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). “ln-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