

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, Snap Trends en Media Sonar tot gevolg gehad dat grote social media platformen besloten om deze bedrijven de toegang tot hun gebruikersdata te ontfemen. Twitter en Facebook besloten Geofeedia in oktober 2016 af te sluiten van haar datastroom. Snap Trends 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 aanleiding 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 gemaïld 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 specifiek 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 specifiekker 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 van 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 Snap Trends. 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 bevreedend 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 \(pdf\)](#)