naar inhoudsopgave Observant #70

Reputatiemanagement bedrijven, de nieuwe private inlichtingendiensten

De Nederlandse politie doet aan social media surveillance en werkt hierin samen met de social media monitoring bedrijven Coosto, OBI4wan en HowAboutYou. Dit blijkt uit onderzoek van Buro Jansen & Janssen.

De Nederlandse bedrijven Coosto, OBI4wan, HowAboutYou, Buzzcapture bieden monitoring tools aan op het terrein van reputatiemanagement of webcare. Deze worden afgenomen door bedrijven en overheidsorganen die negatieve publiciteit willen tegengaan. Essentieel onderdeel van het reputatiemanagement is de sentiment analyse. Bedrijven verzamelen data die worden voorzien van een label goed/positief, slecht/negatief en neutraal. De labels dienen om de publiciteit over een product of dienst te volgen. Daarbij gaat het natuurlijk vooral om negatieve berichtgeving, waar een producent snel op wil reageren.

Reputatiemanagement is dus risicomanagement. Om risico's te vermijden worden zoveel mogelijk gegevens van online en social media verzameld. Coosto, OBI4wan, HowAboutYou, Buzzcapture verzamelen data met zoekmachines die het internet afspeuren. De gegevens komen in principe van open bronnen: informatie die door bedrijven en individuen op het internet wordt gedeeld. Zij bewaren die data in archieven in Nederland. Enkele van deze bedrijven hebben een archief van internet data dat terug gaat tot 2007 of 2009. In deze databanken wordt alle informatie die de bedrijven verzamelen bewaard, ook informatie die mensen later van hun social media account hebben verwijderd.

Coosto, OBI4wan, HowAboutYou en Buzzcapture borduren voort op de traditie van private inlichtingendiensten. Deze schimmige bedrijven werden eind vorige eeuw en begin deze eeuw vooral ingehuurd door multinationals om actiegroepen die campagnes tegen die bedrijven voerden in de gaten te houden. Gaandeweg werden de private inlichtingendiensten ook ingehuurd door politie,

inlichtingendiensten van de overheid en ministeries. Met de komst van social media en uitgebreide mogelijkheden internet data te verzamelen ontstonden social media monitoring of reputatiemanagement bedrijven. De Nederlandse politie en de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) huren de diensten van bedrijven als Coosto, OBI4wan en HowAboutYou in. Niet alleen voor communicatiedoeleneinden, maar ook voor social media surveillance.

Inlichtingen verzamelen van AIVD naar politie

Op grote schaal inlichtingen verzamelen uit open bronnen is van oudsher één van de hoofdtaken van inlichtingendiensten. Zo verzamelt de Nederlandse Algemene Inlichtingen- en Veiligheidsdienst (AIVD) op grote schaal informatie over niet-verdachte burgers. Ten tijde van de Koude Oorlog werden allerlei organisaties en individuen in de gaten gehouden, waarvan men maar enigszins dacht dat ze communistische sympathieën hadden. Veel van hen stonden kritisch tegenover overheden of het bedrijfsleven. De meeste informatie die inlichtingendiensten verzamelen bestaat uit openbare informatie, zoals kranten, tijdschriften, flyers, posters. In het verleden ging het vooral om papieren materiaal, tegenwoordig merendeels digitaal.

Naast open bronnen verzamelen inlichtingendiensten ook informatie uit gesloten bronnen. Dit kunnen gegevens zijn die worden verkregen via een tap bij internetproviders of telefoonmaatschappijen, maar ook gegevens van energie- en waterleidingbedrijven, gemeentelijke diensten en woningbouwverenigingen, of informatie verkregen via informanten, infiltranten en afluisterapparatuur.

Ook de politie verzamelt inlichtingen, al was dat lange tijd op veel kleinere schaal dan inlichtingendiensten. Bij de politie stond inlichtingen verzamelen in het algemeen in het licht van opsporingsonderzoeken en de TCI, het Team Criminele Inlichtingen (de huidige naam voor de Criminele Inlichtingen Eenheden), die geruchten uit het criminele circuit al dan niet via informanten en

infiltranten in kaart brengt. Ook de RID's, de Regionale InlichtingenDiensten, verzamelen informatie over voetbalsupporters, demonstranten en kraakpanden in het kader van de handhaving van de openbare orde. De politie heeft zich de laatste jaren steeds meer gericht op het verzamelen van inlichtingen.

Algemene Beveiligings Consultancy

Lange tijd was inlichtingen verzamelen een staatsaangelegenheid. Voor private partijen was een eigen inlichtingendienst een te kostbaar middel. Multinationals hadden die mogelijkheden wel. In de jaren negentig kwamen de eerste verhalen bovendrijven van private inlichtingenbureaus die werden ingehuurd door multinationals. Buro Jansen & Janssen publiceerde in 1994 een onderzoek naar het bedrijf Algemene Beveiligings Consultancy (ABC) te Vinkeveen. ABC was van Peter Siebelt die zich vanaf eind jaren zeventig met zijn bedrijf Siebelt BV al presenteerde als veiligheidsadviseur.

Met ABC haalde Siebelt onder andere oud papier op bij verschillende organisaties, waaronder de waarnemersdelegatie van de Parlementariërs tegen Apartheid (Awepa) die de verkiezingen in Zuid-Afrika volgde, en de Werkgroep Medische Ontwikkelingssamenwerking (WEMOS). Van beide organisaties doken plotseling interne documenten op in de publiciteit. Siebelt verzamelde het oud papier en verkocht dit door aan de Telegraaf die zich fel keerde tegen de Awepa, en aan Nutricia (tegenwoordig Numico) dat de kritische houding van WEMOS wilde bestrijden. ABC zette ook informanten in die als vrijwilligers aan de slag gingen bij Ngo's om informatie te verzamelen. In 1994 ontmaskerde Buro Jansen & Janssen in dat kader Paul Oosterbeek, die als vrijwilliger werkte onder meer bij Osaci (Oecumenisch Studie- en Actiecentrum voor Investeringen) en het Schone Kleren Overleg.

In 1998 was het opnieuw raak toen Adrian Franks voor het bedrijf Risk Crisis Analyses ASEED, een Nederlandse milieuorganisatie, bespioneerde. Het bleek dat Franks ook in andere Europese landen was geïnfiltreerd in actiegroepen om zo notulen en andere documenten te verzamelen. Adrian Franks probeerde die informatie

te verkopen aan bedrijven. Vijf jaar later bleek dat Franks opnieuw aan de slag was gegaan voor het Britse bedrijf Threat Response International en bij vredesgroepen infiltreerde.

Hij verkocht de informatie over de activiteiten van Campaign Against Arms Trade (CAAT) aan British Aerospace (BAE), een grote speler in de militaire industrie. The Sunday Times maakte openbaar dat Threat Response International vier jaar lang een dagelijks rapport aan BAE Systems stuurde voor een bedrag van 120.000 pond (in die tijd ongeveer 190.000 euro). De rapporten waren voor een groot deel gebaseerd op rapportages van Adrian Franks, die bij de Campaign Against Arms Trade was geïnfiltreerd. De rapporten bevatten daarnaast informatie uit tijdschriften, kranten en andere openbare bronnen.

Global Open Limited

In 2010 kwam een andere inlichtingenbedrijf in het nieuws. Het Britse Global Open Limited had voormalig politieagent Mark Kennedy ingehuurd om voor het Duitse energie bedrijf E.ON te infiltreren in milieuorganisaties om acties bij vervuilende energiecentrales te voorkomen. Kennedy infiltreerde eerder voor de Britse politie in de milieubeweging en had verschillende relaties met vrouwelijke activisten die niets van zijn undercover werk wisten. Die relaties zorgden voor een snelle carrière in de actiewereld. Na zijn vertrek bij de politie zette hij een eigen bedrijf op: Tokra. Het was op hetzelfde adres geregistreerd als de toenmalige directeur van Global Open Limited, Heather Mary Millgate.

Global Open Unlimited werd begin 2001 opgezet door een voormalig politieagent. Het bedrijf hield zich net als Algemene Beveiligings Consultancy, Risk Crisis Analyses en Threat Response International bezig met het verzamelen en doorverkopen van inlichtingen. Naast het verzamelen en ordenen van openbare informatie, zette het bedrijf ook infiltranten in.

ABC en Threat Response International hadden vooral bedrijven als klant, en hadden voor zover bekend geen contact met de politie en inlichtingendiensten. Global Open wist wel door te dringen tot

opsporings- en inlichtingendiensten. De reden hiervoor kan gelegen hebben in het feit dat Global Open geleid werd door Rod Leeming, een voormalig Special Branch agent. "Global Open Limited was founded in the United Kingdom and is run by former New Scotland Yard Special Branch officers," stond op de website van het bedrijf vermeld .

Ook de Nederlandse politie was klant van Global Open. Naar aanleiding van een Wob/WIV verzoek van Buro Jansen & Janssen zijn in 2017 200 pagina´s door de AIVD openbaar gemaakt. De documenten maken duidelijk dat de politieregio Gelderland Midden tussen 2007 en 2009 de zogenaamde Weekly Digest van het bedrijf ontving. De Regionale Inlichtingendienst (RID) bestelde de weekberichten van Global Open in het kader van onderzoeken naar dierenrechtenactivisten. Een groot deel van de samengestelde knipselkranten gaat over acties gerelateerd aan dierenrechten.

Stratfor

Het bedrijf Stratfor wist nog grotere klanten binnen te slepen met een knipselkrant vergelijkbaar met de Weekly Digest van Global Open. Stratfor voegde aan de verzamelde berichten ook een ´intelligence analyse´ toe. Stratfor had veel klanten bij grote bedrijven, ministeries, opsporingsdiensten, waaronder het Amerikaanse leger, politie en inlichtingendiensten en de Nederlandse ministeries van Binnenlandse Zaken (AIVD), Economische Zaken en Buitenlandse Zaken. Kennis over de klantenkring van Stratfor is in 2011 naar buiten gekomen door een hack die ervoor zorgde dat de gegevens van honderdduizenden abonnees en klanten openbaar werden. Stratfor werd gehackt door Jeremy Hammond die hiervoor in 2013 werd veroordeeld tot tien jaar gevangenisstraf.

Stratfor is op het eerste gezicht een gewoon bedrijf met Nederlandse en Amerikaanse bestuursorganen als klanten. Het bedrijf verzamelt data, die opnieuw worden geïndexeerd, van een analyse voorzien en doorverkocht. Stratfor presenteert zich echter iets chiquer dan Global Open. Het doet zich voor als een internationaal kennis instituut, een ´geopolitical intelligence platform´. Stratfor beweert

klanten inzicht geven in een complexe wereld: “To empower members to confidently understand and navigate a continuously changing and complex global environment.”

Global Open richtte zich expliciet op toekomstige klanten die onder vuur zouden kunnen komen te liggen van kritische burgers. “Companies currently being targeted by activists require fast access to information in order to avoid the effects of economic sabotage and personal harassment,” aldus de website van het bedrijf. De anti-globaliseringsbeweging, milieuorganisaties en dierenrechtengroepen werden door Global Open als mogelijk problematisch voor bedrijven omschreven.

Stratfor is minder expliciet als het gaat om het in de gaten houden van burgerrechtenbewegingen, actiegroepen en protestbewegingen, het bedrijf wil zich duidelijk niet afficheren met bedrijven als Global Open. Uit de hack van 2011 blijkt echter dat het bij hun diensten niet alleen gaat om het leveren van informatie over aanslagen, maar ook over actiegroepen en demonstranten. In 2001 omschrijft Barron´s Financial Investment News het bedrijf dan ook als ‘the Shadow CIA’, de Amerikaanse inlichtingendienst Central Intelligence Agency.

Evolutie van de private inlichtingendiensten

De ontwikkeling van de private inlichtingenbedrijven van de jaren tachtig tot ongeveer 2010 is er één van verdergaande acceptatie van deze bedrijven door overheden. Algemene Beveiligings Consultancy, Risk Crisis Analyses en Threat Response International waren private inlichtingendiensten, maar enigszins obscuur. Siebelt vond wel gehoor bij Nutricia. Threat Response International werd ingehuurd door een grote speler binnen de militaire industrie, BAE Systems. Global Open wist begin deze eeuw al een groot energie bedrijf (E.ON) en politiediensten als klant te werven, en Stratfor zelfs enkele Nederlandse ministeries. Rode draad bij de private inlichtingenbedrijven is dat hun slachtoffers altijd mensen zijn die een kritisch geluid laten horen over de bedrijven die hun klanten zijn.

De acceptatie van private inlichtingenbedrijven is met het reputatiemanagement een nieuwe fase in gegaan. Na de eeuwwisseling is het verzamelen van inlichtingen in een hoog tempo gedigitaliseerd. De reputatiemanagement bedrijven hebben van die online en social media data sinds ongeveer 2007 hun handelswaar gemaakt. Verzamelde data worden bewaard, geïndexeerd en doorzoekbaar gemaakt. De zogenaamde sentiment analyse van de verzamelde persoonsgegevens speelt een belangrijke rol in de dienstverlening van de reputatiemanagement bedrijven.

Sentiment analyse

Bij sentiment analyse worden online en social media berichten gelabeld als positief, negatief of neutraal. Ieder bericht krijgt zo een stempel en samen met het aantal volgers, vrienden, retweets, berichten die overgenomen zijn en andere aspecten met betrekking tot de invloed en het sentiment van de auteur kan een profiel van de burger worden gemaakt. Volgens een factsheet over Coosto staat in dat profiel onder andere de "auteur (profiel), invloed auteur, bronnen, invloed bron, bereik bron/site, sociaal netwerk, invloed, sentiment" (Coosto factsheet in de Social media monitoring en webcare tools 2014). Een dergelijk profiel is van groot belang om te beoordelen of de imagoschade mogelijk grote gevolgen kan hebben.

De social media monitoring bedrijven presenteren hun diensten als een service. Het gaat om het verbeteren van de communicatie met de klant of de burger, zoals het afhandelen van vragen, klachten, feedback en informatie. Snelle online communicatie beoogt assertieve burgers snel van dienst te zijn en slechte publiciteit niet lang te laten voortwoekeren.

Social media surveillance

Doelwit van de oude private inlichtingendiensten mensen en groepen die kritisch waren over bedrijven. Kranten en tijdschriften werden uitgeplozen over hun meningen en indien nodig werden papier- en

vuilnisbakken doorzocht of informanten ingezet. De bedrijven die de inlichtingen kochten wisten soms niet waar die vandaan kwamen, maar hadden daar in het algemeen geen interesse in. Net als de afnemers van de reputatietools geen inzicht hebben in de herkomst van de data en de broncode (de precieze werking/technische details) van de sentiment analyse of de zoekmachines.

Tegenwoordig wordt de kritische burger en iedereen die op het internet actief is uit online en sociale media gevist. De sentiment analyse is onderdeel van de screening die de social media monitoring bedrijven uitvoeren. De verzamelde informatie en bijbehorende diensten worden net als in het verleden aangeboden aan bedrijven en overheidsdiensten. Social media monitoring bedrijven hebben de activiteiten van de private inlichtingendiensten omgevormd tot social media surveillance. Daarom toont de overheid zoveel interesse in de tools.

De basis van de social media surveillance zijn, naast live meekijken, de archieven van de bedrijven die bestaan uit grote hoeveelheden data met informatie over woon- en verblijfplaats, werk en andere persoonsgegevens. De bedrijven hebben geen toegang tot overheidsdatabanken als de Gemeentelijke Basisadministratie (GBA), maar veel basisgegevens over burgers kunnen ook worden verzameld via Facebook, Instagram, Google Streetview en Earth, Twitter en andere online diensten. Naast deze basisgegevens verzamelen de bedrijven ook allerlei berichten, meningen, opmerkingen, likes en andere meningsuitingen van burgers op het internet.

Reputatiemanagement bedrijven zijn in tegenstelling tot hun voorgangers (de private inlichtingendiensten) geaccepteerd. Was het twintig jaar geleden ondenkbaar dat Greenpeace een bedrijf als ABC of Global Open zou inhuren, tegenwoordig gebruikt de milieuorganisatie de social media monitoring tool van Coosto. Ook de Consumentenbond maakt gebruik van Coosto. Oxfam Novib huurt OBI4waan. Vice media Buzzcapture. Ook de Nederlandse politie en de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) huren Coosto, OBI4wan, HowAboutYou en Buzzcapture in.

Die acceptatie blijkt uit de ontwikkelingen van de social media monitoring bedrijven waarbij universiteiten ook een belangrijke rol hebben gespeeld zoals blijkt uit de profielen van die bedrijven. Buzzcapture werkt samen met de Universiteit Utrecht. SiteData BV staat aan de oorsprong van OBI4wan en is op de campus van de Technische Universiteit Eindhoven gevestigd. HowAboutYou werkt weer nauw samen met OBI4wan. En Coosto komt voort uit Wiseguys Internet BV dat nauwe banden heeft met de Technische Universiteit Eindhoven.

WiseGuys Internet BV

Het moeder bedrijf van Coosto is WiseGuys Internet BV (Wg Holding B.V.). De website van het bedrijf bevat alleen een contactformulier. De pagina's 'about wiseguys, products en read full story' zijn leeg. Op LinkedIn staat dat het bedrijf gespecialiseerd is in "spider/webcrawler and search technology as well as data mining", ofwel het verzamelen van internet data en die doorzoekbaar maken. Het bedrijf is niet groot, opgericht in 1999 en gevestigd op het terrein van de Technische Universiteit Eindhoven.

De mensen achter WiseGuys Internet BV zijn sinds de jaren negentig actief in het ontwikkelen van de zoekmachine Track. In 1996 ging Toine Verheul met zijn bedrijf Radar Internet samenwerken met enkele studenten van de Technische Universiteit Eindhoven en Universiteit van Tilburg. Vier studenten schreven de software en Verheul wist als zakelijk leider uitgever Wegener Arcade in 1997 te overtuigen om de zoekmachine Track.nl te kopen. Verheul stapte ook direct over naar Koninklijke Wegener NV, een uitgever van regionale dagbladen, huis-aan-huisbladen en tijdschriften, die 2015 werd overgenomen door het Belgische mediabedrijf De Persgroep.

In 1999 wordt WiseGuys Internet BV opgericht door onder andere Verheul. Al die tijd hebben de ontwikkelaars van Track verder aan de zoekmachine gesleuteld. Frank Scheelen, een student in de jaren negentig die meewerkte aan de ontwikkeling van Track, geeft dat tegen voelspriet.nl medewerker Henk van Es in 2001 aan: "Track verandert vooralsnog alleen de indexeer- en zoeksoftware. Het

spideren, gebeurt op dit moment nog met dezelfde spiders die WiseGuys al langer gebruikten voor het vullen van de Track database.” Hoeveel data WiseGuys Internet BV al in 2002 verzamelde geeft Scheelen in een interview in het Reformatorisch Dagblad aan. "De laatste keer kregen we, nadat we alle dubbele pagina's eruit gegooid hadden, 200 gigabyte aan data binnen.” In hetzelfde jaar, 2002, lanceert WiseGuys Internet BV een nieuwe zoekmachine Kobala.

Met spiders bedoelt Scheelen programma´s die lijken op browsers als Firefox, Chrome of Internet Explorer, maar die webpagina’s niet alleen opzoeken maar ook downloaden. Daarnaast gebruiken de bedrijven ook crawlers die op internetpagina’s op zoek gaan naar de verschillende links en die vervolgens ook bezoeken. In de Tech industrie worden de woorden spider en crawler vaak door elkaar gebruikt. Daarnaast wordt ook het woord robot gebruikt. Meestal verwijst dit naar de automatisering van zowel het zoeken op het internet, het opslaan, het crawlen en het indexeren van de opgeslagen pagina’s.

Wiseguys Internet BV leidt een betrekkelijk anoniem bestaan. In 2003 komt het bedrijf nog even in het nieuws omdat adverteerders voor geld een toppositie in de zoekresultaten kopen. Verheul zegt op emerce.nl dat “het idee om de resultaten te verkopen uit nood is geboren. De markt dwingt ons om met dergelijke oplossingen te komen.” Emerce schrijft in het artikel ´Zoekmachine Track verkoopt toppositie´ op 15 mei 2003: “adverteerders invloed laten uitoefenen op de rangschikking wordt traditiegetrouw afgekeurd door de meeste zoekmachines, de ‘objectiviteit’ van de zoekresultaten is voor de meesten nog heilig.”

WiseGuys Internet BV blijft zich richten op zoektechnologie en ontwikkelt ook zoekmachines voor Freeler, Ben, Genie en RDnet (Reformatorisch Dagblad net). De basis van alle zoekmachines van WiseGuys Internet BV vormt het programma Kobala. Scheelen beschrijft het proces van de zoekmachine in het Reformatorisch Dagblad van 21 mei 2002: “We gebruiken daarvoor een spider, een complex computerprogramma dat de tekst uit al die internetpagina's op onze harde schijven zet. … We beginnen met webdirectories, sites die veel verwijzingen naar andere pagina's bevatten."

WiseGuys Internet BV heeft de webcrawler Vagabondo (zwerver) genoemd.

Het ontstaan van Coosto

Met de zoektechnologie van Kobala ontwikkelt WiseGuys Internet BV een nieuwe tool: Bluescope. Bluescope is de voorloper van de reputatiemanagement tool Coosto die in 2010 op de markt werd gezet door het bedrijf Coosto, een dochter firma van WiseGuys Internet BV. WiseGuys Internet BV omschrijft BlueScope als een "een nieuwe vorm van automatische webanalyse die u helpt om de internetpositie van uw bedrijf en uw concurrenten in kaart te brengen."

Eind 2002 koopt het internetbedrijf Ilse (Ilse Media) de broncode van de zoekspider van WiseGuys Internet BV. Ilse Media, begin deze eeuw één van de voornaamste zoekmachines in Nederland is in 2001 overgenomen door Sanoma Media, eigenaar van onder andere nu.nl. Voor WiseGuys Internet BV was de zoektechnologie voor zoekmachines als gevolg van de opkomst van Google een markt waar niet veel meer te verdienen was. Wiseguys Internet BV richtte zich daarom met BlueScope op dienstverlening door middel van reputatiemanagement voor het bedrijfsleven.

Op 30 augustus 2010 presenteren de voormalig ontwikkelaars van de zoekmachine Track Rob de Wit en Frank Scheelen en zakelijk leider van WiseGuys Internet BV Toine Verheul de social media monitoring tool en het bedrijf Coosto. "We spideren de hele dag door. Dan heb je ook de linkstructuur en kun je kijken wie naar wie linkt. Dat kan een virtual host zijn, of een eigen host waar het blog op draait," vertellen de oprichters aan emerce.nl. Coosto beweert ook meteen dat ze "de grootste aantallen van bijvoorbeeld de WordPress-blogs hebben." Daarbij zou het niet alleen om nl domeinen (websites die eindigen op .nl) gaan, maar ook om org domeinen (websites die eindigen op .org). Het bedrijf zoekt dus niet

exclusief in Nederlandse sites. Dit blijkt ook twee jaar later wanneer het bedrijf in het Verenigd Koninkrijk uitbreidt.

Inlichtingen databank Coosto, eens getweet altijd bewaard

In 2010 zeggen De Wit, Scheelen en Verheul, de mannen achter Coosto, dat zij al dagelijks spideren: het internet afzoeken naar data. Ze vertellen er echter in het interview met emerce.nl niet bij dit ze dat al vanaf de jaren negentig doen, en voor Coosto sinds 1 januari 2009. Retecool (redacteur Ome MC) publiceert in juni 2016 een Coosto Open Factsheet waarin staat dat het historisch archief terugloopt tot januari 2009. Dit komt overeen met de gegevens uit de ´Uitgebreide verkenning van de Nederlandse markt voor online monitoring- en webcaretools´ van de bedrijven Upstream en Repmen van november 2012: ”Volume aan data, historisch archief vanaf januari 2009 (onafhankelijk van zoekterm), flexibele snelle manier van zoeken, diepgaande data-analyse.”

In 2012 geven de eigenaren van Coosto aan het Eindhovens Dagblad ook aan dat ze allerlei informatie verzamelen over mensen in Nederland, zoals data over hoe oud hun keuken of cv-ketel is, en dat ze de data ook doorverkopen aan de politie. “Het bedrijf slaat onder meer informatie op over woningen en vacatures. De data (ook over details als ouderdom van cv-ketels, keukens e.d.) worden doorverkocht. Een deel is ook bestemd voor opsporingsdiensten. Die kunnen een archief doorzoeken waarvan de opbouw begon in januari 2009,” aldus De Wit, Scheelen en Verheul in het Eindhovens Dagblad van 4 oktober 2012.

Retecool publiceerde een factsheet van Coosto naar aanleiding van een artikel van RTLZ, ´Op bezoek bij @NS_online: de 'meest gehate mensen' van Nederland´, over het social media team van de Nederlandse Spoorwegen. De NS gebruikt ook de social media monitoring tool Coosto. In het artikel van RTLZ stelt de auteur dat hij ooit eens “een vervelende tweet over NS” geschreven had.” Het blijkt dat de tweet door de sociale media afdeling van de NS nog ingezien kan worden: “De webcare medewerker leest die tweet voor. Ondanks dat deze tweet al tijden geleden is verwijderd.”

In een disclaimer van Coosto staat dat “het bedrijf niet aansprakelijk is voor onjuistheden of onvolledigheden in de aangeboden inhoud.” En klanten van Coosto vrijwaren “het bedrijf … van gerechtelijke en buitengerechtelijke maatregelen en de kosten daarvan.” Het verwijderde Twitter bericht van RTLZ journalist Daniël Verlaan is onderdeel van de disclaimer.

Coosto is de afgelopen jaren een groter bedrijf geworden dan het moederbedrijf WiseGuys Internet BV. Bij het bedrijf werken nu meer dan honderd mensen, waaronder systeembeheerders, ontwikkelaars, data scientists en hitmen. Volgens de Vastgoedcourant van april 2016 zou Coosto werkzaam zijn voor “meer dan 600 bedrijven.” Niet alleen de Nederlandse Spoorwegen, Greenpeace en de Consumentenbond maken gebruik van Coosto. Ook Natuurmonumenten, Ziggo, Microsoft, FNV, CBS, Belastingdienst, ANWB, KWF Kankerbestrijding, Achmea Zorg en andere bedrijven en instellingen.

Overheidsorganen waaronder de politie en de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) behoren ook tot de klantenkring. Zij hebben ook toegang tot een grote database van persoonsgegevens van het bedrijf en gebruiken Coosto voor social media surveillance. De politie heeft geen documenten openbaar gemaakt over de samenwerking met Coosto, de NCTV wel en omschrijft de diensten van Coosto als “webmonitoring/webanalysefunctionaliteiten en webcarefunctionaliteiten.”

Coosto en de overheid

Het imago van Coosto leidt in 2013 even onder de negatieve publiciteit over het moederbedrijf WiseGuys Internet BV. De Telegraaf kopt op 18 september 2013 met ‘Overheid doet zaken met pornoboer.’ Het dagblad schrijft: “Wie zoekt naar seks met dieren, met oma’s of zelfs naar gewelddadige verkrachtingen, komt bij de website askjolene.com goed aan zijn trekken. Vele duizenden filmpjes, verhalen en pornowebcams worden er in de meest bizarre rubrieken gepresenteerd.” Twee dagen later worden er Kamervragen gesteld over het belang van WiseGuys in AJ Beheer B.V., het bedrijf dat de exploitatie verzorgt van de website AskJolene.com.

Op 18 september 2013 reageert algemeen directeur Toine Verheul van Coosto en WiseGuys Internet BV op de beschuldigingen. Verheul stelt op het blog van Coosto dat het bedrijf "in het verleden een belang heeft gehad in de erotische zoekdienst AskJolene.com." Het bedrijf heeft een dag eerder op 17 september 2013 haar aandeel in AJ Beheer BV verkocht, volgens een persbericht van Coosto.

Over het gebruik van Coosto door de politie worden in 2013 geen verdere Kamervragen gesteld. In de beantwoording van de Kamervragen schrijft de minister voor Wonen en Rijksdienst Blok dat "de politie en de ministeries alleen gebruik maken van de zoektechnologie van Coosto om binnen sociale netwerken te zoeken in openbare bronnen. Voor de ministeries is dit een activiteit vergelijkbaar met het maken van een knipselkrant. De ministeries voeren echter zelf het onderzoek uit." Uit de antwoorden wordt niet duidelijk wat de minister onder openbare bronnen en openbare bronnen op sociale netwerken verstaat.

Minister Blok bagatelliseert het werk van Coosto door de databank te vergelijken met een knipselkrant. In een publicatie van Upstream / Repmen de ´Monitoring- & webcaretools 2012 gids voor het managen van de online dialoog,´ stelt Coosto in 2013 dat zij gegevens van Twitter, Facebook, LinkedIn, Hyves en Google+ constant doorzoekt en opslaat. De knipselkrant van Blok bevat gedetailleerde informatie van Nederlandse burgers, met onder andere de naam van de auteur, locatie en andere persoonsgegevens die sinds 1 januari 2009 door het bedrijf worden bewaard. Ook door burgers verwijderde berichten worden bewaard door Coosto.

In antwoorden op vragen van Buro Jansen & Janssen verwijst Coosto naar haar privacyverklaring en wenst het bedrijf geen uitspraken te doen over haar klanten en haar betrokkenheid bij social media surveillance. "Gezien de onderwerpen in uw mail zal ik deze beantwoorden. We vinden het belangrijk om hier transparant over te zijn. Er zijn ook zaken, zoals aangeven wie er nu wel of niet klant is dan wel is geweest, welke we niet mogen delen omdat we

dit met onze opdrachtgevers hebben afgesproken," schrijft het bedrijf.

Buzzcapture

Buzzcapture is in 2006 opgezet door politicoloog Alex van Leeuwen. In een interview in NRC Handelsblad van 1 augustus 2007 zegt hij dat het bedrijf zich "niet alleen bezig houdt met het in kaart brengen van klachten." De politicoloog gaat verder door te stellen dat "bedrijven vaak ook willen weten hoe ze hun dienstverlening kunnen verbeteren." Dat het bedrijf geen gewoon PR-bedrijf is maar zich als inlichtingenbedrijf presenteert, blijkt uit de woordkeuze. "Wij houden 600.000 Nederlandstalige weblogs in de gaten," zegt van Leeuwen.

Buzzcapture houdt echter niet alleen sites in de gaten, maar leest ook mee. "Per merk of dienst lezen we ook relevante discussieforums." Buzzcapture lijkt verder te gaan dan Coosto door ook deel te nemen aan online discussies. "Op verzoek nemen medewerkers van Buzzcapture ook deel aan discussies op weblogs en forums," aldus van Leeuwen. Dit lijkt op het inzetten van informanten/infiltranten door de oude private inlichtingendiensten alleen in een nieuw jasje gegoten, de undercover accounts. Van Leeuwen geeft in antwoord op vragen van Buro Jansen & Janssen in augustus 2017 echter aan geen gebruik te maken van ´schaduw/nepaccounts.´

Buzzcapture houdt niet alleen weblogs in de gaten maar verzamelt en bewaart net als Cosoto ook data. Buzzcapture is hier echter twee jaar eerder mee begonnen dan Coosto. "Doordat Buzzcapture vanaf 2007 een archief heeft opgebouwd van alles wat online en op social media wordt gepost, kunnen we voor het eerst data vergelijken voorafgaand aan de gemeenteraadsverkiezingen. In 2010 was dit nog niet mogelijk," schrijft Jaap van Zessen, voormalig Social Media Analist van Buzzcapture, trots op 18 maart 2014 op de website van het bedrijf.

Van Zessen suggereert dus dat het bedrijf al sinds 2007 persoonsgegevens verzamelt en dat Buzzcapture misschien de gemeenteraadsverkiezingen van 2014 kan voorspellen. Volledig naar

analogie met de knipselkrant van minister Blok schrijft van Zessen dat "Buzzcapture het online archief afstofte en op zoek ging naar data in de eigen tool." Van Zessen bedoelt met afstoffen dat het bedrijf in 2014 alle data van de afgelopen jaren ging gebruiken voor het voorspellen van de gemeenteraadsverkiezingen van 2014.

Volgens van Leeuwen gebruikt Buzzcapture naast technologie ook medewerkers om de verzamelde data te analyseren en te interpreteren. Buzzcapture gebruikt de 'spider' van WiseGuys Internet BV en een andere technische tool, een semantische zoekmachine van Textkernel. In een artikel op emerc.nl van 18 april 2007 geeft van Leeuwen aan dat zijn bedrijf de twee technologieën van Wiseguys Internet BV en Textkernel aan elkaar koppelt.

In antwoord op vragen van Buro Jansen & Janssen in augustus 2017 stelt Buzzcapture dat zij "geen data beschikbaar aan Nederlandse opsporings- en inlichtingendiensten" stellen en tevens "geen oplossing voor opsporing of surveillance" bieden. De directeur van het bedrijf, Alex van Leeuwen, gaat verder door te stellen dat de "dienstverlening zich beperkt tot het faciliteren van corporate communicatie en webcare afdelingen." Uit openbaar gemaakte documenten naar aanleiding van Wob verzoeken van Buro Jansen & Janssen blijkt dat Buzzcapture de communicatie van de Nationale Politie verzorgt. De politie vraagt om "realtime social media analyseren, inzicht in sentimenten, geolocatie, stakeholders, en toegang tot historie/archief."

Universiteiten: Data van scholen

De technologie achter de software van Coosto is in de jaren negentig ontwikkeld door vier studenten van de Technische Universiteit Eindhoven en de Universiteit van Tilburg: Robert Brouwer, Pim van Pelt, Frank Scheelen en Rob de Wit. De laatste twee zijn anno 2017 nog werkzaam bij Coosto. Robert Brouwer is vertrokken naar Oracle en Pim van Pelt naar Google.

Het is opvallend dat meerdere universiteiten een relatie hebben met social media monitoring bedrijven. Coosto en Wiseguys Internet BV waren nauw verbonden met de Universiteit Tilburg en vooral de

Universiteit van Eindhoven, zowel wat betreft de ontwikkeling van de zoekmachine/spider/crawler als wat betreft het vestigingsadres. De Technische Universiteit Eindhoven noemt Coosto in haar campus folder: "Al ruim dertig jaar initieert en faciliteert de TU/e daarom startende bedrijven. Dat leidde tot het ontstaan van meer dan 150 technologiebedrijven, waaronder succesvolle namen zoals: Prodrive, Coosto, Xeltis en Flowid." Ook SiteData BV, het bedrijf waaruit OBI4wan uit voortkomt, is gevestigd op de campus van de Technische Universiteit Eindhoven.

Thomas Boeschoten van de Universiteit Utrecht werkt samen met Buzzcapture dat door de universiteit wordt gepresenteerd als technische partner. Boeschoten gebruikt bij zijn experiment rond de Nuclear Security Summit (NSS) data van Buzzcapture, die volgens het artikel 'Plaats delict: social media' van Vrij Nederland van 18 april 2014 door het bedrijf zijn verzameld. "Het bedrijf Buzzcapture heeft al wekenlang alle tweets en Facebook-updates verzameld en voor de deelnemers in een database gezet." Boeschoten zegt in het artikel niet dat Buzzcapture in 2014 al een database met gegevens van online en social media over Nederlandse burgers van zeven jaar heeft.

Boeschoten wordt door Vrij Nederland gepresenteerd als 'een deskundige op het gebied van social media en dataverwerking.' In 2014 leidt hij een experiment om met behulp van social media monitoring de ontwikkelingen rond de NSS in de gaten te houden. Bij het experiment schuiven politiemensen aan. Hierdoor ontstaat het idee dat het gaat om handhaving van de openbare orde. Dat blijkt ook uit het artikel in Vrij Nederland. Het gaat vooral over het in de gaten houden van burgers en actiegroepen die zich kritisch hebben uitgelaten over de NSS, met daardoor gevolgen voor zowel burgerrechten als bewegingsvrijheid van die burgers. Buro Jansen & Janssen heeft al eerder geschreven over het ontbreken van het demonstratierecht tijdens de NSS.

Dat social media surveillance ook wordt ingezet bij onder andere demonstraties blijkt ook uit de openbaar gemaakte documenten naar aanleiding van de Wob-verzoek van Buro Jansen & Janssen. Zo is de tool van OBI4wan door de politie eenheid Zeeland-West-Brabant ingezet tegen een pro-Gaza demonstratie. Bij de inzet van social media surveillance zijn duidelijk grondrechten als de vrijheid

van meningsuiting en de vrijheid van demonstratie in het geding. Opmerkelijk genoeg plaatst Boeschoten van de Universiteit Utrecht hier zelf ook vraagtekens bij. In het Vrij Nederland artikel merkt Boeschoten op: "Het gekke is: als ik het zelf doe, vind ik het helemaal niet eng, maar als ik bedenk dat anderen het ook kunnen doen, vind ik het wel verontrustend. Dergelijke netwerkanalyses worden pas echt boeiend als je de informatie koppelt aan metadata die niet openbaar toegankelijk is, als je bijvoorbeeld op hetzelfde moment kunt zien wie met wie belt. Of wie naar wie privéberichten stuurt, zoals de NSA en het Britse GCHQ dat kunnen." Boeschoten doelt met de verwijzing naar de NSA en GCHQ op de massale surveillance die door de onthullingen van Edward Snowden aan het licht kwam.

De social media monitoring tools kunnen echter ook al veel. Zo beschikt Buzzcapture over ongeveer dezelfde bronnen en mogelijkheden als Coosto. In het factsheet uit de ´Monitoring- en webcaretools´ van november 2014 van Upstream geeft het bedrijf aan dat zij de volgende bronnen rond de klok monitort: "print, nieuws, fora, blogs, websites video (Youtube), radio/TV, twitter, Facebook, Instagram, Pinterest, Linkedin, Google+ en Hyves." Het bedrijf geeft aan dat er historische analyses gemaakt kunnen worden "van data voorafgaand aan de datum waarop je de tool bent gaan gebruiken." Daarnaast staat bij analyse en selectiemogelijkheden onder andere: "de auteur (profiel), de invloed van auteur, de locatie (GPS/Geo), likes/RT's/Favorites, sociale netwerk, sentiment."

Naast Coosto en Buzzcapture, doet de politie in ieder geval zaken met twee andere social media monitoring bedrijven, OBI4wan en HowAboutYou. Deze bedrijven beschikken over vergelijkbare mogelijkheden en bronnen.

OBI4wan

Het Zaanse bedrijf OBI4wan is opgericht in 2011, maar is al sinds 2009 actief met het verzamelen van online en social media data, reputatiemanagement en webcare. OBI4wan komt voort uit het bedrijf SiteData B.V. dat in 2001 werd opgezet door Alex Slatman.

In dat jaar begon Slatman met de studie Information Retrieval aan de Radboud Universiteit Nijmegen die hij in 2006 afrondde. Slatman werkte tijdens zijn studietijd aan de ontwikkeling van een eigen spider. Vervolgens was hij in 2006 kort werkzaam voor Ilse Media, dat vier jaar eerder een samenwerking was aangegaan met WiseGuys Internet B.V.

Volgens de website van SiteData biedt het bedrijf vanaf 2007 "een breed scala aan producten aan die bijdragen aan een betere vindbaarheid voor uw website." Daarnaast is SiteData ook "actief op het gebied van datamining en information retrieval." SiteData biedt een imago management aan dat er vanuit gaat dat ranking in zoekmachines de strijd met de concurrentie beslechten. Vandaar ook dat het bedrijf diensten aanbiedt als "positiemeting (op basis van zoektermen bekijken wij hoe goed u te vinden bent in Google) en concurrentiecheck (op deze manier kunt u snel zien op welke termen u beter of slechter scoort ten opzichte van uw concurrentie!)."

SiteData is gevestigd op het terrein van de Technische Universiteit Eindhoven. In 2010 ontmoette Slatman Alexander de Ruijter, een consultant met een eigen bedrijf in voorlichting over gebruik van sociale media in het bedrijfsleven. Het klikte tussen Slatman en de Ruijter en in 2011 beginnen zij OBI4wan dat zich richt op reputatiemanagement en webcare.

Bij de lancering van Obi4wan in 2011 waren er drie klanten: ECI, EnergieDirect en Arriva. In 2012 komen daar verschillende nieuwe klanten bij, waaronder de eenheid Zeeland-West-Brabant van de Nationale Politie. Het LinkedIn bedrijfsprofiel van OBI4wan vermeldt: "Sinds 2009 worden alle relevante berichten verzameld van bekende social media platformen en miljoenen (inter)nationale blogs, fora en nieuwsbronnen. Aangevuld met innovatieve oplossingen voor radio-, tv- en printmonitoring mis je nooit meer een relevant bericht!" Het bedrijf verzuimt hier overigens te vermelden dat het ook data van LinkedIn verzamelt.

De data die OBI4wan verzamelt komen van ´400.000 Nederlandstalige bronnen´ schrijft het bedrijf in een presentatie in 2014 (In 2012 waren dit er nog 350.000). OBI4wan gebruikt vergelijkbare bronnen als Coosto en Buzzcapture. Het gaat om radio en TV, nieuwspagina´s, fora, blogs, Youtube en andere video sites,

afbeeldingen platformen, Twitter, Facebook, en andere social media platformen.

HowAboutYou

HowAboutYou is een zelfstandig reputatiemanagement bedrijf, maar richt zich volledig op de inzet van de OBI4wan tool. OBI4wan geeft in de factsheet uit de ´Monitoring- en Webcaretools´ van november 2014 van Upstream aan dat het samenwerkt met HowAboutYou, Engagement Media, Red Banana en Wisse Kommunikatie. Dat OBI4wan nauw samenwerkt met HowAboutYou blijkt ook uit documenten die door de politie openbaar zijn gemaakt over de twee bedrijven. Op haar website schrijft HowAboutYou over OBI4wan: "Een goede mediamonitor helpt enorm. Wij kiezen voor OBI4wan."

HowAboutYou werd in 2010 opgericht. Op de eerste website van het bedrijf in juni 2011 worden Ewoud de Voogd, Paul Suijkerbuijk en Frank Bruijninckx vermeld als de drijvende krachten. Bij de nominatie van het bedrijf voor de 'Grote nieuwe organiseren prijs' ("De prijs is voor de persoon of organisatie die het beste het gedachtegoed van nieuw organiseren belichaamt en realiseert," aldus nieuworganiseren.nu) in 2014 staat dat Voogd en Bruijninckx "merkten dat de overheidscommunicatie niet aansloot op de huidige tijd." HowAboutYou ging zich dan ook richten op de overheid.

Op haar LinkedIn pagina stelt het bedrijf uit het Gelderse Rossum dat het zich bezighoudt met de ondersteuning van "ruim 300 overheden bij de inzet van social media, webcare & monitoring met OBI4wan, omgevingsanalyses, issue- en reputatiemanagement en online campagnes." Op de website van het bedrijf staan de namen van 179 gemeenten, zes provincies en bijna alle veiligheidsregio's (brandweer, geneeskundige diensten gemeenten en politie) vermeld als klant van HowAboutYou.

In een memo van 17 september 2013 aan het Kernteam social media politie Zeeland-West-Brabant gebruikt het bedrijf de kop ´HowAboutYou heeft ervaring met het ondersteunen van (politie-)processen.´ Volgens HowAboutYou moet "een online media monitor niet alleen aan technische functionele eisen voldoen

(zoektermen aanmaken, reageren) maar ook ondersteuning bieden bij de processen van de organisatie zoals opsporing, intelligence, participatie- en beleidsvormingstrajecten. De eerder opgenomen tabel biedt een overzicht van processen die de online media monitor ondersteunt." HowAboutYou gebruikt OBI4wan, maar op haar website en uit de openbaar gemaakte stukken wordt niet duidelijk of het bedrijf kennis heeft over de technische werking van de tool, de sentiment analyse, en het historisch archief.

In dezelfde memo 'Voorstel opzet proef online media monitoring en webcare' schrijft het bedrijf dat het allerlei ervaring heeft op het terrein van veiligheid. "HowAboutYou werkt op online media monitoring en vooral de aanpak en organisatie daarvan samen met de gemeenten Breda, Tilburg (oa ook de TaskForce Tilburg Veilig), … en de veiligheidsregio Midden-West-Brabant." De memo vermeldt tevens: "HowAboutYou ondersteunde met media-analyses bij de brand in Oosterhout en het TGO na de rellen in Haren met rechercheonderzoeken op de online media."

Archieven zijn Big Business

De Nationale Politie en de Nationaal Coordinator Terrorisme en Veiligheid (NCTV) werken samen met Coosto, OBI4wan, HowAboutYou en Buzzcapture. De politie gebruikt de diensten van de bedrijven niet alleen voor haar eigen communicatiebeleid (Buzzcapture) en de contacten met burgers, maar ook voor ondersteuning bij meldingen, aangiften, handhaving, Real Time Intelligence Center en opsporing (Coosto, OBI4wan en HowAboutYou). In 2013 antwoordde de minister voor Wonen en Rijksdienst Blok dat de politie en de ministeries slechts gebruikmaakten van de zoektechnologie van Coosto. Uit de Wob-stukken blijkt echter dat Coosto, evenals OBI4wan en HowAboutYou, wordt ingezet voor social media surveillance.

Die interesse in de databanken en de social media monitoring tools komt niet alleen van de overheid, maar ook van investeerders. Dat blijkt uit ontwikkelingen in de Verenigde Staten en in Nederland. In de Verenigde Staten werkt het social media monitoring bedrijf Geofeedia samen met een internationaal bedrijf, Everbridge, om

haar marktbereik te vergroten. Een ander bedrijf Snaptrends werkt samen met een groot private military contractor Chenega. De tools en databanken zijn belangrijke bezittingen van de bedrijven. Zo is het Amerikaanse Intrado overgenomen door het grote beursgenoteerde West Corporation, en vervolgens West Corporation door het hedgefonds Apollo Global Management.

De ontwikkelingen van internationalisering en overnames zijn ook in Nederland zichtbaar, maar vooralsnog op beperkte schaal. De eerste overname vond plaats in 2017 toen Buzzcapture werd overgenomen door OBI4wan. Buzzcapture probeert zelf het nieuws positiever te brengen door te stellen dat 'OBI4wan en Buzzcapture krachten bundelen.' Die overname word gefinancierd door Main Capital Partners B.V., een Nederlandse investeerder in de IT industrie. Regelmatig verkoopt het zijn belangen door aan grotere investeerders, dit kan in de toekomst dus ook gebeuren met het meerderheidsaandeel in OBI4wan.

OBI4wan was voor de overname van Buzzcapture een betrekkelijk kleine speler. De overname kwam echter niet als een verrassing omdat het bedrijf al in juli 2016 in zee was gegaan met Main Capital. De investeerder schrijft op haar website dat "Main Capital OBI4wan en OBILytics actief gaat ondersteunen met de internationale groei en de uitbouw van de productportfolio, onder meer door selectieve internationale acquisities." Main Capital omschrijft OBI4 wan als een snelgroeiend bedrijf. Naast kennis en inzicht over de analyse-tools zal OBI4wan interesse hebben gehad in de klanten en de grotere database van Buzzcapture. Gezien de ontwikkelingen in de Verenigde Staten en Nederland is het reëel dat de archieven van de Nederlandse social media monitoring bedrijven op termijn in buitenlandse handen terecht komen.

Overheidssteun social media surveillance industrie

Ook overheden maken onderdeel uit van de social media surveillance industrie. Niet alleen als afnemers van de diensten, maar tevens als geldschieter. In de Verenigde Staten is bekend geworden dat diverse social media monitoring bedrijven zoals Geofeedia, Pathar en Dataminr worden gefinancierd door de

investeringsmaatschappij van de CIA: In-Q-Tel (In-Q-It). In hoeverre de CIA toegang heeft tot de data van die bedrijven, is niet bekend.

Of de Nederlandse inlichtingendiensten investeren in social media monitoring bedrijven als Coosto, OBI4wan en Buzzcapture wordt niet duidelijk uit de documenten. Wel op andere manieren is er overheidssteun voor de social media surveillance industrie.

Universiteiten ondersteunen de ontwikkeling van tools om online en social media gegevens te verzamelen en op te slaan. Ook wordt aan startups huisvesting aangeboden op campussen van universiteiten. Zo breidde Coosto in 2015 uit naar 150 talen en financierde dit uit eigen middelen. Het bedrijf was in staat dit te doen omdat het een een groot deel van haar bestaan geholpen is door de TU Eindhoven die Coosto als startup op de campus liet groeien.

Ook het Ministerie van Veiligheid en Justitie heeft Coosto financieel ondersteund door in 2011 geen aanbesteding te doen, losse accounts af te nemen en vervolgens de aanbestedingsgrens te overschrijden. De Nationaal Coördinator Terrorisme en Veiligheid (NCTV) wilde de tool van Coosto blijven gebruiken terwijl de aanbestedingsgrens was overschreden, blijkt uit openbaar gemaakte documenten via een Wob-verzoek van Buro Jansen & Janssen bij het ministerie van Veiligheid en Justitie. De aanbestedingsgrens is de grens waarboven publiek opdrachten openlijk moeten worden gedaan, zodat ieder bedrijf kan meedingen naar die opdracht.

In 2013 schrijft een ambtenaar van het ministerie van Veiligheid en Justitie nog: “Binnen de kaders van het recent gewijzigde inkoopbeleid van VenJ c.q. Rijksbreed zie ik, na controle, geen beperkingen om de overeenkomst met Coosto te verlengen. Het VenJ inkoopbeleid schrijft voor dat er pas boven de 50K concurrentie gesteld dient te worden zie bijlage.” Het contract dat het ministerie met Coosto sloot was een “vierjarige overeenkomst met een eventuele verlenging voor het jaar 2016.” Dit herhaalt zich in 2014. In 2015 gaan de alarmbellen rinkelen.

Op 28 april 2015 schrijft een ambtenaar: een “volgende verlenging zal er voor zorgen dat de grens voor Europees aanbesteden bereikt gaat worden.” Het contract van de NCTV loopt af op 31 december

2015. Toch is het ministerie Coosto blijven gebruiken hoewel in de correspondentie van februari 2016 staat dat het "allemaal moeilijker dan gedacht wordt want, jawel, we gaan met de factuur die nog betaald moet worden dit jaar de aanbestedingsgrens over. Dat betekent dat we de factuur die nu nog ligt niet kunnen betalen." Er wordt geconcludeerd dat er voor 2016 "al een nota onrechtmatigheid opgesteld moet worden."

Hoewel het ministerie verschillende documenten openbaar heeft gemaakt is er nog veel geheim. Uit de openbaar gemaakte documenten blijkt dat de NCTV in 2016 en in 2017 Coosto is blijven gebruiken. Op 17 april 2017 meldt een ambtenaar: "Coosto schijnt handig overal losse accountjes te verkopen en het is waarschijnlijker goedkoper om één aanbesteding te doen." Niet alleen via het vermijden van de aanbesteding, maar ook via extra accounts ondersteunt het ministerie van Veiligheid en Justitie Coosto.

Transparantie bij Surveillance

De social media monitoring tools worden door de politie en de NCTV ingezet voor social media surveillance doeleinden. Uit openbaar gemaakte documenten wordt duidelijk dat Coosto, Obi4wan en HowAboutYou hiervoor zijn ingezet. Over Buzzcapture is dit niet bekend. HowAboutYou heeft geen eigen technologie en gebruikt exclusief OBI4wan. Buro Jansen & Janssen heeft de betreffende bedrijven gevraagd naar de samenwerking met politie en de NCTV.

Twee vragen hadden expliciet betrekking op de samenwerking. "Werkt of werkte u samen met de Nationale politie?" En "wordt of werd de tool van u door de NCTV gebruikt?" Daarnaast vroeg Buro Jansen & Janssen naar de inzet van de tools. "Wij begrijpen dat uw tool bij de politie is ingezet bij in ieder geval het RTIC, opsporing en andere processen. Is dit juist of niet? Ziet u deze overheidsactiviteiten als surveillance van burgers door de overheid?" Tevens vroeg Buro Jansen & Janssen naar de archieven en de verwerking van persoonsgegevens. " U heeft een databank die teruggaat tot 2007/2009. Ziet u die data als persoonsgegevens? Hebt u de verwerking van die persoonsgegevens aangemeld bij de bevoegde instanties en wanneer en wordt daar een regelmatige

audit op uitgevoerd? Houdt u zich aan de wettelijke bewaartermijnen? Wordt informatie die door burgers op online en sociale media zelf wordt verwijderd ook uit uw archief verwijderd?" Tot slot vroeg Buro Jansen & Janssen naar de sentiment analyse en nep- of schaduwaccounts. "In uw tool maakt u gebruik van een zogenaamde sentiment analyse. Maken de politie en de NCTV ook gebruik van die sentiment analyse? Hoe nauwkeurig is die? Is er wetenschappelijk onderzoek dat die nauwkeurigheid bevestigd? Is dat openbaar?" En "Maakt u gebruik van nepaccounts op social media platformen om informatie te verzamelen? Of spreekt u van schaduwaccounts?"

Buzzcapture is zeer stellig door te antwoorden dat het "geen data beschikbaar stelt aan Nederlandse opsporings- en inlichtingendiensten en geen oplossing bieden voor opsporing of surveillance." Het bedrijf geeft aan dat het slechts tools levert voor "corporate communicatie en webcare." "Onze oplossingen worden niet door NCTV gebruikt. Onze oplossing worden ook niet voor opsporing- of inlichtingendiensten gebruikt," stelt het bedrijf.
De Nationale Politie gebruikt Buzzcapture voor communicatiedoeleinden, en de politie wil daartoe "realtime social media analyseren, inzicht in sentimenten, geolocatie, stakeholders, en toegang tot historie/archief," blijkt uit openbaar gemaakte documenten. Uit de bedrijfsgegevens blijkt tevens dat Buzzcapture wel degelijk sentiment analyse en een historisch archief aanbiedt, data die teruggaan tot 2007. Het bedrijf stelt ook nog dat ze "communicatieafdelingen inzicht geven in wat er speelt rond hun organisatie in de publieke sfeer."

OBI4wan antwoordt dat hun reputatiemanagement en webcare tools "niet bedoeld zijn voor surveillance van individuen en daar ook niet voor gebruikt mogen worden." Het bedrijf zegt dat zij geen uitspraak mag doen over het al dan niet samenwerken met de Nationale Politie. Of OBI4wan tools dus door de politie voor social media surveillance doeleinden wordt gebruikt laat het bedrijf in het midden. Op de vraag of de tool van het bedrijf wordt ingezet bij het RTIC, de opsporing en of het bedrijf deze overheidsactiviteiten ziet als surveillance van burgers, antwoordt OBI4wan dat zij daar "geen uitspraak over doen." Het bedrijf antwoordt nog wel dat zij "geen data meer aanbieden die terug gaan tot 2009," maar of de politie toegang heeft tot historische data laat het bedrijf ook in het midden.

Uit de openbaar gemaakte documenten blijkt dat de politie daar wel toegang toe heeft. OBI4wan is het enige bedrijf da ingaat op de vraag over de sentiment analyse. Het bedrijf antwoordt, “niet van toepassing.”

Transparantie van Coosto

Coosto antwoordt dat het bedrijf transparant wil zijn over de samenwerking met de overheid en social media surveillance. Het bedrijf verwijst naar haar privacyverklaring. “Zaken zoals de doorgifte van data aan derden en rechten die over de verzamelde data uitgeoefend kunnen worden, worden hierin tevens besproken,” schrijft het bedrijf. Daarnaast verwijst Coosto naar haar persbericht van 29 juni 2017 waarin het bedrijf stelt dat het zich in de toekomst aan de voorwaarden van de social media platforms gaat houden. Het bedrijf schrijft in antwoord op vragen van Buro Jansen & Janssen dat in dat persbericht zij “hun standpunt rondom surveillance delen.” In het persbericht geeft Coosto echter niet haar eigen standpunt ten aanzien van surveillance, maar dat van Facebook. “For example, the current conditions of Facebook state that Facebook data can’t be used for surveillance purposes.”
Het bedrijf antwoordt ook niet op de vraag of het voor de politie en de NCTV werkt. Coosto sluit de korte e/mail naar aanleiding van vragen van Buro Jansen & Janssen af met de opmerking dat het bedrijf “de voorwaarden van onze partners volgen (zoals Twitter en Facebook etc.) in combinatie met ons moreel kompas en regelgeving.”

Buro Jansen & Janssen heeft ook Wob verzoeken ingediend bij zowel de politie als het Ministerie van Veiligheid en Justitie over de samenwerking met Coosto. Het Ministerie informeerde Buro Jansen & Janssen dat een belanghebbende in december 2016 een zienswijze op de openbaar te maken documenten had ingediend. De ambtenaar van het ministerie gaf telefonisch aan dat de indruk bestond dat deze belanghebbende tegenstander van openbaarmaking van documenten was. Deze belanghebbende kondigde aan ook in bezwaar te gaan tegen de beslissing van het ministerie om de stukken openbaar te maken.

Bij de Wob verzoeken ging het naast Coosto om enkele andere bedrijven. De documenten die het ministerie uiteindelijk openbaar maakte hadden in het algemeen betrekking op Coosto. Op 17 augustus 2017, bij het bezwaar op de beslissing, maakte het ministerie bekend dat Coosto op 15 februari 2017 een zienswijze had ingediend. Coosto heeft uiteindelijk geen bezwaar ingediend. Coosto verzette zich dus in eerste instantie tegen openbaarmaking.

Social media surveillance is een publiek private samenwerking. De politie en de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) zijn afhankelijk van commerciële tools die beschikbaar worden gesteld door bedrijven als Coosto, OBI4wan, HowAboutYou en Buzzcapture. Alle vier de tools worden gebruikt voor communicatie doeleinden. Van Coosto, OBI4wan en HowAboutYou is ook bekend dat de politie en de NCTV ze gebruikt voor social media surveillance en de opsporing.

Daar waar in het verleden private inlichtingendiensten werden gezien als enigszins obscuur, zijn reputatiemanagement of risicomanagement bedrijven volledig geaccepteerd. Zij worden door diverse overheidsorganen ingehuurd. Het feit echter dat bedrijven en de overheid weinig transparant zijn over social media surveillance geeft aan dat er in twintig jaar niet veel is veranderd. De reputatiemanagement bedrijven verschillen niet van de obscure private inlichtingendiensten uit het verleden.

Reputatie management bedrijven, de nieuwe private inlichtingendiensten (pdf)

Gehele Observant #70 social media surveillance in Nederland (pdf)

Andere artikelen

Social Media Surveillance in Nederland

Dagelijkse en structurele monitoring; De Nederlandse politie en social media surveillance

De burger als dreigingsscore; Social media surveillance in de Verenigde Staten

Overgeleverd aan de grillen van social media multinationals; Facebook en Twitter en de Nederlandse social media surveillance

Verder Lezen

Overheid ontmoedigde het protest rondom NSS-top

Wijkagent: Gaat u soms naar de NSS-top?

Beroepsverbod voor familielid activiste

De Telegraaf, Milieudefensie, en de oud papier-affaire

Liefdewerk, oud papier

Bijlagen

AIVD

AIVD besluit Global Open.pdf

ukhomeaffairscommitteeundercoverpolicingglobalopenmarkkennedy.pdf

Coosto

Product Changes Coosto 29 juni 2017 (pdf)

vragen aan Coosto (pdf)

antwoorden coosto (pdf)

vragen aan Wiseguys (pdf)

factsheet Coosto november 2014 (pdf)

Coosto Open facsheet NL 2014 (pdf)

OBI4wan

vragen aan OBI4wan (pdf)

antwoorden OBI4wan (pdf)

vragen aan Sitedata (pdf)

factsheet OBI4wan november 2014 (pdf)

Buzzcapture

vragen aan Buzzcapture (pdf)

antwoorden van Buzzcapture (pdf)

factsheet Buzzcapture november 2014 (pdf)

Reputatiemanagement bedrijven

reputatiemanagenment bedrijven factscheets 2014 (pdf)

reputatiemanagenment bedrijven 2012 (pdf)

Montoring webcare tools 2012 (pdf)

Politie

politie besluit OBI4wan HowAboutYou (pdf)

politie besluit OBI4wan online media monitoring tool en proces (pdf)

politie besluit Buzzcapture (pdf)

Ministerie van Veiligheid en Justitie

besluit ministerie van V en J Coosto Buzzcapture primair (pdf)

Autoriteit Persoonsgegevens

persoonsgegevens_op_internet_2007 (pdf)

brief aan Autoriteit Persoonsgegevens (pdf)

aanvullende brief aan Autoriteit Persoonsgegevens (pdf)

Autoriteit Persoonsgegevens antwoord (pdf)

Naar inhoudsopgave Observant #70

De burger als dreigingsscore

Social media surveillance in de Verenigde Staten

Het op grote schaal monitoren van mensen op online en social media kwam eind 2016 in de Verenigde Staten in het nieuws. De Amerikaanse burgerrechten beweging ACLU (American Civil Liberties Union) publiceerde in oktober 2016 een rapport over het Amerikaanse bedrijf Geofeedia, dat data van Facebook, Instagram, Twitter en andere social media ter beschikking stelt aan Amerikaanse opsporingsdiensten. In reactie op het nieuws besloten Instagram, Facebook en Twitter Geofeedia geen toegang meer te geven tot openbare data van de social media bedrijven. In de Verenigde Staten laaide de discussie over social media surveillance bedrijven als Geofeedia op.

Geofeedia was niet het eerste bedrijf dat onder vuur kwam te liggen. Begin 2016 publiceerde de ACLU documenten die zij via de Freedom of Information Act (FOIA) had gekregen over het gebruik van de software Beware van het bedrijf Intrado Inc. door een Amerikaanse politiedienst. Intrado beweert dat met de tool Beware opsporingsdiensten beter voorbereid kunnen reageren op meldingen. Intrado verzamelt online en social media gegevens en verkoopt die door aan klanten. De berichten en posts worden voorzien van gevarenscores over burgers en zouden daarmee een nauwkeuriger beeld opleveren van een situatie of incident waar de politie op af gaat. De ACLU bekritiseert de tool door te wijzen op het feit dat Amerikanen in het geheim van een label worden voorzien, dat de effectiviteit van de methode niet is onderzocht, de data onnauwkeurig zijn, en er risico is op profilering.

Bij Beware focust de ACLU vooral op de gevarenscores die door de software aan berichten worden gegeven. In het rapport over Geofeedia legt de ACLU daarbij de nadruk op de grootschalige dataverzameling over Amerikaanse burgers en de surveillance van kritische burgers, zoals de beweging Black Lives Matter. Geofeedia gebruikt de slogan ‘See what's happening right now, anywhere’.

Volgens het bedrijf kun je met hun tool social media monitoren via 'precision location-based searches' (zoekopdrachten waarbij locatiebepaling een belangrijke rol spelen).

Wildgroei aan dataverzamelaars

De lijst bedrijven die data van het internet verzamelen is sinds de eerste onthullingen van de ACLU over Intrado en Geofeedia alleen maar langer geworden. In publicaties komen ook de volgende bedrijven langs: Media Sonar, X1 Social Discovery, Dataminr, Snaptrends, Digital Stakeout, LexisNexis, Social Sentinel, LifeRaft - Social Navigator Inc, CES Prism, Brightplanet, Magnet Forensics, Signal Corporation, ZeroFOX, Pathar, Meltwater, SocioSpyder, Babel Street en TransVoyant. Opvallend is dat niet alleen start-ups maar ook grotere bedrijven zoals LexisNexis en Salesforce zich op de surveillance markt begeven.

De bedrijven Intrado, Geofeedia, Snaptrends en Media Sonar staan symbool voor de social media surveillance industrie in de Verenigde Staten. Aan de hand van profielen van deze bedrijven en hun samenwerking met politiediensten wordt de problematiek en het debat over social media surveillance in de Verenigde Staten beschreven.

Beware van Intrado

Beware is een software tool die door het Amerikaanse bedrijf Intrado Inc. is ontwikkeld. Intrado is een bedrijf dat sinds de jaren tachtig alarmcentrales levert aan Amerikaanse overheidsinstanties. Het bedrijf werd in 2006 gekocht door West Corporation, een bedrijf dat communicatiediensten aanbiedt. In 2017 is West Corporation overgenomen door een private equity firm, Apollo Global Management. Intrado ontwikkelt naast alarmcentrales ook inlichtingen software voor onder andere politiediensten.

Het bedrijf presenteerde in augustus 2012 zijn product Beware. Hulpdiensten, maar vooral de politie, krijgen met behulp van Beware

een melding over het risiconiveau als ze op een melding reageren. Intrado presenteerde Beware als een digitale oplossing voor het vergroten van de publieke veiligheid. Beware gebruikt een algoritme dat volgens Intrado allerlei openbare data doorzoekt en op basis van die data tot een 'gevaren' score komt. Deze 'gevaren' score wordt ook wel Facebook Threat Score genoemd.

De Amerikaanse politiediensten beschikken niet over de broncode (de precieze werking/technische details) van zowel de zoektechniek als de scoringstechniek. De presentatie van de tool zorgde in 2012 niet voor ophef. Nieuws over Beware drong eigenlijk alleen door tot de economiepagina´s tussen de berichtgeving over nieuwe producten en tools. Intrado was van oudsher een fabrikant gespecialiseerd in alarmcentrales en heeft nauwe connecties met opsporings- en inlichtingendiensten. Bij de presentatie van Beware ging het om het verbeteren van de veiligheid van hulpdiensten: wie kon daar tegen zijn?

Een jaar later kreeg het bedrijf samen met het bedrijf LexisNexis en diens Risk Solutions, de mogelijkheid om Beware te presenteren tijdens de 120th Annual International Association of Chiefs of Police Conference and Law Enforcement Education and Technology Exposition (IACP). Intrado kreeg hiermee een platform om Beware bij politiediensten te promoten.

Dragnet Days

In 2015, drie jaar na de presentatie van Beware, werd Chicago opgeschrikt door zogenaamde ´Dragnet days.´ Tijdens die dagen werden bewoners van de stad door de politie lastig gevallen op basis van analyses van hun social media gedrag. Agenten werden naar de adressen gestuurd vanuit een ´Intelligent Data Portal´ of ´Real Time Crime Center´ (RTCC).

Tijdens de Dragnet Days werd de gevarenscore tool van Intrado, Beware gebruikt. Intrado werkte voor het project ook samen met LexisNexis en Motorola, een bedrijf dat ook actief is op het terrein van de social en online media monitoring. In een artikel van *ABC*

News van 19 februari 2015 over de Dragnet Days gaf Ryan Seick van Motorola aan dat het bedrijf toegang had tot alle "publicly available social media; Twitter, Facebook, Picasa, Flickr, Instagram, anything along those lines, as long as it's publicly available."

Professor Lori Andrews van de Chicago-Kent College of Law, de rechtenfaculteit van het Illinois Institute of Technology, oordeelde dat de politie zonder een gerechtelijk bevel en zonder een redelijke verdenking, zich geen toegang mag verschaffen tot persoonlijke data. "We've become a nation of suspects," (we zijn een natie van verdachten geworden) zegt ze tegen *ABC News*. Ze verwijst daarbij naar het feit dat mensen op basis van social media gegevens, likes en andere data worden verdacht van de mogelijkheid dat ze een misdrijf gaan plegen.

Pas een jaar later, januari 2016, naar aanleiding van een artikel in de Washington Post en het Wob verzoek (Freedom of Information Act in de Verenigde Staten) van de Amerikaanse burgerrechtenorganisatie ACLU, ontstond er een maatschappelijk en politiek debat over de gevarenscores van Beware en de daarmee samenvallende online surveillance van de politie. De ophef zorgde ervoor dat enkele politiediensten afzagen van het verdere gebruik van Beware.

Facebook Threat Score

De ACLU maakte in 2016 documenten over Beware openbaar en schetste verschillende problemen met het scoren van Amerikanen op een gevaren index. De ACLU stelt dat het scoren van de Amerikanen via Beware geheim is, alleen het bedrijf weet hoe het werkt. De politie beschikt niet over de broncode. Doordat opsporingsdiensten de tool gebruiken en een score grote gevolgen kan hebben, eist de ACLU transparantie over de methode. Het risico bestaat dat Afro-Amerikanen een hogere gevarenscore krijgen zonder dat daar een objectieve rechtvaardiging voor bestaat.

De burgerrechtenbeweging plaatst ook vraagtekens bij de verzamelde data die de basis vormen van de gevarenscore. Politiedatabanken zijn notoir vanwege hun onnauwkeurigheid. Naast

de politiedata wordt door de tool ook de verzamelde online en social media data gebruikt, waarbij betwijfeld kan worden of daar objectieve waarde aan kan worden gehecht om een gevarenscore op te baseren. De ACLU stelt dat de tools gebruikt worden, maar dat de effectiviteit en nauwkeurigheid van de tools niet gemeten is. Volgens de ACLU ontbreekt het aan controle, transparantie en onafhankelijk onderzoek naar het gebruik van Beware.

De ACLU wijst ook op het gevaar van profilering als gevolg van het gebruik van Beware. De organisatie wijst daarvoor niet alleen op de vervuilde databanken, maar stelt dat databanken van de politie een vertekend beeld kunnen opleveren. Op basis van statistische gegevens is aannemelijk dat mensen met een migrantenachtergrond en Afro-Amerikanen meer worden gecontroleerd en staande gehouden, omdat zij vaker in de misdaad statistieken voorkomen. Oververtegenwoordiging is echter geen degelijke voorspellende waarde om een gevarenscore op te baseren. Zo wordt het effect van de algoritmes achter de gevarenscore versterkt. De tool wekt de indruk dat er objectieve mechanismen betrokken zijn bij het berekenen van de gevarenscore, terwijl in werkelijkheid een gehele bevolkingsgroep op achterstand wordt gezet. Technologie draagt dus bij aan etnisch profileren.

Intrado is voor haar software Beware afhankelijk van data van social media bedrijven Facebook, Twitter, LinkedIn. Toegang tot online media data is noodzakelijk voor het creëren van een gevarenscore door de tool. De social media bedrijven hebben niet bekend gemaakt of zij Intrado de toegang tot hun data hebben ontzegd.

Geofeedia

In een ander geval hebben social media bedrijven dat wel gedaan. Geofeedia werd in oktober 2016 afgesloten van Facebook, Instagram en Twitter data. De ACLU kwam Geofeedia op het spoor via het verzoek op basis van de Freedom of Information Act over Beware. Tussen de ontvangen stukken over het gebruik van Beware door politie in het Amerikaanse Fresno bevonden zich ook stukken over het bedrijf Geofeedia uit de Amerikaanse stad Chicago. Geofeedia

werd in 2011 opgezet. Eén van de oprichters Phil Harris stelt bij de oprichting dat de toekomst van het bedrijf zeer rooskleurig is. Het bedrijf drijft op social media intelligence zoals hij dat noemt. In het bedrijf werd volop geïnvesteerd. In 2014 haalde het nog drie en een half miljoen dollar aan investeringen op.

Ook de journalistiek toont zich erg enthousiast over de Geofeedia tool, niet alleen in de Verenigde Staten. Daarbij gaat het niet alleen om positieve reviews, maar ook om het daadwerkelijk gebruik van de tool door journalisten. Het European Journalism Centre met onder andere de Nederlandse partners het Algemeen Dagblad, Free Free Press Unlimited, VPRO, NTR, Waag Society en diverse opleidingen journalistiek en universiteiten, noemt Geofeedia in 2012 een nuttige tool voor journalisten om foto´s en tweets te lokaliseren die mogelijk nieuwswaarde hebben.

In de Australische media wordt een ander aspect van de tool belicht. De *Australian Financial Review* omschrijft op 10 oktober 2015 Geofeedia als een professionele tool voor stalkers. “Professionals use social media monitoring sites like Geofeedia or Ready Or Not” om mensen te stalken. Onder de kop ´cyber security´ geeft het artikel aan dat het huis- en werkadres, tijdstippen dat mensen niet thuis zijn, zijn te achterhalen als iemand zijn ´geo-location tracking´ (plaatsbepaling) op zijn Twitter en Instagram heeft aanstaan. De *Australian Financial Review* laat een voormalig militair en politieagent aan het woord, die uitlegt dat iemand nu in een handomdraai in kaart te brengen is. "Large, expensive surveillance operations used to take a couple of weeks - now we can map someone's life in about seven minutes."

CIA investeringen

De eerste negatieve berichtgeving over Geofeedia verschijnt op 15 april 2016 in *The Intercept* onder de kop ´CIA Tech Firm Seeks More Social Media Spying´. *The Intercept* had een folder van een jaarlijkse bijeenkomst in handen gekregen van In-Q-Tel, een investeringsmaatschappij die zich presenteert als een investeerder

zonder winstoogmerk. “Each year this event brings together significant players in IQT's strategic investment process,” staat in de folder.

In-Q-Tel heeft echter een ander doel, namelijk investeren in technologie voor online en social media surveillance. In-Q-Tel (In-Q-It, IQT) is een frontorganisatie van de Amerikaanse inlichtingendienst de CIA (Central Intelligence Agency). “In-Q-Tel (IQT) is the independent. strategic investor for the Central Intelligence Agency and the broader U.S. Intelligence Community,” is de eerste zin van de mission statement van het bedrijf. Als één van de bedrijven die worden gesponsord door de CIA wordt in de conferentie folder Geofeedia genoemd, maar ook vergelijkbare bedrijven als Pathar, TransVoyant en Dataminr.

Intelligence surge

In juli 2016 komt social media surveillance door bedrijven en de overheid in de Verenigde opnieuw in de belangstelling te bestaan. Een journalist van de *Baltimore Sun* krijgt door middel van een beroep op de Freedom of Information Act documenten over social media surveillance door Geofeedia voor de politie in handen. De politie van Baltimore geeft in antwoord op vragen van de journalist aan dat zij met behulp van Geofeedia demonstraties, parades, events en andere gebeurtenissen in de gaten houdt.

De politie spreekt tegen de journalist over "things that might be of concern" en "the only people that have anything to fear about anything being monitored are those that are criminals and attempting to commit criminal acts." De indruk die zowel Geofeedia als de politie hiermee wekken is dat iedereen in de gaten wordt gehouden en dat van alle burgers data worden verzameld en bewaard. Wanneer vervolgens de Democratische presidentskandidaat Hillary Clinton begin oktober 2016 spreekt over een *intelligence surge* om ISIS te verslaan, breekt er een nationale discussie uit over on line media surveillance.

Clinton bedoelt met de *intelligence surge* hetzelfde als the surge van president Bush in 2007 in Irak. In dat jaar stuurde Bush meer

Amerikaanse militairen naar Irak om het verzet de kop in te drukken. De *intelligence surge* was door Clinton bedacht om met behulp van een massale verzameling van data het terrorisme te bestrijden. Eigenlijk verwijst ze naar de datahonger van de inlichtingendienst NSA die op grote schaal vooral data buiten de Verenigde Staten verzamelt.

De ACLU maakt in de periode van de uitspraken van Clinton bekend dat Geofeedia zichzelf bij de politie aanprijst met de mogelijkheid om demonstraties in de gaten te houden. Op basis van documenten verkregen via de Freedom of Information Act wordt duidelijk dat de politie bijeenkomsten, zoals een marihuana rally en de Martin Luther King Day, met behulp van Geofeedia in de gaten houdt.

In reactie op het publieke debat over sociale media surveillance, het onderzoek van de ACLU en vragen aan social media bedrijven, besluiten Twitter en Facebook in oktober 2016 de toegang tot hun gebruikersdata door Geofeedia op te schorten. Doorslaggevende reden voor het blokkeren van de toegang is dat de internet surveillance door de politiediensten ook gevolgen heeft voor de vrijheid van meningsuiting, de vrijheid van vergadering en het recht op het houden van openbare manifestaties. Het monitoren van onder andere demonstraties en burgerrechtenorganisaties was één van de speerpunten in de verkoop praatjes van Geofeedia, en één van de redenen waarom vele politie-eenheden in de Verenigde Staten de tool van het bedrijf gebruiken.

Het gebruik van social media data voor surveillance doeleinden maakt niet alleen duidelijk dat de Amerikaanse politie iedereen in de gaten wil houden. Bedrijven zijn ook bereid om data te verzamelen en samen te werken met opsporingsdiensten om die surveillance te bewerkstelligen.

Snaptrends

Social media werden in de Verenigde Staten eind 2016 gekoppeld aan de term Big Brother. Om tegemoet te komen aan de kritiek dat

de social media bedrijven bijdragen aan een surveillance staat wordt Geofeedia de toegang tot gebruikersdata ontzegd. Twitter sluit in 2016 ook het bedrijf Snaptrends af van het gebruik van de publieke API om Twitter data te downloaden.

Snaptrends is tot 2016, net als Geofeedia, een onbekend bedrijf. Het bedrijf uit het Amerikaanse Austin in de staat Texas profileert zich met een tool voor een "social media intelligence platform, social observer system of location based social media insights," volgens haar website. Het spreekt over 'empowering' van organisaties: "Snaptrends social media software empowers organizations to visualize social conversations by analyzing social media content in any specified geographic location automatically." In een document dat de ACLU via de Freedom of Information Act heeft verkregen over Geofeedia bevindt zich een e-mail communicatie tussen een Geofeedia medewerker en een medewerker van een politiedienst. Geofeedia noemt Snaptrends hierin haar grootste concurrent.

Geofeedia en Snaptrends geven aan dat zij data verzamelen van acht social media bronnen en dat die toegang 'oneindig' is. Volgens Geofeedia kunnen opsporingsdiensten met een vertraging van rond de 15 minuten ontwikkelingen op social media volgen. Beide bedrijven betaalden voor de 'Twitter Firehose' waarmee zij toegang kochten tot Twitter data en die konden verzamelen en deze ook direct aanboden aan de politie. Snaptrends zou in tegenstelling tot Geofeedia geen contract hebben met Instagram.

Locatiedata – Geodata – Exif data

Naast de inhoud van de verzamelde online en social media data is ook de locatie van smartphones belangrijke informatie die social media monitoring bedrijven verkopen aan politiediensten. In een openbaar geworden mail van Geofeedia wordt aangegeven hoe die plaatsbepaling ongeveer werkt: "When a post is made to a social media site, is the location where they uploaded the post (home) or where they tagged the location (club, bar, beach, etc.)? It's going to be from the location where the post is uploaded. For Twitter and Instagram, you can tag the location (club, bar, beach, etc.) if it's

within a certain vicinity/distance, to ensure its location is still accurate and actionable. Majority of data comes from the location of the upload."

Dit betekent dat de plaatsbepaling van een bericht op social media slechts deels wordt bepaald door de locatie die de persoon aanmerkt als thuis of waar de persoon die het bericht plaatst op dat moment is. Facebook en Twitter hebben locatiedata van gebruikers aan Geofeedia doorgegeven. Op welke wijze Geofeedia aan deze data is gekomen hebben Facebook en Twitter niet bekend gemaakt. Het kan zijn dat de locatiebepaling gebeurde op basis van de plaatsbepaling via de social media app en dat de social media bedrijven deze doorgaven aan de monitoring bedrijven. Geofeedia geeft zelf echter aan dat zij de meeste data voor de plaatsbepaling uit de gegevens van het moment van plaatsen van het bericht halen, en niet zozeer uit de geodata van de persoon zelf. Dit betekent dat zij voor de locatie de zogenaamde Exif data van foto´s en films gebruiken. Exchangeable Image File Format (EXIF) is informatie in foto´s en films waar onder andere locatie in is verwerkt. Die data moeten door Facebook en Twitter aan Geofeedia ter beschikking zijn gesteld.

Undercover social media

Bij de functionaliteit van de verschillende social media monitoring tools gaat het niet alleen om de locatie bepaling van de verschillende berichten maar ook over snelheid en het opnemen van 'undercover accounts' in het systeem. Undercover accounts zijn bijvoorbeeld nep Facebook accounts, waarmee functionarissen van opsporings- en inlichtingendiensten proberen mensen op Facebook te benaderen.

Een advocaat van de ACLU omschrijft dit social media undercover politie werk als een uitbreiding van een regulier rechtshulpverzoek dat de politie bij Facebook kan indienen voor het opvragen van informatie van specifieke Facebook accounts. "By using undercover accounts, they are potentially friending multiple people and getting much broader access than a warrant to Facebook for specific information would allow." De politiedocumenten die openbaar werden gemaakt naar aanleiding van het Freedom of Information Request onthulden het gebruik van undercover accounts bij de

monitoring van protesten tegen politiegeweld in de Verenigde Staten.

Media Sonar

Naast locatie data en undercover social media accounts werken on line en social media surveillance bedrijven met een systeem van steekwoorden. Tussen de stukken die de ACLU via de Freedom of Information Act heeft verkregen, bevindt zich een lijst met sleutelwoorden die door het Canadese bedrijf Media Sonar wordt gebruikt voor social media surveillance: 'Media Sonar Keywords januari 2015.' Veel van deze steekwoorden zijn erg voor de hand liggend. Het bedrijf maakt niet duidelijk of zij eerst online en social media informatie verzamelt en vervolgens pas met sleutelwoorden in de eigen database zoekt, of dat zij verzamelt op basis van de sleutelwoorden. Het bedrijf stelt dat het een database heeft die teruggaat tot 2008.

De lijst bestaat uit allerlei categorieën zoals ´wapens, gangs (bendes), drugs (grootste deel), niet opvolgen van een politie bevel en misdaden tegen de politie, internetpesten/zelfmoord/zelf mutilatie, jeugd/sexting/kinderlokker, vermogensdelicten, mensensmokkel en Mike Brown gerelateerd.´ Onder de categorieën worden alle sleutelwoorden opgesomd. Bij de categorie wapens staat bijvoorbeeld Glock, pistol en semi. Bij de categorie politie gaat het over cops, popo. fuck the police. Bij de categorie vermogensdelicten staan de sleutelwoorden lift en rob.

Het opvallende aan de lijst van sleutelwoorden van Media Sonar is dat deze is opgesteld in samenwerking met een internationale organisatie, Arman/ to Arman Refugee Asylum group. Deze organisatie is gespecialiseerd in de behandeling, het onderzoek en de behandeling van slachtoffers van marteling en mensensmokkelen. De samenwerking tussen Arman en Media Sonar gaat niet over de verkoop van de surveillance tool aan opsporings- en inlichtingendiensten in de wereld, maar over een bijdrage aan de tool zelf. Volgens een email van Media Sonar levert Arman

sleutelwoorden voor het dataminen van online media en voor intelligence gestuurde, proactief politiewerk.

Black Lives Matter

Eén categorie van de 'Media Sonar Keywords januari 2015' lijkt van een andere orde dan alle andere want het gaat over Mike Brown. Deze Afro Amerikaanse jongen werd op 9 augustus 2014 doodgeschoten door een politieagent. Voor Media Sonar is de keuze om een lijst woorden te kiezen over Mike Brown niet vreemd. Het bedrijf gebruikt het monitoren van de Black Lives Matter beweging als succesverhaal om haar surveillance tool aan de politie te slijten. Media Sonar noemt het zelf 'Powering Digital Intelligence'.

Ook andere social media monitoring bedrijven als Geofeedia en Snaptrends gebruikten de monitoring van protesten als succesverhalen om hun product bij andere politiediensten aan te prijzen. Zo schrijft Geofeedia in een email aan een politiedienst over de positieve resultaten van de monitoring van demonstraties in het Amerikaanse Ferguson naar aanleiding van de dood van Michael Brown. Snaptrends gebruikte de monitoring van de protesten rond de dood van een andere Afro Amerikaan, Freddie Gray, die ook werd doodgeschoten door de Amerikaanse politie, om nieuwe klanten te werven.

Snaptrends en repressieve regimes

De discussie over social media monitoring tools in de Verenigde Staten gaat grotendeels over surveillance van burgerrechtenbewegingen en politiek protest. Een ander aspect is echter even verontrustend, namelijk de verkoop van de tools aan repressieve regimes.

Net als de Amerikaanse en Nederlandse politie zijn ook allerlei diensten uit repressieve regimes geïnteresseerd in social media surveillance. *Bloomberg Businessweek* schrijft in oktober 2016 op basis van interne documenten van Snaptrends dat het bedrijf social

media monitoring tools heeft geleverd aan politiediensten in de Verenigde Arabische Emiraten en aan een opsporingsdienst van Bangladesh, die door Human Rights Watch word omschreven als een doodseskader.

Een voormalig medewerker van Snaptrends Kevin Hatline zegt tegen *Bloomberg* dat het bedrijf wist dat de tool gebruikt zou worden om mensen te onderdrukken. "We all knew this could be used to put a black bag over someone's head and make them disappear," (*Bloomberg Businessweek* 27 oktober 2016).

Voor de verkoop in het Midden Oosten en de rest van de wereld werkt Snaptrends samen met Chenega Corporation. Chenega is een private military contractor die, naast het leveren van militaire en operationele diensten, zich ook als private inlichtingendienst aanbiedt. De tools van Snaptrends passen in de dienstverlening die Chenega aanbiedt aan autoritaire regimes. Tijdens de ISS World Middle East in maart 2015 in Dubai, een bijeenkomst van producenten van digitale wapens en surveillance software en apparatuur, ontmoeten vertegenwoordigers van de Amerikaanse bedrijven Chenega en Snaptrends vertegenwoordigers van Hacking Team. Dit Italiaanse bedrijf is in 2015 bekend geworden door een grote hack waarbij gegevens van het bedrijf openbaar werden gemaakt door Wikileaks. Hieruit bleek dat Hacking Team digitale wapens levert aan repressieve regimes zoals Marokko, Ethiopië, Soedan en Oezbekistan.

Chenega onderhandelt vanaf maart 2015 over mogelijke samenwerking met Hacking Team. In de email wisseling tussen Chenega medewerkers David Alley (Vice President Chenega International), Ben Buchholz, Angela Hunziker, April Flores, John Douglas (President Chenega Europe), Lance Swift en John Campagna, en Hacking Team leden Philippe Vinci, Maurico Luppi en David Vincenzetti maken de Italianen duidelijk dat zij het liefst direct met mensen van Snaptrends om de tafel gaan zitten. "We would prefer this particular discussion to be between the Hacking Team and Snaptrends only. As two product companies, it's easier to sort a path forward without pulling in other partners – like Chenega. We do a great deal of work with them (we really like the Chenega / ST partnership) but on the product side, we find discussions regarding joint product development best limited to tech company-to-tech

company," schrijft het Italiaans bedrijf. De bedrijven spreken in een e-mail af elkaar begin juni 2015 in Praag op de ISS World Europe conferentie te ontmoeten.

Uit de e-mail communicatie wordt duidelijk wat voor mogelijkheden er voor zowel Hacking Team als Snaptrends liggen. David Alley van Chenega is als voormalig militair attaché van de Verenigde Staten bekend met de markt in het Midden Oosten. Tegen Hacking Team zegt hij dat er in ieder geval twee landen al als toekomstig klant kunnen worden aangemerkt: Libanon en Marokko. Volgens de drie bedrijven zijn er handelsmogelijkheden in 25 landen in het Midden Oosten. De meeste van deze landen zijn repressieve regimes. Dat Snaptrends werk heeft gemaakt van de contacten van Chenega baas Alley blijkt uit interne documenten waar Bloomberg uit citeert. Volgens die documenten heeft Snaptrends zijn product geprobeerd te verkopen aan Azerbeidzjan, Bahrein, Maleisië, Saoedi-Arabië en Turkije, landen die niet bekend staan om hun vrijheid van meningsuiting en betoging.

Snaptrends is echter niet het enige social media surveillance bedrijf dat op zoek is naar klanten buiten de Verenigde Staten. Geofeedia gaat in de zomer van 2016 een partnerschap aan met het internationale bedrijf Everbridge. Het software bedrijf is gespecialiseerd in alarm systemen, communicatie en beveiliging, en is ook actief in het Midden Oosten.

Topje van de ijsberg

De verontwaardiging over social media surveillance is in de Verenigde Staten vooral ontstaan doordat deze surveillance gericht was op demonstraties, leden van actiegroepen en burgerrechtenbewegingen. Het is ernstig dat in een democratie, mensen die hun stem willen laten horen in de gaten worden gehouden. Bij online en social media surveillance door politie en bedrijven zijn de vrijheid van meningsuiting en het recht op manifestatie in het geding. Informatie over social media surveillance is de afgelopen twee jaar mondjesmaat naar buiten gekomen door onderzoek van de burgerrechten organisatie ACLU. Ook door verzoeken om informatie door de ACLU en journalisten met behulp

van de Freedom of Information Act (Wob verzoeken). Wat er nu bekend is over social media surveillance is slechts het topje van de ijsberg.

De aandacht voor bedrijven als Intrado, Geofeedia, Snaptrends en Media Sonar heeft ertoe geleid dat social media bedrijven als Facebook en Twitter onder druk worden gezet om hun gebruikers beter te beschermen. Facebook en Twitter hebben in hun beleid expliciet opgenomen dat de data van haar gebruikers niet gebruikt mogen worden voor surveillance doeleinden. Dit wil echter nog niet zeggen dat Facebook en Twitter ook alle social media surveillance bedrijven van hun platformen hebben verbannen. Het is wel bekend dat zij Geofeedia hebben verbannen, maar het is bijvoorbeeld niet door de bedrijven bekend gemaakt of Intrado van de Beware tool is geweerd. De enkele bedrijven die Facebook en Twitter hebben verbannen zijn slechts het topje van de ijsberg. Van veel andere bedrijven is dat niet bekend.

De burger als dreigingsscore; Social media surveillance in de Verenigde Staten (pdf)

Gehele Observant #70 social media surveillance in Nederland (pdf)

Andere artikelen

Social Media Surveillance in Nederland

Dagelijkse en structurele monitoring; De Nederlandse politie en social media surveillance

Reputatie management bedrijven, de nieuwe private inlichtingendiensten

Overgeleverd aan de grillen van social media multinationals; Facebook en Twitter en de Nederlandse social media surveillance

Bijlagen

ACLU

20160325-making_smart_decisions_about_surveillance

20160921_Social_Media_Surveillance_PRA_Summary

CIA

CIAinvesteringsvehicleIQT

Geofeedia

20160921-pra_content_ferguson_r.pdf

20160921-pra_geofeedia_overt_threats

20161011_adding_periscope_vine_glendale_pra_response

20161011_Geofeedia_500_law_enforcement_public_safety

20161011_geofeedia_baltimore_case_study

20161011_geofeedia_das_monitoring_protests

20161011_Geofeedia_Facebook_Arrangement_r

20161011_Geofeedia_Instagram_map_to_Glendale_PD

20161011_Geofeedia_Monitoring_emoji_Ventura_Sheriff_0

20161011_geofeedia_twitter_instagram_riverside_pd

20161011_Geofeedia_User_Track_Email_to_Stanislaus_Sheriffs

20161011_Sentiment_analytics

Geofeedia-for-Law-Enforcement-Brochure

Intrado

201512-social_media_monitoring_software_Intrado_Beware

Snaptrends

53180_Email from Snaptrends 1-28-16

Media Sonar

201512-social_media_monitoring_software_media_sonar

Dataminr

20160315_dataminr_email_to_jric

Naar inhoudsopgave Observant #70

Overgeleverd aan de grillen van social media multinationals

Facebook en Twitter en Nederlandse surveillance

Het verzamelen van online en social media informatie door bedrijven die zich bezighouden met social media monitoring of reputatiemanagement, zoals Coosto, OBI4wan/HowAboutYou en Buzzcapture klinkt misschien technisch complex, maar is praktisch zeer eenvoudig. Coosto spreekt bijvoorbeeld van ruim vier miljoen berichten die dagelijks aan hun database worden toegevoegd. Het gemak waarmee berichten van sociale media platformen als Facebook, Instagram, Twitter, LinkedIn, Pinterest, YouTube en Google+ worden verzameld roept niet alleen vragen op over het gedrag van reputatiemanagement bedrijven, maar ook over de rol van social media platformen zelf.

Weet Facebook bijvoorbeeld dat dit soort bedrijven alle berichten van het platform verzamelen en zelf opslaan? Weet Twitter dat die gegevens worden doorverkocht aan instanties waaronder opsporings- en inlichtingendiensten? Weet LinkedIn dat die gegevens worden gebruikt voor surveillance doeleinden? Weten de social media platformen dat er met behulp van hun data gebruikersprofielen voor surveillance worden gemaakt?

De vraag is dus of social media platformen zelf een actief en transparant beleid hebben om te voorkomen dat social media data worden gebruikt voor surveillance. De meeste social media bedrijven publiceren wel regelmatig een Transparency Report. Daarin wordt weergegeven hoe vaak overheidsdiensten gegevens over specifieke accounts hebben opgevraagd. In de Transparency Reports worden echter geen lijsten gepubliceerd van bedrijven die data van de social media platformen mogen verzamelen, en deze data door mogen verkopen aan opsporings- en inlichtingendiensten. Transparency

Reports geven dus geen inzicht in het gebruik van social media data voor surveillance doeleinden.

Blocked by Facebook

In de Verenigde Staten heeft de aandacht voor social media surveillance door reputatiemanagement bedrijven als Intrado, Geofeedia, Snaptrends en Media Sonar tot gevolg gehad dat grote social media platformen besloten om deze bedrijven de toegang tot hun gebruikersdata te ontzeggen. Twitter en Facebook besloten Geofeedia in oktober 2016 af te sluiten van haar datastroom. Snaptrends kreeg een maand later, in november 2016, te maken met sancties van de twee social media bedrijven. Media Sonar werd begin 2017 afgesloten door Twitter en Facebook.

Bovengenoemde Amerikaanse bedrijven zijn allemaal in de publiciteit gekomen naar aanleidingen van onderzoek van burgerrechten beweging American Civil Liberties Union (ACLU). Er zijn in de Verenigde Staten echter veel meer bedrijven actief op het terrein van de social media surveillance. In documenten die via een procedure op grond van de Freedom of Information Act openbaar geworden zijn, komen de volgende bedrijven voor: HootSuite, TweetDeck, X1 Social Discovery, Dataminr, Digital Stakeout, Lexis Nexis, Social Sentinel, LifeRaft - Social Navigator Inc, CES Prism, Brightplanet, Magnet Forensics, Signal Corporation, ZeroFOX, Pathar, Meltwater, SocioSpyder, Babel Street en TransVoyant. Het is niet bekend of Facebook en Twitter deze bedrijven ook hebben afgesloten van hun gebruikersdata. Ook van andere social media platformen zoals Pinterest, Reddit, 4chan, LinkedIn (Microsoft), Google+ en YouTube is niet bekend of zij nog toegang tot hun data aan deze bedrijven geven.

Om te onderzoeken hoe de situatie is in Nederland besloot Buro Jansen & Janssen verschillende social media platformen aan te schrijven over hun beleid om te voorkomen dat social media data worden gebruikt voor surveillance. Buro Jansen & Janssen vroeg naar de kennis die het bedrijf heeft over het verzamelen van data van social media platformen. “Is (name of the company) aware of the fact that companies are downloading (crawling) Google data for

their own purposes?" En specifiek met betrekking tot Nederland: "Does (name of the company) allow companies to collect data from Dutch citizens – and probably other nationalities – in order for the companies to store the data in their own databases?"

Daarnaast is er gevraagd naar social media surveillance. "These companies also make their databases available to law enforcement agencies for social and online media monitoring/surveillance purposes. Is (name of the company) aware of that?" En of gebruikers worden geïnformeerd: "Are users in the Netherlands – and other countries - informed by (name of the company) about the fact that their data might be collected by Dutch companies for other purposes than the initial intention of the (name of the company) users?" Ook is er gevraagd naar specifieke bedrijven. "At the moment we are investigating several companies among which Coosto/Wiseguys Internet, Buzzcapture and Obi4wan/Sitedata. Are these companies known to (name of the company)?

Twitter

Twitter gaat bij herhaling niet in op de vragen van Buro Jansen & Janssen. Het bedrijf verwijst steeds naar haar Transparency Report en de algemene voorwaarden. Op een eerste brief antwoordt de perswoordvoerder van Twitter Inc.: "With regards to the point made about Dutch law enforcement entities, we publish this data twice yearly in our Transparency Report. You can see the latest numbers for the Netherlands here." Twitter stelt dat zij twee keer per jaar gegevens vrijgeeft over vragen van overheidsdiensten met betrekking tot Twitter accounts. Over 2016 gaat het in totaal om ongeveer dertig aanvragen. In negen gevallen gaat het om een verzoek tot verwijdering door een overheidsdienst, politie of een ander bestuursorgaan. Naar alle waarschijnlijkheid betreft het hier gevallen van discriminatie, bedreiging, opruiing of andere overtredingen, dan wel strafbare feiten. In tien gevallen gaat het om een melding over een tweet of een account van een gebruiker. In een enkel geval ging het over het tegenhouden van een account of tweet.

Twitter gaat niet in op vragen over bedrijven die Twitter data verzamelen en doorverkopen voor surveillance doeleinden. Buro Jansen & Janssen vroeg of het Twitter bekend is dat bedrijven de data van haar gebruikers verzamelen, opslaan en doorverkopen onder andere voor surveillance doeleinden, en vroeg specifiek naar de relatie tussen Twitter en Coosto, Buzzcapture en Obi4wan. Het bedrijf weigert echter antwoord te geven. Ook vragen naar het gebruik van de applicatie Tweetdeck door de Nationale Politie worden door Twitter niet beantwoord.

Het is vreemd dat Twitter niet op deze vragen wil ingaan, terwijl de woordvoerder wel zeer expliciet is over het verbod op het verzamelen van informatie voor surveillance doeleinden. "To be clear: We prohibit developers using the Public APIs and Gnip data products from allowing law enforcement - or any other entity - to use Twitter data for surveillance purposes. Period. The fact that our Public APIs and Gnip data products provide information that people choose to share publicly does not change our policies in this area. And if developers violate our policies, we will take appropriate action, which can include suspension and termination of access to Twitter's Public APIs and data products," stelt de woordvoerder in een e-mail.

Informatie delen over andere bedrijven kan opgevat worden als concurrentiegevoelige informatie die bedrijven niet willen delen. In dit geval gaat het echter om mogelijke overtredingen van gebruikersovereenkomsten van Twitter. "We prohibit" en "if developers violate our policies, we will take appropriate action," schrijft het bedrijf. "Period" voegt de perswoordvoerder toe. Stevige woorden, maar Twitter maakt niet bekend of het de bedrijven gaat onderzoeken, hoe meldingen over eventueel misbruik worden onderzocht of afgehandeld, en of Twitter dit publiekelijk bekend maakt.

Het doen van stevige uitspraken lijkt de strategie van Twitter te zijn om specifieke vragen over haar beleid te omzeilen. De perswoordvoerder zegt bijvoorbeeld dat het bedrijf de Amerikaanse overheid heeft aangeklaagd. "In fact, we are suing the US government with regards to surveillance and overreach." Probleem is echter dat niet politiediensten de data verzamelen en doorverkopen, maar dat private bedrijven dit doen. De Amerikaanse overheid huurt

de diensten van de social media monitoring bedrijven in en omzeilt daarmee het overtreden van de voorwaarden van social media platformen.

LinkedIn, Google, Pinterest, Reddit, 4chan

LinkedIn en Google reageren op een vergelijkbare manier als Twitter. Ook LinkedIn verwijst naar de gebruikersovereenkomst: “In order to keep their members' data safe, they do not permit the use of software that scrapes or copies information from LinkedIn under the User Agreement. LinkedIn has technical measures and defences in place to protect against the use of any such tools on the platform, and constantly working to improve them. If any violation of the User Agreements is uncovered or reported, LinkedIn will investigate and take appropriate steps to address any violations.”

In een tweede e-mail stelt LinkedIn opnieuw dat het verzamelen van gebruikersdata een overtreding is van de gebruikersovereenkomst. “We do not permit the use of any software, including crawlers, bots, browser plug-ins, or browser extensions (also called "add-ons"), that scrape or copy member data, or that automate activity on or alter the appearance of LinkedIn pages. Such tools are prohibited by LinkedIn's User Agreement, and may violate the law.” Het bedrijf gaat in beide antwoorden niet in op de vragen naar de relatie met een aantal specifieke bedrijven (Coosto, OBI4wan en Buzzcapture).

Google Nederland stelt dat Buro Jansen & Janssen aan het verkeerde adres is. De vragen moeten worden gesteld aan Google Inc. in de Verenigde Staten. De vragen zijn echter gemaild aan press@google.com, het e-mail adres van het pers team van de multinational. “De meeste diensten van Google worden verleend door Google Inc., een rechtspersoon naar Amerikaans recht, gevestigd in Californië. Dat blijkt ook uit de Servicevoorwaarden van Google Inc. Google Netherlands B.V. kan uw vragen dan ook niet beantwoorden,” aldus Google Nederland.

Na drie keer de vragen te hebben gestuurd naar press@google.com gooit de multinational het over een andere boeg. Eerst schrijft de Nederlandse woordvoerder: “The emailadres press@ is used

exclusively for corresponding with press. Regarding your questions: more information about requests, removals etc can be found in our transparency report." Vervolgens voegt de Amerikaanse perswoordvoerder zich in de correspondentie met dezelfde opmerking. "This email address is used exclusively for corresponding with press."

Buro Jansen & Janssen heeft de vragen ook gesteld aan Pinterest, Reddit en 4chan. Van deze bedrijven werd niets vernomen.

Facebook

Buro Jansen & Janssen heeft dezelfde vragen ook aan Facebook gesteld. Op 14 juni 2017 geeft Facebook in eerste instantie eenzelfde algemeen antwoord als Twitter. "We don't allow developers to use data obtained from us to provide tools that are used for surveillance. We take the enforcement of our policies very seriously and investigate when possible violations are brought to our attention. When we find companies violating our policies we will take swift action, including banning those companies from Facebook and requiring them to destroy all improperly collected data."

Facebook gaat in tegenstelling tot Twitter iets specifieker in op de vragen. Het verzamelen van data van Facebook is volgens de woordvoerder verboden en Facebook probeert misbruik te voorkomen. "This would be against our policies and we have a number of systems in place to try to detect violations." Facebook geeft aan dat het bedrijven wel toestemming kan geven voor het verzamelen van data van haar platform. Hiervoor zijn in 2010 Automated Data Collection Terms opgesteld. In deze voorwaarden staat duidelijk dat data die door bedrijven van het Facebook platform zijn verzameld niet verkocht mogen worden. Daarnaast zijn veel voorwaarden afhankelijk van een specifieke overeenkomst van Facebook met het betreffende bedrijf met betrekking tot het verzamelen van de data. Facebook maakt in haar antwoorden echter niet duidelijk welke overeenkomst Facebook met welke bedrijven heeft gesloten.

Facebook onderstreept in het tweede artikel van de platformvoorwaarden wel dat, indien hiervoor geen toestemming is verleend door Facebook, er geen data mogen worden verzameld. De woordvoerder verwijst naar de Platform Policy punt 3.10: Ontwikkelaars die data van Facebook gebruiken worden gewezen op het vragen van toestemming aan gebruikers om de data te gebruiken voor advertenties.

In een tweede e-mail van 29 juni 2017 verduidelijkt Facebook nog de situatie wanneer een bedrijf een overeenkomst met Facebook heeft voor het verzamelen van gegevens van gebruikers. De bedrijven mogen niet met geautomatiseerde middelen informatie van het platform verzamelen en de informatie mag niet worden verkocht.

Tot zover het algemene standpunt van Facebook. Facebook wijst het gebruik van Facebook data voor surveillance doeleinden af, net als het verzamelen en doorverkopen van die data zonder toestemming van Facebook. Hoewel Facebook iets specifieker ingaat op vragen over haar relatie met social media monitoring bedrijven, blijven de antwoorden onbevredigend en onvolledig. Facebook gaat uiteindelijk wel in op Coosto, maar niet op OBI4wan en Buzzcapture. Het beleid en praktijk rond de opslag van Facebook data door derden blijven onduidelijk.

Bant Facebook Coosto?

Op de vraag of Coosto, Obi4wan en Buzzcapture bekend zijn bij Facebook antwoordt het bedrijf: “We will look into this report and will take any necessary enforcement action.” In de tweede e-mail van 29 juni 2017 schrijft het bedrijf: “In addition, each company has confirmed their commitment to reviewing their services and the clients who use them, and taking any steps necessary to ensure compliance with our terms. They have also given us permission to share their contact information with you.”

Facebook heeft de betreffende bedrijven aangeschreven. Volgens Facebook zijn de bedrijven bereid om naar hun diensten te kijken en tevens naar de klanten die gebruik maken dan die diensten.

Facebook noemt echter niet expliciet de namen van de bedrijven, de diensten en eventueel de klanten. Facebook heeft het wel over meerdere bedrijven. Op 3 juli 2017 mailt de perswoordvoerder vervolgens: “FYI a recent blog of Coosto that might be interesting for you.”

Coosto geeft in dit blogbericht van 29 juni 2017 aan zij zich in de toekomst aan de voorwaarden van de social media platformen gaat houden. Het bedrijf geeft aan dat zij al zeven jaar actief is en samenwerkt met bedrijven als “Facebook, LinkedIn, Twitter, Instagram, etcetera.” Zij heeft de data van die platformen doorgegeven aan haar klanten: “For seven years we have been offering our clients the best social media solutions for engagement, publishing and monitoring.”

Na de vragen van Buro Jansen & Janssen aan Facebook over haar contact met Coosto schrijft het bedrijf: “The Coosto policy blog post was done on their own initiative and not at our request. It was published after we met with them to discuss our policies with respect to collection and use of user data.” Pas na vragen van Buro Jansen & Janssen is Facebook in gesprek gegaan met Coosto, en niet naar aanleiding van de wijziging van haar Platform Policy. Op 13 maart 2017 paste Facebook namelijk haar Platform Policy aan.
Dit gebeurde na druk van vooral de Amerikaanse burgerrechten beweging ACLU en publiciteit in de media over social media surveillance door Amerikaanse bedrijven als Intrado, Geofeedia, Media Sonar en Snaptrends. In de platformvoorwaarden is nu expliciet opgenomen dat data niet gebruikt mogen worden voor surveillance doeleinden. “Protect the information you receive from us against unauthorized access, use, or disclosure. For example, don't use data obtained from us to provide tools that are used for surveillance.”

Facebook spreekt over een ontmoeting met Coosto en dat zij zaken heeft gecheckt bij het bedrijf en dat de verandering van beleid bij Coosto was gebeurd op eigen initiatief van het Eindhovense bedrijf. Facebook heeft Coosto echter pas benaderd nadat Buro Jansen & Janssen vragen aan Facebook heeft gesteld over het bedrijf. Facebook beweert tevens systemen te hebben die overtredingen van de voorwaarden detecteren, maar treedt niet in detail over welke systemen dit dan zijn en hoe die werken.

Op 29 juni 2017 stelt Coosto dat zij aan de nieuwe voorwaarden van Facebook wil voldoen. “As Coosto we need to respect the conditions of social media platforms and partners. For example, the current conditions of Facebook state that Facebook data can’t be used for surveillance purposes. As far as we understand from recent news articles, social platforms like Facebook will from now on only facilitate government organizations directly in case of security requests.”

In antwoorden op vragen van Buro Jansen & Janssen schrijft Coosto nog dat het bedrijf haar “standpunt rondom surveillance” deelt in het bericht van 29 juni 2017. Ook stelt Coosto dat het “de voorwaarden van onze partners volgt (zoals Twitter en Facebook etc.) in combinatie met ons moreel kompas en regelgeving.”

Coosto lijkt met die laatste zin te suggereren dat Facebook het verzamelen en doorverkopen van de data van gebruikers aan opsporings- en inlichtingendiensten in het verleden heeft getolereerd. De zin “social platforms like Facebook will from now on only facilitate government organizations directly in case of security requests,” is nogal bevreemdend in het licht van het feit dat Facebook al voor de verandering van haar platform policy op 13 maart 2017 verzoeken om specifieke informatie van overheidsdiensten beantwoordde. Facebook publiceert net als Twitter sinds 1 januari 2013 elk half jaar een zogenaamd Transparency Report. In 2016 ging het om 1.080 verzoeken om informatie die in totaal op 1.962 Facebook accounts betrekking hadden.

Facebook schrijft in het Transparency Report, dat het bij de vragen van overheden voor een groot deel gaat om informatie voor strafzaken, zoals overvallen of ontvoeringen. De vragen hebben betrekking op informatie over de Facebook gebruiker zoals naam en hoelang iemand al Facebook gebruikt. De vragen hebben ook betrekking op IP adressen waarmee op het social media platform is ingelogd en inhoud van het Facebook account. Facebook geeft geen specifieke voorbeelden van de opgevraagde informatie in Nederland. In de Transparency rapporten van Facebook wordt niet ingegaan op surveillance door opsporings- of inlichtingendiensten, al dan niet door het inhuren van private inlichtingenbedrijven. Een Transparency rapport met getallen over het informatieverzoeken van opsporings- en inlichtingendiensten levert niet veel inzicht op.

De opmerking van Coosto in haar blog bericht van 29 juni 2017 over de behandeling van ‘security requests’ van overheidsorganisaties door Facebook is dus nietszeggend. Ook IT bedrijven moeten ingaan op een vordering voor informatie van politie en justitie.

Facebook laat echter zelf ook geen actief beleid ten aanzien van de bestrijding van social media surveillance zien. Er zijn namelijk geen aanwijzingen dat Facebook zelf na 13 maart 2017 actief bedrijven heeft aangeschreven om hen te wijzen op de nieuwe voorwaarden.

Facebook vermijdt tot haar e-mail van 21 augustus 2017 ook vragen over het aanleggen van databanken van online en social media data. Facebook antwoordt dan dat zij contact hebben gehad met Coosto die Facebook te kennen geeft alleen specifieke informatie te bewaren en die alleen te delen met specifieke Facebook accounts. “They are storing information but only specific information and only sharing it with the specific Page owners.” Volgens Facebook is dit in overeenstemming met de platformvoorwaarden want het bedrijf verbiedt niet het bewaren van data van je eigen Facebook account. Vraag is echter wat zowel Facebook als Coosto bedoelen met ´specific information´ en ´sharing it with the specific Page owners.´ In de verduidelijking van Coosto staat namelijk niet dat Coosto alleen de Facebookpagina´s van hun klanten onderhoudt en bewaart.

Geen transparantie over social media surveillance

Social media platformen hebben geen actief en transparant beleid om surveillance te voorkomen. Twitter, LinkedIn, Google, Pinterest, 4chan, Reddit nemen niet de moeite om in te gaan op specifieke vragen over social media surveillance. Facebook is naar aanleiding van vragen van Buro Jansen & Janssen wel in gesprek gegaan met Coosto, al gaat Facebook niet in op vragen met betrekking tot andere social media monitoring bedrijven, Obi4wan en Buzzcapture. Hoewel Facebook zich dus iets actiever opstelt dan andere sociale media bedrijven maakt het bedrijf niet duidelijk of het zelf actief op zoek gaat naar bedrijven die data verzamelen en doorverkopen voor surveillance doeleinden.

Facebook geeft ook niet aan welke bedrijven op de vingers zijn getikt en afgesloten van de social media datastromen en of de databanken van deze bedrijven daadwerkelijk zijn vernietigd. Ook heeft het bedrijf geen transparante procedure om bedrijven te melden die mogelijk Facebook data gebruiken voor surveillance doeleinden. Ook publiceert Facebook geen algemene lijst met de namen van bedrijven waarmee Facebook een overeenkomst heeft voor het gebruik van Facebook data en onder welke voorwaarden dit dan gebeurt. Het bedrijf heeft misschien wel haar voorwaarden aangepast, maar van een actief en transparant beleid om te voorkomen dat social media data worden gebruikt voor surveillance doeleinden is ook bij Facebook geen sprake.

Overgeleverd aan de grillen van social media multinationals; Facebook en Twitter en de Nederlandse social media surveillance (pdf)

Gehele Observant #70 social media surveillance in Nederland (pdf)

Andere artikelen

Social Media Surveillance in Nederland

Dagelijkse en structurele monitoring; De Nederlandse politie en social media surveillance

Reputatie management bedrijven, de nieuwe private inlichtingendiensten

De burger als dreigingsscore; Social media surveillance in de Verenigde Staten

Bijlagen

Facebook

letter to Facebook (pdf)

eerste e-mail van Facebook (pdf)

tweede e-mail van Facebook (pdf)

derde e-mail van Facebook (pdf)

vierde e-mail van Facebook (pdf)

Twitter

letter to twitter (pdf)

eerste e-mail van Twitter (pdf)

tweede e-mail van Twitter (pdf)

Google

letter to Google (pdf)

eerste e-mail van Google (pdf)

tweede e-mail van Google (pdf)

LinkedIn

letter to LinkedIn (pdf)

eerste e-mail van LinkedIn (pdf)

tweede e-mail van LinkedIn (pdf)

4chan

letter to 4chan (pdf)

Pinterest

letter to Pinterest (pdf)

Reddit

letter to Reddit (pdf)

Naar inhoudsopgave Observant #70

Maak het werk van Buro Jansen & Janssen mogelijk

Word donateur

Wilt u dat Buro Jansen & Janssen de komende jaren onderzoek blijft doen naar politie, justitie en inlichtingendiensten, overheidsoptreden in het algemeen, bedrijven die meewerken aan repressief overheidsbeleid en/of zelf ook repressief of diep ingrijpen in het leven van burgers in Nederland en Europa steun ons dan.
Word donateur of vraag familie, vrienden en bekenden donateur te worden. Bankrekening NL56 INGB 0000 6039 04 ten name van Stichting Res Publica, Postbus 11556, 1001 GN Amsterdam.
Stichting Res Publica 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.

Al 30 jaar diepgravend, kritisch en doortastend burgerrechten onderzoek. Buro Jansen & Janssen, gewoon inhoud

Doorlopend Jaarverslag activiteiten
Buro Jansen & Janssen 2013 – 2017

Publicaties

Zeven edities van de Observant (zie inhoud onderaan)
In 2013 één, 2014 twee, in 2015 ook twee, in 2016 één, in 2017 één

Een Observant in 2017 in het teken van Politie Mercenaries
https://www.burojansen.nl/category/observant/observant-69/

Een brochure in 2016 over de nauwe band tussen wetenschappers en de politie en een falende multicultureel beleid bij de Nationale Politie
https://respubca.home.xs4all.nl/pdf/Observant68BuroJansenJanssenapril2016.pdf
Een brochure in 2015 in het teken van veiligheid van data op het internet
https://respubca.home.xs4all.nl/pdf/Observant67BJJaug2015.pdf

Een brochure in 2015 in het teken van het criminaliseren van politiek protest
https://respubca.home.xs4all.nl/pdf/Observantnummer6630maart2015.pdf

Een brochure in 2014 in het teken van G4S, lopend onderzoek, en Facebook ook lopend onderzoek
https://respubca.home.xs4all.nl/pdf/BuroJansen&Janssenobservant65mintweebijdragen.pdf

Een Observant in 2014 in het teken van de profielschetsen vreemdelingen in detentie
http://respubca.home.xs4all.nl/pdf/observant64profielvluchtelingingevangenis.pdf

Een Observant in 2013 in het teken van Ideologische orde

Algemene ondersteuning

- hulpvragen via internet en telefoon
Divers tussen teruggestuurd van een vlucht naar de VS, tot vrijheid van meningsuiting op koningsdag, tot werknemers van provincie en

universiteit die last hebben van een privaatrechercherchebureau tot beleid rond homo ontmoetingsplek tot recherche bij uitkeringsgerechtigden, mishandeling door politie, gebrekkig politie optreden bij ongelukken, etc. Gemiddeld twee of drie per week, rond de 200/250 op jaar basis.

Specifieke Ondersteuning
- diverse andere groepen en individuen die actief zijn rond politiek/sociaal/maatschappelijke thema's
- studenten nieuwe universiteit (advies, interventie, steun bij klachten en informatieverzoeken)
- gaswinning in Groningen (onderzoek inlichtingenoperatie, voorlichting, advies)
- jacht campagne (onderzoek zowel naar inlichtingenoperatie als de jacht)
- dierenrechten (onderzoek inlichtingenoperatie)
- hackers/politieke internet gebruikers (onderzoek inlichtingenoperatie)
- groepen in het buitenland (onderzoek inlichtingenoperatie)

Online

Jansen & Janssen probeert duizenden unieke bezoekers per dag zo goed mogelijk van dienst te zijn met diverse websites die allemaal verschillende delen van het Jansen werk openbaren.

- burojansen.nl de centrale site die hopelijk dit jaar wordt vernieuwd
- justitieenveiligheid.nl met directe reacties op veiligheid en justitie
- nieuwsblog.burojansen.nl met buitenlands nieuws
- openbaarheid.nl Wobstukken
- hetnationaalveiligheidsarchief.nl met inlichtingendiensten stukken
- crowddigging.nl de Nederlandse cables

Lopend onderzoek

Naast het reguliere onderzoek van Jansen & Janssen
- publiek – private samenwerking: op dit moment G4S, Fox-IT en andere bedrijven
- wetenschap en politie/justitie/inlichtingendiensten, is er een onderscheid?
- aanhoudingseenheden onderzoek
- radicale moslims in het vizier, maatregelen van de overheid tegen moslim jongeren

- anti terreur maatregelen onderzoek, samenwerking van Nederland met discutabele regimes.
- de overheid online onderzoek, surveillance door de politie, acties tegen radicale uitingen etc.
- facebook surveillance onderzoek
- gearresteerd en wat nu?
- politiecontroles onderzoek in breedste zin van het woord
- digitale tips tegen tralies onderzoek
- AIVD publicatie

Nog enkele andere onderzoeken gericht op Nederland en/of Europa

Inhoud van de zeven edities van de Observant

Inhoudsopgave Observant #69, januari 2017, Politie Mercenaries
Boeven vangen met dubieuze software van dubieuze bedrijven
De Nederlandse politie en Hacking Team
Gamma Group en de politie
Providence en de Nationale Politie
Hacking Team; Italiaanse staatsnerds in dienst van dictators
Gamma Group/Louthean Nelson; Wapenhandelaars pur sang
Providence; SAS tussenhandelaar van inbrekers-kits tot digitale wapens
Kailax; De magische hand van de Israëlische inlichtingendienst
Na privacy en de onschuld, is nu ook de veiligheid dood
Dutch secret service tries to recruit Tor-admin
AIVD benadert Tor-beheerder (NL)
Vernieuwde website J&J en Contrast Network
Stay Secure Online 2016
Sympathie voor het werk van Buro Jansen & Janssen?

inhoudsopgave Observant #68
Wetenschappers in dienst van de overheid (samenvatting)
Wetenschappers in dienst van de overheid
Het onderzoek van de Universiteit van Leiden naar etnisch profileren in Den Haag: een reconstructie
Professoren als spreekbuis van de politie (samenvatting)
Professoren als spreekbuis van de politie
De Universiteit van Leiden en etnisch profileren
In vogelvlucht, Wetenschappelijk onderzoek naar politiediscriminatie
Meervoudig Wegkijken (samenvatting)

Meervoudig Wegkijken, Multicultureel vakmanschap bij de politie
Ode aan data-bevrijders als Chelsea Manning, Jeremy Hammond
Justitie en veiligheid blog: justitieenveiligheid.nl
Maak het werk van Buro Jansen & Janssen mogelijk

Inhoudsopgave Observant #67

Overheid blijft verdienen aan ID-controles
Jouw data is zelden veilig bij een beheerder
Hoe zit het eigenlijk met mijn data?
Het COA stuurde vrijwilliger weg om geëngageerdheid
Dubieus onderzoek VU/NSCR naar cybercriminaliteit
Solidarity with imprisoned activists with/without Facebook
Exposed on Facebook
Amsterdam Oost ten onrechte preventief fouilleren
Veiligheidsarchief, daar hebben we AIVD niet voor nodig
Nieuw blog over justitie- en veiligheidsbeleid
Onderzoek naar politieoptreden Haaglanden
Voorzichtig de vijand heeft grote oren
Tips om veiliger te e-mailen
Buro Jansen & Janssen heeft geld nodig

Inhoudsopgave Observant # 66

Korte overzicht van de artikelen
Het terroriseren van politiek protest
De terreurambtenaar van de NCTV
De jihadistische tunnelvisie van de NCTV
Radicaal Extremistisch Terroristisch Groningen
Beroepsverbod voor familielid activiste
Verstoring van politiek protest
Inlichtingendienst intimideert anti-monarchist
Linkse activist krijgt politie stempel terrorist
Grasduinend door mijn politiedossiers
Doelgroep monitoring: Politiek protest
Politie registreert politiek engagement
DTN: Dreigingsbeeld diarree
Charlie Hebdo: Wat rest is schaamte en vragen...
Politie Haaglanden kan niet tegen kritiek
Overheid ontmoedigde het protest rondom NSS-top
Wijkagent: Gaat u soms naar de NSS-top?
De schaduw van de staat
Occupyer benaderd door de RID
Undercover, True Story of Britain’s Secret Police

Het verwrongen wereldbeeld van de NCTV I kort NL
Het verwrongen wereldbeeld NCTV I analyse NL
Jihadistische angstvisioenen NCTV II kort wereld
Jihadistische angstvisioenen NCTVII analyse wereld
The Criminalization of Dissent by Law Enforcement
Prevent and Tame. Protest under (Self)Control
Bringing the War Home
Buro Jansen & Janssen heeft geld nodig

Inhoudsopgave Observant #65

G4S: Media, privatisering en burger-/mensenrechten
Media smullen van G4S
The United Nations and G4S
Dangerous Partnership
Overheidstaken G4S in strijd duurzaamheidsbeleid
Met de billen bloot op Facebook
Facebook, het ultieme inlichtingenbedrijf
Google zoekt met je mee...
AIVD benadert IT
Van bemiddelaar tot doelwit AIVD
Boekrecensie: The Way of the Knife
migratie-beleid.nl
Grensgevangenen
Donateurs gezocht

inhoudsopgave Observant #64

profiel vreemdelingen in detentie: Justitie Spasme
profiel vreemdelingen in detentie: openbaarmaking
profiel vreemdelingen in detentie: leeswijzer
profiel vreemdelingen in detentie: onderzoek
overheid benadert hackers
UK: Special Branch Spied on Animal Rights Movement
NSA: Uncle Sam’s grote oren
NSA: Op het spoor van de afluisteraars
NSA: It Greate Ear
Ana Montes: de Cubaanse Poor Man's NSA
donateurs gezocht

Inhoudsopgave Observant #63

Ideologische orde: Gaan we protesteren?
Discrimineert de politie?
Preventief fouilleren omdat het mag!/moet?

Chiquita & Myth of Corporate Social Responsibility
"Hallo, met de AIVD"
NL strijders in Syrië verdienen onderscheiding
Inside British Intelligence
Administratieve Apartheid
Bedankt voor de sympathie voor Jansen & Janssen

Naar inhoudsopgave Observant #70

Your mind is programmable – if you're not programming your mind, someone else will program it for you.
— Jeremy Hammond —

As a result of the Stratfor hack, some of the dangers of the unregulated private intelligence industry are now known. It has been revealed that Stratfor maintained a worldwide network of informants that they used to engage in intrusive and possibly illegal surveillance activities on behalf of large multinational corporations.
— Jeremy Hammond —