arsaequi.nl/maandblad AA20150287

Burgers tegen Plasterk: het Nederlandse staartje van de Snowden-saga

Ot van Daalen*

De Snowden-onthullingen haalden niet alleen wereldwijd de media en het parlementair debat. Ze leidden zelfs tot een Nederlandse rechtszaak over communicatieprivacy. Een principiële rechtszaak over burgerrechtenactivisme, surveillance en politieke intrige, met een verrassende, maar ook teleurstellende uitkomst. Dit moet je weten.

1 Inleiding

In een kamer in hotel The Mira in Hong Kong zette een Amerikaanse systeemadministrator in juni 2013 de wereld van geheime diensten volledig op zijn kop. Na maandenlang aandringen had hij de relatief onbekende journalist Glenn Greenwald en documentairemaker Laura Poitras zo ver gekregen dat ze op stel en sprong in het vliegtuig stapten om hem te ontmoeten. Ze wisten niet wie ze moesten verwachten, en waren verrast dat een jongensachtige nerd met een Rubiks kubus hen stond op te wachten bij de afgesproken plek. Maar toen ze deze nerd aan een kruisverhoor onderwierpen werd al snel duidelijk: dit was de *real deal*. Deze systeemadministrator had een ware schatkist aan geheime documenten van de afluistereenheid van de Amerikaanse geheime dienst, de National Security Agency (NSA), meegenomen omdat hij zich ernstig zorgen maakte. Hij wilde dat de journalisten die informatie met de wereld deelden.

Vanaf juni 2013 tot nu zijn tientallen meer en minder belangrijke onthullingen over geheime diensten, en vooral de NSA, door journalisten wereldkundig gemaakt

De klokkenluider, die zich een paar dagen na de eerste publicatie onthulde als Edward Snowden, had zich geen betere boodschappers kunnen wensen. Vanaf juni 2013 tot nu zijn tientallen meer en minder belangrijke onthullingen over geheime diensten, en vooral de NSA, door journalisten wereldkundig gemaakt. Zo weten we dat de NSA een budget van bijna een kwart miljard dollar per jaar vrijmaakt om de belangrijkste beveiligingstechnologieën van het internet te ondermijnen. De NSA bleek op het IT-netwerk van nieuwszender Al Jazeera te hebben ingebroken, en jarenlang toegang te hebben gehad tot communicatie van medewerkers. De Engelse afluisterdienst, de Government Communications Headquarters (GCHQ), heeft ingebroken op de Belgische telecomprovider Belgacom, en kon vermoedelijk op die manier telefoongesprekken van het Europees Parlement en de Europese Commissie afluisteren. Politieke leiders, zoals Merkel, en industriegiganten, zoals Petrobras, zijn afgeluisterd. Soms werd zelfs de communicatie van hele landen, zoals de Bahama's, afgeluisterd. Na het lezen van de eindeloze stroom berichten is het misschien makkelijker om je af te vragen wat de NSA en de andere geheime diensten *niet* hebben gehackt.

Al snel nadat Edward Snowden de documenten aan Greenwald had overgedragen onthulde *The Guardian* twee zeer ingrijpende

* Mr. O.L. van Daalen is advocaat te Amsterdam en onderzoeker privacy- en securityrecht bij het Instituut voor Informatierecht. Voorheen was hij directeur van de digitale burgerrechtenbeweging Bits of Freedom.

surveillanceprogramma's. Met het eerste programma, Prism, zou de NSA direct toegang krijgen tot sociale media, zoals Facebook en Gmail. Met het tweede surveillanceprogramma, Tempora, zou de Engelse afluisterdienst al het internetverkeer dat via zeekabels langs het Verenigd Koninkrijk loopt onderscheppen. Het zijn twee uitwassen van een instelling die in een uitgelekte dia van GCHQ werd samengevat onder het motto: 'collect it all'.

Na het lezen van de eindeloze stroom berichten is het misschien makkelijker om je af te vragen wat de NSA en de andere geheime diensten *niet* hebben gehackt. Ook de communicatie van Nederlanders werd onderschept

Deze twee programma's hebben één ding gemeen: ook de communicatie van Nederlanders werd hierdoor onderschept. Immers: als je gebruik maakte van Facebook, dan had de NSA direct toegang tot jouw gegevens. Omdat een serieus deel van het internetverkeer via het Verenigd Koninkrijk liep, was er ook een grote kans dat communicatie van Nederlanders via Tempora werd binnengehaald.

Dat was al erg genoeg, en in verschillende landen leidde dit tot rechtszaken. Zo lopen er rechtszaken tegen de Engelse regering over Tempora, en lopen er in de VS rechtszaken over de grootschalige afluisterprogramma's van de NSA. Eén punt dat hierin echter niet word geadresseerd, is de vraag of de Nederlandse geheime diensten, de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), ook van deze programma's gebruik maakte. De Nederlandse geheime diensten hebben namelijk niet de verstrekkende bevoegdheden om programma's zoals die van NSA en GCHQ op te zetten. Meer specifiek hebben de Nederlandse diensten niet de bevoegdheid om communicatie die via kabels loopt – zogenoemde 'kabelgebonden' communicatie – ongericht te onderscheppen. Het is dan ook denkbaar dat de Nederlandse geheime diensten door uitwisseling van gegevens met de Amerikaanse en de Engelse afluisterdiensten gegevens konden verkrijgen, die ze zelf niet hadden *kunnen* verzamelen. Sterker nog: die ze zelf niet hadden *mogen* verzamelen.[1]

Het is denkbaar dat de Nederlandse geheime diensten door uitwisseling van gegevens met de Amerikaanse en de Engelse afluisterdiensten gegevens konden verkrijgen, die ze zelf niet hadden *kunnen* verzamelen. Sterker nog: die ze zelf niet hadden *mogen* verzamelen

De gegevensuitwisseling met de Nederlandse geheime diensten wordt in grote lijnen geregeld in de Wet op de inlichtingen- en veiligheidsdiensten (Wiv). In grote lijnen, want er is niet erg veel geregeld over deze uitwisseling. Artikel 59 van de Wiv bepaalt slechts dat er 'verbindingen' worden onderhouden met andere geheime diensten, dat de Nederlandse diensten daartoe gegevens mogen verstrekken aan buitenlandse diensten en dat ze die andere diensten mogen ondersteunen. Er staat niet dat de Nederlandse diensten ook gegevens mogen krijgen of vragen van buitenlandse diensten. Toch is er al jaren een praktijk van het uitwisselen van gegevens op basis van wederkerigheid: dat wordt in de kringen van geheime diensten het *quid pro quo*-beginsel genoemd. Dat betekent dat Nederlandse diensten niet alleen gegevens verstrekken, maar ook mogen ontvangen en daar zelfs om vragen, ook al staat de bevoegdheid daarvoor niet met zoveel woorden in de wet. Onderdeel van deze praktijk is dat geheime diensten *ook* niet vragen naar de herkomst van informatie: dit zou – zo is de redenering – de bronnen van de verstrekkende dienst in gevaar kunnen brengen.

Mogen de AIVD en de MIVD gegevens ontvangen van andere geheime diensten, als die verkregen zijn op een manier die volgens Nederlands recht niet toelaatbaar zou zijn?

2 De insteek van de rechtszaak

Dat is de aanleiding van de te bespreken rechtszaak, waar de vraag centraal staat of de AIVD en de MIVD gegevens mogen ontvangen van andere geheime diensten, als die verkre-

1 Zie art. 25 en 26 WIV 2002.

Ontwerp: Irene Poppelier
Foto: Marten Hoogstraat(*www.whiteframe.nl*)

gen zijn op een manier die volgens Nederlands recht niet toelaatbaar zou zijn.[2] Volgens de eisers mogen de Nederlandse diensten dat niet, omdat ze in strijd handelen met artikel 8 (het grondrecht op privacy) en artikel 10 (het grondrecht op vrijheid van meningsuiting) van het EVRM en met de Wiv zelf.

Een brede coalitie belanghebbenden dagvaardden de Staat. Die coalitie bestond uit privépersonen met eigen belangen en niet-gouvernementele organisaties (NGO's) die een meer algemeen belang vertegenwoordigen. De privépersonen zijn een bont gezelschap die allemaal stellen dat ze er rekening mee moeten houden dat de Amerikaanse overheid interesse heeft in hun gegevens. Eén van de personen waar die zorg zonder enige twijfel terecht is, is Rop Gonggrijp, een van de meer bekende hackers van Nederland. Hij stelde dat de Amerikaanse overheid geïnteresseerd was in zijn gegevens naar aanleiding van een lopend onderzoek van het Amerikaanse Openbaar Ministerie over zijn betrokkenheid bij WikiLeaks. Andere privé-eisers waren een beveiligingsonderzoeker, een journalist, een advocaat en een wetenschapper. De groep van

2 Rb. Den Haag 23 juli 2014, ECLI:NL:RBDHA:2014:8966.

organisaties die belang hebben bij vertrouwelijkheid van hun communicatie is ook breed: de Nederlandse Vereniging voor Journalisten (NVJ), de Nederlandse Vereniging voor Strafrechtadvocaten (NVSA), de stichting Privacy First (die zich inzet voor privacy) en de Internet Society (die zich inzet voor de ontwikkeling van het internet).

Het doel van de eisers is om een einde te maken aan de ontvangst en het gebruik van gegevens van buitenlandse diensten die, volgens Nederlands recht, via ongeoorloofde middelen zijn vergaard. Daarnaast willen de eisers dat zij worden geïnformeerd als inderdaad ongeoorloofd verkregen gegevens over hen van een buitenlandse dienst zijn ontvangen.

De inzet van de eisers is om een einde te maken aan de ontvangst en het gebruik van gegevens van buitenlandse diensten die, volgens Nederlands recht, via ongeoorloofde middelen zijn vergaard

In een uitgebreid vonnis bespreekt een meervoudige kamer van de Rechtbank Den Haag deze vorderingen. Maar in het kader van deze bespreking gaat ze ook in op meer algemene vragen: in hoeverre hebben de eisers wel een belang bij hun vorderingen, en in hoeverre wordt de privacy wel geschaad door het uitwisselen van dit soort gegevens? Deze twee vragen komen eerst aan de orde.

3 Procederen over wetten wordt makkelijker

Deze rechtszaak tegen de Staat is niet de eerste keer dat een fundamentele vraag over burgerrechten aan de rechter wordt voorgelegd. Je zou zelfs kunnen spreken van een voorzichtige trend: er wordt steeds meer geprocedeerd tegen de Staat om wetten aan te vechten. Zo is de afgelopen jaren de centrale opslag van vingerafdrukken die worden afgenomen in het kader van de uitgifte van een paspoort aangevochten via de rechter (door Privacy First, die ook in deze zaak partij is).[3] Ook is de Staat is gedaagd vanwege het ongericht opslaan van communicatiegegevens (de Wet bewaarplicht telecommunicatiegegevens).[4]

Een belangrijke horde die bij de meeste van die zaken moet worden genomen, is of de eisers wel voldoende belang hebben bij hun vordering, zoals vereist op grond van artikel 3:303 BW. In dit geval, maar ook in de twee zaken die hierboven zijn genoemd, maken de eisers bezwaar tegen de verwerking van gegevens met een ongericht karakter: de surveillance is niet speciaal op hen gericht, maar het is niet uitgesloten, en misschien zelfs aannemelijk, dat zij wel slachtoffer zijn daarvan. In de Verenigde Staten is geoordeeld dat eisers in een vergelijkbaar geval geen belang hebben – geen *standing* – omdat ze niet kunnen bewijzen dat ze zelf zijn afgeluisterd.[5]

De eisers maken bezwaar tegen de verwerking van gegevens met een ongericht karakter: de surveillance is niet speciaal op hen gericht, maar het is niet uitgesloten, en misschien zelfs aannemelijk, dat zij wel slachtoffer zijn daarvan

De Nederlandse rechter is minder streng: de rechtbank neemt de belanghebbende-horde vrij makkelijk. Daarbij moet onderscheid worden gemaakt tussen de vraag of de privé-eisers voldoende belang hebben, en de vraag of de stichtingen ontvankelijk zijn.

Voor privépersonen moet volgens de rechtbank aannemelijk zijn dat een eiser, 'meer dan de gemiddelde burger van Nederland', onderwerp van onderzoek door de geheime diensten zou kunnen zijn.[6] Dit hoeft dus niet daadwerkelijk zo te zijn. Bovendien loopt iedereen het risico dat gegevens op grond van de Wiv over hem verzameld worden. Met een verwijzing naar artikel 6 EVRM, dat het grondrecht op toegang tot de rechter waarborgt, concludeert de rechtbank dat de privé-eisers een voldoende concreet en eigen belang hebben bij hun vorderingen.

Voor de stichtingen overweegt de rechtbank dat de NVSA en de NVJ kunnen profiteren van het recht op collectieve actie van artikel 3:305a BW.[7] De NVSA bundelt de belangen van strafrechtadvocaten bij de vertrouwelijke communicatie met hun cliënten. De NVJ bundelt de belangen van journalisten. Ten aanzien van Privacy First en Internet Society stelde de Staat dat de bestuursrechtelijke rechtsgang voor de belanghebbenden die zij

3 Hof Den Haag 18 februari 2014, ECLI:NL:GHDHA:2014:412.
4 Rb. Den Haag 11 maart 2015, ECLI:NL:RBDHA:2015:2498.
5 US Supreme Court (Verenigde Staten) 26 februari 2013 (*Clapper v. Amnesty International USA.*), 568 U.S. (2013).
6 Rb. Den Haag 23 juli 2014, ECLI:NL:RBDHA:2014:8966, r.o. 5.2.
7 Rb. Den Haag 23 juli 2014, ECLI:NL:RBDHA:2014:8966, r.o. 5.3.

vertegenwoordigen openstaat. De rechtbank gaat hierin niet mee: ook deze stichtingen zijn ontvankelijkin deze rechtszaak.[8]

Het is mooi om te zien dat de rechtbank alle eisers in deze zaak ontvankelijk verklaart, en dat redelijk uitgebreid motiveert. Die overwegingen openen namelijk verder de weg naar rechtszaken tegen andere ongerichte verwerking van gegevens door eisers die niet kunnen bewijzen dat hún gegevens zijn verwerkt. De inhoudelijke toetsing door de rechtbank van de ongerichte surveillance door de Staat pakt echter minder positief uit voor die toekomstige rechtszaken.

Het is mooi om te zien dat de rechtbank alle eisers in deze zaak ontvankelijk verklaart, en dat redelijk uitgebreid motiveert

4 Zijn gegevens in strijd met artikel 8 EVRM verzameld?

De eerste vraag die de rechtbank zich stelt, is of het inderdaad bewezen is dat de Nederlandse diensten gegevens hebben ontvangen die door buitenlandse diensten mogelijk in strijd met het grondrecht op privacy zoals neergelegd in artikel 8 EVRM zijn verzameld. Dat is volgens de rechtbank het geval. Het probleem is natuurlijk dat er over de werkwijze van de Nederlandse geheime diensten weinig bekend is – het zijn per slot van rekening *geheime* diensten. Een rapport van 5 februari 2014 van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) biedt echter enig inzicht.[9]

Is het inderdaad bewezen dat de Nederlandse diensten gegevens hebben ontvangen die door buitenlandse diensten mogelijk in strijd met het grondrecht op privacy zoals neergelegd in artikel 8 EVRM zijn verzameld?

De CTIVD constateert dat de Nederlandse diensten geregeld 'sigint' – wat staat voor *signal intelligence*, oftewel kennis vergaard door het onderscheppen van communicatie – ontvangen. Sommige buitenlandse diensten van wie zij die gegevens ontvangen hebben de bevoegdheid om ongericht kabelgebonden communicatie te onderscheppen – iets wat de Nederlandse diensten, zoals hierboven al is opgemerkt, dus niet mogen. Zij ontvangen daardoor wellicht ook gegevens die het resultaat zijn van dat soort interceptie, aldus de CTIVD. De rechtbank sluit zich hierbij aan en concludeert dat de Nederlandse diensten 'mogelijk' gegevens ontvangen van buitenlandse diensten die zijn verzameld met bevoegdheden waarover de Nederlandse diensten niet beschikken.

Vervolgens concludeert de rechtbank na een korte analyse van de Amerikaanse regelgeving dat er rekening mee moet worden gehouden dat de Nederlandse diensten gegevens ontvangen die zijn verzameld op een manier die niet in overeenstemming is met artikel 8 EVRM. Overigens kan je bij deze formulering nog wel een vraagteken zetten, want artikel 8 EVRM is natuurlijk niet van toepassing op de NSA, omdat de Verenigde Staten geen verdragspartij is. De *strekking* van die conclusie, namelijk dat als het EVRM op de NSA van toepassing was geweest, de NSA mogelijk in strijd met het EVRM gegevens verzamelt, is natuurlijk wel verdedigbaar vanwege het ongerichte karakter van de verzameling.

De rechtbank concludeert dat er rekening mee moet worden gehouden dat de Nederlandse diensten gegevens ontvangen die zijn verzameld op een manier die niet in overeenstemming is met artikel 8 EVRM

5 Drie tegenstellingen in het privacydebat

De volgende vraag is of de 'uitwisseling' (aldus de rechtbank, hoewel ze natuurlijk slechts de ontvangst van gegevens bedoelt) in overeenstemming met artikel 8 EVRM is. Voorstanders van surveillanceprogramma's spelen in het publieke debat vaak drie troefkaarten. Ze stellen ten eerste dat het onderscheppen van de *inhoud* van communicatie ernstiger is dan het onderscheppen van de gegevens *over* die communicatie (de 'metadata'). Ook stellen ze dat het *verzamelen* van gegevens op zich niet inbreukmakend is, mits de *daaropvolgende verwerking* maar met voldoende waarborgen omkleed is. Tot slot zou het *gericht* analyseren

8 Rb. Den Haag 23 juli 2014, ECLI:NL:RBDHA:2014:8966, r.o. 5.4.

9 *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, CTIVD nr. 38, 5 februari 2014, te vinden op: *www.aivd.nl/publish/pages/2605/ctivd_toezichtsrapport_gegevensverwerking_telecommunicatie_nr_38.pdf*.

van gegevens een minder ernstige inbreuk vormen dan het geautomatiseerd verwerken van die gegevens *in bulk*. Die drie tegenstellingen – metadata versus inhoud, verzameling versus verwerking en gericht versus bulk – spelen een belangrijke rol in de inhoudelijke toetsing door de rechtbank.

De rechtbank bespreekt deze tegenstellingen in het kader van de toetsing van de uitwisselingspraktijk aan artikel 8 EVRM. Hoewel dat niet heel duidelijk uit de verf komt, lijkt de rechtbank zich vooral te richten op de vraag of deze praktijk aan de voorzienbaarheidseis voldoet. Hoe meer inbreukmakend de wet, hoe hoger de eisen die daaraan moeten worden gesteld, en dan vooral aan de voorzienbaarheid ervan, zo lijkt de rechtbank te redeneren. En de rechtbank komt vervolgens tot de opmerkelijke conclusie dat de enkele ontvangst van metadata in bulk niet zo inbreukmakend is. Hieronder komen de belangrijkste elementen van die analyse aan bod.

Hoe meer inbreukmakend de wet, hoe hoger de eisen die daaraan moeten worden gesteld, zo lijkt de rechtbank te redeneren. En de rechtbank komt vervolgens tot de opmerkelijke conclusie dat de enkele ontvangst van metadata in bulk niet zo inbreukmakend is

Metadata versus inhoud

De rechtbank waagt zich allereerst aan de grondrechtelijke beoordeling van de verwerking van de inhoud versus de metadata van communicatie. Metadata zijn zoals hierboven besproken de gegevens óver communicatie, zoals wie belde, wanneer, hoe lang, waar, et cetera. Je zou metadata ook gedragsgegevens kunnen noemen, omdat je daarmee het gedrag van de betrokkene in kaart kan brengen. Metadata wordt in het grondrechtelijk debat vaak afgezet tegen de inhoud van de communicatie: *wat* iemand communiceert.

De rechtbank is niet de eerste die een oordeel moet vellen over de relatieve ernst van de inbreuk van de verwerking van metadata versus de inhoud van communicatie. Er wordt in dit debat vaak teruggegrepen naar EHRM-jurisprudentie uit de jaren tachtig, waarin het Hof minder bescherming toekende aan zogenoemde *metering*-informatie (dat is informatie over wie, wanneer en hoe lang belde) – dan aan de inhoud van die communicatie.[10] Hoewel de rechtbank het niet met zoveel woorden zegt, lijkt ze dit onderscheid te bevestigen.[11]

Daar valt tegenwoordig wat op af te dingen. Wetenschappers zijn het erover eens dat gedragsgegevens vaak juist méér over iemand zeggen dan de inhoud van die communicatie.[12] Dat komt deels doordat er zo ontzettend veel meer gegevens worden verzameld: met de 'metadata' die wordt verzameld via programma's als Tempora en Prism kan je iemands netwerk en gedrag gedetailleerd in kaart brengen. Onderzoekers stellen dat ze op basis van iemands *likes* kunnen vaststellen of iemand homoseksueel is.[13] Onlangs verscheen zelfs een onderzoek waaruit zou blijken dat een computerprogramma aan de hand van iemands *likes* op Facebook zijn karakter beter kan inschatten dan een partner.[14] Ook het onderzoek van een medewerker van Bits of Freedom, die zijn metadata liet analyseren door een privédetective en daar vervolgens een artikel over liet schrijven op *De Correspondent*, is illustratief: metadata geven een zeer indringend beeld van de medewerker.[15]

Het registreren van telefoniegegevens uit 1979 is in geen enkel opzicht meer relevant voor de beoordeling van de constitutionaliteit van het verwerken van metadata anno 2015

De rechtbank zou er goed aan hebben gedaan te luisteren naar haar Amerikaanse ambtsgenoot Leon, die zich eind 2013 de vergelijkbare vraag stelde of Amerikaanse jurisprudentie uit 1979 over het verzamelen van metadata nog relevant was voor het beoordelen van de surveillanceprogramma's van de NSA. Hij schrijft:

'the almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States is unlike anything that could have been conceived in 1979. […] [N]ot only is the Government's ability to collect, store and analyse phone data greater now than it was in 1979, but the nature and quantity of the information contained in people's telephony metadata is much greater, as well.'[16]

Het is belangrijk dat rechters zich realiseren dat het registreren van telefoniegegevens uit 1979 in geen enkel opzicht meer relevant is voor de beoordeling van de constitutionaliteit van het verwerken van metadata anno 2015.

10 EHRM 2 augustus 1984, 8691/79 (*Malone v. United Kingdom*), r.o. 84.

11 Rb. Den Haag 23 juli 2014, ECLI:NL:RBDHA:2014:8966, r.o. 5.31.

12 Written Testimony of Edward W. Felten, Professor of Computer Science and Public Affairs, Princeton University, United States Senate, Committee on the Judiciary Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act, October 2, 2013, *www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf*.

13 M. Kosinski, D. Stillwell & T. Graepel, 'Private traits and attributes are predictable from digital records of human behavior', *PNAS* 110/15, *www.pnas.org/content/110/15/5802.abstract*, p. 5802-5805. Zie ook de website You Are What You Like (*http://youarewhatyoulike.com/*).

14 Zie W. Youyou, M. Kosinski & D. Stillwell, 'Computer-based personality judgments are more accurate than those made by humans', *Proceedings of the National Academy of Sciences* (112) 2015, p. 1036-1040.

15 D. Tokmetzis, 'Hoe je onschuldige smartphone bijna je hele leven doorgeeft aan de geheime dienst', *De Correspondent* 20 december 2013.

16 US District Court for the District of Columbia (Verenigde Staten) 16 december 2013 (*Klayman v. Obama*).

Verzameling versus verwerking
Het volgende onderscheid dat de rechtbank bespreekt, is dat tussen de verzameling van gegevens en de daaropvolgende verwerking daarvan. De privacyinbreuk is volgens de rechtbank vooral afhankelijk van wat er met de verzamelde gegevens gebeurt, en de rechtbank wekt daarmee de suggestie dat de verzameling op zich vrijwel niet problematisch is.[17] Ook daar valt veel op af te dingen.

Eén van de grootste problemen van ongerichte surveillance is namelijk het *chilling effect* – het gegeven dat mensen zich anders gaan gedragen als ze weten dat ze worden gevolgd. De onthullingen van Snowden hebben het mogelijk gemaakt om hiernaar onderzoek te doen, en dat bevestigt deze zorg. Zo typen mensen na de Snowden-onthullingen significant minder controversiële zoektermen op Google in.[18] Dit *chilling effect* doet zich al voor bij de verzameling van persoonsgegevens, niet slechts bij de verwerking daarvan. Daarbij komt dat de opslagtermijn van door de NSA verzamelde gegevens onduidelijk en mogelijk oneindig is, zodat iedereen wiens gegevens worden opgeslagen er serieus rekening mee moet houden dat die gegevens ooit ook verwerkt worden.

Het is teleurstellend dat de rechtbank zonder overtuigende analyse vergaande conclusies trekt uit het onderscheid tussen verzameling en verwerking van gegevens

Het is teleurstellend dat de rechtbank zonder overtuigende analyse vergaande conclusies trekt uit het onderscheid tussen verzameling en verwerking van gegevens.

Gericht versus bulk
Maar verreweg de meest controversiële conclusie trekt de rechtbank over de beoordeling van de verwerking van gegevens in bulk. Volgens de rechtbank zou namelijk de ontvangst van gegevens in bulk en zonder dat die op relevantie zijn beoordeeld niet aan de strenge eisen hoeven te voldoen die de eisers voor ogen hebben. De suggestie die de rechtbank daarmee wekt is dat het ontvangen van 'ruwe' *intelligence* – bulkgegevens, dus zonder selectie – minder privacyschendend zou zijn dan het ontvangen van gerichte informatie. Dat is een opmerkelijke redenering.

Het is onbegrijpelijk hoe de rechtbank tot de conclusie kan komen dat verwerken in bulk minder problematisch is dan verwerken van gerichte informatie

De kans dat tussen informatie in bulk ook gegevens zitten van mensen die niet eens een doelwit van de geheime diensten zijn, is immers groot. Juist het verwerken van de gegevens van onverdachte mensen maakt een grote inbreuk op de privacy. Het is onbegrijpelijk hoe de rechtbank toch tot de conclusie kan komen dat verwerken in bulk minder problematisch is dan ververwerken van gerichte informatie. Er is een goede kans dat deze redenering in hoger beroep onderuitgaat. Ze overtuigt in ieder geval niet.

Op basis van de bovenstaande redenering, waarbij de rechtbank nog een keer onderstreept dat het hier 'slechts' gaat over het ontvangen van gegevens in bulk, wijst ze de vorderingen af.

Het was de eisers niet alleen te doen om de uitkomst van deze rechtszaak: men wilde ook een politiek punt maken. Dat is gelukt

6 Tot slot
Veel mensen die privacy belangrijk vinden, zullen dit een teleurstellende uitspraak vinden. Maar zoals ik in het begin opmerkte was het de eisers niet alleen te doen om de uitkomst van deze rechtszaak: men wilde ook een politiek punt maken. Dat is gelukt. De media heeft veel aandacht aan de zaak besteed. Het parlement heeft erover gedebatteerd. Sterker nog: de positie van minister van Binnenlandse Zaken en Koninkrijksrelaties Plasterk was even aan het wankelen door feiten die in deze rechtszaak naar boven kwamen (hij zou het parlement onjuist hebben geïnformeerd). En dat is misschien wel de belangrijkste les van deze rechtszaak: burgerrechtenactivisme vindt plaats in de rechtszaal, de media en het parlement. Zelfs als het spaak loopt bij de rechter, kan je nog steeds verandering bewerkstelligen. En gelukkig is hoger beroep aangetekend. Ik wacht de uitkomst met spanning af.

17 Rb. Den Haag 23 juli 2014, ECLI:NL:RBDHA:2014:8966, r.o. 5.32.
18 A. Marthews & C. Tucker, *Government Surveillance and Internet Search Behavior*, gepubliceerd via SSRN: *http://ssrn.com/abstract=2412564*.