

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 Snap Trends 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 sentimentanalyse. 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, Snaptrrends 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 bevestigt? 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, Snap Trends 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 dreigingscore; 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 factsheet 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

[reputatiemanagement bedrijven factsheets 2014 \(pdf\)](#)

[reputatiemanagement bedrijven 2012 \(pdf\)](#)

[Monitoring 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 \(pdf\)](#)