Masterthesis MA Internationale Betrekkingen in Historisch Perspectief,
Universiteit Utrecht

Europa en de Verenigde Staten: privacy op straat?

Privacy, elektronische surveillance en metadata na Edward Snowden

J.S. van Tongeren, 3464784
20-6-2016
Begeleider: dr. C. Klep

Voorwoord

Deze masterthesis vindt zijn oorsprong in mijn interesse voor inlichtingendiensten, opgedaan tijdens mijn bachelor Geschiedenis aan de Universiteit Utrecht, en bij de opmerkelijke gebeurtenissen rondom Edward Snowden in juni 2013. Ik fascineerde me over het feit dat zijn onthullingen slechts een relatief korte periode nieuws waren voor de media, terwijl er tegelijkertijd geen nieuwsberichten te zien of te lezen waren over veranderingen met betrekking tot de inlichtingenwereld. Vandaar dat besloot om onderzoek te doen naar de gevolgen van de onthullingen van Snowden op het gebied van privacy en inlichtingendiensten met als resultaat een beschouwing op de ontwikkelingen van de laatste jaren.

Tijdens het doen van het onderzoek was het uiteraard lastig om goed, relevant bronnenmateriaal te vinden. De bronnen zijn deels juridisch van aard: wetsteksten, beleidsmemo's en adviesrapporten. Aangezien ik niet als jurist ben opgeleid, ben ik mij er daarom bewust van dat wellicht op dat vlak aanvullende verdieping mogelijk is geweest. Toch hoop ik dat het eindresultaat de moeite waard is.

Voor het schrijven van deze thesis wil ik een aantal mensen bedanken. Als eerste mijn begeleider Christ Klep, die mij op uitstekende wijze heeft ondersteund en mij ook kon helpen met nieuwe ideeën. Daarnaast wil ik Miriam en Anne-Ruth bedanken die – zij het Miriam in een erg vroeg stadium – ervoor hebben gezorgd dat ik de rit heb weten af te maken. Tot slot wil ik nog mijn ouders bedanken die erg veel geduld hebben moeten opbrengen om dit project tot een goed einde gebracht zien te worden.

Inhoudsopgave

Inleiding: Privacy, inlichtingendiensten en metadata in Europa en de Verenigde Staten

They who can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.

— Benjamin Franklin, Amerikaans politicus

De aanslagen in Parijs op 13 november 2015 deden een schokgolf door Europa gaan. Mensen hadden verdriet, zaten vol onbegrip en boosheid, maar waren daarnaast ook vastberaden en eensgezind. Deze "Europese versie van *9/11*", een vergelijking die her en der in de media opdook, leek Europa net zo te raken als dat de Amerikanen geraakt waren door de aanslagen van 11 september 2001. De connectie met *9/11* was overigens niet nieuw. Ook na de aanslag op *Charlie Hebdo* van 7 januari 2015 werd er gesproken over een "Europese *9/11*".[1]

Waar de Amerikaanse president George W. Bush zich na de aanslagen van *9/11* richtte op de 'As van het Kwaad', Al Qaida en de *War on Terror*, verklaarde de Franse president François Hollande dat Frankrijk in oorlog was met Islamitische Staat (IS), de organisatie die de aanslagen in Parijs had opgeëist.[2] Vervolgens begon Hollande aan een internationale rondgang om steun te verkrijgen voor een coalitie tegen IS.[3]

Aan de andere kant van de Atlantische Oceaan klonk een heel ander geluid. Volgens James Woolsey, van 1993 tot 1995 directeur van de *Central Intelligence Agency* (CIA), kleefde het bloed van de 130 doden van de aanslagen in Parijs niet alleen aan de handen van de daders, maar ook aan de handen van iemand die ruim 2800 kilometer verderop zat: Edward Snowden. Woolsey gaf in een interview met CNN aan dat wat hem betreft Snowden in de Verenigde Staten (VS) berecht diende te worden en wegens landverraad diende te worden opgehangen.[4] Hoewel bij lange na niet met zulke extreme bewoordingen, vond de strekking van het verhaal van Woolsey – dat Edward Snowden debet

[1] Lyse Doucet, 'Paris attack: From 9/11 to 1/11' (versie 12 januari 2015), http://www.bbc.com/news/world-europe-30786552 (15 januari 2016); Dominique Moïsi, 'Charlie Hebdo. Un 11-Septembre de la France?' (versie 9 januari 2015), http://www.ouest-france.fr/debats/editorial/charlie-hebdo-un-11-septembre-de-la-france-3103540 (15 januari 2016).

[2] De term 'de As van het Kwaad' werd door President George W. Bush voor het eerst gebruikt in zijn State of the Union-toespraak in 2002. De kwalificatie gold in eerste instantie voor de landen Irak, Iran en Noord-Korea. Later werden Cuba, Libië en Syrië aan de lijst toegevoegd. De landen maakten zich in de ogen van de Amerikaanse regering schuldig aan het beschermen van terroristen.

[3] AD.nl, ''Hollande's coalitie' tegen IS krijgt steeds meer vorm' (versie 26 november 2015), http://www.ad.nl/ad/nl/1013/Buitenland/article/detail/4195814/2015/11/26/Hollande-s-coalitie-tegen-IS-krijgt-steeds-meer-vorm.dhtml (15 januari 2016).

[4] Bradford Richardson, 'Ex-CIA Director: Snowden should be 'hanged' for Paris' (versie 19 november 2015), http://thehill.com/blogs/blog-briefing-room/260817-ex-cia-director-snowden-should-be-hanged-for-paris (15 januari 2016).

zou zijn aan grotere onveiligheid in de westerse wereld – wel weerklank bij het huidige hoofd van de CIA. John Brennan gaf na de aanslagen in Parijs aan dat de onthullingen van Snowden de Amerikaanse veiligheid hebben ondermijnd.[5]

Edward Snowden zelf zat op het moment van de aanslagen in Moskou. De voormalig zelfstandig opdrachtnemer van de *National Security Agency* (NSA) was naar de Russische hoofdstad gevlucht nadat hij in juni 2013 geheime documenten naar de pers had gelekt. Deze documenten had hij zijn tijdens zijn werkzaamheden voor de NSA verzameld en gaven een inkijkje in de werkwijze van de NSA, het toezicht op de NSA door de Amerikaanse president, het *Foreign Intelligence Surveillance Court* (FISC) – de federale rechtbank die de verzoeken voor bevelschriften voor buitenlandse surveillance beoordeeld – en het Amerikaanse Congres. De informatie verschafte het grote publiek eveneens een inkijkje in de verhouding tussen nationale veiligheid en de rechten van het individu.

Geschat wordt dat Snowden in totaal ongeveer 1,7 miljoen pagina's aan documenten van de computers van de NSA wist te bemachtigen. De reden waarom hij de documenten vrijgaf? Snowden kwam tot de conclusie tijdens zijn werkzaamheden in de inlichtingenwereld dat de elektronische surveillance, die werd uitgevoerd door de NSA, op grote schaal het internationaal en Amerikaans recht zou schenden.[6] Door de activiteiten in de openbaarheid te brengen zou er een publieke discussie over de activiteiten van de dienst losbarsten, met hervormingen als gewenst gevolg.

In de ogen van Woolsey en Brennan is Snowden echter geen verdediger van Amerikaanse idealen, maar eerder een verrader die de vijanden van de VS heeft geholpen door hen informatie te verschaffen over de Amerikaanse inlichtingendienst die verantwoordelijk is voor het elektronisch 'afluisteren' van doelwitten en het ontcijferen van informatie. De VS wil Snowden dan ook berechten voor spionage.[7]

Uit de documenten kwam naar voren dat de NSA op grote schaal gegevens verzamelt, ook van Amerikaanse burgers. Dit was ook te merken aan berichtgeving in de Amerikaanse media: die was vooral gericht op het op grote schaal verzamelen van metadata door de NSA van binnenlandse, en

[5] The Economic Times, 'CIA Director John Brennan blasts Edward Snowden in wake of Paris attacks' (versie 18 november 2015), http://articles.economictimes.indiatimes.com/2015-11-18/news/68382544_1_paris-attacks-edward-snowden-islamic-state-group (16 januari 2016).

[6] Onder 'surveillance' wordt verstaan het volgen en/of observeren van individuen of groepen. In deze thesis wordt verder zowel gesproken over grootschalige surveillance als massasurveillance. Met beide termen wordt het uitgebreid, op grote schaal én ongericht volgen van grote groepen mensen tegelijkertijd. Ook wordt er gesproken over elektronische surveillance. Daarbij gaat het om het uitvoeren van surveillance met elektronische middelen.

[7] Peter Finn en Sari Horwitz, 'U.S. charges Snowden with espionage' (versie 21 juni 2013), https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html (16 januari 2016).

internationale, telefoongesprekken en het onderscheppen van buitenlandse internetcommunicatie. In het laatste geval konden namelijk ook onbedoeld berichten van Amerikanen worden onderschept.[8]

Het verzamelen van metadata door de NSA valt overigens in een bredere trend, die van Big Data. Big Data gaat om het verzamelen van zoveel mogelijk (persoons)gegevens met behulp van technologie zoals camera's, telefoontaps of het internet.[9] Metadata zijn datagegevens die geen betrekking hebben op de specifieke inhoud van communicatie, maar zijn gegevens die de karakteristieken van bepaalde gegevens beschrijven. Metadata hebben bijvoorbeeld betrekking op informatie zoals de duur van een telefoongesprek, de plek vanaf waar getelefoneerd wordt of het waarnemen van het versturen van een (SMS-)bericht.[10] Overigens kunnen metadata tal van nuttige toepassingen hebben in de maatschappij. Een voorbeeld in de agrarische sector is het registreren van het aantal hoestingen binnen een varkenshouderij om (uitbraak van) ziektes vroeg te kunnen waarnemen.

De praktijken van de NSA zorgden voor enige onrust binnen de VS en Europa**.** *The Economist* schreef begin augustus 2013 dat George W. Bush na 11 september 2001 *"tipped the balance too far from liberty towards security, and it has stayed there under Barack Obama."*[11] Een algemene teneur was zichtbaar in de VS: de burgerrechten worden door de overheid te veel beperkt ten faveure van meer veiligheid. Er volgden diverse rechtszaken bij federale rechtbanken waarbij de rechtsgeldigheid van het 'telefonie metadata programma' werd aangevochten. Het Vierde Amendement werd geschonden door het uitvoeren van het NSA-programma, zo was de klacht. Het Vierde Amendement van de Amerikaanse Grondwet beschermt mensen immers tegen onredelijke doorzoekingen en inbeslagnames.[12]

Alhoewel het niet vreemd is om te denken dat de onthullingen rondom de NSA niet van directe invloed zouden zijn op Europa, kwam er ook al snel een stevige reactie vanaf het Europese continent. Uit berichtgeving bleek namelijk al gauw dat de NSA met diverse Europese inlichtingendiensten samenwerkt om communicatiedata te verzamelen, bewaren en analyseren.[13] En hoewel Europeanen niet 'in rechte' kunnen opkomen tegen de afluisterpraktijken van de NSA, hebben de onthullingen, door de onderlinge samenwerking, ook zeker betrekking op Europeanen.[14] En hoewel in Europa het

[8] Edward C. Lui, Andrew Nolan en Richard M. Thompson II, Overview of Constitutional Challenges to NSA Collection Activities (Congressional Research Service Report, Damascus 2015) Summary.
[9] Bart van der Sloot, 'Privacy in het post-NSA tijdperk', *Nederlands Juristenblad* 17 (2014) 1172-1179, 1172.
[10] Van der Sloot, 'Privacy in het post-NSA tijdperk', 1177.
[11] The Economist, 'Liberty's lost decade' (versie 3 augustus 2013), http://www.economist.com/news/leaders/21582525-war-terror-haunts-america-still-it-should-recover-some-its-most-cherished (17 januari 2016).
[12] Lui, Nolan en Thompson II, Overview of Constitutional Challenges to NSA Collection Activities, 5.
[13] Pieter Omtzigt, Mass surveillance (rapport parlementair assemblée Raad van Europa, Straatsburg 2015) 1.
[14] Van der Sloot, 'Privacy in het post-NSA tijdperk', 1172.

recht op privacy in het bijzonder is vastgelegd in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) zorgt het gebruik van Big Data – bij inlichtingendiensten – ervoor dat er wordt getwijfeld aan de huidige invulling ervan: privacy als een individueel klachtrecht waarbij persoonlijke belangen worden afgewogen tegen algemene belangen.[15]

De houding van de samenleving in de VS en Europa ten opzichte van inlichtingendiensten en privacy is, door de onthullingen van Snowden, veranderd. Na *9/11* helde de balans tussen veiligheid en vrijheid over naar de kant van de veiligheid. Deze keuze was te rechtvaardigen door de vele aanslagen in de VS en Europa in de jaren na 11 september 2001.

De uitvoerende machten in de VS en de Europese Unie (EU) vervullen in dit debat een opvallende dubbelrol. Naast het feit dat ze de uitvoerende tak van de overheid zijn, vervullen ze vaak nog een wetgevende taak naast de volksvertegenwoordiging. Hierdoor vervullen ze een gecompliceerde rol. Een sprekend voorbeeld hiervan is het feit dat de Obama-regering na de onthullingen van Snowden duidelijk maakte dat de surveillancepraktijken in overeenstemming waren met de wet.

Het Witte Huis had hier misschien wel gelijk in, maar dat kwam mede door het feit dat de wetgeving nog niet was aangepast aan de nieuwste technologische veranderingen. En juist die technologische veranderingen zorgen er voor dat de privacyverwachtingen van burgers in het digitale tijdperk veranderen.

Naast (het gebrek aan) de overeenstemming van de wet met de stand van de technologie is ook een tweede aspect van belang: privacybescherming. In de VS ligt privacybescherming primair vastgelegd in het Vierde Amendement van de grondwet. Hierdoor is privacybescherming in de VS voor een groot deel gekoppeld aan de manier waarop het Hooggerechtshof dat Vierde Amendement interpreteert. In tegenstelling tot de Amerikaanse situatie is privacybescherming in Europa over het algemeen bij wet bepaald. Dit zorgt voor een belangrijk en praktisch verschil. Privacybescherming is in Europa vaak een discussieonderwerp en de regels worden met enige regelmaat herzien door de wetgevende macht, terwijl in de VS de volksvertegenwoordiging meer geneigd is de rechter te laten oordelen over de mate van privacybescherming.

De vraag is dus hoe de uitvoerende machten in de VS en Europa (in het bijzonder de Europese Commissie) zijn omgegaan met de veranderende, meer kritische houding vanuit de burgermaatschappij ten opzichte van privacy na Snowden. Worden de veranderende opvattingen in de samenleving weerspiegeld door veranderingen in Amerikaanse en/of Europese beleid? Is dus, om nogmaals in de welbekende metafoor te spreken, de balans tussen veiligheid en vrijheid veranderd?

[15] Ibidem, 1179.

Het publieke debat over privacy is sinds Snowden namelijk een onderwerp dat voor een groot deel draait om de wenselijkheid en mogelijkheden van politieke regulering. De bescherming van persoonlijke data gaat tegenwoordig immers iedereen aan.[16]

Wat het geheel extra complex – maar ook interessant – maakt, is het feit dat de uitvoerende machten in westerse democratieën in de loop der tijd een parallelle wetgevende taak hebben verworven. Alhoewel het systeem van de trias politica een fundamenteel principe van de westerse democratieën is, is de scheiding der machten vaak niet volledig aanwezig. In de praktijk vinden wetsvoorstellen vaak hun oorsprong in de uitvoerende macht. Dit heeft als gevolg dat de uitvoerende machten dus enerzijds verantwoordelijk zijn voor de inlichtingendiensten, die er overigens zijn om enerzijds de regering te dienen en anderzijds om de staat te beschermen, maar anderzijds ook (mede)verantwoordelijk zijn voor wetgeving die de slagkracht van de diensten bepaalt.

Om te bepalen hoe de uitvoerende machten zich hebben opgesteld na Snowden zal eerst de belangrijkste privacywetgeving in zowel de VS als Europa worden geduid. Daarbij worden uiteraard ook de onderlinge verschillen geanalyseerd. Door dit aspect in het begin te behandelen, wordt duidelijk in welk maatschappelijk speelveld de Amerikaanse en Europese inlichtingendiensten opereren.

Op basis van de in kaart gebrachte privacywetgeving wordt het handelen van de inlichtingendiensten aan beide zijden van de Atlantische Oceaan bediscussieerd. Daarbij zal speciaal worden gekeken naar de rol die Big Data en data mining daarin spelen.[17] Uiteraard wordt daarbij ook gekeken naar de ruimte die de inlichtingendiensten wordt geboden door speciale wetgeving voor de inlichtingendiensten.

In het tweede deel worden de gevolgen van de onthullingen van Edward Snowden, op het gebied van inlichtingendiensten en privacy, in kaart gebracht. In hoeverre kan er verder een verandering worden waargenomen in de handelingsruimte van de inlichtingendiensten in de periode na ‘Snowden’? Hoe heeft de politiek zich opgesteld, als uitvoerende macht én als wetgevende macht? Welke politieke keuzes zijn er aan beide kanten van de Atlantische Oceaan gemaakt? Zijn bevoegdheden uitgebreid of is het toezicht op de inlichtingendiensten bijvoorbeeld uitgebreid?

Privacy staat sinds *9/11* nog meer dan voorheen op gespannen voet met veiligheid. De metafoor over de balans tussen veiligheid en vrijheid wordt regelmatig aangehaald. Na de aanslagen van 11 september 2001 werd in de context van de discussie rondom privacy en de bevoegdheden van inlichtingendiensten vaak gezegd dat mensen niks te verbergen hebben en dus ook geen problemen

[16] Beate Roessler en Dorota Mokrosinska (red.), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge 2015) 303.

[17] Data mining heeft betrekking op het op grote schaal verzamelen van informatie op verschillende manieren. Vervolgens wordt met behulp van verschillende technologische middelen de verzamelde data doorzocht en geanalyseerd in een poging om zo patronen in de data te ontdekken.

hadden met extra bevoegdheden voor de inlichtingendiensten. De onthullingen van Snowden hadden daarentegen echter een hoop verontwaardigde reacties tot gevolg.

Bovenstaande schijnbare tegenstelling toont aan dat de balans tussen veiligheid en privacy heel precair is. De onthullingen van Snowden hebben de bestaande verhouding tussen het veiligheidsaspect en het belang van privacy op de schop genomen. Het in kaart brengen van dat proces maakt inzichtelijk dat privacy en veiligheid niet zomaar inwisselbaar is.

1 Privacywetgeving in de Verenigde Staten en de Europese Unie

Privacywetgeving zegt iets over het recht dat burgers hebben op een persoonlijke levenssfeer, waarin zij hun eigen leven zonder inmenging of bemoeienis van anderen kunnen en mogen vormgeven. Privacy staat echter sinds de jaren na de aanslagen van 11 september 2001 steeds op gespannen voet met veiligheid. Logischerwijs in de VS, maar ook in Europa. Aanslagen in onder andere Madrid (2004), Londen (2005), Parijs (2015) en Brussel (2016) hebben ook in Europa geresulteerd in een spanningsveld tussen privacy en veiligheid. Het debat over de strijd tegen terrorisme is sindsdien niet zelden voorgesteld als een keuze tussen privacy en veiligheid. De onthullingen van Snowden maakten duidelijk dat de NSA veel vrijheid kreeg bij het uitvoeren van massasurveillance en die vrijheid verkreeg het van de Amerikaanse overheid mede omdat de privacy werd opgeofferd om de veiligheid van de bevolking te vergroten.[18]

Het recht op privacy kan echter op gespannen voet staan met een belang van het grotere geheel: nationale veiligheid. In dit spanningsveld opereren inlichtingen- en veiligheidsdiensten voortdurend en daarom gelden er voor de inlichtingen- en veiligheidsdiensten dan ook speciale regels. Kunnen die regels en de privacywetgeving elkaar bijten? Zo ja, gebeurt dat dan ook?

In het Britse opinieblad *The Economist* verscheen op 10 oktober 2015 een artikel over data en privacy. In het artikel, verschenen nadat het Europees Hof van Justitie vier dagen eerder de zogeheten *Safe Harbour*-overeenkomst tussen de VS en de Europese Commissie (EC) onwettig had verklaard, wordt gesproken over een aanstaande strijd over privacy en de databescherming tussen Europa en de VS. Ook in andere media waren berichten over het nieuwsfeit te lezen.[19] Wat maakte dit nieuws zo belangrijk? In de *Safe Harbour*-overeenkomst lagen de regels vastgelegd waaronder Amerikaanse bedrijven, die in Europa gevestigd waren, gegevens in de VS mochten opslaan. Dit mochten deze bedrijven pas doen als ze bepaalde maatregelen hadden ingesteld die gelijk gesteld waren aan de maatregelen die de Europese regelgeving voor databescherming vereiste. Zo kon het verschil in bescherming van persoonsgegevens tussen de VS en de EU worden opgeheven.

De *Safe Harbour*-overeenkomst werd in 2000 ingesteld nadat in 1995 het Europees Parlement een richtlijn had aangenomen aangaande de rechten die mensen hebben betreffende hun persoonlijke data en in het geval hun data zou worden verzonden van een EU-lidstaat naar een niet-EU-lidstaat. Het ontvangende land moest ervoor zorgen dat er ‘adequate mate van bescherming’ aanwezig zou zijn om die data te beschermen. Om deze talige richtlijn om te zetten in concreet te nemen maatregelen

[18] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (New York 2015) 113.
[19]

werden door het Amerikaanse ministerie van Handel en de EU de zogeheten *Safe Harbor Privacy Principles* opgesteld. Deze punten konden vervolgens door Amerikaanse organisaties gebruikt worden om te kijken op ze kwalificeerden als een *´Safe Harbour´* volgens de Europese wetgeving.[20]

Waarom werd de overeenkomst dan uiteindelijk onwettig verklaard? Het Europees Hof van Justitie oordeelde dat de VS in onvoldoende mate bescherming bood voor persoonsgegevens van EU-burgers. Dit deed het Hof nadat Oostenrijker Max Schrems een rechtszaak had aangespannen om aan te tonen dat de gegevens van Facebook niet veilig werden opgeslagen in de VS. Onderdeel van de rechtsoverweging waren de onthullingen van Snowden aangaande de afluisterprogramma's van de NSA. De Amerikaanse overheid zou toegang hebben tot veel persoonlijke gegevens. Het Hof volgde deze redenatie en besloot in het voordeel van de Oostenrijker.[21]

Toen de EC in 2000 de overeenkomst ondertekende, waren de datastromen tussen beide kanten van de Atlantische Oceaan echter nog beperkt. De EC ging mede daarom akkoord met de afspraak dat bedrijven zelf een privacybeleid konden schrijven om zichzelf vervolgens in overeenstemming met de overeenkomst te kunnen verklaren. Amerikaanse bedrijven konden zichzelf dus certificeren. Onthullingen van Edward Snowden brachten dus een aantal tekortkomingen in de uitvoering van de overeenkomst aan het licht. Zo was onder andere sprake van een zwakke handhaving van de afspraken aan Amerikaanse kant en slechte afhandeling van klachten. De titel van het persbericht dat de EC op 27 november 2013 deed uitgaan liet dan ook geen ruimte voor twijfel: *European Commission calls on the U.S. to restore trust in EU-U.S. data flows*.[22]

In het artikel van *The Economist* wordt de *Safe Harbour*-overeenkomst gezien als een poging om de culturele en politieke verschillen tussen de EU en de VS aangaande online privacy te overbruggen. De EU ziet de bescherming van persoonlijke gegevens namelijk als een primair mensenrecht, terwijl in de VS de bescherming van persoonlijke data wordt gezien in de context van consumentenbescherming, wat is afgeleid van het recht op vrijheid van informatie. Het verschil zou hem zitten in het feit dat de tweede opvatting ruimte overlaat voor een uitwisseling van voordelen, oftewel een *trade-off*, tussen bedrijven en consumenten.[23]

Het verschil in inzichten aangaande privacy tussen de VS en de EU kan worden gezien als een kenmerk van de zogeheten 'balkanisering' van het internet waarbij elk land zijn eigen standaarden wat betreft het internet opstelt en implementeert. De *Safe Harbour*-overeenkomst was echter een manier

[20] Megan Graham, 'Adding Some Nuance on the European Court's Safe Harbor Decision' (versie 7 oktober 2015), https://www.justsecurity.org/26651/adding-nuance-ecj-safe-harbor-decision/ (23 januari 2016).
[21] Hof van Justitie van de EU, Arrest in zaak C-362/14 Maximillian Schrems/Data Protection Commissioner (Perscommuniqué nr. 117/15, Luxemburg 2015).
[22] Europese Commissie, 'European Commission calls on the U.S. to restore trust in EU-U.S. data flows' (27 november 2013), beschikbaar via europa.eu/rapid/press-release_IP-13-1166_en.pdf.
[23] The Economist, 'Get off of my cloud', *The Economist*, 10 oktober 2015.

om een brug te slaan tussen die verschillende standaarden en de verschillende plekken waar de data werd opgeslagen in een poging om een 'vrij en grenzeloos internet' te creëren. Uiteindelijk bleek dit echter niet mogelijk vanwege de verschillende opvattingen aangaande *data localization*, wat betrekking heeft op de plek waar gegevens worden opgeslagen. De positie van de EU werd hierbij in grote mate bepaald door Europese wetgeving die bepaalt dat data binnen de EU moet worden opgeslagen ongeacht de vraag of dat in de praktijk leidt tot een betere databescherming. De Amerikanen bezien deze datalocalisatie maatregelen door een protectionistische bril, maar tegelijkertijd schort het aan Amerikaanse zijde aan de erkenning dat juridische kwesties over de online bescherming van individuen serieuze zaken zijn.[24]

De ontwikkeling van de 'balkanisering' van het internet werd versterkt door de onthullingen van Edward Snowden.[25] En terwijl er vele overeenkomsten zijn tussen de VS en de EU, blijven er grote verschillen tussen de twee partijen op het gebied van de privacy. Het eerder genoemde verschil tussen privacy als mensenrecht of als consumentenrecht wordt op een interessante manier beschreven in een rapport van het Witte Huis over *Big Data* uit mei 2014:

> *Despite some important differences, the privacy frameworks in the United States and those countries following the EU model are both based on the FIPPs (= Fair Information Practice Principles. The European approach, which is based on a view that privacy is a fundamental human right, generally involves top-down regulation and the imposition of across-the-board rules restricting the use of data or requiring explicit consent for that use. The United States, in contrast, employs a sectoral approach that focuses on regulating specific risks of privacy harm in particular contexts, such as health care and credit. This places fewer broad rules on the use of data, allowing industry to be more innovative in its products and services, while also sometimes leaving unregulated potential uses of information that fall between sectors.*[26]

Het verschil tussen de Europese en Amerikaanse visie is dus in de kern prima als volgt omschrijven. De Europese opvatting over het recht op privacy gaat richting 'ja, tenzij…', terwijl de Amerikaanse opvatting eerder het tegenovergestelde behelst: 'nee, behalve bij…'. Maar is dit ook echt zo zwart-wit?

[24] Christopher Kuner, ´Data Nationalism and its discontents´, Emory Law Journal Online 64 (2015), beschikbaar via http://law.emory.edu/elj/elj-online/volume-64/responses/data-nationalism-its-discontents.html (23 januari 2016).
[25] The Economist, 'Get off of my cloud'.
[26] Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values (Rapport Witte Huis, 2014) 17-18.

Kan de EU worden beschouwd als een beschermheer van de privacy, terwijl de VS toch meer de privacy van haar inwoners te grabbel gooit?

Zo simpel is het niet. Het recht op privacy wordt in de VS immers als een fundamenteel recht gezien dat ligt vastgelegd in het Vierde Amendement van de Amerikaanse grondwet: *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…"*.[27]

De tekst uit het Vierde Amendement maakt duidelijk dat privacy ruim 200 jaar geleden, toen de Amerikaanse grondwet werd opgesteld, al een belangrijk fenomeen was. Tegelijkertijd is de privacy van toen en de privacy van nu heel anders: in het Vierde Amendement wordt immers gesproken over (persoonlijke) 'papieren' en 'onredelijke huiszoekingen en inbeslagnames'. Uiteraard bestaan er tegenwoordig nog steeds papieren documenten, of vinden er huiszoekingen en inbeslagnames plaats, maar tegelijkertijd heeft het idee van privacy zich ook naar een heel andere dimensie, het internet, verplaatst. In 2015 werd er voor ongeveer 76 exabytes aan data via het internet de wereld rondgestuurd. Om dit in perspectief te plaatsen: één exabyte staat gelijk aan één miljard gigabytes of 500 miljard tekstpagina's.[28] Kortom, het verschil tussen de privacy van nu en die van 200 jaar gelden is als een verschil tussen dag en nacht.

Daarnaast zijn de doelwitten van inlichtingendiensten in de loop der tijd veranderd. In vroegere tijden hielden de inlichtingendiensten zich meer bezig met spionage dat gericht was op andere regeringen en de agenten die voor een regering werkten. Tegenwoordig is dat vanwege de terroristische dreigingen wel anders. De wereld is minder stabiel dan tijdens de Koude Oorlog en inlichtingendiensten dienen daarom dan ook gevarieerder en flexibeler te werk te gaan dan voor de val van de Sovjet-Unie.[29] Overheidssurveillance is daarom tegenwoordig gericht op iedereen, in zowel binnen- als buitenland, en van een grotere orde dan ten tijde van de Koude Oorlog.[30]

Privacy, en het wel of niet adequaat beschermen daarvan, is tegenwoordig dan ook een belangrijk thema en een grote uitdaging waar overheden mee te maken hebben. Privacy wordt over het algemeen wel erkend als een fundamenteel recht dat mensen hebben, maar tegelijkertijd wordt de privacy van mensen tegenwoordig ook op grote schaal aangetast. Dit komt doordat er veelvuldig technologie wordt gebruikt, of in ieder geval kan worden gebruikt, om persoonlijke gegevens van

[27] Richard A. Clarke e.a., *The NSA Report: Liberty and Security in a Changing World* (Princeton 2014) 43-52; Zie ook Tim Sharp, 'Right to Privacy: Constitutional Rights & Privacy Laws' (versie 12 juni 2013), http://www.livescience.com/37398-right-to-privacy.html (23 januari 2016). Behalve in het Vierde Amendement ligt ook in het Eerste, Derde, Vijfde, Negende en Veertiende Amendement het recht op persoonlijke autonomie vastgelegd.
[28] Schneier, *Data and Goliath*, 16.
[29] Michael Herman, *Intelligence power in peace and war* (10e druk; Cambridge 2010) 360.
[30] Schneier, *Data and Goliath*, 47-59.

mensen te kunnen verzamelen, bewaren en analyseren.[31] Niet alleen zijn er mogelijkheden beschikbaar om gegevens te kunnen verzamelen en te analyseren, ook is er genoeg data voorhanden om te kunnen verzamelen en te analyseren. Wie maakt er tegenwoordig immers geen gebruik van het internet of een smartphone. Of anders van diensten van grote multinationals als Google, Facebook of Apple? Het merendeel van de mensen doet dat en maakt derhalve automatisch enorm veel data aan over het daadwerkelijke gebruik of de gebruiker zelf.[32] Dankzij de onthullingen van Edward Snowden is het grote publiek te weten gekomen dat inlichtingendiensten, zoals de NSA in de VS of de Britse *Government Communications Headquarters* (GCHQ), hier dankbaar gebruik van maken. Zo werd uit de vrijgegeven documenten van Snowden duidelijk dat de NSA drie verschillende programma's had om gegevens van Gmail-gebruikers te verzamelen en dat de omvang van gegevens die de NSA in bezit had over onschuldige mensen vele malen groter was dan de gegevens die het in bezit had over geautoriseerde doelwitten.[33]

In een tijd waarin de middelen erg geavanceerd zijn om verschillende soorten data te vergaren en aan elkaar te koppelen, is het belangrijk om, zoals professor in de informatietechnologie Sophie Stalla-Bourdillon zegt, de interactie tussen de bescherming van privacy en de bevordering van veiligheid goed te begrijpen voordat er wellicht beperkingen worden gesteld aan de gangbare surveillancepraktijken.[34]

Om een begin te maken met het begrijpen van die interactie zal hieronder eerst de Amerikaanse privacywetgeving worden geanalyseerd, gevolgd door de Europese privacyrichtlijn die de basis vormt voor de verschillende nationale Europese wetgevingen aangaande privacy van de lidstaten van de EU. De privacywetgeving van zowel de VS als de EU bepalen namelijk voor een groot deel de speelruimte voor inlichtingen- en veiligheidsdiensten doordat ze de algemeen geldende kaders in de samenleving aangeven. Eventuele opmerkelijke verschillen zullen daarna nog worden uitgelicht en besproken.[35]

1.1 Privacywetgeving in de VS

Tweehonderd jaar geleden zou – zo is een gangbare mening – het grondrecht op privacy zijn vastgelegd in de Amerikaanse grondwet. Dit is niet helemaal juist. In de Amerikaanse grondwet wordt immers

[31] Sophie Stalla-Bourdillon, Joshua Phillips en Mark D. Ryan, *Privacy vs. Security* (Londen 2014) V.
[32] Stalla-Bourdillon, Phillips en Ryan, *Privacy vs. Security*, 4.
[33] Schneier, *Data and Goliath*, 47; 50.
[34] Stalla-Bourdillon, Phillips en Ryan, *Privacy vs. Security*, 5.
[35] Het is uiteraard mogelijk dat de inlichtingen- en/of veiligheidsdiensten bepaalde uitzonderingsposities hebben binnen de privacywetgeving.

met geen woord gerept over het 'recht op privacy'. Wel kan worden gesteld dat het idee dat Amerikanen het recht hebben om alleen gelaten te worden ten grondslag ligt aan de Amerikaanse *Bill of Rights*. Voordat er namelijk expliciet een recht op privacy werd ontwikkeld of erkend, werden Amerikanen al binnen hun eigen huis beschermd tegen bemoeienis van de eigen overheid. Mensen vonden namelijk, en verwachtten ook, dat persoonlijke informatie privé zou blijven. Zelfs wanneer de informatie het eigen huis zou verlaten. Persoonlijke correspondentie per post werd in de VS gedurende de 19e eeuw zelfs wettelijk beschermd tegen een bemoeizuchtige overheid. [36]

Het 'recht op privacy' werd in de VS in 1890 voor het eerst geformuleerd in een artikel in de *Harvard Law Review*. De auteurs van het artikel, Samuel Warren en Louis Brandeis, schreven over het onderwerp naar aanleiding van de ontwikkeling van de fotocamera en het feit dat mensen zelf het recht zouden moeten hebben om te bepalen hoe ze overkomen binnen het publieke domein. Daarbij dachten de auteurs niet aan bemoeienis van de overheid, maar juist wel aan bemoeienis van de pers of een enig ander persoon of organisatie die ieders recht om alleen gelaten te worden zou schenden. Alhoewel kan worden gesteld dat het idee over een recht op privacy al eerder werd ontwikkeld, waren Warren en Brandeis de eersten die een juridisch argument ontwikkelden voor een breder recht op privacy dan tot op dat moment gangbaar was. Het artikel is door het onderwerp nog zeker relevant voor de hedendaagse discussies over privacy.[37] Sinds het verschijnen van het artikel, dat als titel *The Right to Privacy* droeg, heeft het recht op privacy zich in de loop der tijd doorontwikkeld.

Pas tien jaar na het verschijnen van het artikel begon het recht op privacy met enige regelmaat aandacht te krijgen in de Amerikaanse rechtbanken. Gedurende de daaropvolgende decennia bleef er echter een strijd voortduren in de rechtszalen of het recht op privacy überhaupt bestond. Pas vanaf de jaren '30 begon er een kentering plaats te vinden waardoor rechtbanken in de jaren erna in grote mate overgingen tot erkenning van het recht op privacy.[38] Tot dan toe werd privacy niet als een gegronde rechtvaardiging erkend om als ene burger een rechtszaak te beginnen tegen een andere burger. In de meeste staten werd binnen het burgerrecht vier mogelijke onrechtmatige daden ten opzichte van de schending van de privacy erkend die aanleiding konden geven tot een rechtszaak.[39] Dit gewoonterecht vormt tot op de dag van vandaag een belangrijke basis voor privacybescherming in de VS.

[36] Kirby Goidel, Craig Freeman en Brian Smentkowski, *Misreading the Bill of Rights: top ten myths concerning your rights and liberties* (Santa Barbara 2015) 120-122.
[37] Goidel, Freeman en Smentkowski, *Misreading the Bill of Rights*, 121-122.
[38] William L. Prosser, 'Privacy', *California Law Review* 48 (1960) 3, 383-423, 386-387.
[39] De vier mogelijke onrechtmatige daden zijn: 1.Het inbreuk maken op iemands eenzaamheid of afzondering, of inbreuk maken op diegene's privézaken. 2.Het openbaar maken van pijnlijke private feiten over een persoon. 3.Iemand publiekelijk in een vals daglicht zetten. 4.Toeëigening van iemands beeltenis ten gunste van een ander. Zie Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values, 16.

Hier kwam ook nog bij dat het Amerikaanse Hooggerechtshof in 1965 verklaarde dat elk individu een grondwettelijk recht op privacy heeft. Deze uitspraak werd gebaseerd op de 'vrijheidszones' die volgens de rechter impliciet onderdeel uitmaakten van de *Bill of Rights*. Dit betekende dat het recht op privacy ook opgevat kon worden als een recht om vrij te zijn staatsbemoeienis. Er moeten immers ook vrijheden zijn die voorbij gaan aan enige controle door de staat, zo was de gedachte. Met deze uitspraak begon in feite het grondwettelijke recht op privacy.[40]

De term 'privacy' kreeg in de VS in het midden van de jaren '60 dus een tweetal belangrijke betekenissen. Enerzijds werd het gebruikt binnen het civiel recht als referentie naar een systeem van onrechtmatige daden en anderzijds werd het binnen het staatsrecht toegepast als een verwijzing naar de rechten van individuen om eventuele inmengingen van overheidsinstanties te weigeren. In het laatste geval gaat het dus om het recht op autonomie en het recht op zelfbeschikking.[41]

Naarmate de Amerikaanse samenleving steeds bekender werd met het fenomeen 'computer' begonnen beleidsmakers zich opnieuw over het recht op privacy te buigen. In 1973 leidde dat tot een rapport van het Amerikaanse ministerie van Gezondheidszorg, Onderwijs en Welzijn met de titel *Records, Computers and the Rights of Citizens*. Hierin werden bepaalde waarborgen aanbevolen voor het gebruik van informatie, zeker met het oog op de mogelijke schadelijke gevolgen van het gebruik van geautomatiseerde persoonlijke datasystemen. Het werd namelijk noodzakelijk geacht dat zowel de organisatie die de persoonlijke data in handen had als degene naar wie de data verwees ook controle had over de data. Er waren dus waarborgen nodig waar de organisaties, die in het bezit waren van de persoonlijke data, aan moesten voldoen om de privacy, in termen van wederkerigheid, te beschermen.[42] Deze waarborgen, de *Fair Information Practice Principles* (FIPPs), werden de grondslag voor de moderne databescherming door basale bescherming te bieden voor de omgang met persoonlijke data: *'They provide that an individual has a right to know what data is collected about him or her and how it is used. The individual should further have a right to object to some uses and to correct inaccurate information. The organization that collects information has an obligation to ensure that the data is reliable and kept secure.'*[43]

De bovenstaande principes vormden de basis voor de *Privacy Act* van 1974. Deze wet had als officieel doel om de privacy van het individu te beschermen tegen eventueel misbruik van gegevens die in het bezit zijn van de federale overheid. Ook kregen individuen door deze wet toegang tot hun

[40] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Heidelberg 2014) 28.
[41] González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, 28.
[42] Ibidem, 34.
[43] Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values, 17; In 1980 werden de FIPPs overgenomen als basis voor de privacyrichtlijnen van de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) en daarmee voor een groot deel van de Westerse wereld.

persoonlijke federale gegevens. Misbruik werd met deze wet tegengegaan doordat de federale overheid specifieke regels kreeg opgelegd aangaande de handhaving, verzameling, het gebruik en verspreiding van persoonlijke gegevens in (digitale) informatiesystemen.[44]

De Privacy Act werd aangevuld met privacywetgeving die zich toespitste op specifieke sectoren en daarmee op specifieke soorten data. Deze vorm van wetgeving begon het gewoonterecht te vervangen dat gebaseerd was op het idee van aansprakelijkheid. Een voorbeeld van een dergelijke wet is de *Health Insurance Portability and Accountability Act* (1996), die zich onder andere richt op het gebruik en verstrekken van medische informatie. Een belangrijk aspect van de wet is het principe van 'minimale noodzaak' voor het gebruik en verstrekken van informatie. Zodoende worden gegevens van mensen zoveel mogelijk beschermd. Andere sectorale privacywetgeving beschermt informatie over onderwijs, communicatiemiddelen, videoverhuur of genetische informatie.[45]

De 21ste eeuw vraagt om het aanpassen van de regels omtrent privacybescherming. Sinds het begin van deze eeuw is zowat iedereen immers online en worden gegevens ook op grote schaal gedeeld via onder andere smartphones. In februari 2012 kondigde de Amerikaanse president Barack Obama daarom de *Consumer Privacy Bill of Rights* aan. Opmerkelijk aan het voorstel, dat van toepassing is op commercieel gebruik van persoonlijke data, is dat de bescherming van de privacy van consumenten steeds wordt gekoppeld aan het bevorderen van innovatie. Zo schrijft president Obama in de begeleidende brief het volgende:

> *I am pleased to present this new Consumer Privacy Bill of Rights as a blueprint for privacy in the information age. These rights give consumers clear guidance on what they should expect from those who handle their personal information, and set expectations for companies that use personal data. (…) With this Consumer Privacy Bill of Rights, we offer to the world a dynamic model of how to offer strong privacy protection and enable ongoing innovation in new information technologies.*[46]

Verder wordt in voorwoord gesproken over het, aan de hand van deze wet, realiseren van privacybescherming die het consumentenvertrouwen behoudt en innovatie bevordert.[47] Hierdoor is het duidelijk een wetsvoorstel dat een dubbel doel nastreeft. In het wetsvoorstel is bijvoorbeeld wel

[44] Ibidem, 17; Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, 36.
[45] Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values, 18-19.
[46] Het Witte Huis, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (Rapport Het Witte Huis, Washington 2012) C3.
[47] Het Witte Huis, Consumer Data Privacy in a Networked World, ii.

vastgelegd dat consumenten bepaalde rechten hebben, maar ook dat de context bepalend is om de balans tussen, en het relatieve belang van, bepaalde principes te bepalen.[48]

Het wetsontwerp, dat tot op heden (juni 2016) nog niet in werking is getreden, kan echter op redelijk wat kritiek rekenen. Het wetsvoorstel roept bedrijven op om hun eigen gedragscodes in te stellen wat betreft het omgaan met consumenteninformatie. Het is dan vervolgens aan de *Federal Trade Commission* om na te gaan of die gedragsregels voldoen aan de voorwaarden die in de wet zijn opgenomen. Daarmee zou te veel macht bij bedrijven komen te liggen die zo zelf kunnen bepalen of hun beleid aangaande datagebruik van consumenten risico's op het gebied van privacy oplevert voor de consumenten.[49]

De Amerikaanse overheid ziet het wetsvoorstel echter als een manier om de privacy van consumenten te beschermen en om tegelijkertijd ook innovatie te bevorderen. Vandaar dat het wetsvoorstel ook geen rigide set van maatregelen behelst, maar meer uitgaat van flexibiliteit om innovatie van bedrijven niet te laten verzanden in strak omlijnde regels. De achterliggende gedachte is dat de combinatie van brede basisprincipes en specifieke (vrijwillig opgestelde) gedragsregels de privacy van consumenten kan beschermen, terwijl tegelijkertijd de innovatie kan worden ondersteund.[50]

Het wetsontwerp van de Obama-regering is een voorbeeld van privacybescherming tegen eventueel opdringerige commerciële partijen, terwijl het Vierde Amendement van de Amerikaanse grondwet de Amerikaanse bevolking moet beschermen tegen een opdringerige overheid. Amerikanen zijn van oudsher niet gediend van een overheid die zich (in grote mate) bemoeit met de levens van haar inwoners. De Amerikaanse vrijheidstraditie heeft zich doorontwikkeld vanuit de bescherming van het huis (kijk maar naar de tekst van het Vierde Amendement).[51] Ook de sectorale wetgeving, waar de *Health Insurance Portability and Accountability Act* een voorbeeld van is, is erop gericht om gegevens over burgers te beschermen tegen misbruik door derden.

Het Amerikaanse rechtssysteem kent overigens sinds de jaren zeventig de *third-party doctrine*. Het Vierde Amendement bepaalt dat de overheid niet zonder bevel zomaar zich toegang mag verschaffen tot onder andere je huis, persoonlijke papieren en andere bezittingen. Onder deze

[48] Ibidem, 10. Volgens het wetsvoorstel hebben consumenten 1.het recht op het kunnen uitoefenen van individuele controle 2.transparantie wat betreft de toegepaste privacy- en veiligheidsvoorschriften 3.zekerheid wat betreft gebruik van data in de context waarin het is aangeleverd 4.beveiliging van data 5.toegang tot de data en nauwkeurige verwerking van data 6.het recht op redelijke beperking aangaande de persoonlijke data die wordt verzameld en 7.gepaste aansprakelijkheidsmaatregelen van bedrijven.
[49] Natasha Singer, 'White House Proposes Broad Consumer Data Privacy Bill' (versie 27 februari 2015), http://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data-privacy-bill.html (23 januari 2016).
[50] Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values, 20.
[51] Stalla-Bourdillon, Phillips en Ryan, *Privacy vs. Security*, 7.

doctrine kan je als persoon geen 'legitieme verwachting van privacy' hebben, met betrekkingen tot de overheid, als je vrijwillig informatie afstaat aan een derde partij. Met andere woorden, de overheid mag als je informatie vrijwillig hebt afgestaan aan een derde partij zonder bevelschrift zichzelf toegang verschaffen tot die informatie.[52]

Tegenwoordig bevindt heel veel informatie zich echter in handen van derde partijen door gebruik van het internet, GPS, applicaties op smartphones of opslagruimte in de *cloud*. Dat betekent dat de overheid in theorie aan heel veel informatie kan komen. Sinds de onthullingen van Snowden, en onder andere het bekend worden van het op grote schaal verzamelen van metadata door de NSA, gaan discussies aangaande de *third-party doctrine* niet meer over informatie van kleine groepen mensen die meestal verdachten waren in een rechtszaak, maar over de gegevens van miljoenen mensen.[53] Aangezien de lopende discussie over de geldigheid van de *third-party doctrine* van groot belang is voor de mogelijke werkwijze van de inlichtingendiensten zal hier in het volgende hoofdstuk nog nader op worden ingegaan.

De *Bill of Rights* beschermt Amerikanen tegen de overheid en vormt daarmee een belangrijke basis voor het recht op privacy, maar de grondwet beschermt Amerikanen niet tegen bedrijven of andere individuen. Daarvoor zijn andere wetten ingesteld die moeten voorkomen dat gevoelige informatie van burgers, zoals financiële informatie of informatie over iemands gezondheid, zomaar wordt gedeeld. Dat geldt niet voor informatie die iemand vrijwillig afstaat aan derden. Met behulp van de technologie van tegenwoordig zijn bedrijven in staat om veel persoonlijke data te verzamelen en te gebruiken.

Resulterend kan worden gesteld dat de houding van Amerikanen ten opzichte van privacy dubbelzinnig is. Aan de ene kant zijn Amerikanen erg vóór privacy, maar overhandigen tegelijkertijd wél op grote schaal persoonlijke data aan commerciële bedrijven. Hetzelfde geldt voor surveillance van de overheid. De gemiddelde Amerikaan vindt dat de overheid zo min mogelijk van zijn of haar persoonlijke leven moet weten, maar tegelijkertijd is diegene die zijn privacy ten opzichte van de overheid beschermt, verdacht. In de Amerikaanse privacywetgeving is deze bekende tweedeling duidelijk terug te zien. De *Bill of Rights* beschermt de Amerikaan tegen zijn eigen overheid en ook latere wetgeving, zoals de *Privacy Act* uit 1974 of andere wetgeving, is erop gericht om persoonlijke gegevens in handen van de overheid te beschermen tegen misbruik door de overheid. Het wetsvoorstel van Obama, de *Consumer Privacy Bill of Rights*, maar ook de *third-party doctrine* tonen echter aan dat

[52] John Villasenor, 'What You Need to Know about the Third-Party Doctrine' (versie 30 december 2013), http://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/ (23 januari 2016).
[53] Ibidem.

gegevens in handen van derden veel makkelijker mis- dan wel gebruikt kunnen worden.[54] Waar gaat het recht op privacy in de VS dan over? In de VS gaat het grondwettelijke recht op privacy vooral over keuze. Waar het artikel van Warren en Brandeis sprak over het recht om alleen gelaten te worden, gaat de Amerikaanse privacywetgeving tegenwoordig in de kern over (vrije) keuze. Het liefst zonder inmenging van de overheid.[55]

1.2 Privacywetgeving in de EU

De Europese privacywetgeving vindt zijn oorsprong in het Europese Verdrag voor de Rechten van de Mens (EVRM), dat stamt uit 1953. In het EVRM werd met artikel 8 het 'recht op eerbiediging van het privéleven' opgenomen als een mensenrecht. Deze brede invulling van de bescherming van het privéleven betekende dat het EVRM een tamelijk vooruitstrevend document werd, zeker aangezien het doel van het EVRM was om de deelnemende landen – die weinig gemeenschappelijke overeenkomsten hadden – bij elkaar te brengen. En alhoewel wordt gezegd dat de specifieke bewoordingen en bedoelingen van het verdrag onduidelijk zijn, zeker met het oog op het maken van nationale wetgeving, wordt het desalniettemin als een succesvol verdrag gezien. Het verdrag voorziet namelijk ook in het instellen van een gerechtshof waar partijen naar toe kunnen gaan als ze de nationale gerechtelijke weg helemaal zijn doorlopen.[56]

Het EVRM vormde een belangrijke grondslag voor nationale wetgeving, maar het duurde nog tot in de jaren '70 en '80, als gevolg van toenemende zorgen omtrent individuele privacy, totdat de meeste (industriële) landen wetgeving aannamen om privacy te beschermen. Een voorbeeld daarvan is de Amerikaanse *Privacy Act* van 1974. De verschillende nationale wetgevingen kwamen logischerwijs in verschillende vormen en maten. Onder andere de Amerikaanse en Franse wetgeving legde bescherming vast in termen van 'privacy', terwijl de wetgeving in veel Europese landen sprak over 'gegevensbescherming'. Daarnaast verschilde de wetgeving ook nog qua vorm. Zo was er sectorale wetgeving, zoals in de VS, die verschillende standaarden vastlegde, terwijl er ook alomvattende wetgeving werd aangenomen waarin dus sprake was van een algemene regel.[57]

De verschillende vormen van privacywetgeving leidde tot een poging om die Europese varianten te integreren. In 1980 kwam de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) met de vrijwillige *Guidelines on the Protection of Privacy and Transborder Flows*

[54] Goidel, Freeman en Smentkowski, *Misreading the Bill of Rights*, 129.
[55] Lawrence M. Friedman, *The Human Rights Culture: a study in history and context* (New Orleans 2011) 92.
[56] Stalla-Bourdillon, Phillips en Ryan, *Privacy vs. Security*, 9-10.
[57] Priscilla M. Regan, 'Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows', *Journal of Social Issues* 59 (2003) 2, 263-282, 265-266.

of Personal Data. De nadruk lag hierbij op het instellen van beperkingen op het gebied van datavergaring, dataopslag en het gebruik van data. Op basis van deze richtlijnen sloot de Raad van Europa in 1981 een overeenkomst, genaamd *For the Protection of Individuals with Regard to Automatic Processing of Personal Data*, waarmee Europese landen werden opgeroepen om data privacywetgeving op het nationale niveau te implementeren. Deze oproepen waren helemaal in lijn met de toentertijd toenemende rol van computers, dataopslag en internationaal dataverkeer. Dit laatste was ook de reden dat de conventie ook onderstreepte dat mogelijke beperkingen op het gebied van internationaal dataverkeer wenselijk, of zelfs noodzakelijk, werden geacht mocht de bescherming in het ontvangende land niet afdoende geregeld zijn.[58] Databescherming werd in de jaren '80 steeds belangrijker en dat gold zeker voor Europa, waar de economische integratie steeds dieper werd.[59]

De overeenkomst trad in 1985 in werking en diende ertoe om een goede balans te vinden tussen de bescherming van grondrechten enerzijds en de noodzaak om vrij verkeer van persoonlijke data anderzijds te bevorderen, voor zowel de publieke als de private sector. Elke verwerking van persoonlijke gegevens diende daarom te voldoen aan vier fundamentele principes die ervoor moesten zorgen dat gegevens op een goede manier werden verwerkt en behandeld. Daarnaast kregen de *data subjects*, mensen over wie de data gaan, ook bepaalde rechten om de veiligheid van gegevens te kunnen waarborgen. Al met al leek het beschermen van grondrechten de overhand te hebben in de tekst ten opzichte van het bevorderen van vrij verkeer van informatie tussen mensen, het oorspronkelijke doel van de overeenkomst. Echter, zoals gezegd, het ging om een oproep en dus om niet-bindende richtlijnen voor het opstellen van gedragsregels.[60]

De overeenkomst bleek, mede daardoor, niet het gewenste effect te hebben. Aangezien de overeenkomst het resultaat was van onderhandelingen binnen de OESO, een forum waarbinnen wordt gesproken sociaal en economisch beleid én waarin zowel Europese landen als de VS in zitten, was de uitkomst ook een compromis tussen de belangen van de VS – behouden van een vrije stroom van informatie tussen de verschillende landen – en de Europese landen – het vastleggen van samenhangende regels voor het beschermen van persoonlijke informatie.[61]

Het uitvoerende orgaan van de Europese Gemeenschap, de EC, deed voor het einde van 1982 een aanbeveling aan de lidstaten om de overeenkomst van de OESO te ratificeren en om te zetten in nationale wetgeving. Deze poging om de verschillende nationale wetgevingen te harmoniseren bleek niet succesvol. Hoewel in 1990 zeven van de twaalf lidstaten nationale wetgeving had

[58] Stephen J. Kobrin, 'Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance', *Review of International Studies* 30 (2004) 1, 111-131, 118.
[59] Kobrin, 'Safe harbours are hard to find', 118.
[60] Stalla-Bourdillon, Phillips en Ryan, *Privacy vs. Security*, 39.
[61] Regan, 'Safe Harbors or Free Frontiers?', 269.

geïmplementeerd, liepen deze op een aantal belangrijke punten uiteen.[62] De EC besloot daarom om zelf met wetgeving te komen. Door de verschillen in wetgeving werd vrij dataverkeer tussen de Europese grenzen bemoeilijkt terwijl dat wel als noodzakelijk werd gezien voor onder andere onderzoek en handel. Het was tevens noodzakelijk om de grenzen binnen de EU open te kunnen gooien en om een interne markt te kunnen creëren.[63] Voor de EC was het voorgestelde pakket aan wetgeving dus primair een middel om de interne markt in Europa beter te kunnen laten functioneren. De EC wilde het beschermen van de rechten van de inwoners van Europa, aangaande dataverkeer, in eerste instantie overlaten aan de lidstaten zelf. Doordat het Europees Parlement echter in 1975 een resolutie had aangenomen om de rechten van Europese burgers te beschermen én die oproep sindsdien regelmatig had herhaald, werd het beschermen van de privacy uiteindelijk opgenomen in het voorstel in 1990.[64]

Uiteindelijk werd in 1995 het EU *Data Protection Directive* aangenomen. De hoofddoelen van richtlijn 95/46/EG, zoals de richtlijn officieel heette, waren: *"(1) to allow for the free flow of data within Europe, in order to prevent member states from blocking inter-EU data flows on data protection grounds; and, (2) to achieve a harmonized minimum level of data protection throughout Europe"*.[65] In het tweede doel wordt er gesproken over een '*minimum level of data protection*'. De EC was het dus duidelijk primair te doen om economische belangen in plaats van bescherming van de privacy. In dat geval lag de het uitvoerende orgaan van de EU toentertijd niet ver af van het standpunt wat de Amerikaanse regering heeft ten opzichte van de *Safe Harbour*-overeenkomst. Hoe komt dit? Op 1 juli 1987 was de in 1986 gesloten *Single European Act* in werking getreden. Deze wet, gericht op het vervolmaken van de interne Europese markt, had de deadline daarvoor op het jaar 1992 gezet.[66]

In de preambule van richtlijn 95/46/EG wordt wel expliciet gespraken over het recht op privacy. Er wordt namelijk gesteld dat het doel van de nationale wetgeving op het gebied van het verwerken van persoonlijke data is '*to protect fundamental rights and freedoms, notably the right to privacy*'.[67] Daarmee bleek de richtlijn een belangrijk Europees ijkpunt voor de privacybescherming.

De algemene richtlijn 95/46/EG werd in de jaren daarna opgevolgd door speciale richtlijnen die specifieke regels vastlegden. Richtlijn 95/46/EG had betrekking op de bescherming van persoonlijke data, en het woord 'privacy' sloeg in die context dan ook daarop, maar dat was anders in het geval van een speciale wet, de zogeheten *lex specialis*, voor een specifieke sector. Zo werd er bij

[62] Stalla-Bourdillon, Phillips en Ryan, *Privacy vs. Security*, 40.
[63] Serge Gutwirth, Ronald Leenes, Paul de Hert en Yves Poullet (red.), *European Data Protection: Coming of Age* (Dordrecht 2013) 62.
[64] Gutwirth e.a., *European Data Protection*, 63.
[65] Ibidem, 269 (zie voetnoot 6).
[66] Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, 126.
[67] Ibidem, 131.

richtlijn 97/7/EG, ter bescherming van consumenten tegen overeenkomsten die op afstand worden gesloten, en richtlijn 97/66/EG, ter bescherming van data en privacy in de telecommunicatiesector, uitgegaan van het beschermen van de privacy van de consument. Daarmee had het woord 'privacy' in deze context betrekking op artikel 8 van het EVRM: 'het recht op eerbiediging van het privéleven'.[68]

In de jaren na het aannemen van richtlijn 95/46/EG werd de richtlijn in de verschillende EU-lidstaten omgezet in nationale wetgeving. Daarmee werd ook het idee van 'persoonlijke data' en 'databescherming' door Europa verspreid. Wel werd in slechts een beperkt aantal landen expliciet vastgelegd dat de persoonlijke databescherming ten dienst stond van het beschermen van de privacy, terwijl dit wel in de algemene richtlijn was opgenomen. Hierdoor bleven bepaalde nationale verschillen op het gebied van de relatie tussen persoonlijke databescherming en grondrechten bestaan.[69]

Richtlijn 95/46/EG geeft het kader aan waar de nationale wetgevende machten binnen moeten werken, maar de richtlijn geeft ook aan wanneer de lidstaten bepaalde beperkende maatregelen mogen nemen, bijvoorbeeld ter voorkoming, opsporing of vervolging van misdaden.[70]

Inmiddels is de richtlijn, die leidend is voor de Europese omgang met databescherming, al meer dan 20 jaar oud. In die tussenliggende jaren zijn er allerlei nieuwe technologische ontwikkelingen in gebruik genomen, ander andere op het gebied van het ontcijferen van geanonimiseerde data. Nieuwe technologie is echter niet het enige aspect dat er voor heeft gezorgd dat de EC op 25 januari 2012 een voorstel introduceerde op de bestaande regels voor databescherming aan te passen. In de loop der jaren werden er ook grote verschillen zichtbaar tussen lidstaten aangaande het concept van bescherming van persoonlijke data.

Zo vallen in Italië en Frankrijk ook overledenen onder de databeschermingswet, terwijl in het Verenigd Koninkrijk de wetgeving zich alleen maar beperkt tot "*living individuals*". Dit is een heel duidelijk verschil, maar wat is het probleem? Als voorbeeld geeft Mario Viola de Azevedo Cunha de begunstigden van een levensverzekering. Die informatie heeft betrekking op een overleden persoon en wordt daarom in het Verenigd Koninkrijk niet als persoonlijke data beschouwd.[71] Dit, en vergelijkbare, verschil(len) kunnen een belemmering vormen voor het vrij verkeer van diensten in de EU aangezien aanbieders van diensten met verschillende regels te maken krijgen in verschillende lidstaten. En doordat handel tussen lidstaten er ook voor zorgt dat de stroom van persoonlijke data

[68] Ibidem, 140-141; Latere richtlijnen dienden onder andere ter vervanging van de bestaande richtlijnen. Zo verving richtlijn 2002/58/EG de oude richtlijn 97/66/EG om ook de bescherming van privacy vast te leggen voor elektronische communicatie, zie Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, 216.
[69] Ibidem, 156.
[70] Normann Witzleb, David Lindsay, Moira Paterson en Sharon Rodrick (red.), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge 2014) 82.
[71] Serge Gutwirth, Ronald Leenes, Paul de Hert en Yves Poullet (red.), *European Data Protection: In Good Health?* (Dordrecht 2012) 279.

wordt geïntensifieerd, is het voor de EC van belang om te voorkomen dat er verschillende niveaus aangaande persoonlijke databescherming bestaan in het Europese handelsblok.[72]

Het bovenstaande geval is een voorbeeld van de verschillende interpretaties die er toe hebben geleid dat de EC met een nieuwe wetsvoorstel kwam. Het nieuwe wetsvoorstel is er overigens niet alleen op gericht om deze verschillen weg te nemen, maar ook om een grondrecht van Europeanen, het recht op databescherming, beter te verankeren in de wetgeving.

In het jaar 2000 werd bij de Europese Raad te Nice namelijk het Handvest van de Grondrechten van de EU uitgeroepen. Onder artikel 3 van het Handvest werd 'de bescherming van persoonsgegevens' als een erkende vrijheid in de EU vastgelegd. Het Handvest had toentertijd geen enkel bindend rechtsgevolg, maar dat veranderende op 1 december 2009. Toen trad het Verdrag van Lissabon in werking en daarmee werd het Handvest wettelijk bindend voor alle EU-instellingen en nationale overheden.[73]

De in 2012 voorgestelde wetgeving is ook weer sterk gericht op databescherming. Databescherming vormde dan ook een belangrijk onderdeel van de *European Agenda on Security* van de EC.[74] Maar hoe zit het met de privacywetgeving in de EU? Naast artikel 8 van het EVRM geldt ook artikel van het Handvest van de Grondrechten van de EU als een belangrijke pijler voor de privacy. In artikel 7 staat namelijk dat '*[e]veryone has the right to respect for his or her private and family life, home and communications*'. Het probleem met deze definitie is dat nergens duidelijk staat omschreven wat een 'privéleven' precies inhoudt.[75]

Hierdoor spelen het EVRM en uitspraken van het Europees Hof voor de Rechten van de Mens (EHRM) in Straatsburg een belangrijke rol voor het bepalen wat 'privacy' inhoudt. De jurisprudentie van het Hof beschouwt het EVRM daarbij als een instrument dat zich in feite steeds weer aanpast aan de omstandigheden, en dus aan nieuwe technische ontwikkelingen en zaken aangaande databescherming.[76]

Het databeschermingsbeleid van de EC biedt overigens een aantal belangrijke voordelen bij het reguleren van surveillance. De regels zorgen immers voor regulering voor het verzamelen, verwerken en uitwisselen van data; ze creëren belangrijk wettelijke principes voor de toegang tot en

[72] Gutwirth e.a., *European Data Protection: In Good Health?*, 279-281.
[73] Europese Commissie, 'EU Charter of Fundamental Rights' (versie 8 januari 2016), http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm (26 oktober 2012); Lidstaten van de EU, 'Charter of Fundamental Rights of the European Union' (versie 31 januari 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (31 januari 2016).
[74] Europese Commissie, The European Agenda on Security (Straatsburg 2015), beschikbaar via http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf (31 januari 2016).
[75] Normann Witzleb e.a. (red.), *Emerging Challenges in Privacy Law*, 76.
[76] Ibidem, 90-91.

het gebruik van persoonlijke data; ze leiden tot innovatie op het gebied van wetgeving, zoals 'het recht om vergeten te worden', en de ontwikkeling van regels voor databescherming hebben geleid tot een raamwerk van toezichtsorganen die enerzijds hun advies geven over wetgevende ontwikkelingen met betrekking tot databescherming en anderzijds toezicht houden op de naleving van databeschermingswetgeving.[77]

Tegelijkertijd zijn er ook twee beperkingen te noemen wat betreft de effectiviteit van databescherming ten opzichte van preventieve surveillance. De effectiviteit van databescherming is beperkt wat betreft het reguleren van de politieke keuzes om het verzamelen en verwerken van persoonlijke data te maximaliseren en te generaliseren. Het idee van 'privacy' draait namelijk onder meer om het creëren van non-invloedssferen: plekken waar de staat geen zeggenschap over heeft. Databescherming draait daarentegen juist om het idee dat de overheid wel degelijk persoonlijke data kan en mag verwerken. Men kan stellen dat preventieve surveillance op deze manier wordt gedepolitiseerd. Als gevolg hiervan worden er eigenlijk weinig vraagtekens gesteld bij het nut van surveillance of het beperken ervan. In plaats daarvan wordt als oplossing voor het probleem gekeken naar nieuwe vormen van toezicht.[78]

Daarnaast is het ook belangrijk om te noemen dat databescherming slechts over specifieke zaken gaat, wat als gevolg heeft dat de bescherming daardoor steeds op verschillende categorieën van persoonlijke informatie gericht is. Privacy, daarentegen, gaat over (de identiteit van) 'de persoon' in het algemeen en vormt zodoende een holistisch raamwerk om de impact van surveillance op de relatie tussen het individu en de staat te kunnen bepalen. Doordat databescherming zich richt op verschillende aspecten kan dat tot fragmentatie leiden waarbij het grotere beeld verloren gaat – zoals profiling, discriminatie en de impact van surveillance op mensenrechten.[79]

1.3 Vrijheid versus waardigheid

Dit hoofdstuk begon met de *Safe Harbour*-overeenkomst die door het Europees Hof van Justitie onrechtmatig werd verklaard. Het opschorten van de overeenkomst betekende in feite dat Europa de VS niet meer als een 'veilige haven' beschouwde voor de (opgeslagen) gegevens van Europeanen. De bestaande *Safe Harbour*-overeenkomst uit 2000 kwam door de rechtszaak onder een vergrootglas te

[77] Valsamis Mitsilegas, 'The Value of Privacy in an Era of Security: Embedding Constitutional Limits on Preemptive Surveillance', *International Political Sociology* 8 (2014) 1, 104-108, 105-106.
[78] Mitsilegas, 'The Value of Privacy in an Era of Security', 106.
[79] Ibidem, 106.

liggen en, mede door de onthullingen vanaf 2013 door Snowden, werd besloten dat de overeenkomst onwettig werd verklaard.

Zowel het recht op privacy als het recht op databescherming speelden daarbij een rol, maar wat bepalen deze twee grondrechten eigenlijk? Ze schetsen, samen met andere grondrechten, de grenzen van de macht van de staat. Het zijn zogezegd de 'wettelijke consequenties van de politieke institutionalisering van de privésfeer'. Het individu heeft bepaalde onvervreemdbare grondrechten als bescherming tegen de macht van de staat, terwijl de macht van de staat – maar ook andere machten, zoals die van bedrijven – beperkt wordt door (grond)wettelijke regels. Die regels moeten er immers voor zorgen dat de overheid zich aan de eigen regels houdt. Bovendien zorgen de scheiding der machten, transparantie en verantwoording die aan de burger moeten worden gegeven ervoor dat de staat onder toezicht staat.[80]

Het recht op privacy en het recht op databescherming bepalen dus mede de politieke privésfeer in verhouding tot de publieke sfeer. Dat doen beide rechten op een verschillende manier. Het recht op privacy stelt namelijk grenzen die het individu beschermt tegen de staat, en andere machten, die een bepaalde mate van 'dekkend vermogen' van het individu willen oplichten. Databescherming voorziet in legitiem machtsgebruik door een bepaalde mate van transparantie en machtsverantwoordelijkheid op te leggen. Oftewel, privacy beschermt het individu terwijl databescherming de organisaties controleert en stuurt die persoonlijke data verwerken.[81]

Dat er binnen de EU veel aandacht is voor databescherming is niet verbazingwekkend. Niet alleen is goede, en vooral eenzijdige, regelgeving op het gebied van databescherming van belang voor het functioneren van een Europese gemeenschappelijke markt, maar moderne vormen van communicatie zorgen er ook voor dat individuen kwetsbaarder zijn voor inbreuk op de privacy. Zeker in het geval van de toenemende (online) dataopslag en de steeds geavanceerdere afluisterpraktijken. Bovendien kan metadata al heel veel over persoon vertellen.[82]

Hoe gaan de VS en Europa in hun wetgeving dan om met privacy en databescherming? Het eerste juridische argument voor een brede opvatting van het recht op privacy kwam uit de koker van twee Amerikanen in de jaren '90 van de 19e eeuw. Samuel Warren en Louis Brandeis, die spraken over 'het recht om alleen gelaten te worden', hadden hun betoog deels gebaseerd op Engelse jurisprudentie uit de eerste helft van de 19e eeuw en beweerden daarnaast dat het recht op privacy ook al in de

[80] Serge Gutwirth e.a., D1: Legal, social, economic and ethical conceptualisations of privacy and data protection (Rapport PRESCIENT project, zp 2011) 7.
[81] Gutwirth e.a., D1: Legal, social, economic and ethical conceptialisations, 8.
[82] Schneier, *Data and Goliath*, 13; 18-20.

Franse wet terug te vinden was.[83] Europese opvattingen lagen dus aan de basis van de Amerikaanse ontwikkeling van het recht op privacy.

Toch is er tegenwoordige een andere omgang met privacy en data zichtbaar in de VS dan in Europa. In de VS is de privacybescherming gebaseerd op de concepten autonomie en vrijheid die terug te vinden zijn in de Amerikaanse grondwet en de *Bill of Rights*. Hierdoor hebben Amerikanen ook het recht om zelf keuzes te maken op het gebied van 'fundamentele' vrijheden, zoals abortus, huwelijk of het onderwijs. Daarnaast toont de opkomst van de specifieke sectorale (privacy)wetgeving de Amerikaanse omgang met privacy: het opzetten van privacy statuten om de vergaring en het gebruik van specifieke informatie te reguleren die, volgens het Congres, gevoelig is en dus extra bescherming nodig heeft.[84] In Europa wordt juist gewerkt met algemene richtlijnen voor de gehele EU. Dat wil overigens niet zeggen dat de wetgeving in alle lidstaten er hetzelfde is. De wetgeving aangaande databescherming, maar ook de handhaving, verschilt juist sterk tussen de lidstaten. Juist om die verschillende vormen wetgeving te harmoniseren kwam de EC in 2012 met een hervormingsvoorstel.[85]

Een ander duidelijk feit is dat de Europese wetgeving voor databescherming vereist dat er een wettelijke basis is en dat er een legitiem doel bestaat voordat persoonlijke data mag worden verwerkt, terwijl in de VS commerciële data in het algemeen mag worden verwerkt, tenzij er een wettelijke regel is die dat voorkomt. De Amerikaanse *Privacy Act* stelt echter wel voorwaarden aan het verwerken van persoonlijke data, maar die wet is specifiek gericht op het gebruik van data door de overheid.[86]

Cultuurverschillen in de omgang met privacy zijn ook van belang. Wanneer er sprake was van een spanning tussen de vrijheid van meningsuiting en het recht op privacy heeft het Amerikaanse Hooggerechtshof in het verleden met regelmaat het recht op vrijheid van meningsuiting, dat is vastgelegd in het Eerste Amendement, laten prevaleren boven het recht op privacy. Het Europese Hof van Justitie laat het belang van databescherming en privacy juist vaak zwaarder wegen dan de vrijheid van meningsuiting.[87] Dit is, om professor vergelijkend en internationaal recht James Whitman aan te halen, een uiting van het fundamentele verschil in houding tussen de VS en Europa wat betreft privacy(wetgeving). De privacywetgeving, en volgens Whitman de wetgeving in het algemeen, is een uiting van het verschil in sociale tradities. In de VS zijn die sterk gericht op vrijheid, terwijl ze in Europa meer gericht zijn op waardigheid.[88]

[83] Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, 27.
[84] Ibidem, 16.
[85] Ibidem, 15-16.
[86] Ibidem, 19.
[87] Ibidem, 19.
[88] James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty', *The Yale Law Journal* 113 (2004) 6, 1151-1223, 1220.

Er wordt getwist over de beste manier om de privacy van burgers te waarborgen. Is de Europese manier, waarbij een Europese richtlijn een raamwerk vormt voor basisrechten die nationaal worden gecontroleerd door databeschermingsautoriteiten (zoals de Autoriteit Persoonsgegevens), beter? Of is dat de Amerikaanse manier, waar het belang van privacy wordt bezien als een consumentenrecht en waar wetgeving zich specifiek richt op bepaalde kwaden en gevoelige informatie met als doel het vergroten van het consumentenvertrouwen en de handel?

Zowel in de VS als de EU is, ondanks de aanwezigheid van sterke verschillen ten opzichte van privacy, een hoge mate van privacybescherming aanwezig.[89] Zegt dit echter iets over de handelswijzen van de inlichtingendiensten? De ontwikkeling van het inlichtingenwerk heeft altijd onderdeel uitgemaakt van trends in het gebruik van informatie, zowel binnen de overheid als daarbuiten. Op dat terrein hebben inlichtingendiensten zich sinds het einde van de negentiende eeuw ontwikkeld tot een belangrijk instrument voor overheden. Een instrument dat overheden de ontwikkelingen in de wereld toont. Hierdoor zijn inlichtingendiensten belangrijk voor het nemen van overheidsbesluiten.[90] Het is daarom maar de vraag of een hoge mate van privacybescherming wel van invloed is op de handelswijzen van de inlichtingendiensten.

[89] Kenneth A. Bamberger en Deirdre K. Mulligan, 'Privacy on the Books and on the Ground', *Stanford Law Review* 63 (2011) 2, 247-316, 281-284.
[90] Herman, *Intelligence power in peace and war*, 35.

2 De inlichtingen- en veiligheidsdiensten

Toen Edward Snowden in juni 2013 de documenten vrijgaf die aantoonden dat de NSA op grote schaal mensen afluisterde en volgde, gaf hij de volgende verklaring voor het vrijgeven van de gegevens:

> So long as there's broad support amongst a people, it can be argued there's a level of legitimacy even to the most invasive and morally wrong program, as it was an informed and willing decision….However programs that are implemented in secret, out of public oversight, lack that legitimacy, and that's a problem. It also represents a dangerous normalization of "governing in the dark," where decisions with enormous public impact occur without any public input.[91]

Het heimelijke aspect van de surveillanceprogramma's van de NSA stootte Snowden dus duidelijk tegen de borst. Snowden heeft het over een gebrek aan openbaar toezicht en is tevens bang voor het feit dat het normaal gevonden gaat worden dat belangrijke besluiten, die een grote publieke impact hebben, worden genomen zonder dat er inspraak van de volksvertegenwoordiging aan te pas komt. Volgens Snowden schort het aan legitimiteit voor het uitvoeren van de surveillanceprogramma's: een wettelijke basis ontbreekt. Dit zou als gevolg hebben dat inlichtingendiensten, die de programma's uitvoeren, onrechtmatig handelen.

Wanneer surveillanceactiviteiten in het geheim worden uitgevoerd, is de verwachting dat er ook dingen gebeuren die het daglicht niet kunnen verdragen en wellicht illegaal zijn. Zeker bij inlichtingen- en veiligheidsdiensten kan dat het geval zijn. De diensten zijn immers bezig met beschermen (en bevorderen) van de nationale veiligheid, bevinden zich daarbij binnen een spanningsveld tussen veiligheid aan de ene kant en privacy aan de andere kant én handelen daarbij in het duister.

Dat laatste aspect, het opereren in het duister, zorgde er voor dat er zo veel woede en verbijstering was over de onthullingen van Snowden. De pers, het publiek en buitenlandse staatshoofden wisten immers niks af van de activiteiten die de NSA ondernam, en dus wisten zij ook niet of de activiteiten toegestaan waren volgens de geldende regels.[92] Het grote publiek wist dus niks af van de feiten, terwijl een kleine groep – binnen de uitvoerende, wetgevende en rechtsprekende macht – het wel wist. Het is dan ook niet verbazingwekkend dat er vervolgens vraagtekens werden gezet bij de legitimiteit van de NSA-praktijken, zeker aangezien Snowden zelf het label "illegaal"

[91] George R. Lucas Jr., 'NSA Management Directive #424: Secrecy and Privacy in the Aftermath of Edward Snowden', *Ethics & International Affairs* 28 (2014) 1, 29-38, 29.
[92] Fidler (red.), *The Snowden Reader*, 23.

gebruikte. Toch werd er na de onthullingen van Snowden door voorstanders van het NSA-programma gewezen op de regels, procedures, instituties en toezicht die van toepassing waren op de activiteiten van de dienst. Er waren, kortom, genoeg *checks and balances* aanwezig.

Om die bewering beter op waarde te kunnen schatten zal in dit hoofdstuk de privacywetgeving binnen de EU en de VS naast de bevoegdheden van de Europese en Amerikaanse inlichtingendiensten worden gelegd. Er zal worden gekeken of de privacywetgeving met de bevoegdheden van de diensten correspondeert en dus het een wel met het ander in overeenstemming is. Dat daarbij ook naar Europa wordt gekeken valt niet alleen te rechtvaardigen doordat Europese en Amerikaanse inlichtingendiensten veel met elkaar samenwerken, maar ook doordat de Britse inlichtingendienst *Government Communications Headquarters* (GCHQ), zo bleek uit de documenten die Snowden gelekt heeft, nauw samenwerkte met de NSA.

In relatie tot praktijken van de NSA en de onthullingen van Snowden zijn er door zowel Amerikaanse rechters als Europese rechters ook nog een aantal rechterlijke overwegingen uitgesproken tijdens de diverse rechtszaken die op dit vlak de afgelopen jaren zijn gehouden. Alhoewel deze overwegingen per definitie niets zeggen over de legitimiteit van de praktijken, geven ze vaak wel een interessante, nieuwe kijk op bestaande praktijken. Vandaar dat een aantal van deze gerechtelijke overwegingen in dit hoofdstuk bediscussieerd zal worden.

In dit hoofdstuk wordt gesproken over 'legitimiteit'. Het begrip 'legitimiteit' heeft niet alleen betrekking op het al dan niet aanwezig zijn van een wettelijke basis, maar zal vrijwel altijd ook slaan op het eventueel bestaan van een maatschappelijk draagvlak. Dit zijn logischerwijs twee verschillende zaken. Over dat maatschappelijk draagvlak ging het in de quote van Snowden aan het begin van dit hoofdstuk, maar daar zal in dit hoofdstuk niet de focus op liggen. Wanneer er verderop over 'legitimiteit' gesproken zal worden, zal het gaan over het wel of niet aanwezig zijn van een wettelijk basis. Een breed maatschappelijk draagvlak voor de surveillanceprogramma's van de Amerikaanse overheid lijkt slechts beperkt aanwezig te zijn. Zo bleek uit een peiling van het *Pew Research Center*, uitgevoerd tussen 26 november 2014 en 3 januari 2015, dat Amerikanen verdeeld zijn over het publiek belang van de surveillanceprogramma's van de Amerikaanse overheid.[93]

[93] Zo is 61 procent van de mensen die van surveillanceprogramma's hebben gehoord er minder zeker van dat de programma's het publiek belang dienen, terwijl 37 procent aangeeft zekerder te zijn van het feit dat de programma's het publiek belang dienen. Zie Lee Rainie en Mary Madden, 'Americans' Privacy Strategies Post-Snowden' (versie 16 maart 2015), http://www.pewinternet.org/2015/03/16/Americans-Privacy-Strategies-Post-Snowden/ (26 maart 2016).

2.1 (On)Wettig handelen?

Als er wordt gekeken naar de verschillende praktijken van de inlichtingendiensten, die door middel van de onthullingen van Snowden aan het licht kwamen, zou een eerste logische reactie kunnen zijn om te zeggen dat de diensten onrechtmatig hebben gehandeld. Uit de gelekte documenten bleek immers dat de diensten in het geheim veel verschillende soorten gegevens onderschepten. Door middel van elektronische surveillanceprogramma's werden telefoon- en internetgegevens van veel Amerikanen buitgemaakt. Enorme hoeveelheden telefoongegevens, bekend als metadata, werden verzameld. Ook werd gepoogd encryptie van internetcommunicatie te breken en werden staatshoofden van andere (bevriende) landen, waaronder de Braziliaanse president Dilma Rousseff, afgeluisterd.[94]

De onthullingen van Snowden begonnen op 5 juni 2013 met het vrijgeven van het document dat later bekend kwam te staan als de *'Verizon Order'*.[95] In dat document beval de FISC telefoonprovider Verizon om dagelijks een uittreksel van gegevens over telefoongesprekken tussen de VS en het buitenland te verschaffen aan de NSA. De volgende dag kreeg deze onthulling een vervolg met het bekend worden van het bestaan van de PRISM- en UPSTREAM-programma's.[96]

Het BULLRUN-project was de naam voor het geheime NSA-project waarmee getracht werd om de encryptie van internetcommunicatie van buitenlandse inlichtingendoelwitten te breken. Nadat het bestaan van dit programma in de openbaarheid kwam, brak er meteen een hoop kritiek los over het feit dat de NSA blijkbaar zou proberen om encryptie te omzeilen terwijl juist encryptie erg belangrijk wordt geacht voor het beveiligen van communicatie via internet.[97]

Hoe zit het met de legitimiteit van bovenstaande en andere surveillanceprogramma's van de NSA?[98] Op welke gronden worden de programma's bij de NSA, gericht op het vergaren van buitenlandse inlichtingen, gelegitimeerd? Van belang daarvoor is in ieder geval *Executive Order* (EO)

---

[94] Daniel Byman en Benjamin Wittes, 'Reforming the NSA. How to Spy after Snowden' (versie 17 april 2014), https://www.foreignaffairs.com/articles/united-states/2014-04-17/reforming-nsa (26 maart 2016).
[95] Fidler (red.), *The Snowden Reader*, 92-95.
[96] Het PRISM-programma stelde de NSA – de Britse GCHQ had toegang tot de gegevens van de NSA – in staat om data te verzamelen van de servers van een aantal Amerikaanse technologiebedrijven: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, Youtube en Apple. Het UPSTREAM-programma betekende het aftappen van communicatiegegevens, via commerciële partijen, op het moment dat die door glasvezelkabels heen gingen. Zie Washington Post, 'NSA slides explain the PRISM data-collection program' (versie 10 juli 2013), http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (26 maart 2016).
[97] Fidler (red.), *The Snowden Reader*, 167-168.
[98] Voor een overzicht van de bekende *surveillance*-programma's van de NSA zie de website van ProPublica: Julia Angwin en Jeff Larson, 'The NSA Revelations All in One Chart' (versie 30 juni 2014), https://projects.propublica.org/nsa-grid/ (27 maart 2016).

12333. EO 12333 is een decreet dat president Ronald Reagan in 1981 uitvaardigde en dat, in de woorden van hoogleraar recht Samuel J. Rascoff, *'governs the intelligence community'*.[99]

Verder speelden ook nog andere wetgeving een rol in de regulering van het handelen van de NSA: sectie 702 van de *Foreign Intelligence Surveillance Act* en sectie 215 van de *USA Patriot Act*.[100]

Bij de behandeling van de wetgeving moet in gedachte worden gehouden dat inbreuk maken op iemands privacy niet zomaar is toegestaan. Wanneer de staat besluit wordt om inbreuk te maken op iemands privacy, moet die inbreuk worden goedgekeurd door de bevoegde autoriteiten en moet er dus sprake van wettelijke toestemming zijn. Edward Snowden heeft aangegeven dat dit in zijn ogen betekent dat de desbetreffende wetgeving ook inzichtelijk moet zijn voor burgers. Dit moet gepaard gaan met juridisch toezicht met betrekking tot de uitvoering van de wetgeving. Deze punten zijn volgens Snowden niet van toepassing op de Amerikaanse praktijken.[101] Hieronder zal daarom niet alleen de relevante wetgeving behandeld worden, maar zal tevens worden gekeken hoe de Amerikaanse praktijk zich verhoudt tot de uitspraken van Snowden.

2.2 Inlichtingendiensten en wetgeving in de Verenigde Staten

De NSA opereert niet alleen grotendeels in het duisternis, ook het bestaan van de inlichtingendienst was in eerste instantie in duisternis gehuld. President Truman richtte in 1952 de NSA op om het decodeerwerk, opgezet in de Tweede Wereldoorlog, in stand te houden.[102] De dienst opereerde echter in eerste instantie dusdanig in het geheim dat het bestaan van de dienst pas vijf jaar later – in 1957 – officieel door het Witte Huis werd erkend.[103]

In de jaren '70 kwam er mondjesmaat steeds meer informatie naar buiten over misstanden binnen de Amerikaanse inlichtingengemeenschap. De Vietnamoorlog had de presidenten Johnson en Nixon er toe bewogen om de inlichtingendiensten op te dragen zo veel mogelijk onderzoek te doen naar mogelijke subversieve elementen binnen de antioorlog-beweging.[104]

Uiteindelijk bleek dat zowel de *Federal Bureau of Investigation* (FBI), de *Central Intelligence Agency* (CIA), als diverse inlichtingendiensten van het Amerikaanse leger (waaronder de NSA)

[99] Samuel J. Rascoff, 'Presidential Intelligence', *Harvard Law Review* 129 (2016) 3, 633-716, 645.
[100] De *USA Patriot Act* heet voluit de *Uniting and Strengthening America by Providing Appropiate Tools Required to Intercept and Obstruct Terrorism Act of 2001*.
[101] Zygmunt Bauman e.a., 'After Snowden: Rethinking the Impact of Surveillance', *International Political Sociology* 8 (2014) 2, 121-144, 131-132.
[102] Newton Lee, *Counterterrorism and Cybersecurity: Total Information Awareness* (New York 2015) 153.
[103] Fidler (red.), *The Snowden Reader*, 4. Doordat het bestaan van de NSA tot 1957 werd ontkend, werd er gezegd dat NSA zou staan voor '*No Such Agency*'.
[104] Clarke e.a., *The NSA Report*, 11.

binnenlandse spionageprogramma's hadden opgezet om (mogelijke) tegenstanders van de Vietnamoorlog in de gaten te houden. Die tegenstanders, onder wie leden van het Congres, journalisten en burgerrechtenactivisten, werden onder meer gevolgd door infiltratie en elektronische surveillance.[105]

Verschillende onderzoekscommissies van het Congres deden in die jaren onderzoek naar de misstanden. De bekendste van deze commissies was de *Senate's Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, oftewel de commissie-Church, genoemd naar de voorzitter senator Frank Church. Onder andere naar aanleiding van de bevindingen van deze commissie werd geconcludeerd dat de president te veel macht had binnen de inlichtingengemeenschap.[106] Vandaar dat er werd besloten om de macht van de uitvoerende macht (lees: de president) te balanceren door ook de andere machten van de overheid – de wetgevende en rechtsprekende macht – een bepaalde mate van toezicht toe te kennen. Uiteindelijk resulteerde dat in het oprichten van de FISC, het instellen van speciale commissies binnen het Congres voor toezicht op de inlichtingendiensten, het aanstellen van inspecteur-generaals binnen de verschillende diensten zelf en het oprichten van de federale *Intelligence Oversight Board*.[107]

Voor de NSA betekende dit dat wettelijke bepalingen de activiteiten van de dienst gingen inkaderen. Een belangrijk moment vond in 1981 plaats, toen president Reagan EO 12333 uitvaardigde. De achterliggende gedachte daarbij was het vergroten van de slagkracht van de NSA, en de Amerikaanse inlichtingengemeenschap in het algemeen, te vergroten met betrekking tot het vergaren van buitenlandse inlichtingen. Tot slot zal hieronder ook een ander belangrijke wet behandeld worden: de *USA Patriot Act* uit 2001. Deze wet werd door president Bush in het leven geroepen om de inlichtingendiensten beter in staat te stellen om de VS te 'verdedigen' na de aanslagen van 11 september 2001.

2.2.1 FISA: Foreign Intelligence Surveillance Act

In 1978 zag de *Foreign Intelligence Surveillance Act* (FISA) het levenslicht. Het initiatief voor het instellen van deze wet kwam van senator Ted Kennedy en gaf concrete vorm aan het gerechtelijke en wetgevende toezicht van de geheime surveillanceactiviteiten van de overheid tegen *"the activities of foreign powers, within or without this country"*.[108] Het specifieke doel van de wet was uiteraard niet

[105] Ibidem, 11.
[106] Het ging hierbij niet alleen om de misstanden rondom de Vietnamoorlog. In diezelfde periode vond ook het Watergate-schandaal plaats.
[107] Rascoff, 'Presidential Intelligence', 635-636.
[108] Lee, *Counterterrorism and Cybersecurity*, 154; Clarke e.a., *The NSA Report,* 64.

het beschermen van buitenlandse mogendheden tegen de inlichtingendiensten, maar juist het beschermen van de communicatiestromen van *U.S. persons* binnen de VS.[109] Er werden daarom geen beperkingen in de wet vastgelegd voor wat betreft de surveillance van doelwitten die zich buiten de VS bevonden.[110]

Het centrale punt van de wet ging om het belang van de rechtsgeldigheid van elektronische surveillance voor buitenlandse inlichtingendoeleinden. De gedachte was dat het land beschermd moest worden tegen de misstanden van de inlichtingendiensten zoals die onder andere door de commissie-Church waren vastgesteld, terwijl tegelijkertijd ook de slagkracht van de inlichtingendiensten om buitenlandse dreigingen tegen te gaan niet in het gedrang moest geraken.

Sinds 1967, na een uitspraak van het Amerikaanse Hooggerechtshof in de zaak *Katz v. United States*, gold de opvatting dat het Vierde Amendement niet alleen plaatsen beschermt – zoals de huizen van Amerikanen – maar juist ook mensen. Het Hooggerechtshof gebruikte de redenatie dat het Vierde Amendement in zijn ogen de '*reasonable expectation of privacy*' van mensen garandeert. Met de opkomst van de telecommunicatie bleek dit een zeer belangrijke uitspraak. Aan de uitspraak werd namelijk de conclusie gekoppeld dat de overheid geen afluisterapparatuur mag inzetten, tenzij het eerst een bevelschrift heeft verkregen van een (onafhankelijke) rechtbank. Ook tijdens een telefoongesprek mag iemand namelijk een redelijke verwachting van privacy hebben. Om de inzet van afluisterapparatuur te rechtvaardigen moest er daarom sprake zijn van een vondst of een gerede aanleiding die de doorslaggevende factor is in de gedachte dat onderschepping van communicatie bewijs van een strafbaar feit zal opleveren.[111]

Een andere reden voor het Congres om het FISA-voorstel te behandelen was de macht van de president met betrekking tot het onderzoeken van activiteiten van buitenlandse mogendheden. Er werd namelijk tot dan toe, en niet ten onrechte, over het algemeen aangenomen dat de president, op basis van de grondwet, veel beslissingsbevoegdheid had om besluiten te nemen om het land te beschermen op het gebied van inlichtingenvergaring in het buitenland. Daarbij hoefde president zich niet aan de vereisten te houden die door het Vierde Amendement werden gesteld.[112] Op het gebied

[109] De federale rechtsprekende en uitvoerende macht van de VS definiëren een *U.S. person* als: 1.een Amerikaans staatsburger; 2.een buitenlander die wettelijk tot de VS is toegelaten met het oog op een permanent verblijf; 3.een onderneming zonder rechtspersoonlijkheid met een substantieel aantal leden die Amerikaans staatsburger zijn óf buitenlanders die wettelijk tot de VS zijn toegelaten met hoog op een permanent verblijf; 4.een bedrijf dat in de VS is gevestigd. Zie National Security Agency, 'SIGINT Frequently Asked Questions' (versie 15 januari 2009), https://www.nsa.gov/sigint/faqs.shtml#sigint4 (28 maart 2016).
[110] Amos Toh, Faiza Patel en Elizabeth Goitein, Overseas Surveillance in an Interconnected World (Rapport *Brennan Center for Justice*, New York 2016) 12.
[111] Clarke e.a., *The NSA Report*, 64-65
[112] Ibidem, 66.

van de buitenlandse inlichtingenvergaring was er dus sprake van een hoge mate van autonomie voor de uitvoerende macht.

Een uitspraak van het Amerikaanse Hooggerechtshof in 1972 geeft de binnenlandse context weer waarin FISA tot stand kwam. De zaak waar de uitspraak betrekking op had draaide om de geldigheid van de inzet, zonder bevelschrift, van elektronische opsporingsmiddelen (zoals afluisterapparatuur) tegen leiders van de radicale White Panther Party. Volgens de overheid was de inzet van dergelijke middelen in deze zaak gerechtvaardigd omdat de personen in kwestie van plan waren geweest om een aanslag te plegen op een overheidsgebouw en daarmee schade wilden toebrengen aan de Amerikaanse overheid.[113] Toch oordeelde het Hooggerechtshof dat overheidsbeambten verplicht waren om op voorhand een bevelschrift te verkrijgen voordat er zou worden gestart met elektronische surveillance, zelfs wanneer het om de binnenlandse veiligheid zou gaan.[114]

Onder aan de streep werd de wet een compromis tussen diegenen die veel speelruimte voor de inlichtingendiensten wilden handhaven en diegenen die de buitenlandse inlichtingenvergaring dezelfde beperkingen wilden opleggen als bij gewone inlichtingenactiviteiten, zoals bijvoorbeeld in 1972 door het Hooggerechtshof was vastgesteld.[115] Er dient gezegd te worden dat het hierbij dus wel ging om het beschermen van Amerikanen tegen elektronische surveillance, niet van buitenlanders.

Normaal gesproken moet er bij het gebruik van een bevelschrift namelijk sprake zijn van gerede aanleiding om aan te nemen dat er een misdrijf is of wordt begaan. Ook het onderscheppen van communicatieverkeer wordt normaal gesproken gezien als een ernstige inbreuk op het recht op privacy en het recht op vrijheid van meningsuiting. Beide punten zijn echter niet de uitgangspunten onder FISA. Onder FISA is het uitvoeren van surveillance namelijk wel mogelijk wanneer er een gerede aanleiding bestaat dat het doelwit een (vertegenwoordiger van een) buitenlandse mogendheid is. Indien het doelwit een *U.S. person* betreft, moet er gerede aanleiding bestaan dat diegene zich bezig houdt met spionage. Een *U.S. person* mag echter niet als een vertegenwoordiger van een buitenlandse mogendheid worden gezien op basis van activiteiten die vallen onder het Eerste Amendement van de Amerikaanse grondwet.[116]

---

[113] De *Omnibus Crime Control and Safe Streets Act* (1968), waar de Staat zich op baseerde, maakt namelijk een uitzondering voor binnenlandse *surveillance* zonder officiële toestemming wanneer het bestaan, of bestaande structuren, van de Amerikaanse overheid bedreigd wordt.
[114] Zie voor de uitspraak in deze zaak: Legal Information Institute, 'United States v. United States District Court' (versie 28 maart 2016), beschikbaar via https://www.law.cornell.edu/supremecourt/text/407/297.
[115] Clarke e.a., *The NSA Report*, 64-65.
[116] Electronic Privacy Information Center, 'Foreign Intelligence Surveillance Act (FISA)' (versie 28 maart 2016), https://epic.org/privacy/surveillance/fisa/ (28 maart 2016).

Met FISA werden specifieke procedures vastgelegd voor het toestaan van verschillende onderzoeksmethoden: elektronische surveillance, onderzoek van het lichaam, *pen register/trap & trace surveillance* – een *pen register* apparaat registreert en bewaart de uitgaande informatie van een apparaat, terwijl met *trap & trace* inkomende elektronische pulsen worden geregistreerd – en het gebruik van bevelschriften om iemand te dwingen bepaalde bedrijfsgegevens beschikbaar te stellen.[117] Vastgestelde objectieve criteria maken onderdeel van de procedures om de buitenlandse zoekacties te reguleren.[118] In 2008 werd de wet gewijzigd waardoor de inlichtingendiensten voortaan ook verplicht werden om een bevelschrift op te vragen voor het uitvoeren van surveillance in het buitenland waarbij *U.S. persons* of buitenlanders bewust het doelwit zijn.[119]

Om de verzoeken van inlichtingendiensten voor een bevelschrift te kunnen beoordelen werd een speciale rechtbank, de *Foreign Intelligence Surveillance Court*, opgericht met als taak het beoordelen en vervolgens toe- of afwijzen van overheidsverzoeken om de hierboven genoemde onderzoeksmethoden in te zetten. Deze rechtbank bestaat tegenwoordig uit elf federale rechters die de aanvragen onder de loep nemen. Deze aanvragen zijn afkomstig van de minister van Justitie, wat betekent dat de minister van Justitie zelf alle verzoeken van de diensten moet goedkeuren voordat ze ook daadwerkelijk worden ingediend. Het verzoek moet inhoudelijk aan diverse eisen voldoen.[120] Tijdens de behandeling van een zaak wordt slechts één partij gehoord, namelijk de partij die het verzoek indient. In de FISA is namelijk de bepaling vastgelegd dat de hoorzittingen over de verzoeken *"must be ex parte and conducted within the Court's secure facility"*.[121] *Ex parte* houdt in dat de rechtbank slechts één partij hoort. De rechtbank doet in de regel niet aan hoor en wederhoor: er is geen procedure vastgelegd voor het gebruik van meningen van non-gouvernementele partijen binnen de FISC. Daarmee is de enige partij die de rechtbank hoort de uitvoerende macht.[122]

Als de FISC een verzoek voor elektronische surveillance goedkeurt is het bevelschrift geldig voor negentig dagen in het geval van een vertegenwoordiger van een buitenlandse mogendheid of één

[117] Oorspronkelijk had FISA alleen betrekking op het gebruik van elektronische surveillance. In de jaren daarna is de reikwijdte van de wet steeds verder uitgebreid naar andere onderzoeksmethoden: in 1995 kwam het uitvoeren van een lichamelijke zoekacties onder FISA te vallen, in 1998 *pen register/trap & trace surveillance* en het beschikbaar laten stellen van materiële zaken zoals bedrijfsgegevens. Zie Lui, Nolan en Thompson II, Overview of Constitutional Challenges to NSA Collection Activities, 1; Clarke e.a., *The NSA Report*, 68.
[118] Zygmunt Bauman e.a., 'After Snowden: Rethinking the Impact of Surveillance', 125.
[119] Toh, Patel en Goitein, Overseas Surveillance in an Interconnected World, 12.
[120] Electronic Privacy Information Center, 'Foreign Intelligence Surveillance Act (FISA)' (versie 28 maart 2016), https://epic.org/privacy/surveillance/fisa/ (28 maart 2016).
[121] Conor Clarke, 'Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp? Ex Parte Proceedings and the FISC Win Rate', *Stanford Law Review Online* 66 (2014) 125, 125-133, 127.
[122] Clarke, 'Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp?', 127.

jaar in het geval van een daadwerkelijke buitenlandse mogendheid. Dossiers van de zaken die de FISC heef behandeld zijn en blijven in principe geheim.[123]

Doordat de besluiten van de FISC niet openbaar te raadplegen zijn, hangt er veel geheimzinnigheid rondom de besluitvorming van de FISC. Dit gevoel wordt alleen maar versterkt wanneer er wordt gekeken naar het goedkeuringspercentage van de besluiten van de FISC. Conor Clarke heeft onderzoek gedaan naar verzoeken die de FISC heeft behandeld in de eerste 33 jaar van diens bestaan. Tussen 1979 en 2012 werden er door de federale diensten 33.900 verzoeken ingediend bij de rechtbank en daarvan werden slechts 11 verzoeken afgewezen, terwijl het overige deel werd toegekend: een goedkeuringspercentage van 99,97 procent.[124]

Uit deze cijfers blijkt dat de uitvoerende macht dus nagenoeg altijd in het gelijk wordt gesteld bij deze geheime rechtbank. Het is echter niet terecht om daarom te beweren dat de FISC niet goed functioneert. Ex-parte zaken kennen namelijk in veel gevallen een onevenwichtig succespercentage en die statistieken zijn dus niet slechts voorbehouden aan de zaken die bij de FISC terecht komen.[125] Om iets zinnigs te kunnen zeggen over de rol van de FISA en de FISC is het daarom van belang om verder te kijken dan het goedkeuringspercentage. En alhoewel het goedkeuringspercentage onverminderd hoog is gebleven, hebben sinds 11 september 2001 ontwikkelingen binnen de inlichtingenwereld er wel voor gezorgd dat de rol van de FISA, en de werking van de FISC, werd(en) aangepast. Om dit te illustreren zullen ook zaken die de laatste jaren door de FISC zijn behandeld hieronder aan bod komen.

2.2.2 Aanpassingen van FISA: Protect America Act & Sectie 702 van de FISA Amendments Act

De buitenlandse inlichtingenactiviteiten die Snowden in de openbaarheid bracht werden deels gerechtvaardigd op basis van belangrijke wetswijzigingen van de FISA die te plaatsen zijn in een brede ontwikkeling op het gebied van Amerikaanse inlichtingen sinds de aanslagen op 11 september 2001.

Na de aanslagen op de *Twin Towers* in New York duurde het niet lang voordat de Amerikaanse president Bush van zijn presidentiële macht gebruik maakte om extra bevoegdheden aan de inlichtingendiensten toe te kennen. Eind 2005 bracht de *New York Times* naar buiten dat Bush in oktober 2001 door middel van een geheim presidentieel decreet een programma had goedgekeurd dat de NSA de mogelijkheid gaf om, zonder rechterlijk bevel, *"communications between individuals on*

123 Electronic Privacy Information Center, 'Foreign Intelligence Surveillance Act (FISA)' (versie 28 maart 2016), https://epic.org/privacy/surveillance/fisa/ (28 maart 2016).
124 Clarke, 'Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp?', 125.
125 Ibidem, 130-132.

American soil and individuals abroad" te onderscheppen.[126] Elektronische surveillance werd daarmee toegepast buiten de regels van FISA om. Het *Terrorist Surveillance Program* (TSP) was volgens Bush desondanks in overeenstemming met de wet doordat hij had gehandeld in overeenstemming met zijn bevoegdheden als opperbevelhebber van het leger en de extra bevoegdheden die hem door het Congres waren toegekend in de nasleep van 11 september 2001.[127] De meningen lopen hierover echter uiteen, aangezien Bush voorbij ging aan FISA én er bovendien geen sprake was van toezicht door ofwel een commissie van het Congres of FISC.

Ook de rol die telecombedrijven binnen het programma speelden werd onder de loep genomen. Alhoewel het principe van data mining opkwam in de jaren '90 – vanaf die periode neemt de hoeveelheid opgeslagen online data hand over hand toe, terwijl tegelijkertijd de kosten voor de computerkracht die nodig is om de data te analyseren sterk dalen – wordt het met name sinds 11 september 2001 gebruikt om informatie te vergaren van criminelen, en terroristen in het bijzonder.[128] De Amerikaanse telecombedrijven stelden metadata van binnenlandse telefoongesprekken beschikbaar die de NSA vervolgens gebruikte om, gebaseerd op communicatiegegevens, relaties tussen mensen in kaart te brengen.[129]

Nadat het geheime programma door de *New York Times* was geopenbaard, kwamen er al snel onderzoeken vanuit het Congres, maar ook rechtszaken, waarin vraagtekens werden gezet bij de rechtsgeldigheid van het programma én de specifieke rol die de telecombedrijven hadden. De rechtszaken werden voornamelijk opgezet door burgerrechtengroepen tegen de telecombedrijven namens hun klanten vanwege de vermeende samenwerking met het NSA-programma en het daarmee schenden van de grondrechten van de eisers.[130]

---

[126] Michelle Louise Atkin, 'The Future of Privacy in Post-9/11 America', *International Journal of Intelligence Ethics* 4 (2013) 2, 13-47, 16.

[127] De extra bevoegdheden vloeiden voort uit speciale wetgeving die het Congres op 14 september 2001 aannam, en die door president op 18 september 2001 werd ondertekend, waarmee de president bevoegd werd om alle noodzakelijke en gepaste middelen te gebruiken *"against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occured on September 11, 2001, or harbored such organizations or persons…"*. In deze context mocht de president ook gebruik maken van militaire middelen om dat doel te bereiken. Eén dergelijk militair middel was de NSA, aangezien die dienst onder het ministerie van Defensie valt. Zie Richard F. Grimmett, Authorization for Use of Military Force in Response to the 9/11 Attacks (P.L. 107-40): Legislative History (Congressional Research Service Report, Damascus 2007) 1.

[128] Christopher Slobogin, 'Government Data Mining and the Fourth Amendment', *The University of Chicago Law Review* 75 (2008) 317-341, 317.

[129] Jeffrey W. Seifert, Data Mining and Homeland Security: An Overview (Congressional Research Service Report, Damascus 2008) 24.

[130]Elizabeth B. Bazan, Gina Marie Stevens en Brian T. Yeh, Government Access to Phone Calling Activity and Related Records: Legal Authorities (Congressional Research Service Report, Damascus 2007) 2; Zie voor een overzicht van rechtszaken de NSA Surveillance Lawsuit Tracker van ProPublica, bereikbaar via https://projects.propublica.org/graphics/surveillance-suits.

Kort na de onthulling van het programma werd er vanaf begin 2006 binnen het Congres over gediscussieerd. Uitgangspunt was daarbij het instellen van verbeterd toezicht op de activiteiten van de NSA. Dat er iets gedaan moest worden was in de ogen van het Congres wel duidelijk. De *surveillance* vond immers plaats zonder bevelschrift van de FISC of zonder dat de overheid hoefde aan te tonen dat er een gerede aanleiding was dat het beoogde doelwit een vertegenwoordiger van een buitenlandse mogendheid was.[131] Om dat doel te ondersteunen werden er wetsinitiatieven opgesteld om of FISA aan te passen of nieuwe wetsregels in te stellen op het gebied van elektronische surveillance.[132]

De wetgeving die uiteindelijk in 2007 door het Congres werd doorgevoerd beperkte niet de bevoegdheden van de NSA, maar zorgde er juist voor dat de procedures die in de FISA lagen vastgelegd niet meer van toepassing waren op het zonder bevelschrift monitoren van internationaal communicatieverkeer, zelfs in het geval dat een doelwit Amerikaans staatsburger zou zijn. Maar waarom voerde het Congres deze wetgeving door?

De *Protect America Act* (PAA) werd hevig bekritiseerd omdat de wet de overheid te veel macht zou geven om naar eigen inzicht het internationaal communicatieverkeer van Amerikaanse burgers te monitoren. Toch is het wel logisch dat de wet werd aangenomen. De wet zorgde er namelijk voor dat een ander, onwettelijk programma van de NSA werd gelegaliseerd. Rond de jaren 2001/2002 begon de NSA namelijk niet alleen met het verzamelen van metadata van telefoonverkeer, maar ook met het, zonder bevelschrift, vergaren van internetcommunicatie van buitenlandse doelwitten.[133] De wettelijke bevoegdheid voor de NSA om dat programma te mogen uitvoeren werd met het aannemen van de PAA wettelijk geregeld.[134]

De PAA verliep op 1 februari 2008 en pogingen om de wet te verlengen liepen op niets uit, terwijl er vanuit het ministerie van Justitie werd opgeroepen om de extra bevoegdheden voor de inlichtingendiensten om te zetten in permanente wetgeving.[135] Ondertussen werden er eind 2007 diverse wetsvoorstellen geïntroduceerd. Deze draaiden om de rol van de rechtsprekende macht in het toestaan en overzien van *surveillance* waarbij *U.S. persons* niet het doelwit waren, maar waar ze wel bij betrokken zouden zijn. Hoewel sommige senatoren benadrukten dat een onafhankelijke rechterlijke macht noodzakelijk was om er voor te zorgen dat inlichtingenactiviteiten niet op illegale of ongepaste wijze Amerikanen als doelwit zouden hebben. Anderen gaven echter ook terecht aan dat

[131] Clarke e.a., *The NSA Report*, 134.
[132] Marshall Curtis Erwin, Intelligence Issues for Congress (Congressional Research Service Report, Damascus 2013) 21.
[133] Het gaat hierbij om de PRISM- en Upstream-programma's.
[134] Lui, Nolan en Thompson II, Overview of Constitutional Challenges to NSA Collection Activities, 10.
[135] Departement van Justitie, 'FISA 101: Why FISA Modernization Amendments Must Be Made Permanent', https://www.justice.gov/archive/ll/index.html (29 maart 2016).

technologische veranderingen er sinds 1978 voor hebben gezorgd dat het per zaak bekijken van een internationale communicatieverbinding waarbij mogelijk een *U.S. person* betrokken kon zijn wel erg onpraktisch is en mogelijk gevaarlijk voor de nationale veiligheid.[136]

Uiteindelijk werd er op 19 juni 2008 een nieuw wetsvoorstel ingediend. Dit wetsvoorstel, dat later de *FISA Amendments Act* (FAA) zou worden, betekende een grotere rol voor de FISC voor wat betreft het goedkeuren van procedures voor inlichtingensurveillance. Daarmee werd het probleem van surveillance zonder gerechtelijke toestemming en toezicht opgelost. Bovendien verschafte het wetsvoorstel telecombedrijven de mogelijkheid om bij rechtbanken te kunnen aantonen dat zij hadden meegewerkt met de inlichtingendiensten in reactie op een verzoek vanuit de uitvoerende macht. Het wetsvoorstel werd op 10 juli 2008 door de president ondertekend.[137]

Een specifiek onderdeel van de wet, sectie 702, zo bleek uit de onthullingen van Snowden, werd door de NSA gebruikt om het geheime PRISM-programma te rechtvaardigen. Er werd namelijk in vastgelegd dat een buitenlander, die een doelwit is van buitenlandse inlichtingensurveillance en waarvan redelijkerwijs kan worden gesteld dat diegene zich buiten de VS bevindt, kan worden gevolgd zonder dat overheid aan bepaalde voorwaarden hoeft te voldoen. Zo hoeft er bij de inlichtingendiensten geen redelijke aanleiding te bestaan om het doelwit als vertegenwoordiger van een buitenlandse mogendheid te zien. Daarnaast hebben de diensten onder sectie 702 ook geen geïndividualiseerd bevelschrift van de FISC nodig om iemand te kunnen monitoren, zelfs als diegene zich binnen de grenzen van de VS bevindt.[138] De categorieën wiens communicatiestromen door de diensten verzameld mogen worden liggen vastgelegd in jaarlijkse certificeringen. Deze worden goedgekeurd door de FISC en worden aangeleverd door de minister van Justitie en de *Director of National Intelligence* (DNI). Echter, welke individuen het doelwit van de diensten zijn mogen de diensten zelf bepalen, zonder verdere goedkeuring van de FISC. Daarbij baseert de NSA zich op specifieke *identifiers*, zoals e-mailadressen of telefoonnummers.[139]

Kortom, onder sectie 702 worden door de FISC certificaten afgegeven in plaats van geïndividualiseerde bevelschriften. Dus wanneer er wordt gesproken over het aantal doelwitten onder sectie 702 dan gaat het niet om het precieze aantal personen dat doelwit is, maar om een schatting van het aantal gebruikers van bepaalde *identifiers*.

[136] Erwin, Intelligence Issues for Congress, 23.
[137] Ibidem, 24
[138] Clarke e.a., *The NSA Report*, 135.
[139] Ibidem, 135-136.

Alhoewel het misschien wel zo kan worden geïnterpreteerd betekent dit deel van de wet niet dat de NSA zomaar buitenlanders kan monitoren. De NSA moet namelijk onder deze wet bij elke poging duidelijk aantonen dat het daarmee buitenlandse inlichtingen wil vergaren; niet met opzet een Amerikaanse burger als doelwit heef; niet met opzet iemand als doelwit heeft die op het moment van het verzamelen van de gegevens zich binnen de VS bevindt; niet een persoon buiten de VS als doelwit heeft om daarmee een doelwit binnen de VS te treffen en ten slotte moet de inlichtingenvergaring ook voldoen aan de voorwaarden die door het Vierde Amendement worden gesteld.[140]

Daarmee zorgde wetswijziging van 2008 voor een belangrijke verandering van FISA. Voor de wetswijziging waren er binnen de FISA namelijk geen beperkingen vastgelegd voor wat betreft de overzeese surveillance van doelwitten buiten de VS. Vanaf 2008 zijn inlichtingendiensten echter verplicht om een bevelschrift van de FISC te bemachtigen voordat ze tot overzeese surveillance van Amerikanen overgaan. Let wel, de wetswijziging betekende dus een verbetering van de positie van Amerikaanse ingezetenen, maar niet van buitenlanders. Die konden nog steeds het doelwit van Amerikaanse inlichtingendiensten zijn zonder toestemming van de daartoe ingestelde instanties.

De kritiek op de wet, en sectie 702 in het bijzonder, richtte zich bij velen op het feit dat de wet de rechten onder het Vierde Amendement zouden schenden. Buitenlanders genieten echter geen bescherming van het Vierde Amendement en dit was dan ook de verdediging die vanuit de NSA werd gevoerd.[141] Critici wijzen eveneens op het PRISM-programma dat op grond van sectie 702 wordt uitgevoerd. Zoals hierboven echter al aangegeven heeft dat programma alleen betrekking op niet-Amerikanen en is het daarnaast ook in een overeenstemming met de FISA-wetgeving. Dit betekent dat de FISC op voorhand de certificering, afkomstig van de minister van Justitie en de DNI, en de verplichte doelwit- en minimalisatieprocedures beoordeeld.

Sectie 702 van FISA was, en is, omstreden. Verschillende rechtszaken werden daarom gestart om de wettelijkheid van de sectie en de eruit voortvloeiende surveillanceprocedures aan de kaak te stellen. Eén van die rechtszaken werd opgestart door een aantal non-profit organisaties en was gericht op de autorisatieprocedure onder sectie 702 voor de *surveillance* van niet-Amerikaans ingezetenen in het buitenland. De claim was dat deze vorm van autorisatie het verbod op *unreasonable searches* in het Vierde Amendement zou schenden. De FISC is onder sectie 702 namelijk bevoegd om surveillance toe staan zonder dat er sprake is van een *probable cause* dat het doelwit een vertegenwoordiger van een buitenlandse mogendheid is. Doordat de eisers volgens het Hooggerechtshof echter niet duidelijk

[140] Ibidem, 137-138.
[141] Deze redenatie wordt ook ondersteund door een gerechtelijke uitspraak in de zaak *United States v. Verdugo-Urquidez*.

genoeg konden maken dat de VS gebruik zou maken van sectie 702 om hun gesprekken te onderscheppen, werd de zaak niet in behandeling genomen.[142]

Binnen de FISC en de *Foreign Intelligence Surveillance Court of Review* (FISCR), de federale rechtbank die afwijzingen van 'FISA'-bevelschriften door de FISC herziet, is er ook gekeken naar de geldigheid van de PAA en sectie 702. In 2008 was de overweging van de FISCR dat het uitvoeren van elektronische surveillance zonder bevelschrift, in overeenstemming met de PAA, is toegestaan. Jurisprudentie had tot dan toe steeds uitgewezen dat de overheid alleen in het geval van een uitzondering zonder een bevelschrift elektronische surveillance mocht toepassen. De achterliggende gedachte hiervoor was dat elektronische surveillance een inbreuk maakt op iemands *reasonable expectation of privacy*. De FISCR bepaalde echter dat er in het geval van buitenlandse inlichtingen sprake is van een uitzonderingspositie aangezien er gesproken kan worden over *special needs*.[143] Daarbij overtreft het overheidsbelang het algemene belang van de normale wetshandhaving.[144]

In augustus 2013 werden, in reactie op de onthullingen van Snowden, door de Amerikaanse regering delen van enkele gerechtelijke overwegingen van de FISC vrijgegeven. Deze stamden uit oktober 2011 en hadden betrekking op de procedures rondom inlichtingenvergaring onder sectie 702. Uit de documenten bleek dat de overheid had ontdekt dat als onderdeel van het UPSTREAM-programma ook niet-gerelateerde internationale, en zelfs binnenlandse, communicatieverkeer werd binnengehaald.[145]

De rechters zetten in de stukken echter hun vraagtekens bij de vanuit de overheid voorgestelde nieuwe minimalisatieprocedures. Doordat analisten zich namelijk primair zouden focussen op de benodigde informatie in plaats van de vergaarde informatie, bestond het gevaar dat binnenlandse en/of niet-gerelateerde communicatieverkeer toch illegaal zou worden bewaard. FISA stelt immers dat de bewaartermijn van gegevens over Amerikanen of Amerikaanse ingezetenen tot een minimum beperkt dient te worden. Daarnaast vond de FISC, in tegenstelling tot het besluit van de FISCR met betrekking tot de PAA, dat de procedures niet overeenkwamen met het Vierde Amendement. Er was volgens de rechters geen sprake van een *reasonable search*, zeker met het oog op statutaire tekortkomingen.[146]

---

142 Lui, Nolan en Thompson II, Overview of Constitutional Challenges to NSA Collection Activities, 15.
143 De *special needs* uitzondering is van toepassing *"when special need, beyond the normal need for law enforcement, make the warrant requirement and propable-cause requirement impracticable".* Zie Lui, Nolan en Thompson II, Overview of Constitutional Challenges to NSA Collection Activities, 9.
144 Ibidem, 9.
145 Ibidem, 13.
146 Ibidem, 13-14.

De Amerikaanse overheid besloot daarom de minimalisatieprocedures aan te passen. De belangrijkste aanpassingen hadden betrekking op de wijze waarop er met verzameld communicatieverkeer zou worden omgegaan. Communicatieverkeer zou in het vervolg worden gescheiden tussen relevant en (waarschijnlijk) niet-relevant communicatieverkeer.[147] Daarnaast werd ook de bewaarperiode van verzamelde gegevens uit het UPSTREAM-programma teruggebracht van vijf jaar naar twee jaar. De rechtbank oordeelde hierop dat de zoekacties onder het UPSTREAM-programma weer in overeenstemming waren met de grondwet.[148]

Bovenstaande gerechtelijke overwegingen van de FISC werden door de overheid vrijgegeven in de nasleep van de onthullingen van Snowden, maar normaal gesproken blijven de uitspraken van de FISC geheim. De vraag is dan ook opgeworpen of de geheime uitspraken van de FISC wel in overeenstemming zijn met de Amerikaanse grondwet. De rechtbank is namelijk een zogeheten 'artikel III rechtbank'. Dit wil zeggen dat de rechtbank is opgericht onder artikel III van de Amerikaanse grondwet en dat artikel bepaalt de randvoorwaarden van het Amerikaanse juridisch stelsel. In dat artikel van de grondwet is vastgelegd dat federale rechtbanken alleen hun interpretaties van de wet mogen geven in het geval van de daadwerkelijke behandeling van een rechtszaak of meningsverschil.[149]

In het geval van de FISC is het echter de vraag of de statutaire verantwoordelijkheden van de rechtbank in overeenstemming zijn met de zogeheten *case or controversy requirement*. Behandelingen van zaken door de FISC vinden namelijk in het geheim plaats en er is bij de behandeling van die zaken geen sprake van hoor en wederhoor. Alleen de overheid wordt immers in de regel door de rechters als partij gehoord.[150] Het is hierdoor zeer moeilijk om bevelschriften die door de FISC zijn afgegeven in latere gerechtelijke procedures op betekenisvolle wijze te kunnen gebruiken. Hierdoor kan dus gesteld worden dat de uitspraken van de rechtbank niet in overeenstemming zijn met de *case or controversy requirement*. De wettelijkheid van de FISC, die toezicht moet houden op de buitenlandse inlichtingenvergaring onder FISA, kan daarmee ter discussie worden gesteld.

[147] Waarbij onder het niet-relevante communicatieverkeer ook het binnenlandse communicatieverkeer zou vallen.
[148] Lui, Nolan en Thompson II, Overview of Constitutional Challenges to NSA Collection Activities, 14.
[149] Douglas O. Linder, 'Constitutional Limitations on the Judicial Power: Standing, Advisory Opinions, Mootness, and Ripeness' (versie 6 januari 2015), http://law2.umkc.edu/faculty/projects/ftrials/conlaw/caseorcontroversy.htm (4 april 2016).
[150] Stephen I. Vladeck, 'The FISA Court and Article III', *Washington and Lee Law Review* 72 (2015) 3, 1161-1180, 1169.

2.2.3 Erfenis van 11 september 2001: Sectie 215 van de Patriot Act

In het onderzoeksrapport *Liberty and Security in a Changing World* van de *The President's Review Group on Intelligence and Communications Technologies*, dat na de onthullingen van Snowden werd opgesteld, stellen de onderzoekers dat FISA van 1978 tot 2001 een belangrijk wettelijk raamwerk bood om de balans te bewaren tussen de twee verplichtingen van de staat: *'to "provide for the common defence" and to "secure the Blessings of Liberty."'*.[151]

In 2001 kwam daar, in navolging van de aanslagen van 11 september 2001, de *USA Patriot Act* bij. Zoals de volledige naam van deze wet duidelijk maakt – voluit de *Uniting and Strengthening America by Providing Appropiate Tools Required to Intercept and Obstruct Terrorism Act of 2001* geheten – omvat de wet verschillende maatregelen op verschillende gebieden van terrorismebestrijding. Een veelvoorkomend verwijt na de aanslagen van 11 september 2001 was dat stukjes informatie over de op handen zijnde aanslagen wel aanwezig was bij verschillende inlichtingen- en veiligheidsdiensten, maar dat die puzzelstukjes niet bij elkaar kwamen. De wet maakte daarom een einde aan belemmerende regels op het gebied van informatiedeling tussen justitie en de inlichtingenwereld.[152]

Specifiek werd in sectie 215 – *Access to records and other items under the Foreign Intelligence Surveillance Act* – vastgelegd onder welke voorwaarden overheidsinstellingen zichzelf toegang konden verschaffen tot gegevens. Met de strijd tegen het terrorisme als legitimatie werden algemene, niet toegespitste, zoekacties toegestaan. Dit betekent dat de overheid iemand kan monitoren zonder dat op voorhand vast staat dat diegene een terroristische dreiging vormt. Daarnaast is de overheid bevoegd om databases van derde partijen te doorzoeken zonder dat de verdachten daarvan op de hoogte worden gesteld, zolang de informatie relevant is voor een terrorismeonderzoek.[153]

Een ander onderdeel van sectie 215 bepaalt dat bevelschriften tot inzage van bepaalde bedrijfsgegevens – wat mogelijk is onder FISA – niet meer hoeven te verwijzen naar *'specific and articulable facts'* zolang de gegevens betrekking hebben op een buitenlandse mogendheid of een vertegenwoordiger van een buitenlandse mogendheid. Bedrijven bij wie de bevelschriften binnenkomen, zoals telecomproviders, zijn niet zomaar verplicht om mee te werken. Ze kunnen namelijk om een herziening van het bevelschrift vragen bij de rechter. Amerikaanse personen kunnen echter niet zomaar het doelwit worden van elektronische surveillance onder FISA. Sectie 215 verbiedt

[151] Clarke e.a., *The NSA Report*, 68.
[152] Erwin, Intelligence Issues for Congress, 17.
[153] Amitai Etzioni, 'NSA: National Security vs. Individual Rights', *Intelligence and National Security* 30 (2015) 1, 100-136, 115.

namelijk dat Amerikaanse personen als een vertegenwoordiger van een buitenlandse mogendheid worden beschouwd puur op basis van wat iemand zegt of gelooft.[154]

Sectie 215 van de *Patriot Act* is in een uitspraak van de FISC, waarbij werd gekeken naar een herziening van een afgegeven bevelschrift, genoemd als belangrijke wettelijke pijler van het NSA-programma waarmee de dienst telefoondata verzamelt.[155] Sectie 215 mag echter als basis voor de surveillanceprogramma's van de NSA dienen, maar of sectie 215 zelf in overeenstemming is met het Vierde Amendement is nog maar de vraag. Sectie 215 stelt namelijk niet als voorwaarde voor een zoekactie dat er sprake moet zijn van *probable cause*. Het Hooggerechtshof heeft lange tijd vastgehouden aan de redenatie dat het Vierde Amendement niet op gaat als er bij het gebruik van een bevelschrift om bewijs te vergaren sprake is van een bepaalde aannemelijkheid dat er met behulp van het bevelschrift bewijs gevonden kan worden. Die gedachtegang werd met sectie 215 in feite losgelaten.[156]

Daarnaast worden onder sectie 215 vaak gegevens verzameld die privéinformatie over personen bevatten terwijl de gegevens zich bij een derde partij bevinden. Vanuit een privacyoogpunt zou je verwachten dat het vergaren van dit soort gegevens niet is toegestaan. Je overhandigt immers als consument bijna dagelijks persoonlijke, en soms zeer vertrouwelijke, informatie aan een derde partij. De NSA maakt hier gebruik van door private bedrijven, die zeer regelmatig grote hoeveelheden persoonlijke data verzamelen, te dwingen die gegevens aan de dienst te overhandigen, zonder medeweten van de klanten van het bedrijf.[157]

Het verzamelen van dergelijke data, zij het via telecomproviders of via servers van technologiebedrijven – zoals Yahoo!, Google, Apple en Facebook – wordt door de Amerikaanse overheid gerechtvaardigd op basis van de *third-party doctrine*. Die doctrine is in de loop der jaren een standaardgebruik geworden binnen het Amerikaanse rechtssysteem op basis van verschillende jurisprudentie. De gedachtegang achter de doctrine is dat een persoon redelijkerwijs geen recht op privacy meer kan verwachten wanneer hij of zij op vrijwillige basis informatie aan een andere partij openbaart. De persoon doet in feite afstand van de bescherming die hij of zij geniet onder het Vierde Amendement met betrekking tot die geopenbaarde informatie. De eerste rechtszaak waarbij deze

[154] Etzioni, 'NSA: National Security vs. Individual Rights', 115.
[155] Foreign Intelligence Surveillance Court, Rechterlijke overweging in 'In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]', 15. Beschikbaar via https://www.aclu.org/files/assets/br13-09-primary-order.pdf.
[156] Clarke e.a., *The NSA Report*, 82.
[157] Zygmunt Bauman e.a., 'After Snowden: Rethinking the Impact of Surveillance', 123; Dit programma van de NSA staat bekend als *Xkeyscore* en houdt in dat de NSA gegevens van derde partijen opslaat in een database om later te kunnen raadplegen. Bedrijven zijn verplicht gevoelige informatie af te staan als de autoriteiten wettige dagvaardingen en/of bevelschriften overhandigen.

gedachtegang werd gevolgd was *United States v. Miller* (1976), waarin het Hooggerechtshof bepaalde dat klanten van een bank hun redelijke verwachting van privacy verliezen wanneer ze persoonlijke informatie aan een bank overhandigen.[158]

Een aantal jaren later, in 1979, besloot het Hooggerechtshof in de zaak *Smith v. Maryland* dat het Vierde Amendement het gebruik van *pen registers* zonder bevelschrift niet verbood. De rechters schreven namelijk dat er een verschil is tussen het verzamelen van telefoonverkeer met behulp van elektronische afluisterapparaat, dat in *Katz v. United States* als zoekactie onder het Vierde Amendement werd geschaard, en het verzamelen van elektronische pulsen, met behulp van een *pen register*, die de telefoonnummers kunnen registreren waar naartoe wordt gebeld. Die laatste gegevens worden vrijwillig ´afgestaan´ aan het telefoonbedrijf en daarmee bestaat het risico dat de gegevens aan de overheid worden overhandigd. Er kan volgens de rechters dan ook geen sprake zijn van een redelijke verwachting van het recht op privacy. Hierdoor is het installeren en gebruik van een *pen register* geen zoekactie waarvoor een bevelschrift onder het Vierde Amendement nodig is.[159]

De *third-party doctrine* is echter omstreden binnen het Amerikaanse rechtssysteem en wordt dan ook door sommigen gezien als een zwakke basis voor de surveillancepraktijken van de Amerikaanse overheid. In de huidige tijd zijn veel privégegevens opgeslagen in de '*cloud*' of op een andere manier online terug te vinden. Des te opmerkelijker is het dat de *third-party doctrine* in eerste instantie juist door de NSA werd opgegeven als verdediging van de surveillanceprogramma's. Een terecht punt wordt door socioloog Amitai Etzioni – voorstander van de surveillanceprogramma's, maar tegenstander van het gebruik van de *third-party doctrine* als verdediging ervan – aangedragen. Het gebruik van de *third-party doctrine* laat weinig ruimte over voor de volgende vraag: van welke persoonlijke informatie mag redelijkerwijs nog verwacht worden dat ze nog bescherming geniet tegen zoektochten onder het Vierde Amendement?[160]

De geldigheid van de *Patriot Act* is in de loop der jaren steeds verlengd, maar de houdbaarheid van de *third-party doctrine* als *good law*, zeker in combinatie met de praktische toepassing van de *Patriot Act*, is wel een punt van aandacht geweest voor het Amerikaanse Hooggerechtshof. In 2012 schreef rechter Sotomayor, als rechterlijke overweging bij de uitspraak in *United States v. Jones*, dat het wellicht noodzakelijk is om de gedachte achter de *third-party doctrine* te herzien. Ook een andere rechter gaf aan dat *'modern technological advances can seriously undermine our traditional*

[158] Amitai Etzioni, 'NSA: National Security vs. Individual Rights', 111.
[159] Bazan, Stevens en Yeh, Government Access to Phone Calling Activity and Related Records: Legal Authorities, 4.
[160] Etzioni, 'NSA: National Security vs. Individual Rights', 112.

expectations of privacy'.[161] Volgens hem moest daar onder het Vierde Amendement rekening mee worden gehouden.

Naast sectie 215 van de *Patriot Act*, en de *Foreign Intelligence Surveillance Act*, speelt echter nog een heel ander aspect een rol in de regelvorming rondom de surveillanceprogramma's. Dit aspect is *Executive Order* (EO) 12333. Dit presidentieel decreet is van grote invloed op de slagkracht en mogelijkheden waar de Amerikaanse inlichtingendiensten over beschikken. Verschillende onderzoekers wijzen daarom ook juist op het belang van EO 12333 voor de Amerikaanse inlichtingenwereld. Dit wordt onderstreept door het feit dat er onder EO 12333 veel meer verzoeken voor surveillance vallen dan onder sectie 702 van FISA.

2.2.4 Executive Order 12333

Executive Order 12333 werd oorspronkelijk uitgevaardigd door president Reagan in 1981 en trad het jaar daarop in werking.[162] Het decreet betekende een aanpassing van *Executive Order* 11905. Dit decreet stamde uit 1977 en was een reactie van president Ford op de onthullingen van diverse onderzoekscommissies aangaande misstanden in de Amerikaanse inlichtingengemeenschap. Door het instellen van EO 11905 wilde Ford de inlichtingengemeenschap hervormen. Daarbij lag de focus met name op het verbeteren van het toezicht op de buitenlandse activiteiten van de inlichtingendiensten en het instellen van een verbod op het plegen van politieke moorden. Dit verbod kwam in reactie op onthullingen van missies van de CIA waarbij politieke moorden werden gepleegd.

De gedachte achter EO 12333 was het vergroten van de slagkracht van de Amerikaanse inlichtingengemeenschap met betrekking tot het vergaren van buitenlandse inlichtingen, maar ook om de gemeenschap beter in staat te stellen om internationaal terrorisme, de verspreiding van massavernietigingswapens en spionage tegen te gaan.[163]

De kern van EO 12333 is hiermee al meteen aangestipt: EO 12333 heeft betrekking op inlichtingenactiviteiten in het buitenland. EO 12333 vormt zodoende de belangrijkste autoriteit van de uitvoerende macht op het gebied van buitenlandse inlichtingenactiviteiten die niet door de FISA

[161] Clarke e.a., *The NSA Report*, 85.
[162] *Executive Orders* zijn, kortgezegd, geschreven documenten die worden uitgegeven door de president van de VS die het effect van wetgeving hebben en zijn over het algemeen gericht op het aansturen van overheidsambtenaren en overheidsinstellingen. Zie Vivian S. Chu en Todd Garvey, Executive Orders: Issuance, Modification, and Revocation (Congressional Research Service, z.p. 2014), 1-2.
[163] Toh, Patel en Goitein, Overseas Surveillance in an Interconnected World, 3.

worden geregeld. Het decreet is daarom zeer belangrijk aangezien het merendeel van de Amerikaanse inlichtingenvergaring niet onder de autoriteit van de FISA valt, maar onder EO 12333.[164]

Uit de documenten die vanaf de zomer van 2013 door Snowden zijn onthuld, blijkt dat er onder EO 12333 diverse programma's zijn geautoriseerd voor het verzamelen van communicatie wereldwijd. Het gaat daarbij om veel verschillende programma's waarbij veel verschillende soorten communicatie wordt verzameld:

Naam programma	**Verzamelde informatie**	**Betrokken diensten**
MYSTIC	Gegevens van mobiele telefoongesprekken	NSA
SOMALGET	Audio van mobiele telefoongesprekken	NSA
CO-TRAVELER	Informatie over locatie mobiele telefoon	NSA
OPTIC NERVE	Beelden en geluiden van webcamgesprekken	NSA, GCHQ
MUSCULAR	E-mail adresboeken en contactlijsten	NSA, GCHQ
DISHFIRE	SMS-berichten	NSA, GCHQ
XKEYSCORE	Opslaan van verzamelde internetdata	NSA, GCHQ en diensten Canada, Nieuw-Zeeland en Duitsland

Tabel 1: Overzicht buitenlandse surveillanceprogramma's van de NSA[165]

EO 12333 heeft betrekking op veel aspecten binnen de inlichtingengemeenschap. Dit komt doordat oprichtingsstatuten van de inlichtingendiensten, die deels de macht van de diensten bepalen, vaak erg vaak zijn of in het geheel ontbreken. Dit laatste is bijvoorbeeld het geval bij de NSA. Die dienst werd namelijk door een geheime memo van president Truman opgericht. Hierdoor worden de mogelijkheden en beperkingen van de dienst bepaald door EO 12333 en in de praktijk door de FISA.[166]

Wat ligt er dan zoal in EO 12333 vastgelegd? De missies en bevoegdheden van elk onderdeel van de inlichtingengemeenschap liggen erin vastgelegd en daarnaast zet het decreet de

[164] Rechter Bates gaf in 2011 aan dat de NSA meer dan 250 miljoen keer internetcommunicatie jaarlijks vergaarde onder sectie 702 van FISA. De *Washington Post* onthulde daarentegen dat één programma onder *Executive Order 12333* bijna 5 miljard keer per dag de locatiegegevens van mobiele telefoons verzamelde.
[165] Gebaseerd op: Toh, Patel en Goitein, Overseas Surveillance in an Interconnected World, 5-8.
[166] Rascoff, 'Presidential Intelligence', 668.

grondbeginselen uiteen die er toe dienen om een gepast evenwicht te creëren tussen het vergaren van informatie enerzijds en het beschermen van persoonlijke informatie anderzijds. Tot slot bepaalt het decreet de regels voor het verzamelen, het beheren en het verspreiden van informatie van Amerikaanse ingezetenen.[167]

In EO 12333 ligt vastgelegd dat de minister van Justitie de bevoegdheid krijgt om richtlijnen op te stellen waar elk onderdeel van de inlichtingengemeenschap aan dient te voldoen als het gaat om het verzamelen, beheren en verspreiden van informatie van Amerikaanse ingezetenen. In de richtlijnen is vastgelegd hoe *signals intelligence* (SIGINT, het onderscheppen elektronische communicatie en het uitvoeren cryptoanalyse) mag worden verzameld, ook wanneer het gaat om inlichtingenactiviteiten die niet door de FISA worden beheerd.[168]

Hierdoor zijn er andere mogelijkheden onder EO 12333 dan onder de richtlijnen van de FISA. Zo is het grootschalig vergaren van inlichtingen, het zogeheten *bulk collection*, toegestaan onder de regels van EO 12333, terwijl onder sectie 702 van de FISA alleen inlichtingen mogen worden vergaard van specifieke doelwitten. De bevoegdheden onder Sectie 702 kunnen zodoende alleen worden gebruikt om communicatieverkeer naar, van of over een specifiek doelwit te verzamelen.[169] Dit houdt dus in dat er geen oneindig aantal aan doelwitten is. Uit het jaarrapport van het *Office of the Director of National Intelligence* kwam naar voren dat het in 2013 ging om 89.138 doelwitten onder de autoriteit van sectie 702 van de FISA.

EO 12333 heeft betrekking op het vergaren van buitenlandse inlichtingen. Elektronische surveillance van niet-Amerikanen buiten de VS moet voldoen aan een aparte reeks regels en dat betekent dat er verschillende regels gelden als het gaat om surveillance van Amerikanen en niet-Amerikanen, ook in het buitenland.

Het probleem met EO 12333 is dat het decreet een algemene richtlijn geeft over hoe inlichtingendiensten buitenlandse missies mogen uitvoeren, maar de diensten zijn bevoegd om zelf invulling te geven aan belangrijke details. De diensten zijn verplicht om deze details vast te leggen in procedures. De procedures van sommige diensten zijn echter geheim, terwijl de openbare procedures van andere diensten uit de jaren ’80 stammen. Er zijn zelfs diensten die nog steeds geen procedures hebben opgesteld.[170]

[167] Clarke e.a., *The NSA Report*, 69.
[168] Zie voetnoot 45 van Clarke e.a., *The NSA Report*, 70.
[169] Alvaro Bedoya, ‘Executive Order 12333 and the Golden Number’ (versie 9 oktober 2014), https://www.justsecurity.org/16157/executive-order-12333-golden-number/ (20 april 2016).
[170] Toh, Patel en Goitein, Overseas Surveillance in an Interconnected World, 11.

Voor de NSA zijn in deze twee procedures van belang: de *Department of Defense Directive 5240.1-R* (1982) en de *United States Signals Directive SP 0018* (1993, herzien in 2011). Deze richtlijnen geven de dienst veel ruimte op het gebied van het bewaren en delen van gegevens van Amerikaanse ingezetenen. De dienst is namelijk bevoegd om gegevens tot vijf jaar te bewaren en bovendien zijn er in de wetgeving ook allerlei uitzonderingen opgenomen waardoor de NSA, en andere inlichtingendiensten, informatie ook gedurende een langere periode mogen bewaren. Dit is bijvoorbeeld het geval wanneer de desbetreffende informatie onder de categorie *foreign intelligence or counterintelligence* valt.[171] Binnen de regels wordt over het algemeen echter met een vrij brede interpretatie van relevante begrippen gewerkt, waardoor de regels erg vaag blijven. Zo worden begrippen als '*pertinent*', '*possible threat*' of '*any person or organization*' niet nader gedefinieerd.[172] Voor buitenlanders, of niet-ingezetenen, zijn de regels nog minder strikt:

Wanneer mag informatie van Amerikaanse ingezetenen worden gedeeld?	Wanneer mag informatie van buitenlanders/niet-ingezetenen worden gedeeld?
*The information is **necessary to understand** the foreign intelligence information or assess its importance.*	*There is **some indication** that information about "**routine activities…is related** to an authorized foreign intelligence requirement."*
*The information **indicates** that the U.S. person may be engaged in international narcotics trafficking activities, or is evidence that **the individual may be involved in** a crime that has been, is being or is about to be committed.*	*The information is **related** to a crime that has been, is being, or is about to be committed.*
*The information **indicates** that the identity of the U.S. person is **pertinent** to a possible threat to the safety of any person or organization.*	*The information **indicates** a possible threat to the safety of any person or organization.*

Tabel 2: Vergelijking tussen *U.S. Persons* en *non-U.S. persons*[173]

[171] Andere categorieën waar dit voor geldt zijn: *evidence of a crime*, *communcations that are enciphered or have a secret meaning*, *communications between non-U.S. persons*, *protection of imminent threat to human life*, *technical assistance* en *national security*. Zie Toh, Patel en Goitein, Overseas Surveillance in an Interconnected World, 25-26.

[172] Ibidem. 27.

[173] Ibidem, 28. Accenten overgenomen door auteur.

De bovenstaande tabel maakt duidelijk dat er een lagere drempel is voor het delen van informatie van niet-ingezetenen of buitenlanders dan voor Amerikaanse staatsburgers of ingezetenen. Alhoewel het verschil in woordkeuze überhaupt veel speelruimte aan de inlichtingendiensten geeft, ook wanneer het Amerikanen betreft, lijkt het alsof de inlichtingendiensten al helemaal niet beperkt worden als het om informatie van buitenlanders gaat.

2.2.5 Analyse

FISA werd in 1978 ingesteld om de NSA en andere inlichtingendiensten in de VS in staat te stellen om ten eerste gebruik te kunnen maken van nieuwe technologieën, terwijl de diensten ten tweede in staat werden gesteld om noodzakelijke buitenlandse inlichtingen volgens de wet te kunnen verzamelen. Diezelfde wet moest de inlichtingengemeenschap er tegelijkertijd van weerhouden om grootschalige inlichtingen van Amerikaanse burgers te verzamelen.

De vergaring van metadata door met name de NSA, zoals die na 11 september 2001 werd geautoriseerd door president Bush, druist echter volledig in tegen de gedachte achter de aanname van FISA. Veranderingen in de wetgeving maakten het na 11 september 2001 makkelijker voor de NSA om aan de voorwaarden van FISA te voldoen. De PAA van 2007 versoepelde de belemmeringen voor wat betreft de surveillance van buitenlanders in het geval dat een van de partijen in het buitenland was gevestigd. Deze communicatiegevallen vielen niet meer onder de FISA-definitie van 'elektronische surveillance' en dus viel vanaf dat moment alleen nog binnenlandse communicatie binnen de elektronische surveillance. Buitenlandse communicatie kwam er helemaal los van te staan. Doordat daarnaast de FISC ook geen controle meer uitoefende op het onderscheppen van communicatiestromen die begonnen of eindigden in het buitenland, werd het makkelijker om een buitenlands doelwit te kunnen volgen. De PAA zorgde er namelijk voor dat minister van Justitie en de DNI het vergaren van communicatie in/naar het buitenland konden autoriseren. Een individu kon voortaan op basis van de geografische locatie worden gevolgd. Terwijl daarvoor onder FISA een doelwit van elektronische surveillance een buitenlandse mogendheid, of een vertegenwoordiger van een buitenlandse mogendheid, diende te zijn.[174]

De tijdelijke wet verliep in februari 2008 en werd uiteindelijk vervangen door de FAA. Deze wet bracht drie belangrijke wijzigingen aan in FISA. Daarvan sprong sectie 702 er het meeste uit. De sectie verschafte veel macht aan de minister van Justitie en de DNI voor wat betreft het autoriseren van elektronische surveillance, net zoals dat al het geval was onder de tijdelijke PAA. De rol van de

[174] Laura K. Donohue, 'Section 702 and the Collection of International Telephone and Internet Content', *Harvard Journal of Law and Public Policy* 38 (2015) 1, 117-265, 136.

gerechtelijke macht is hierdoor redelijk beperkt aangezien de FISC de afgegeven certificering, de doelwitprocedures en de minimalisatieprocedures niet kan herzien.

Het is aan de ene kant dus goed om te constateren dat de gerechtelijke macht in de VS een rol speelt in het vergaren van buitenlandse inlichtingen. Het zorgt immers voor betere bescherming van Amerikaanse burgers tegen ongerichte inlichtingenvergaring. Tegelijkertijd dient echter ook wel geconstateerd te worden dat de rol die de gerechtelijke macht speelt redelijk beperkt is. Juist in de jaren na 11 september 2001 is het aandeel van de gerechtelijke macht onder FISA eigenlijk steeds beperkter geworden, terwijl daarnaast de rol van de uitvoerende macht groter is geworden.

Onder EO 12333 wordt ook buitenlandse inlichtingen verzamelt. In 1978 besloot het Congres om drie vormen van buitenlandse inlichtingenvergaring buiten FISA te laten vallen: *(1) electronic communications outside U.S. borders, (2) intelligence in the U.S. and overseas falling outside the statutory definition of "electronic communications," and (3) incidental collection of U.S. persons' communications*.[175] De achterliggende gedachte hierachter was dat de er wellicht andere standaarden en procedures nodig waren voor overzeese surveillance dan bij elektronische surveillance binnen de VS of elektronische surveillance gericht tegen Amerikaanse ingezetenen binnen de VS.

Uiteindelijk werd door de regering van president George W. Bush het initiatief genomen om de bestaande wetgeving te veranderen, door middel van de PAA en de FAA. De regering gaf hiervoor als reden op dat veranderingen in telecommunicatietechnologie had betekend dat bepaalde communicatiemiddelen nu onder de regels van FISA vielen, waar diezelfde communicatiemiddelen eerder nog onder de minder strenge regels van EO 12333 vielen.

Ten tijde van het instellen van FISA had het Congres kabelcommunicatie in het buitenland uitgezonderd van de wetgeving. Een telefoongesprek tussen een Brit in Londen en een Fransman in Parijs ging niet over Amerikaanse grondgebied: de telefoonkabel lag gewoon tussen Groot-Brittannië en Frankrijk. Het Congres redeneerde zodoende dat het erg onpraktisch was en veel gedoe zou opleveren als de inlichtingengemeenschap voor elke onderschepping van buitenlandse inlichtingen tussen buitenlanders in het buitenland over een bevelschrift moest beschikken.[176]

Tegenwoordig valt e-mailverkeer echter onder de regels van FISA, ook als het een e-mailverkeer betreft tussen dezelfde Brit in Londen en de Fransman in Parijs. Amerikaanse internetproviders bewaren namelijk e-mails op Amerikaanse servers. Hierdoor valt de Brit die in Londen zijn of haar e-mails bekijkt of binnenhaalt van een server in de VS, in een keer onder de regels

[175] Laura Donohue, Section 702 and the Collection of International Telephone and Internet Content, 144.
[176] Ibidem, 147.

van FISA. Het communicatieverkeer vindt in dat geval immers plaats over Amerikaans grondgebied. Hierdoor vallen mensen die geen Amerikaans staatsburger zijn onbedoeld onder de bescherming van de FISA-regels, die in veel grotere mate de rechten van doelwitten erkennen dan EO 12333.

Het probleem met EO 12333 is dat de regels van het decreet én de programma's die onder het decreet worden uitgevoerd nog grotendeels geheim zijn. Bovendien kan ook het Congres slechts in beperkte mate toezicht uitoefenen. De minister van Justitie is verplicht om de toegestane procedures onder EO 12333 door te sturen aan de inlichtingencommissies van het Congres. Toch heeft de voorzitter van de *Senate Select Committee on Intelligence*, senator Dianne Feinstein, aangegeven dat de commissie niet in staat is om uitgebreid toezicht te kunnen uitoefenen op de vergaring van inlichtingen onder EO 12333.[177]

Afgezien van de dan al niet beperkte toezicht, speelt een ander aspect ook nog een belangrijke rol. Of de acties van de NSA wel in overeenstemming zijn met de Amerikaanse grondwet. Door verschillende betrokkenen wordt het verzamelen van metadata namelijk als ongrondwettelijk beschouwd. Randy Barnett stelt dat de *third-party doctrine* moet worden aangepast naar de hedendaagse omstandigheden en dus niet zoals die werd toegepast tijdens *Smith v. Maryland*. Hetzelfde geldt in zijn ogen ook voor de *reasonable expectation of privacy* uit *Katz v. United States*.[178]

Ook Laura Donohue gaat hierin mee. Zij stelt, zeer terecht, dat elektronische communicatiemiddelen nog een veel belangrijkere sociale rol spelen dan in 1967, ten tijde van *Katz v. United States*. Daarnaast zijn ze ook zeer belangrijk voor regelen van allerlei privézaken. Ook rechtbanken gaan steeds vaker mee in deze gedachtegang. In 2010 stelde een rechtbank, in de zaak *United States v. Warshak*, dat de overheid de rechten van Warshak onder het Vierde Amendement had geschonden door e-mailgegevens van Warshak bij de internetprovider op te eisen zonder dat de opsporingsinstanties beschikten over het juiste bevelschrift. Volgens de rechtbank had Warshak een *reasonable expectation of privacy* in de e-mail die hij bij de internetprovider had opgeslagen.[179]

Volgens Donohue is een verschuiving waarneembaar binnen het Amerikaanse Hooggerechtshof. Rechters met tegengestelde visies komen nader tot elkaar waar het gaat om beschermen van de rechten van Amerikaanse staatsburgers tegen bovenmatige bemoeienis van de overheid met de levens van Amerikanen. In de zaak *Florida v. Jardines*, die draaide om de inzet van een drugshond op de veranda van het huis van de verdachte, gaf de meerderheid van de rechters aan

[177] Ibidem, 151.
[178] Randy E. Barnett, 'Why the NSA Data Seizures Are Unconstitutional', *Harvard Journal of Law and Public Policy* 38 (2015) 1, 3-20, 16.
[179] Laura K. Donohue, 'Bulk Metadata Collection: Statutory and Constitutional Considerations', *Harvard Journal of Law and Public Policy* 37 (2014) 1, 757-900, 890.

de zoekactie ongrondwettelijk te vinden vanwege het feit dat de zoekactie op iemands eigendom plaatsvond. Alhoewel niet meegenomen in de veroordeling, was de minderheid van de rechters daarnaast ook nog van mening dat de privacybelangen van Jardines in het geding waren. Bezien in het licht van nieuwe (communicatie)technologieën kan het in bulk verzamelen van data gezien worden als een schending van het Vierde Amendement. Welke aanpak, schending van het eigendomsrecht of iemands privacy, er ook wordt gehanteerd.[180]

Hiermee lijkt het Hooggerechtshof in te gaan op de kritiek die Amerikaans jurist Christopher Slobogin in 2007 uitte in zijn boek *Privacy at Risk: The New Government Surveillance and the Fourth Amendment*. Daarin stelt hij dat overheidssurveillance in de VS sterk is toegenomen na 11 september 2001. Op zich zelf is dit niet slecht aangezien het namelijk zeker te rechtvaardigen is als reactie op de gebeurtenissen van 11 september 2001. Slobogin stelt wel dat ongereguleerde surveillance als onredelijk (*unreasonable*) kan worden beschouwd onder de Amerikaanse grondwet. Het Vierde Amendment, dat concreet ingevuld wordt door het Hooggerechtshof, liet tot dan toe namelijk de ruimte aan de overheid om burgers naar eigen goeddunken in de gaten te houden.

Volgens Slobogin is er niets mis met het Vierde Amendement in de huidige tijd, maar is de implementatie van *Katz v. United States* door het Hooggerechtshof wel verkeerd. Op dat punt maakt het Hooggerechtshof al een draai. Het Hooggerechtshof heeft namelijk erkend dat er sprake is van een *reasonable expectation of privacy* bij het gebruik van moderne communicatiemiddelen. Een ander punt van zorg voor Slobogin is het feit dat elektronische surveillance 'onzichtbaar' is voor de grondwet. Dit komt door de karakterisering van verantwoordingen van uitspraken door het Hooggerechtshof. Deze verantwoordingen moeten volgens hem niet meer gebaseerd worden op de primaire aanhankelijkheid van het Hooggerechtshof op de uitsluitingsregel onder het Vierde Amendement, en het misplaatste idee dat er een individuele *probable cause* standaard moet zijn bij een zoekactie.[181] Deze zaken zijn volgens Slobogin niet noodzakelijk onder het Vierde Amendement en zouden niet elektronische surveillance moeten reguleren. Slobogin ziet eerder wat in het toepassen van de principes van proportionaliteit en noodzakelijkheid.[182]

Met bovenstaande aanpassingen zou het Vierde Amendement beter toepasbaar zijn voor elektronische surveillance, maar het is de vraag of dat wenselijk is. Het is namelijk niet voor niets dat

[180] Donohue, 'Bulk Metadata Collection: Statutory and Constitutional Considerations', 891-892.
[181] De uitsluitingsregel onder het Vierde Amendement houdt in dat onwettig verkregen bewijs niet in een strafzaak gebruikt mag worden. *Probable cause* houdt in dat er niet slechts sprake mag zijn van een vermoeden voordat de politie overgaat tot een arrestatie, een zoekactie of een bevelschrift krijgt. Er moet een redelijke basis zijn om aan te nemen dat een misdrijf is begaan of dat er bewijs van een misdrijf aanwezig is.
[182] Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* (Chicago 2007) 47.

de uitsluitingsregel een belangrijke plaats inneemt binnen het Vierde Amendement. Machtsmisbruik door de overheid wordt zo namelijk tegengegaan**.**

In de VS heeft de NSA bij het uitvoeren van elektronische surveillance zich te houden aan het Vierde Amendement en diverse wetgeving. Daarnaast heeft ook nog EO 12333 betrekking op de inlichtingengemeenschap. In dit woud aan regels is er een duidelijk verschil zichtbaar tussen de rechten die Amerikaanse staatsburgers, en ingezetenen, hebben ten opzichte van buitenlanders. Dit was dan ook één van de punten waar de regering Obama op inspeelde na de onthullingen van Snowden. Ook op het gebied van de (verregaande) bevoegdheden van de NSA onder EO 12333 deed Obama een concessies. Het Vierde Amendement zorgt duidelijk voor een grijs gebied. Gezien het feit dat de aanpassing van de grondwet uit 1788 stamt, is het aan het Hooggerechtshof om concrete invulling aan de tekst te geven. Lange tijd heeft de opvatting van het amendement niet in pas gelopen met de technologische vooruitgang, maar het ziet er naar uit dat het Hooggerechtshof de laatste jaren het Vierde Amendement meer en meer beziet in de context van de moderne samenleving. Dit gebeurt specifiek op het gebied van privacybescherming.

Tegelijkertijd blijft data mining, uitgevoerd door de overheid, nog een probleem vormen. Het Hooggerechtshof heeft namelijk tot op heden nog niet het Vierde Amendement op een dusdanige manier geïnterpreteerd dat het extra regulering van data mining door de overheid noodzakelijk acht. Dit probleem werd in 2004 al aangekaart in een rapport van de *Technology and Privacy Advisory Committee*.[183] Het probleem wordt daarbij vergroot doordat bestaande wetgeving om data mining door de overheid te reguleren erg beperkt is.

Toch is er ook op dat punt een kentering waar te nemen. Uit recente uitspraken van het Hooggerechtshof – in de zaken *Ferguson v. City of Charleston* en *Georgia v. Randolph* – blijkt dat het Hooggerechtshof steeds minder geneigd is om de overheid een vrijstelling te geven voor wat betreft de traditionele regels van het Vierde Amendement, puur om het feit dat relevante informatie voor een crimineel onderzoek gedeeld of afgegeven is aan een derde partij. Beweringen vanuit de overheid dat versoepeling van de regels noodzakelijk is om criminele activiteiten op te kunnen sporen, vinden dus niet per definitie gehoor bij het Hooggerechtshof. Daarmee ondermijnt het Hooggerechtshof de bestaande rationale dat *heightened-need* als reden geldt om de bescherming van het Vierde Amendement te verlagen.

Toch lijkt het metadataprogramma van de NSA in overeenstemming te zijn met de Amerikaanse wetgeving, dat wil zeggen sectie 215 van de *Patriot Act* en het Vierde Amendement.

[183] The Technology and Privacy Advisory Committee, Safeguarding Privacy in the Fight Against Terrorism (Rapport The Technology and Privacy Advisory Committee, Washington 2004) 48.

Sectie 215 van de *Patriot Act* geldt als belangrijke pijler van het metadataprogramma van de NSA. Dit valt ook op te maken uit de uitspraak van de rechters in de zaak *ACLU v. Clapper* waarbij de rechtszaak werd geseponeerd op basis van het feit dat de aanklagers hun claim niet konden hardmaken dat het metadataprogramma van de NSA het Vierde Amendement en de FISA zou schenden.

De opvatting van de overheid dat het metadataprogramma van de NSA wel in overeenstemming is met de wet wordt niet alleen ondersteund door de uitspraak in de zaak *ACLU v. Clapper*, maar wordt ook gesteund vanuit de academische wereld. Ten slotte is het Hooggerechtshof van mening dat het verzamelen van gegevens van derde partijen niet gezien kan worden als een *search* onder het Vierde Amendement.

Hier valt wel het een en ander over op te merken. Volgens sectie 215 is de *Federal Bureau of Investigation* (FBI) de dienst die bevoegd is om verzoeken in te dienen om gegevens te verzamelen, terwijl de NSA het programma uitvoert. Onder sectie 215 mogen gegevens worden verzameld zolang ze 'relevant' zijn. Het probleem is echter dat gebruikte interpretatie van het begrip 'relevant' zeer breed is, waardoor bijna elke bulkvergaring van persoonsgegevens als legaal kan worden beschouwd. Bovendien worden praktisch dagelijks nieuwe gegevens verzameld in plaats van als reactie op verzoeken vanuit de FBI. De reactie van de Amerikaanse overheid op deze kritiek zal in het volgende hoofdstuk behandeld worden.

Dat het Hooggerechtshof het verzamelen van metadata niet beschouwt als een *search* onder het Vierde Amendement is eigenlijk anachronisme. Die opvatting is namelijk terug te voeren op de uitspraak in de zaak *Smith v. Maryland*, een zaak die stamt uit 1979. Niet alleen hebben technologische veranderingen de uitspraak doen verouderen, ook de rechters van het Hooggerechtshof lijken van gedachten te veranderen. De rechterlijke overwegingen in de zaak *United States v. Jones* wijzen erop dat de rechters wellicht de bestaande theorie van het Vierde Amendement willen wijzigen. Daarbij zou een normatievere benadering van privacy kunnen worden gehanteerd in de jurisprudentie rondom het Vierde Amendement. Een benadering waarbij er meer oog is voor de context en de steeds meer toenemende onthullende capaciteiten van metadatasurveillance.

De uitspraak in de zaak *United States v. Warshak* (2010) is uniek omdat het de eerste keer betrof dat een rechtbank expliciet aangaf dat er sprake is van een *reasonable expectation of privacy* voor wat betreft e-mails die op de server van een internetprovider staan opgeslagen. De inhoud van die e-mails valt daarmee onder bescherming van het Vierde Amendement. Tot op heden heeft het Hooggerechtshof deze zienswijze echter nog niet overgenomen. Mocht het hof hier in de toekomst toe besluiten dan wordt daarmee het gat gedicht waar de overheid gebruik van maakt om bulkgegevens van Amerikanen te verzamelen. Tot dan blijft de *third-party doctrine* van kracht en blijft

informatie, die gedeeld met een derde partij, uitgesloten van bescherming onder het Vierde Amendement.

II.II Inlichtingendiensten en wetgeving in de Europese Unie

Als het om databescherming gaat wordt de EU over het algemeen gezien als een partij die de standaard zet voor de rest van de wereld. Toen het Europese blok in de jaren '90 met databeschermingsregels kwam, werd de Databeschermingsrichtlijn 95/46/EG als revolutionair beschouwd. Deze databeschermingsrichtlijn is sindsdien een aantal keren aangepast, onder andere op het gebied van elektronische bescherming.[184]

Het is belangrijk om te noteren dat de Europese privacyrichtlijn geen wet is. Het vormt een richtlijn die het verwerken van persoonsgebonden gegevens in de EU regelt. De richtlijn is door lidstaten zelf omgezet in nationale wetgeving. Zo is in Nederland de Wet bescherming persoonsgegevens uit de richtlijn voortgekomen. Doordat uiteindelijk elke EU-lidstaat dus eigen nationale privacywetgeving heeft geïmplementeerd, vertoont de Europese situatie, zeker in relatie tot de inlichtingendiensten, grote verschillen met de situatie in de VS.

Reden hiervoor is dat de nationale veiligheid in de EU uiteindelijk een zaak is van de individuele lidstaten en niet van de EC in Brussel. De bevoegdheden van nationale inlichtingen- en veiligheidsdiensten in verhouding tot de privacywetgeving liggen daardoor ook vastgelegd in de verschillende nationale wetgevingen.

De capaciteiten van de EC om zelf inlichtingen te vergaren zijn vrij beperkt. Europese privacywetgeving heeft zich in de loop der jaren dan ook meer ontwikkeld op het gebied van markt dan op terrein van de rechtshandhaving. Marktregulering vindt plaats op het supranationaal niveau, terwijl veiligheidsbeleid een zaak is van de lidstaten en op intergouvernementeel niveau wordt besproken.

De eerste wetgeving betreffende databescherming in de EU stamt uit de jaren '70. Deze wetgeving had met name betrekking op het grote schaal verzamelen van data van burgers door de overheid. Het verzamelen van die gegevens was daarbij primair bedoeld voor het verlenen van diensten aan burgers: gezondheidszorg, onderwijs en welzijn. Inlichtingendiensten hadden nauwelijks iets van doen met deze regels voor databescherming. Over het algemeen was het inlichtingendiensten en andere wetshandhavingsinstanties door nationale wetgeving al verboden om zichzelf toegang te

[184] Een belangrijke wijziging vormde richtlijn 2002/58/EG: de e-privacyrichtlijn uit 2002 waarmee de databeschermingregels ook van toepassing werden op de elektronische communicatiesector.

verschaffen tot gegevens van andere overheidsdiensten zonder gegronde reden.[185] De regels voor de diensten waren minder strikt en de controle van de naleving van de regels was over het algemeen geen taak van rechtbanken, maar van onafhankelijke ambtenaren of parlementaire commissies.

Wetgeving ten behoeve van databescherming was in de loop der jaren gericht op het voorkomen van rechtsmisbruik door de overheid en marktactoren, maar ook hier vormen de aanslagen van 11 september 2001, en de verschillende aanslagen in Europa daaropvolgend, een belangrijke cesuur. Sinds 11 september 2001 is 'veiligheid' een zeer belangrijk punt van aandacht geworden waar veel zaken onder vallen: terrorisme, georganiseerde misdaad, cybercrime, grensoverschrijdende criminaliteit, geweld en (natuur)rampen. Binnen de EU zijn lidstaten dan ook meer gaan samenwerken op het gebied van wetshandhaving. Toch voltrekt het Europese veiligheidsbeleid zich hoofdzakelijk aan de hand van een economische agenda en daardoor hanteert de EC een op de markt georiënteerde aanpak wat betreft de relatie tussen privacy enerzijds en veiligheid anderzijds.[186] De EC blijft zich primair bezig houden met commerciële regulering en heeft in veel mindere mate directe invloed op het veiligheidsbeleid van de lidstaten.

Het is dan ook niet verwonderlijk dat de zeggenschap van de EU op het gebied van nationale veiligheid beperkt is. Tekenend hiervoor is artikel 13 van de Europese databeschermingsrichtlijn. Daarin wordt gesteld dat activiteiten op veiligheidsgebied – zoals defensie, openbare veiligheid en staatsactiviteiten op strafrechtelijk gebied – onder bepaalde voorwaarden niet onder de strekking van de richtlijn vallen.[187]

In Europese wetgeving ligt daarentegen wel vastgelegd dat individuen het eigendomsrecht hebben over hun eigen data, terwijl in de VS juist de bedrijven of diensten die de data hebben verzameld dat eigendomsrecht hebben. Denk in dit verband bijvoorbeeld aan de *third-party doctrine* in het Amerikaanse rechtssysteem. Met betrekking tot de activiteiten van de NSA is dit belangrijk om aan te halen. In de EU mogen immers alleen nationale instanties die elektronische data beheren en reguleren, met het in acht nemen van bestaande Europese en internationale regels, toestaan dat van de bestaande regels wordt afgeweken ten behoeve van nationale veiligheid. Als de samenwerking

[185] Francesca Bignami, 'Privacy and Law Enforcement in the European Union: The Data Retention Directive', *Chicago Journal of International Law* 8 (2007) 1 233-255, 234-235.
[186] Serge Gutwirth, Ronald Leenes en Paul de Hert (red.), *Reforming European Data Protection Law* (Dordrecht 2015) 275.
[187] Het Europees Parlement en de Raad van de Europese Unie, 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data', http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046 (29 april 2016).

tussen de NSA en de Europese diensten dus zonder medeweten of toestemming van de nationale toezichthouders is gebeurd, gaat het om diefstal van persoonlijke gegevens.[188]

Afgezien van het feit dat richtlijnen en/of wetgeving op het Europees niveau met betrekking tot buitenlandse inlichtingenvergaring ofwel ontbreekt dan wel een beperkte reikwijdte heeft, is nationale wetgeving in de EU met betrekking tot buitenlandse inlichtingenvergaring ook nog eens minder gedetailleerd en in beperktere mate publiekelijk te raadplegen dan de wetgeving in de VS. Daarnaast is er minder bekend over de staande praktijk in Europa dan in de VS. Deze zaken zorgen ervoor dat het maken van een directe vergelijking tussen de verschillende stelsels enigszins problematisch is.[189]

De verschillende nationale wetgevingen in de EU-lidstaten, die het vergaren van buitenlandse inlichtingen reguleren, zijn in grote lijnen hetzelfde. Dit is het geval ondanks het feit dat er verschillen in de organisatiestructuren of in de technologische capaciteiten van de diensten aanwezig zijn. Bij veel diensten wordt het verzamelen van communicatieverkeer in het buitenland toegestaan omwille van de 'nationale veiligheid', externe militaire dreigingen, om ernstige misdaden zoals terrorisme te voorkomen en ten gunste van het buitenlands beleid of de nationale economie.[190]

Over het algemeen wordt door lidstaten gesteld dat de activiteiten van nationale inlichtingendiensten onder de eigen nationale bevoegdheden en dus buiten het wettelijk systeem van de EU vallen. De vraag is echter of dit wel klopt.

In het eerste hoofdstuk werden het EVRM en het Handvest van de Grondrechten van de EU aangehaald. In deze verdragen liggen de Europese kernwaarden voor mensenrechten vastgelegd. Deze documenten zijn opgenomen in de verschillende nationale wetgevingen waardoor ook het EHRM en het Europees Hof van Justitie zich over zaken van nationale veiligheid, en dus de surveillanceprogramma's, kunnen oordelen.

Toch sprak het EHRM (EHRM) zich al veel eerder, in 1978, uit over surveillance van geheime diensten in relatie tot het recht op privacy en databescherming en wees daarbij op de mogelijke gevaren voor het ondermijnen van democratie, terwijl werd gesteld dat de surveillanceactiviteiten er juist erop gericht zijn om diezelfde democratie te verdedigen.[191]

---

[188] Bigo e.a., National Programmes for Mass Surveillance of Personal Data in EU Member States and their Compatibility with EU Law (Rapport Europees Parlement, Brussel 2013) 27.
[189] Ian Brown e.a., Towards Multilateral Standards for Surveillance Reform (Oxford Internet Institute Discussion Paper, Oxford 2015) 9.
[190] Brown e.a., Towards Multilateral Standards for Surveillance Reform, 10.
[191] Commissie burgerlijke vrijheden, justitie en binnenlandse zaken, Electronic mass surveillance of EU citizens (Onderzoeksrapport Europees Parlement, Brussel 2013) 81.

In het recentere verleden (2006) heeft het EHRM (EHRM) zich gebogen over de vraag in hoeverre de rechtvaardigingen van nationale overheden om inbreuk te maken op de rechten vastgelegd binnen het EVRM in overeenstemming zijn met de wet, een legitiem doel nastreven en in hoeverre de maatregelen noodzakelijk zijn in een democratische samenleving. Het Hof deed dit in de zaak *Weber and Savaria v. Germany*. De zaak betrof de legitimiteit van de machtsmiddelen van de Duitse inlichtingendienst, de *Bundesnachrichtendienst* (BND), met betrekking tot het opnemen van telecommunicatie als onderdeel van het 'strategisch monitoren' en het gebruiken, en doorgeven aan andere autoriteiten, van verzamelde persoonlijke data.

Het oordeel van het Hof luidde dat de Duitse wetgeving voldoende en effectieve bescherming bood tegen machtsmisbruik door de Duitse staat. Daarnaast werd de inmenging van de dienst in geheime telecommunicatie door het Hof ook als noodzakelijk gezien in een democratische samenleving, om zo de belangen van nationale veiligheid te behartigen en misdrijven te voorkomen. De aanklacht, gebaseerd op artikel 8 van het EVRM, werd daarmee verworpen. Desondanks stelde het Hof wel een aantal criteria op – op basis van hetzelfde artikel 8 van het EVRM – om voortaan te kunnen bepalen of geheime surveillance in overeenstemming zou zijn met de wet. De achterliggende gedachte was dat volgens het Hof het risico van machtsmisbruik en willekeur op de loer lag wanneer een taak van de uitvoerende macht in het geheim zou worden uitgevoerd. Het Hof stelde daarom dat er minimale waarborgen in de nationale wetgeving moesten worden geïmplementeerd om machtsmisbruik te voorkomen:

> *…the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed…*[192]

Het Hof gaf in de uitspraak ook aan dat het in strijd zou zijn met de westerse rechtsstaat als de macht van uitvoerende of de rechtsprekende macht tot uiting zou komen in een ongebonden macht, daarmee

[192] Europees Hof voor de Rechten van de Mens, *Weber and Saravia v. Germany*, No. 54934/00, 29 juni 2006, § 95.

doelende op de macht van inlichtingendiensten.[193] Het draait dus feitelijk om een kwestie van autoriteit en wie die autoriteit bezit om te bepalen wat er gedaan wordt.

De Duitse zaak staat niet op zichzelf. In een andere zaak, *Liberty v. UK*, stelde het Hof dat de geheime onderschepping van communicatieverkeer door de Britse overheid in strijd was met artikel 8 van het EVRM. Het verschil met de zaak *Weber* zat hem erin dat de Britse wet volgens het Hof niet genoeg duidelijkheid gaf over de (on)mogelijkheden voor de inlichtingendiensten. Het Hof had het in die context speciaal over het ontbreken van *foreseeability* in de wetgeving. Het Hof doelde daarmee op het feit dat de Britse wetgeving in onvoldoende mate toegankelijk was en daarnaast te onzorgvuldig geformuleerd was. Doordat er sprake was van bepaalde wetgeving die in een systeem voorzag waarmee in het geheim communicatieverkeer in gaten kon worden gehouden, bestond automatisch de reële dreiging dat een ieder die onder de paraplu van de wet viel slachtoffer van surveillance kon worden. Deze dreiging beknopte de vrijheid van communicatie tussen de gebruikers van telecomdiensten en betekende dus een beperking van de rechten van gebruikers onder artikel 8 van het EVRM.[194] Mede daarom concludeerde het Hof dat Britse wetgeving onvoldoende bescherming bood tegen mogelijk machtsmisbruik.[195]

Het EHRM heeft in zijn jurisprudentie eveneens meerdere malen het belang benadrukt van het hanteren van een enge interpretatie voor wat betreft de in zaken toegestane uitzonderingen op de fundamentele mensenrechten in EVRM. Hiermee wordt bedoeld dat de uitspraak alleen voor de desbetreffende zaak geldt en niet moet worden doorgetrokken naar andere gevallen. Het Hof heeft dit gedaan om het individu zoveel mogelijk te beschermen tegen enig machtsmisbruik en om aan te geven dat mensenrechten voor iedereen gelden en dat daar in de regel geen uitzondering op bestaat.

Naast de rol die het EVRM en het EHRM spelen met betrekking tot de reikwijdte van buitenlandse inlichtingenactiviteiten van Europese diensten, is het ook nog belangrijk om aandacht te schenken aan de relatie tussen grootschalige surveillanceprogramma's in EU-lidstaten en het Handvest van de Grondrechten van de EU. Net als het EVRM raakt ook dit document namelijk aan terreinen die, volgens de EU-lidstaten zelf, het terrein van 'nationale veiligheid' aanhalen.

Zoals eerder al benoemd is het Handvest van de Grondrechten van de EU wettelijk bindend voor alle EU-lidstaten sinds het in werking treden van het Verdrag van Lissabon op 1 december 2009.

[193] Europees Hof voor de Rechten van de Mens, *Weber and Saravia v. Germany*, No. 54934/00, 29 juni 2006, § 94.
[194] Europees Hof voor de Rechten van de Mens, *Liberty and Others v. the United Kingdom*, no. 58243/00, 1 juli 2008, § 56.
[195] Europees Hof voor de Rechten van de Mens, *Liberty and Others v. the United Kingdom*, no. 58243/00, 1 juli 2008.

De EC concludeerde in 2012 in een jaarverslag dat het Handvest in toenemende mate door de individuele lidstaten binnen het binnenlandse wettelijk systeem was geïmplementeerd. Ook het Europees Hof voor Justitie kwam tot dezelfde conclusie door te stellen dat het Handvest een belangrijk onderdeel werd van de nationale wetgevingstradities van de EU-lidstaten.[196] Ook vice-voorzitter van de EC, Viviane Reding, deed hierover een belangrijke uitspraak in reactie op de onthullingen van Edward Snowden:

> *The concept of national security does not mean that "anything goes": States do not enjoy an unlimited right of secret surveillance. In Europe, also in cases involving national security, every individual – irrespective of their nationality – can go to a Court, national of European, if they believe that their right to data protection has been infringed. Effective judicial redress is available for Europeans and non-Europeans alike. This is a basic principle of European law.*[197]

Het kan namelijk niet zo zijn dat de fundamentele rechten van de EU niet meer van toepassing zijn op het werkterrein van de inlichtingendiensten, simpelweg omdat dat werkterrein toevallig niet onder vleugels van de EU valt, aldus Reding.[198]

Ook vanuit een andere Europese invalshoek kan een belangrijke kanttekening worden geplaatst bij de grootschalige surveillanceprogramma's van diverse EU-lidstaten. Het verzamelen van inlichtingen – ook ten behoeve van de 'nationale veiligheid' – is in steeds grotere mate een supranationale aangelegenheid, waarbij zowel via binnenlandse en buitenlandse bronnen gegevens worden verzameld. Hierdoor bestaat er de reële mogelijkheid dat Europese surveillanceprogramma's de veiligheid en de fundamentele mensenrechten van burgers en inwoners van andere EU-lidstaten *compromitteren*. Met name op het gebied van de privacy en wettelijke bescherming is dat het geval.

Zo kunnen EU-burgers het eigendomsrecht over hun persoonlijke data verliezen omdat Europese bedrijven deelnemen aan programma's van de NSA of kunnen burgers het slachtoffer worden van ongelijke behandeling. Dit laatste is bijvoorbeeld mogelijk wanneer burgers in de ene EU-lidstaat disproportioneel vaker slachtoffer zijn van grootschalige surveillanceprogramma's doordat ze onterecht minder gunstig behandeld worden dan burgers van de andere EU-lidstaat. Dit kan bijvoorbeeld gebeuren omdat inwoners van de ene staat meer privacyrechten hebben als hun communicatieverkeer wordt onderschept, simpelweg vanwege het feit dat het dan om de onderschepping van binnenlandse communicatie kan gaan.

---

[196] Bigo e.a., National Programmes for Mass Surveillance of Personal Data in EU Member States, 33.
[197] Viviane Reding, "PRISM scandal: The data protection rights of EU citizens are non-negotiable", Persverklaring, EU-U.S. Justice and Home Affairs Ministerial, Dublin, 14 June 2013. Beschikbaar via http://ec.europa.eu/ireland/press_office/media_centre/june2013_en.htm#12 (25 april 2016).
[198] Bigo e.a., National Programmes for Mass Surveillance of Personal Data in EU Member States, 34.

Wat dat betreft kan hier één-op-één de vergelijking worden getrokken met de VS, waar buitenlanders ook minder privacyrechten hebben dan Amerikanen (of Amerikaanse ingezetenen). Belangrijk verschil is alleen dat men juist zou verwachten dat binnen de EU, waar sprake is van Europese mensenrechten en grondrechten, dat er geen onderscheid zou mogen bestaan tussen inwoners van verschillende lidstaten.

Privacy International maakte daar dan ook een punt van toen het bij de rechter aanhankelijk probeerde te maken dat het Britse Tempora-programma ongegronde discriminatie toepaste jegens niet-Britten en andere EU-burgers.[199] Wat was er precies aan de hand? Volgens de Britse wet kan er alleen een bevelschrift worden afgegeven voor het onderscheppen van communicatie in en/of naar het buitenland. Aangezien de kans veel groter is dat niet-Britten hier onder vallen, is de kans veel groter dat het communicatieverkeer van andere EU-burgers wordt onderschept, geanalyseerd en bewaard. Tegelijkertijd stelde *Privacy International* dat zowel Britten als niet-Britten een bedreiging vormen voor de nationale veiligheid van Groot-Brittannië. De verschillen in behandeling zouden dus niet te rechtvaardigen zijn, laat staan in overeenstemming zijn met Europese wetgeving.

Dezelfde organisatie heeft nog een ander punt aanhangig gemaakt bij het Hof van Justitie van de Europese Unie en dat was het bestaan van een belangrijk lacune in de Europese wetgeving waardoor de kwetsbaarheid van de privacyrechten en vrijheden van EU-burgers zou worden versterkt. De lacune zijnde het bestaande verschil tussen het verzamelen van buitenlandse en binnenlandse inlichtingen. Hierdoor kunnen inlichtingendiensten de eigen nationale beperkingen omzeilen door een bevriende inlichtingendienst te vragen bepaald (binnenlands) communicatieverkeer te onderscheppen om die vervolgens uit te ruilen. De centrale vraag die *Privacy International* stelde was dus of het bestaande onderscheid tussen zogeheten interne en externe communicatieverkeer nog steeds relevant is met betrekking tot de benodigde bevelschriften voor onderschepping van communicatieverkeer binnen de rechtssystemen van EU-lidstaten?

Hierboven is al benoemd dat de EC zelf niet of nauwelijks eigen inlichtingen vergaard, maar dat betekent niet dat diensten van de EC niet zelf inlichtingenproducten maken. Instituties en diensten van de EU houden zich immers wel degelijk bezig met (gezamenlijke) activiteiten op het gebied van veiligheid. De EU is zich sinds 11 september 2001 steeds meer gaan bezig houden met het interne veiligheidsbeleid, in dat kader werd in 2003 de eerste Europese Veiligheidsstrategie geschreven en zijn ook Europese agentschappen zich nog meer gaan toeleggen op interne veiligheidsvraagstukken. Een voorstel van de EC om nationale inlichtingendiensten daarbij verplicht

[199] Met het Tempora-programma kan de Britse GCHQ data aftappen van kabels op de bodem van de oceaan. Daar zitten onder meer gegevens bij van Britse staatburgers en andere EU-burgers.

inlichtingen te laten delen, werd door alle EU-lidstaten afgewezen. De reden daarvoor was dat iedere EU-lidstaat zijn inlichtingen(bronnen) beschermt en samenwerking kan daarom beter plaats vinden op een bilaterale basis.[200]

Europese diensten, zoals Europol (politie), Frontex (grensbewaking) en INTCEN (inlichtingen), zijn voor hun analyses en rapportages echter wel afhankelijk van de bijdragen van nationale veiligheids- en inlichtingendiensten. De manier waarop die informatie tussen de nationale diensten en de Europese agentschappen wordt gedeeld is ondoorzichtig. Zo gaf de directeur van Europol in 2013 in het Europees Parlement aan dat zijn organisatie geen contacten onderhoudt met de NSA of de CIA, maar tegelijkertijd kon hij niet garanderen dat ingewonnen informatie niet van de NSA afkomstig is. Die reactie is te begrijpen, maar het is enigszins problematisch dat agentschappen van de EU mogelijk met gegevens werken die naar Europese wetgeving onrechtmatig verkregen is.[201]

De huidige Europese databeschermingsrichtlijn is gebaseerd op een aantal belangrijke principes: doelbeperking, dataminimalisering, de rechten van het datasubject (waaronder het recht om geïnformeerd te worden over de verwerking van de gegevens, bezwaar aan te kunnen tekenen tegen die verwerking, toegang krijgen tot iemands gegevens en om niet slachtoffer te worden van ingrijpende geautomatiseerde beslissingen aangaande de data). EU-lidstaten mogen volgens artikel 13 van de Europese databeschermingsrichtlijn deze rechten door middel van nationale wetgeving beperken, onder meer vanwege nationale veiligheid. Nationale veiligheid valt onder de bevoegdheden van de individuele lidstaten, maar de omvang van dat begrip wordt ook beperkt door verschillende Europese wetgeving.[202]

In de EU kan er van vijf landen – Verenigd Koninkrijk, Duitsland, Zweden, Frankrijk en Nederland – met enige zekerheid worden gesteld dat inlichtingendiensten van die landen zich toeleggen op het gebruik van grootschalige elektronische surveillance naast de meer traditionele, doelgerichte surveillance.[203] Het is de vraag of de surveillanceprogramma's in kwestie in overeenstemming zijn met Europese wetgeving.

Surveillance van communicatieverkeer wordt in het Verenigd Koninkrijk gereguleerd door de uit 2000 stammende *Regulation of Investigatory Powers Act* (RIPA). Onder bepaalde voorwaarden

[200] Robert Dover, 'From CFSP to ESDP: the EU's Foreign, Security, and Defence Policies', in: Michelle Cini en Nieves Pérez-Solórzano Borragón (red.), *European Union Politics* (Oxford 2010) 239-257, 254.
[201] Bigo e.a., National Programmes for Mass Surveillance of Personal Data in EU Member States, 37-38.
[202] Commissie burgerlijke vrijheden, justitie en binnenlandse zaken, Electronic mass surveillance of EU citizens, 81-82.
[203] Julian Borger, 'GCHQ and European spy agencies worked together on mass surveillance' (versie 1 november 2013), http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden (25 april 2016).

kunnen onder die wet bevelschriften worden afgegeven door de minister of, in sommige gevallen, door de hoofden van de diensten zelf. Een gespecificeerd bevelschrift is echter niet nodig wanneer communicatieverkeer buiten het Verenigd Koninkrijk wordt onderschept. Dan volstaat een bevelschrift van de minister waarin alleen wordt aangegeven wat voor een soort materiaal onderschept dient te worden.[204] Onder dit systeem werd ook het Tempora-programma geautoriseerd en werd verzamelde data uitgewisseld met de VS.[205] De Britse overheid heeft weliswaar beweerd dat RIPA in overeenstemming is met het EVRM doordat er expliciete proportionaliteitstesten in de wet zijn ingebouwd, maar experts zijn kritisch. De standaarden voor die testen zijn namelijk voor het merendeel niet openbaar en worden bovendien, met beperkt toezicht, uitgevoerd door de overheid zelf.[206]

De Duitse inlichtingen- en veiligheidsdiensten, met de BND als belangrijkste speler, zijn in staat om verbinding te maken met knooppunten voor internetverkeer om buitenlands internetverkeer af te kunnen tappen.[207] De BND kan dataverkeer opslaan, kopiëren en later analyseren. Sinds 2001 mogen de Duitse diensten ook onderling, en met andere wetshandhavingsdiensten, data uitwisselen, iets dat daarvoor strikt door de Duitse wet werd verboden. De surveillance van communicatieverkeer wordt in Duitsland geregeld met de *G-10* wet. Onder deze wet mogen de Duitse diensten in specifieke gevallen zonder bevelschrift geautomatiseerde telefoontaps plaatsen op binnenlands en buitenlands communicatieverkeer wanneer het bijvoorbeeld gaat om de strijd tegen het terrorisme of het beschermen van de Duitse grondwet. Ook elektronisch- en stemverkeer mag worden gemonitord.[208]

Een uitspraak van het grondwettelijk hof, het *Bundesverfassungsgericht*, bepaalde in 2004 echter dat bepaald communicatieverkeer – met bijvoorbeeld naaste familieleden, dokters, priesters en advocaten – daarbuiten valt. Het gaat dan namelijk om zulke persoonlijke gesprekken dat de overheid daar geen inbreuk op mag maken. Vervolgens besloot het Hof in 2008 dat bepaalde onderdelen van de regionale wet van Noordrijn-Westfalen niet in overeenstemming waren met de grondwet. Volgens die lokale wet mocht een overheidsdienst ter bescherming van de grondwet in het geheim data van privécomputers verzamelen. Het Hof bepaalde echter dat de integriteit en betrouwbaarheid van IT-systemen door de staat gegarandeerd dienden te worden. Alleen bij acuut

[204] Ian Brown, Deskundigeverklaring bij Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK (27 september 2013), no. 581780/13, § 52.
[205] Ian Brown, Deskundigeverklaring bij Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK (27 september 2013), no. 581780/13, § 35.
[206] Bigo e.a., National Programmes for Mass Surveillance of Personal Data in EU Member States, 56.
[207] Patrick Beuth, 'Wie der BND das Netz überwacht' (versie 18 juni 2013), http://www.zeit.de/digital/datenschutz/2013-06/internet-ueberwachung-bnd (25 april 2016).
[208] Bigo e.a., National Programmes for Mass Surveillance of Personal Data in EU Member States, 69-70.

gevaar voor iemands leven, de mensheid of de staatsveiligheid kan daar een uitzondering op worden gemaakt.[209]

De Zweedse inlichtingendienst, de *Försvarets radioanstalt* (FRA), is misschien de minst voor de hand liggende Europese partner van de NSA van het vijftal. Toch bleek al in 2008 dat de dienst dataverkeer aftapte en die data doorspeelde naar de VS. Daarbij mag volgens de letter van de wet alleen communicatieverkeer worden opgeslagen dat Zweden binnenkomt of uitgaat, maar intern communicatieverkeer dat via knooppunten buiten Zweden wordt verstuurd kan toch als 'extern' worden bestempeld en dus worden opgeslagen. Daarbij mag van het leeuwendeel van de onderschepte gegevens alleen de metadata worden geanalyseerd, tenzij het van belang is voor militaire inlichtingen. Dit onderscheid is echter in de praktijk vaag aangezien de onderschepte data voor zogeheten *auxiliary operations*, ook mag worden ingezet ter ondersteuning van militaire inlichtingenoperaties.[210]

Wettelijke toestemming voor surveillanceoperaties van FRA wordt gegeven door een speciale inlichtingenrechtbank, de *Underrättelsedomstolen*. Het wettelijke kader waar de rechtbank mee te maken heeft stelt echter wel dat de afgegeven bevelschriften ruim kunnen worden opgesteld en niet beperkt hoeven te blijven tot een bepaald individu.[211]

Volgens Bernard Barbier, technisch directeur bij de *Direction générale de la sécurité extérieure* (DGSE), hoort de Franse inlichtingendienst tegenwoordig tot de belangrijkste inlichtingendiensten ter wereld als het gaat om de vergaring van data.[212] Voor het vergaren en analyseren van de data wordt door de dienst gebruik gemaakt van een Parijse supercomputer. Uit hoorzittingen met de hoofden van de Franse inlichtingendiensten van de commissie voor nationale defensie werd duidelijk dat de DGSE in staat is om internetverkeer en communicatieverkeer via sociale media en telefoons te onderscheppen en te analyseren.[213] Of op dat gebied samenwerking plaats vindt met de NSA is echter onduidelijk. Door onthullingen van de *Washington Post* bestond er vanaf 2005 een geheim inlichtingencentrum in Parijs, genaamd *Alliance Base*, waar op regelmatige basis informatie werd uitgewisseld door zes landen: de VS, het Verenigd Koninkrijk, Frankrijk, Duitsland, Canada en

[209] Ibidem, 71.
[210] Ibidem, 59-60.
[211] Ibidem, 60.
[212] Barbier maakte opmerkingen van deze strekking tijdens een speech op een bijeenkomst van *l'Association des Réservistes du Chiffre et de la Sécurité de l'Information* op 30 september 2010. Zie Jean-Marc Manach, 'Frenchelon: la DGSE est en « 1ère divison »' (versie 2 oktober 2010), http://bugbrother.blog.lemonde.fr/2010/10/02/frenchelon-la-dgse-est-en-1ere-division/ (2 mei 2016).
[213] Bigo e.a., National Programmes for Mass Surveillance of Personal Data in EU Member States, 63-64.

Australië.[214] De samenwerking zou echter in de zomer van 2009 beëindigd zijn vanwege onenigheid tussen Frankrijk en de VS over een door Frankrijk gewenste overeenkomst om niet bij elkaar te spioneren. Het was echter het Witte Huis dat een dergelijk afspraak niet formeel op papier wilde zetten.[215]

Elektronische surveillance is sinds 2012 in de Franse wet geregeld door de *Code de la Sécurité Intérieure* en in die wet liggen de randvoorwaarden vastgelegd voor het uitvoeren van zogeheten 'veiligheidsonderscheppingen'. Dit soort onderscheppingen worden goedgekeurd door de premier op basis van een advies van de *Commission nationale de controle des interceptions de sécurité* (CNCIS). De wet kon echter op veel kritiek rekenen van de CNCIS vanwege het feit dat het nieuwe pakket aan regels voor het onderscheppen veel breder, en vager, was dan de bestaande regels. Daarbovenop had de nieuwe anti-terrorismewet van 2006 al extra bevoegdheden toegekend aan de inlichtingendiensten. Met ingang van die wet mochten de diensten voortaan direct, zonder tussenkomst van de rechter, telecomdata opvragen bij de internetproviders en werd daarnaast ook opslagtermijn voor die data verlengd.[216]

Voor het uitvoeren van grootschalige surveillanceprogramma's, én de opslag van data, maakt de DGSE gebruik van een maas in de wetgeving, aldus een senior medewerker van één van de inlichtingendiensten. De wet vormt namelijk wel een inkadering voor het uitvoeren van de 'veiligheidsonderscheppingen', maar niet voor de grootschalige opslag van (technische) data door de inlichtingendiensten. Het verzamelen en opslaan van metadata vindt dus plaats 'buiten de wet' om.[217] Dit werd echter tegengesproken door de onafhankelijke organisatie ter bescherming van de privacy. Die gaf aan dat grootschalige ongerichte surveillance volgens de letter van de wet juist verboden was.[218]

Van het laatste land van het vijftal, Nederland, wordt over het algemeen aangenomen dat de inlichtingendiensten zich op dit moment niet bezighouden met grootschalige surveillanceprogramma's. De gezamenlijke organisatie van de Algemene Inlichtingen- en

[214] Dana Priest, 'Help From France Key In Covert Operations' (versie 3 juli 2005), http://www.washingtonpost.com/wp-dyn/content/article/2005/07/02/AR2005070201361.html (3 mei 2016).
[215] David Servenay, 'Terrorisme: pourquoi Alliance Base a fermé à Paris' (versie 24 mei 2010), http://rue89.nouvelobs.com/2010/05/24/terrorisme-fermeture-dalliance-base-a-paris-152349 (3 mei 2016).
[216] Bigo e.a., National Programmes for Mass Surveillance of Personal Data in EU Member States, 65-66.
[217] Jacques Follorou en Franck Johannès, 'Révélations sur le Big Brother français' (versie 7 juli 2013), http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html (3 mei 2016).
[218] Follorou en Johannès, 'Révélations sur le Big Brother français' (versie 7 juli 2013), http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html (3 mei 2016).

Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) voor het uitvoeren van SIGINT is sinds 2014 de *Joint Sigint Cyber Unit* (JSCU).

De aanname dat de Nederlandse inlichtingendiensten zich momenteel niet bezighouden met grootschalige surveillance is gebaseerd op het feit dat de diensten volgens de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) alleen gerichte surveillance is toegestaan.[219] Het uitvoeren van grootschalige, ongerichte surveillance – via kabelverkeer – is bij wet verboden. De diensten mogen daarentegen wel door middel van een telefoontap of internettap gerichte communicatie onderscheppen en ongerichte, niet-kabelgebonden telecommunicatie van of naar andere landen onderscheppen.[220] Voor het ongericht aftappen is géén bevoegdheid van de desbetreffende minister nodig, maar voor het gericht aftappen wel.[221]

De verdenking bestaat dat de Nederlandse inlichtingen- en veiligheidsdiensten toegang hebben tot informatie van de NSA. Dit zouden anonieme bronnen binnen de diensten hebben bevestigd. Dit zou de diensten in staat stellen om, via het PRISM-programma, informatie over Nederlandse staatsburgers op te vragen zonder gebruik te maken van een wettelijk verplicht bevelschrift. Volgens de verantwoordelijke minister wordt er echter geen gebruik gemaakt van het PRISM-programma, maar zou uitgewisselde informatie met andere inlichtingendiensten wel informatie kunnen bevatten die onder het PRISM-programma verzameld is.[222]

Volgens de Wiv 2002 mogen de Nederlandse diensten dus helemaal geen communicatieverkeer via de kabel aftappen. De Nederlandse regering is, mede naar aanleiding van de conclusies van een onderzoekscommissie over de Wiv 2002, bezig met het doorvoeren van een nieuwe wet aangaande de inlichtingen- en veiligheidsdiensten om onder andere het onderscheppen van communicatieverkeer via de kabel, en niet alleen via de ether, mogelijk te maken.[223]

---

[219] Logischerwijs is de Wet bescherming persoonsgegevens, waarmee Nederland de Europese richtlijn 95/46/EG in de nationale wetgeving heeft geïmplementeerd, niet van toepassing op verwerking van persoonsgegevens door of ten behoeve van de inlichtingen- en veiligheidsdiensten. Zie art. 2: lid 2 sub b Wet bescherming persoonsgegevens.

[220] Art. 25:1-8 Wiv 2002, Art. 26: 1-5 Wiv 2002 en Art. 27: 1-10 Wiv 2002.

[221] Art. 25: 2 Wiv 2002, Art. 26: 2 Wiv 2002 en Art. 27: 2 Wiv 2002.

[222] NOS, 'Onderzoek naar rol AIVD, MIVD' (versie 3 juli 2013), http://nos.nl/artikel/525332-onderzoek-naar-rol-aivd-mivd.html (3 mei 2016); Zie ook: Rijksoverheid, 'Geen onbelemmerde toegang tot internet en telefoon voor AIVD en MIVD' (versie 21 juni 2013), https://www.rijksoverheid.nl/actueel/nieuws/2013/06/21/geen-onbelemmerde-toegang-tot-internet-en-telefoon-voor-aivd-en-mivd (3 mei 2016).

[223] Zie hoofdstuk 5 van het jaarverslag 2014-2015 van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten: CTIVD, Jaarverslag 2014-2015 (Jaarverslag Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, Den Haag 2015) 27-29.

2.3 Nationale veiligheid, privacy en surveillance

Zowel in de VS als in (lidstaten van) de EU worden er in de wetgeving waarborgen gesteld om de privacy van burgers te beschermen. De privacywetgeving is vaak niet van toepassing op de activiteiten van de inlichtingen- en veiligheidsdiensten. Zowel in de VS als in de EU is de privacywetgeving primair gericht op de verhouding tussen burger en economie enerzijds en mis- en/of gebruik van gegevens door de overheid anderzijds (zie in de VS de *Privacy Act*, in de EU de richtlijn 95/46/EG).

In de VS is die privacywetgeving geregeld via speciale sectorale wetgeving: privacyrichtlijnen die per sector in aparte wetgeving vastgesteld worden. Zo geldt de *Privacy Act* voor gegevens die in handen van de overheid zijn. In de EU is richtlijn 95/46/EG, de algemene richtlijn, per lidstaat geïmplementeerd in nationale wetgeving. Voor de vijf EU-lidstaten die hierboven aan bod zijn gekomen zijn dit: de *Data Protection Act* 1998 in het Verenigd Koninkrijk, de *Bundesdatenschutzgesetz* in Duitsland, de *Personuppgiftslagen* in Zweden, de *Loi informatique et libertés* in Frankrijk en de Wet bescherming persoonsgegevens in Nederland.

Exemplarisch voor het feit dat de Europese richtlijn betrekking heeft op privacy en databescherming vanuit een economisch oogpunt is het feit dat de nationale wetgeving van de Europese landen uitzonderingen kent op het gebied van nationale veiligheid. Zo hebben Franse vertegenwoordigers van justitie geen toestemming van de Franse toezichthouder nodig voor het verzamelen en verwerken van data bij het uitvoeren van hun taak om 'betrokkenen' te beschermen.[224] In artikel 2 van de Nederlandse Wet bescherming persoonsgegevens staat zelfs expliciet dat die wet geen betrekking heeft verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten.[225] Ook in de Duitse, Britse en Zweedse wet zijn uitzonderingen opgenomen met betrekking tot (bescherming van) nationale veiligheid.

De invloed van de Europese databeschermingsrichtlijn op het handelen van nationale inlichtingen- en veiligheidsdiensten is zodoende beperkt te noemen. Nationale veiligheid is in principe de uitsluitende verantwoordelijkheid van elke lidstaat en valt daarmee buiten de autoriteit van de EC.[226] Doordat onder de vlag van de EU echter ook een gemeenschappelijk buitenlands- en veiligheidsbeleid is opgezet, waardoor de Unie ook de internationale en eigen interne veiligheid dient te waarborgen, heeft de Unie toch gedeelde belangen met de individuele lidstaten op

[224] Art. 8: *Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* en Art. 25: 3 *Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*.
[225] Art. 2 lid 2 sub b Wet bescherming persoonsgegevens.
[226] Art. 4: 2 Verdrag betreffende de EU.

veiligheidsgebied.[227] Dit heeft gevolgen voor de maatregelen die lidstaten onder het mom van nationale veiligheid mogen nemen:

> *'National measures which seek to maintain national security may not interfere with the fundamental freedoms and, insofar as they fall within the scope of EU law, must respect fundamental rights as understood in the EU legal order.'*[228]

Hierdoor is een belangrijk punt van frictie, dat zich in de praktijk voor doet, de concrete invulling die 'nationale veiligheid' wordt gegeven. Het begrip staat namelijk niet omschreven in Europese wetgeving, met als gevolg dat de nationale definities vaag blijven. Een voorbeeld is de situatie in het Verenigd Koninkrijk waar er geen officiële definitie bestaat van het begrip 'nationale veiligheid'. De politiek hanteert een brede definitie, die ook door de rechters als dusdanig wordt erkend, om op veel verschillende terreinen de veiligheid van het land te kunnen waarborgen. Daarbij gaat het niet alleen om spionage of militaire dreigingen, maar ook om energieveiligheid, pandemieën en cyberdreigingen.[229] Het hanteren van een dergelijke brede definitie is te rechtvaardigen, maar creëert tegelijkertijd wel een grijs handelingsgebied voor inlichtingendiensten.

In de VS worden met betrekking tot nationale veiligheid eveneens brede definities gehanteerd. Een voorbeeld hiervan is de nieuwe definitie voor *foreign intelligence information* die in 2008 in FISA werd opgenomen. *Foreign intelligence information* kan volgens artikel 1801 elke vorm van informatie, met betrekking tot een in het buitenland gevestigde politieke organisatie, inhouden die relateert aan het uitvoeren van buitenlands beleid door de VS.[230] Hierdoor is het legaal voor de NSA om politieke en/of economische surveillance uit te voeren op (elektronische) communicatieverkeer van buitenlanders.

Officieel wordt binnen de EU het recht op privacy beschermd door artikel 8 van het EVRM en artikel 7 en 8 van het Handvest van de Grondrechten van de EU, wat sinds de invoering van het Verdrag van Lissabon officiële wetgeving is. Daarnaast geldt binnen de VS het Vierde Amendement als een belangrijke bescherming tegen de overheid. Toch wordt door wetgeving, zowel in de EU als de VS, de grenzen opgezocht van de wettelijke mogelijkheden en dat wringt zo nu en dan. Het is niet voor niets

[227] Art. 21: lid 2 sub a en sub c Verdrag betreffende de EU en Art. 4: lid 2 sub j Verdrag betreffende de werking van de EU.
[228] Diamond Ashiagbor, Nicola Countouris en Ioannis Lianos (red.), *The European Union after the Treaty of Lisbon* (Cambridge 2012) 57.
[229] *Big Brother Watch and Others v. United Kingdom*, no. 58170/13, 30 september 2013, rechterlijke overweging 105 - 112.
[230] Art. 1801: sub a en sub e *Foreign Intelligence Surveillance Act*.

dat aan beide kanten van de oceaan rechters zich buigen, of hebben gebogen, over de bevoegdheden van de inlichtingendiensten.

Daar komen ook nog andere zaken bij kijken. Zo speelt in de VS de discussie dat buitenlanders niet hetzelfde recht op privacy zouden hebben als Amerikanen, terwijl de VS wel degelijk het Internationaal verdrag inzake burgerrechten en politieke rechten heeft geratificeerd.[231] Ook is het opvallend dat de VS in de jaren '60 een van de eerste landen ter wereld was waar werd erkend dat de privacy van individuen moest worden beschermd tegen de mogelijkheden om data te vergaren en elektronisch te verwerken.

Het vergaren van metadata door middel van data mining lijkt inmiddels gemeengoed te worden voor de meeste inlichtingendiensten. Onder meer de VS, Frankrijk en het Verenigd Koninkrijk maken gebruik van data mining om aan informatie te komen. Metadata zijn *an sich* niet slecht, maar de onduidelijke praktijken van inlichtingendiensten zorgden ervoor dat vaak niet duidelijk is volgens welke regels de gegevens worden verzameld, hoeveel er wordt verzameld en hoe de gegevens vervolgens worden gebruikt.

Het is zeer onwaarschijnlijk dat alle lidstaten van de EU schrokken van de onthullingen van Snowden. Van de inlichtingendiensten van een aantal Europese landen is namelijk bekend dat die zich ook al bezig hielden met massasurveillance. Tegelijkertijd kon het nieuws voor het Witte Huis echtergeen verrassing betekenen, maar was dat het dan wel voor Brussel? In het volgende hoofdstuk staan de reacties op de onthullingen van Snowden centraal en de gevolgen die eruit voortkwamen. Is er een nalatenschap van Snowden merkbaar voor de inlichtingendiensten? Aangezien de rechterlijke machten daar een belangrijke rol in spelen, en hebben gespeeld, zullen die – als onafhankelijke macht binnen de trias politica – zeker niet vergeten worden. De verontwaardigde reactie vanuit Europa en de naïeve, verontschuldigende reactie in de VS uit de doeken worden gedaan.

[231] Eén van de beschermende rechten van de mens is volgens het verdrag artikel 17: recht op privacy.

3 Post-Snowden

Sinds de onthullingen van Edward Snowden over de surveillanceprogramma's van de VS en diens Europese bondgenoten, is voor veel mensen de opvatting over het concept privacy veranderd. Consumenten, maar ook bedrijven, hebben zich verontwaardigd uitgelaten over de vraag wat privacy eigenlijk inhoudt en welke rol metadata daar in speelt. Uit de berichtgeving werd duidelijk dat de NSA metadatagegevens van alle telefoongesprekken binnen de VS zou opslaan, data van *non-US persons* zou verzamelen en opslaan en de Britse GCHQ die informatie van trans-Atlantische glasvezelkabels zou onderscheppen. Later bleek dat de NSA verschillende bevriende staatshoofden afluisterde en dat communicatieverkeer vanuit datacenters van grote Amerikaanse bedrijven werd onderschept.[232]

De reacties van de uitvoerende overheden van de VS en de EU hierop zijn zeer interessant om in kaart te brengen. De onthullingen konden namelijk in eerste instantie op veel verontwaardiging rekenen in zowel de VS als Europa, maar inmiddels zijn we al weer bijna drie jaar verder. En er is in de tussentijd veel gebeurd: aanslagen in Europa, de opkomst van Islamitische Staat, maar ook Amerikaanse en Europeaanse rechters die over de grootschalige surveillanceprogramma's hebben geoordeeld. Wat kan uit al die ontwikkelingen worden opgemaakt? Is er een andere houding zichtbaar ten opzichte van grootschalige surveillance door de Amerikaanse overheid en die van de EU, of is er na Snowden in feite niks veranderd?

3.1 Initiële reacties in de Verenigde Staten en Europa

Het is niet verbazingwekkend dat het Witte Huis en Brussel in eerste instantie allebei verontwaardigd reageerde op de feiten uit de onthullingen van Snowden. Viviane Reding, toenmalig vicevoorzitter van de EC, kwam al snel met de volgende reactie aangaande de gevolgen voor EU-lidstaten. Ze refereerde aan het feit dat staten niet zomaar geheime, grootschalige surveillance mogen toepassen onder het mom van 'nationale veiligheid':

[232] Scott Shane, 'No Morsel Too Minuscule for All-Consuming N.S.A.' (versie 2 november 2013), http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?pagewanted=2&_r=0 (9 mei 2016); Barton Gellman en Ashkan Soltani, 'NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say' (versie 30 oktober 2013), https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (9 mei 2016).

> *The concept of national security does not mean that 'anything goes': States do not enjoy an unlimited right of secret surveillance. In Europe, also in cases involving national security, every individual – irrespective of their nationality – can go to a Court, national or European, if they believe that their right to data protection has been infringed. Effective judicial redress is available for Europeans and non-Europeans alike. This is a basic principle of European law.*[233]

Reding, die naast vicevoorzitter ook eurocommissaris voor Justitie was, had enkele dagen voor bovenstaande persconferentie ook de Amerikaanse minister van Justitie gewaarschuwd dat de praktijken van de NSA ernstige consequenties konden hebben voor de grondrechten van EU-burgers. Daarbij legde ze specifiek de nadruk op het feit dat door Amerikaanse wetgeving, zoals de *Patriot Act*, bedrijven gedwongen kunnen worden om gegevens van EU-burgers af te staan aan de Amerikaanse autoriteiten, terwijl er officiële kanalen bestaan voor samenwerking op justitieel vlak.[234]

De aanvankelijke verontwaardiging vanuit de EC werd echter niet gevolgd door een krachtige pan-Europese reactie. Daarvoor lagen de lidstaten, die hun eigen bevoegdheden op het gebied van 'nationale veiligheid' wilden veiligstellen, dwars. Een voorbeeld hiervan was de werkgroep, tussen de EU en de VS, over surveillance en privacy die werd opgezet. Op aandringen van de lidstaten zou die werkgroep met twee verschillende trajecten werken. Binnen één traject zouden onderhandelaren van de EU en de VS zich focussen op databescherming, terwijl de lidstaten op bilateraal niveau met de VS zouden praten over veiligheid en surveillance.[235]

De Europese media sloegen in eerste instantie aan op het feit dat de NSA volgens de wet veel meer mogelijkheden had om communicatieverkeer van niet-Amerikanen te onderzoeken dan van Amerikanen. Mede hierdoor daalde dan ook het Europese vertrouwen in de VS. Vooral in Duitsland was het percentage dat in de VS een betrouwbare bondgenoot zag extreem laag: slechts 35 procent. Overigens was ook het vertrouwen in de Britse overheid afgenomen: van 80 procent naar 50 procent.[236] Toch betekende al die media-aandacht niet per se dat het vertrouwen in de VS afnam.

---

[233] Viviane Reding, 'PRISM scandal: The data protection rights of EU citizens are non-negotiable' (versie 22 oktober 2015), http://europa.eu/rapid/press-release_SPEECH-13-536_en.htm (9 mei 2016).
[234] Viviane Reding, Brief aan de Amerikaanse minister van justitie Eric Holder (10 juni 2013), beschikbaar via http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/p6_ltr_holder_/p6_ltr_Holder_en.pdf (9 mei 2016).
[235] Anthony Dworkin, Surveillance, privacy and security: Europe's confused response to Snowden (Beleidsmemo European Council on Foreign Relations, z.p. 2015) 3.
[236] *Spiegel Online*, 'Spying Fallout: German Trust in United States Plummets' (versie 8 november 2013), http://www.spiegel.de/international/germany/nsa-spying-fallout-majority-of-germans-mistrust-united-states-a-932492.html (9 mei 2016).

Vooral in Frankrijk, Zweden en het Verenigd Koninkrijk nam de publieke steun voor de VS amper af.[237] Wellicht niet geheel toevallig ook landen waarvan de inlichtingendiensten, volgens de vrijgegeven documenten van Snowden, nauwe banden zouden hebben met de VS.

Vanwege de beperkte mogelijkheden voor de EC om invloed uit te oefenen op het veiligheidsbeleid van individuele lidstaten, heeft de EC zich gericht op de commerciële regulering. Daarbij is de strategie van de commissie geweest om de regels voor technologiebedrijven zo vorm te geven dat Europeanen zo min mogelijk bloot kunnen worden gesteld aan Amerikaanse surveillance. Hiervoor werden eind 2013 voorstellen gedaan om de *Safe Harbour*-overeenkomst met de VS te wijzigen. De Amerikaanse regering wilde echter niet akkoord met een tweetal wijzigingen: meer transparantie vanuit bedrijven en beperking van de reikwijdte voor wat betreft de uitzondering van 'strikt noodzakelijk en proportioneel' gebruik van (Europese) data ter bescherming van de nationale veiligheid.[238] Hierdoor raakten de EU en de VS op dat moment in een impasse.

De initiële reactie van de EC was dus tamelijk fel, waarbij de aandacht werd gevestigd op de schending van het fundamentele recht op privacy van EU-burgers. Doordat de macht van Commissie op het gebied van nationale veiligheid erg beperkt is, was zij niet in staat om lidstaten te straffen en/of te corrigeren voor het ondernemen van grootschalige surveillance. Daarvoor moest de Commissie zich gaan richten op de commerciële regulering: hét beleidsterrein van de EC.

In de VS kwam het Witte Huis kort na de onthullingen van Snowden met een reactie waarin werd gesteld dat er geen illegale activiteiten werden ondernomen door de NSA. Vanwege de onrust die in de VS ontstond over de mogelijke binnenlandse activiteiten van de dienst, stelde president Obama dat de NSA niet naar binnenlandse gesprekken luisterde zonder een bevelschrift. Het leek hierdoor wel of de Amerikaanse overheid de onthullingen over het verzamelen van metadata minder groot wilde maken. Obama adresseerde namelijk het wettelijke aspect van de onthullingen, maar liet de impact op privacy en het gebrek aan transparantie achterwegen. De president gaf wel aan dat de surveillanceprogramma's werden gesteund door volksvertegenwoordigers en de rechterlijke macht. Tegelijkertijd zou een open discussie over het evenwicht tussen privacy- en veiligheidsaspecten 'gezond zijn voor de Amerikaanse democratie'.[239]

[237] Anthony Dworkin, Surveillance, privacy, and security, 2.
[238] Europese Commissie, 'Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU' (27 november 2013), beschikbaar via http://ec.europe.eu/justice/data-protection/files/com_2013_847_en.pdf (9 mei 2016).
[239] Peter Finn en Ellen Nakashima, 'Obama defends sweeping surveillance efforts' (versie 7 juni 2013), https://www.washingtonpost.com/politics/obama-defends-sweeping-surveillance-efforts/2013/06/07/2002290a-cf88-11e2-9f1a-1a7cdee20287_story.html (9 mei 2016).

Het privacyaspect en het gebrek aan transparantie kwamen wel aan bod toen president Obama op 8 augustus een persconferentie hield. Tijdens de persconferentie vestigde Obama specifiek de aandacht op het gebrek aan vertrouwen van de Amerikaanse bevolking in de programma's van de inlichtingendiensten en het herstellen van dat vertrouwen. Om dat te bewerkstelligen kwam de president met vier voorstellen. Het eerste voorstel was het hervormen van Sectie 215 van de *Patriot Act*, het tweede voorstel betrof het samen met het Congres herstellen van het vertrouwen in het toezicht van de FISC, als derde was meer transparantie vanuit de inlichtingengemeenschap noodzakelijk en ten slotte zou er een onafhankelijke expertgroep worden ingesteld om de inlichtingengemeenschap en de surveillancetechnologieën onder de loep te nemen.[240]

Deze initiatieven van de president resulteerden eind 2013 in het rapport *Liberty and Security in a Changing World*. Dit rapport was afkomstig van de expertgroep die was opgericht op initiatief van het Witte Huis: *The President's Review Group on Intelligence and Communications Technologies*. Niet lang daarna kwam de *Privacy and Civil Liberties Oversight Board* begin 2014 met een rapport aangaande sectie 215 van de *Patriot Act*: *Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and the Operations of the Foreign Intelligence Surveillance Court*.

III.II Gevolgen in Washington en Brussel

Een gebrek aan vertrouwen vormde de kern van zowel de Amerikaanse reactie als de Europese reactie. Een belangrijk verschil was dat de reactie vanuit het Witte Huis zich centreerde op een gebrek aan vertrouwen van de eigen bevolking, terwijl vanuit de EC een gebrek aan vertrouwen in de trans-Atlantische relatie centraal stond.

3.2.1 Reactie in de Verenigde Staten

In de VS vond dat gebrek aan vertrouwen weerklank in doorgevoerde hervormingen, waarvan de eerste hervorming de uitgave was van *Presidential Policy Directive 28* (PPD-28), getiteld *Signals Intelligence Activities*.[241] Met de uitgifte van dit presidentieel decreet reageerde Obama op kritiek van de *Review Group* dat er bij surveillance een onderscheid gemaakt wordt tussen Amerikanen en

[240] Het Witte Huis, Remarks by the President in a Press Conference (9 augustus 2013), beschikbaar via https://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference (9 mei 2016).
[241] Het Witte Huis, Presidential Policy Directive/PPD-28 (17 januari 2014), beschikbaar via www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf (9 mei 2016).

buitenlanders. De voornaamste kritiek in het rapport was gebaseerd het feit dat de VS geen onderscheid zou moeten maken op basis van nationaliteit als het aankomt op surveillance.[242]

EO 12333 werd door PDD-28 op een belangrijk punt aangepast: het gelijk behandelen van Amerikanen en niet-Amerikanen voor wat betreft de minimalisatieprocedures voor het delen en bewaren van persoonlijke gegevens, toegang tot data en de veiligheid van opgeslagen data. Ook werden individuele bevelschriften van de FISC verplicht gesteld voordat de NSA toegang kon krijgen tot data die door telecombedrijven zou worden verzameld. Met dit laatste werd een einde gemaakt aan het gebruik van brede, algemene bevelschriften als autorisatiemiddel voor surveillance. Daarnaast werd met PDD-28 het afluisteren van regeringsleiders van bevriende landen verboden – tenzij er een dwingend nationaal veiligheidsdoel zou zijn – en werd het de NSA alleen nog maar toegestaan om twee, in plaats van drie, "hops" van een gekozen doelwit af te luisteren.[243]

Obama besloot daarnaast echter ook om een aantal belangrijke aanbevelingen niet over te nemen. Zo raadde de adviesgroep aan om telefoongegevens voortaan in bezit te laten van private bedrijven in plaats van dat de overheid de gegevens verzameld. Obama besloot echter om deze beslissing niet over te nemen. Een andere belangrijke aanbeveling die niet werd overgenomen was het plan om de periode dat telefoongegevens bewaard mochten worden terug te brengen van vijf naar twee jaar.[244]

De uitgifte van PPD-28 vormde een uniek moment. Het betekende namelijk dat de Amerikaanse overheid voor de eerste keer erkende dat buitenlanders privacybelangen hebben. Daarnaast werden er basisregels opgesteld om te bepalen hoe er met data van buitenlanders omgegaan diende te worden. Ondanks dit unieke aspect, en de andere hervormingen, blijft nog veel informatie rondom reikwijdte en de invloed van EO 12333 op de werkwijze van de NSA nog geheim.[245]

---

[242] In het rapport wordt gesteld dat wellicht het belangrijkste argument voor het respecteren van de privacy van buitenlanders: '*is the simple and fundamental issue of respect for personal privacy and human dignity—wherever people may reside. The right of privacy has been recognized as a basic human right that all nations should respect. Both Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights proclaim that "No one shall be subjected to arbitrary or unlawful interference with his privacy. . . ." Although that declaration provides little guidance about what is meant by "arbitrary or unlawful interference," the aspiration is clear. The United States should be a leader in championing the protection by all nations of fundamental human rights, including the right of privacy, which is central to human dignity.'* Zie Clarke e.a., *The NSA Report*, 155-156.

[243] Analisten van de NSA mochten gegevens van telefoongesprekken onderzoeken van mensen die tot drie connecties, of 'hops', van enig telefoonnummer – waarvan er een redelijke verwachting bestond dat er een verband met terrorisme was – verwijderd waren.

[244] Voor een overzicht van andere aanbevelingen van de *Review Group*, zie: Josh Keller e.a., 'Obama's Changes to Government Surveillance' (versie 17 januari 2014), http://www.nytimes.com/interactive/2014/01/17/us/nsa-changes-graphic.html (9 mei 2016).

[245] Het rapport *Overseas Surveillance in an Interconnected World* eindigt met een aantal nog te beantwoorden vragen aangaande EO 12333. De vragen gaan over mogelijk onbekende regelgeving die overzeese

Belangrijke aandachtspunten zijn de standaardpraktijk van bulkcollectie bij buitenlandse inlichtingenvergaring, het uitvoeren van zoekacties op basis van de tekstuele inhoud van communicatieverkeer in plaats van doelgerichte zoekacties op personen en het bestaan van veel uitzonderingen om de verplichte bewaarperiode van vijf jaar te kunnen verlengen.[246] Tegelijkertijd vormen de uitgevoerde operaties onder EO 12333 het grootste aandeel van de Amerikaanse surveillanceactiviteiten. Dat die operaties in het buitenland worden uitgevoerd, betekent niet dat Amerikanen geen doelwit kunnen vormen. Tegenwoordig gaan data- en informatiestromen immers de hele wereld over.

Het rapport van de *Privacy and Civil Liberties Oversight Board* (PCLOB) over sectie 215 van de *Patriot Act* verscheen niet lang na het rapport van de *Review Group*. De onthullingen over sectie 215 konden op zeer veel kritiek rekenen binnen de VS. Ook de PCLOB had een duidelijk oordeel over het deel van de wet waarmee het in bulk verzamelen van gegevens over telefoongesprekken mee werd gelegitimeerd. De toezichthouder concludeerde dat het verzamelen van telefoongegevens slechts beperkte voordelen opleverde in het bestrijden van terrorisme. Alhoewel de leden van de PCLOB niet unaniem waren in hun oordeel dat het programma in strijd was met de wet, raadden ze wel aan om het programma stop te zetten. Het programma ontbrak het namelijk aan een levensvatbare wettelijke basis: de redenatie van de overheid dat de FBI relevante bedrijfsgegevens voor een onderzoek mag bemachtigen en dat de daarom de NSA de toestemming heeft om telefoongegevens in het hele land op te vragen.[247]

Een andere aanbeveling die door president Obama werd overgenomen was het instellen van een panel van onafhankelijke advocaten die als openbare verdedigers zullen optreden in specifieke rechtszaken – waar nodig – over de geheime surveillanceprogramma's. Hiermee kwam president Obama tegemoet aan de kritiek dat er bij de FISC slechts het verhaal van de uitvoerende macht gehoord zou worden.[248]

---

inlichtingensurveillance reguleert; het beperkte openbare toezicht op de inlichtingengemeenschap vanuit onder andere het Congres; hoe en in welke hoeveelheid informatie in het buitenland wordt verzameld en hoe informatie wordt gebruikt, bewaard en gedeeld. Zie Toh e.a., Overseas Surveillance in an Interconnected World, 35-37.

[246] Elizabeth Goitein, 'Overseas Surveillance in an Interconnected World' (versie 17 maart 2016), https://www.justsecurity.org/29994/overseas-surveillance-interconnected-world/#more-29994 (9 mei 2016).

[247] Charlie Savage, 'Watchdog Report Says N.S.A. Program is Illegal and Should End' (versie 23 januari 2014), http://www.nytimes.com/2014/01/23/us/politics/watchdog-report-says-nsa-program-is-illegal-and-should-end.html?_r=0 (9 mei 2016).

[248] Er zijn vragen te stellen wat betreft de wettelijke positie van deze advocaten, zie: Marty Lederman en Steve Vladeck, 'The Constitutionality of a FISA "Special Advocate"' (versie 4 november 2013), https://www.justsecurity.org/2873/fisa-special-advocate-constitution/ (9 mei 2016).

Het tweede rapport van de PCLOB, dat in juli 2014 werd uitgebracht, verdedigde, in tegenstelling tot het rapport in het begin van het jaar, wel de programma's voor internetsurveillance van de NSA onder sectie 702 van de FISA. Het onderdeel heeft de overheid namelijk in staat gesteld om snel en op effectieve wijze meer buitenlandse inlichtingen te vergaren dan anderszins mogelijk zou zijn.[249]

Toen de *USA Freedom Act* op 2 juni 2015 tot wet werd getekend door president Obama betekende dat er een aantal aanpassingen werden ingesteld aangaande de praktijken onder Sectie 215 van de *Patriot Act*.[250]

De voornaamste wijziging vormde uiteraard de beëindiging van het programma waarmee de NSA in bulk gegevens van telefoongesprekken verzamelde. Daarnaast werden echter ook wijzigingen doorgevoerd die de FISC aangingen. Voor de FISC werd het voortaan mogelijk om onafhankelijke visies bij nieuwe zaken te horen en daarnaast werden de mogelijkheden uitgebreid om in hoger beroep te gaan na uitspraken van de FISC. Aangaande meer transparantie betekende de wet het instellen van openbare rapportage over het functioneren van de openbare verdedigers bij de FISC en het feit dat bedrijven voortaan informatie mochten vrijgeven over de ontvangst van productieorders voor bepaalde gegevens onder FISA. Verder werd met de wet ook vastgelegd dat er voortaan meer openbare informatie zou worden gegeven over besluiten van de FISC.[251]

Verder zijn er sinds juli 2014 ook hervormingen doorgevoerd die betrekking hebben op sectie 702 van FISA. De meest in het oog springende van die hervormingen betreft eveneens de FISC. Het Witte Huis heeft namelijk één document opgesteld, waarin alle relevante regels zijn opgesteld voor het uitvoeren van operaties onder het sectie 702-programma, en deze opgestuurd naar de FISC. Tamelijk opmerkelijk is het dus dat een dergelijk document nog niet bestond voor de rechtbank die moet oordelen over aanvragen voor bevelschriften onder dat regime.[252]

De totstandkoming van de *USA Freedom Act* betekende de eerste keer sinds 11 september 2001 dat de surveillancemogelijkheden van de Amerikaanse overheid werden beperkt. Toch dienen er

[249] David E. Sanger, 'U.S. Privacy Panel Backs N.S.A.'s Internet Tapping' (versie 2 juli 2014), http://www.nytimes.com/2014/07/03/world/privacy-board-backs-nsa-program-that-taps-internet-in-us.html (9 mei 2016).
[250] De *USA Freedom Act* is een acroniem voor *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act*.
[251] *Privacy and Civil Liberties Oversight Board*, Fact Sheet: PCLOB Recommendations Implemented by the Government (5 februari 2016), beschikbaar via https://www.pclob.gov/library/Recommendations_Assessment_FactSheet_20160205.pdf (9 mei 2016).
[252] *Privacy and Civil Liberties Oversight Board*, Fact Sheet: PCLOB Recommendations Implemented by the Government (5 februari 2016), beschikbaar via https://www.pclob.gov/library/Recommendations_Assessment_FactSheet_20160205.pdf (9 mei 2016).

een tweetal kanttekeningen geplaatst te worden bij deze mijlpaal. Sectie 702 van FISA en EO 12333 blijven van kracht en waar onder sectie 215 van de *Patriot Act* metadata werd verzameld over telefoongesprekken, is het onder de andere twee voorzieningen mogelijk om daadwerkelijke communicatieverkeer te onderscheppen, zonder individueel bevelschrift.

Daarnaast blijft het toezicht op de inlichtingendiensten in de VS beperkt. Alhoewel de overheid steeds heeft aangegeven dat het toezicht op de inlichtingendiensten omvangrijk is, valt dat slechts in beperkte mate te controleren. Zo is onbekend hoe het toezicht vanuit het Congres eruitziet voor EO 12333: hoe vaak wordt er vanuit het Witte Huis informatie gestuurd naar de inlichtingencommissies en welke informatie wordt gedeeld? Ook wat betreft de toekenning van het budget, het functioneren van zelfstandige opdrachtnemers, intern toezicht en de effectiviteit van de inlichtingenactiviteiten onder EO 12333 bestaat er geen duidelijkheid.

De *National Security Act* stelt de inlichtingendiensten als taak om de inlichtingencommissies in het Congres op de hoogte te houden van inlichtingenactiviteiten, maar de daadwerkelijke plicht om te informeren is beperkt. Dit komt doordat er in de wet verschillende beperkingen zijn vastgelegd voor het delen van informatie. Zo hoeft de president slecht een beperkt aantal congresleden te informeren als de inlichtingen betrekkingen hebben op zogeheten *covert actions* die belangrijk zijn om vitale Amerikaanse belangen te beschermen. Daarbovenop beperkt de uitvoerende macht geregeld de notificaties van inlichtingenprogramma's die als zeer gevoelig worden beschouwd. Dit betreft geen officiële procedure, maar staande praktijk. In sommige gevallen, wanneer het gaat om *'sensitive intelligence sources and methods or other exceptionally sensitive matters'*, is überhaupt geen notificatie noodzakelijk.[253]

Afgezien van de beperkte informatievoorziening vanuit de inlichtingengemeenschap hebben de, in totaal, 37 leden van de twee inlichtingencommissies van het Congres te weinig capaciteit om de Amerikaanse inlichtingengemeenschap effectief te controleren. Dat is overigens niet verbazingwekkend wanneer men bedenkt dat de inlichtingengemeenschap uit 17 diensten bestaat met honderdduizenden medewerkers, een openbaar budget van bijna 70 miljard dollar, terwijl er surveillanceoperaties worden uitgevoerd waarbij dagelijks miljoenen keren per dag elektronisch communicatieverkeer en andere data wordt verzameld.[254]

Het interne toezicht wordt door de overheid beschreven als uitvoering en gelaagd, maar door de geheimhouding rondom inlichtingenoperaties is het lastig om vast te stellen of de interne toezicht op de juiste manier functioneert. Daarnaast zou het interne toezicht binnen diensten doorspekt zijn

[253] Toh e.a., Overseas Surveillance in an Interconnected World, 32.
[254] Ibidem, 33.

van legalisme, waarbij er dus veel meer wordt gehandeld naar de letter van de wet in plaats van de geest van de wet. Hierdoor zou er weinig plaats zijn voor het afwegen verschillende belangen en mogelijkheden om tot beleid te komen waarmee een goede balans wordt gecreëerd tussen veiligheid en privacy.[255]

Het toezicht op uitvoering van surveillanceprogramma's onder sectie 702 van FISA wordt bij de NSA geregeld door verschillende interne onderdelen. Deze zien er op toe dat er binnen de dienst wordt gehandeld in overeenstemming met de vastgestelde doelwit- en minimalisatieprocedures. Dit betekent bijvoorbeeld dat de NSA verplicht is om elk besluit om iemand te volgen vast te leggen. Deze gegevens worden herzien door de *National Security Division* van het ministerie van Justitie en de *Office of the Director of National Intelligence*. Deze organisaties bekijken daarnaast ook de minimalisatieprocedures. Verder is ook de inspecteur-generaal van de desbetreffende dienst belast met het beoordelen van het sectie 702-programma. De rol van de FISC is het beoordelen van certificaten voor het sectie 702-programma en de bijbehorende doelwit- en minimalisatieprocedures en om aan te geven of ze in overeenstemming zijn met de statutaire regels en het Vierde Amendement. De rechtbank kan ook al uitgegeven certificaten herzien als die het bericht krijgt dat er geen sprake is van overeenstemming met het uitgegeven certificaat bij de uitvoering. Het toezicht vanuit het Congres is dusdanig geregeld dat de minister van Justitie een halfjaarlijks rapport verschaft waarin de diverse beoordelingen en besluiten van de verschillende instanties in worden meegenomen.[256]

3.2.2 Reactie in de Europese Unie

Zoals hierboven al duidelijk werd, werd er door de EC afkeurend gereageerd op de onthulde praktijken van de NSA. De EC was echter niet in staat om op beleidsniveau aanpassingen te doen om surveillance door de VS tegen te gaan. Daarmee zou de EC immers in het vaarwater komen van de nationale veiligheid. Daarom gooide de EC het over een andere boeg: koers blijven houden.

Het vasthouden aan de gekozen koers valt ook op te maken uit het feit dat de EC besloot om een oproep van het Europees Parlement, om de gegevensuitwisseling over vliegtuigpassagiers en banktransacties op te schorten, naast zich neer te leggen.[257] De Commissie dreigde wel bij de VS dat de *Safe Harbour*-overeenkomst mogelijk opgeschort kon worden als de VS niet de noodzakelijke hervormingen zou doorvoeren en de Commissie riep zowel de lidstaten als de VS op om gerichte acties

[255] Ibidem, 33.
[256] Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Rapport *Privacy and Civil Liberties Oversight Board* (z.p. 2014) 66-77.
[257] Europese Commissie, 'Rebuilding Trust in EU-US Data Flows' (Paper Europese Commissie, Brussel 2013) 4-5. Beschikbaar via http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf (10 mei 2016).

te ondernemen op het gebied van databescherming.[258] De Commissie maakte daarmee gebruik van de ophef rondom Snowden om de onderhandelingen over datahervormingen een impuls te geven.

De EC kwam namelijk al in 2012 met een voorstel voor een uitgebreide herziening van de bestaande richtlijn voor de bescherming van persoonsgegevens. De achterliggende redenatie was dat de bestaande richtlijn stamde uit de beginjaren van het internet, terwijl sindsdien globalisering en technologische vernieuwingen steeds omvangrijker zijn geworden. Eurocommissaris Reding noemde de nieuwe, aanstaande EU-regelgeving een antwoord op de noodkreet van Snowden en ze spoorde de lidstaten dan ook in juni 2014 aan om gehoor te geven aan die oproep.[259]

De nieuwe regelgeving, die dit jaar afgerond wordt en die uiterlijk in 2018 in de nationale wetgeving moet zijn geïmplementeerd, moet de bescherming van persoonsgegevens in de verschillende lidstaten verder harmoniseren. Regels die hier toe dienen zijn onder meer het instellen van een verplicht minimum aan maatregelen om het lekken van persoonsgegevens te voorkomen, regels voor het gebruik en inkijken van persoonlijke gegevens bij politieonderzoek en bedrijven buiten de EU moeten aan de Europese eisen voldoen wanneer zij in de EU hun diensten gaan aanbieden (denk hierbij aan de *Safe Harbour*-overeenkomst).[260]

Ondertussen was de verontwaardiging bij verschillende EU-lidstaten merkbaar. Alhoewel in sommige gevallen de verontwaardigde reactie wellicht primair gedreven werd door geschokte reacties onder de eigen bevolking, was de aangenomen resolutie over digitale privacy bij de Algemene Vergadering bij de Verenigde Naties wel degelijk het gevolg van (onder meer) Europees handelen. De resolutie, die in november 2013 werd aangenomen, werd onder meer gesteund door Duitsland en Frankrijk.[261] Tot concrete hervormingen leidde het rapport van de Hoge Commissaris voor de mensenrechten, dat in juli 2014 werd gepresenteerd en was opgesteld in reactie op de resolutie, echter niet.[262]

---

[258] Europese Commissie, 'European Commission calls on the U.S. to restore trust in EU-U.S. data flows' (Persverklaring Europese Commissie, 27 november 2013). Beschikbaar via http://europa.eu/rapid/press-release_IP-13-1166_en.pdf (10 mei 2016).

[259] Kelly Fiveash, 'EU ministers respond sleepily to Viv Reding's 'Snowden wake-up call' on data protection' (versie 9 juni 2014), http://www.theregister.co.uk/2014/06/09/viv_reding_justice_council_of_ministers_data_protection/ (11 mei 2016).

[260] Zie voor een uitgebreider overzicht van de nieuwe regels: Europa Nu, 'Bescherming van persoonsgegevens in Europa' (versie 10 mei 2016), https://www.europa-nu.nl/id/vhkejco8liwc/bescherming_van_persoonsgegevens_in (10 mei 2016).

[261] Ewen McAskill en James Ball , 'UN surveillance resolution goes ahead despite attempts to dilute language' (versie 21 november 2013), http://www.theguardian.com/world/2013/nov/21/un-surveillance-resolution-us-uk-dilute-language (11 mei 2016).

[262] Anthony Dworkin, Surveillance, privacy, and security, 3.

De Europese verontwaardiging was echter wel misplaatst, aangezien veel Europese landen tegelijkertijd wisten dat de eigen nationale inlichtingendiensten ook aan (grootschalige) surveillance deden en dat die diensten samenwerkten met de NSA, soms op grote schaal. Het was Edward Snowden die sprak over een 'Europese bazaar' voor het verzamelen van data, waarbij Europese inlichtingendiensten data verzamelden over andere landen en onderling uitwisselden indien noodzakelijk. Op deze manier werden wettelijke beperkingen ontweken.[263]

Hier bovenop komt nog het feit dat veel Europese landen de bevoegdheden voor de inlichtingendiensten sinds Snowden juist hebben verruimd in plaats van beperkt.[264] Islamitische Staat vormt een blijvende bedreiging voor de interne veiligheid in Europa. Bovendien hebben diverse terroristische aanslagen het Europese continent opgeschrikt: de aanslag in Brussel van 24 mei 2014, de aanslagen in Parijs van 7 januari 2015 en 13 november 2015, de aanslag in Kopenhagen van 14 februari 2015 en recentelijk de aanslagen in Brussel op 22 maart 2016.

Alhoewel in sommige landen, zoals Nederland, al werd gewerkt aan ruimere bevoegdheden voor de inlichtingendiensten vóór deze aanslagen, is in andere landen juist sinds Snowden werk gemaakt van ruimere bevoegdheden.[265] Zo heeft het Franse parlement in juni 2015 een nieuwe wet voor de inlichtingendiensten (*Loi relative au renseignement*) aangenomen. Deze wet ging op 3 oktober 2015 van kracht. Door deze wet moet metadata volgens vooraf ingestelde algoritmes worden verwerkt door de internetproviders. De anonieme data kan na toestemming van de premier, die een niet-bindend advies krijgt van een nieuw opgericht adviesorgaan, worden geïdentificeerd.[266] Daarnaast heeft de Britse overheid in november 2015 een wetsvoorstel gepubliceerd voor herziening van de wet voor de inlichtingendiensten. Het wetsvoorstel is erg omvangrijk en op het moment van schrijven, juni 2016, nog niet omgezet naar definitieve wetgeving. Het ziet er echter niet naar uit dat het wetsvoorstel er voor zal zorgen dat de wet op de inlichtingendiensten overzichtelijker en consistenter zal worden.[267] Sterker nog, de speciale rapporteur voor het recht op privacy van de

[263] Ibidem, 4.
[264] Ibidem, 4; Nils Muiznieks, 'Europe is Spying on You' (versie 27 oktober 2015), http://www.nytimes.com/2015/10/28/opinion/europe-is-spying-on-you-mass-surveillance.html (11 mei 2016).
[265] Ook Denemarken en Finland hebben plannen om in bulk internetgegevens te gaan verzamelen. Zie The Local, 'Denmark wants to watch everything you do online' (versie 29 januari 2016), http://www.thelocal.dk/20160129/denmark-eyes-massive-online-surveillance-of-citizens (13 mei 2016) & Nomi Byström, 'Finland: New surveillance law threatens fundamental rights' (6 oktober 2015), https://edri.org/finland-surveillance-law-threatens-fundamental-rights/ (13 mei 2016).
[266] Europees Bureau voor de grondrechten, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Mapping Member States' legal frameworks. (Rapport Europees Bureau voor de grondrechten, z.p. 2015) 23-24.
[267] Nadia O'Mara, 'UK Government Introduces Revised Investigatory Powers Bill in Parliament' (versie 2 maart 2016), https://www.justsecurity.org/29668/uk-government-introduces-revised-investigatory-powers-bill-parliament/ (13 mei 2016).

Verenigde Naties heeft sterke kritiek geuit op het wetsvoorstel omdat met het voorstel het in bulk vergaren van data gelegaliseerd zou worden in plaats van dat het verboden zou worden.[268]

Alhoewel het lastig is om een volledige inschatting te maken van de gevolgen van de onthullingen van Snowden voor eventuele wettelijke hervormingen, is het wel duidelijk dat verschillende (parlementaire) onderzoeken tot de conclusie kwamen dat nationale wetgeving hervormd zou moeten worden. Zowel in Frankrijk als in het Verenigd Koninkrijk kwamen parlementaire commissies tot die conclusie. In het Verenigd Koninkrijk zei de onafhankelijke toezichthouder voor terrorismewetgeving het volgende over de wetgeving voor de inlichtingendiensten:

> *Obscure since its inception, has been patched up so many times as to make it incomprehensible to all but a tiny band of initiates. A multitude of alternative powers, some of them without statutory safeguards, confuse the picture further. This state of affairs is undemocratic, unnecessary and – in the long run – intolerable.*[269]

In het algemeen geldt binnen EU-lidstaten dat de nationale wetgeving alleen voorwaarden schetst voor doelgerichte surveillance, hetzij voor individuen of specifieke groepen. Alleen in Duitsland, Frankrijk, het Verenigd Koninkrijk, Nederland en Zweden zijn er specifieke voorwaarden in de wet vastgelegd voor het gebruik van SIGINT zoals die ook bij massasurveillance wordt gebruikt. Verder ontbreekt het binnen de verschillende nationale wetgeving aan duidelijke definities die bepalen welke personen en activiteiten het doelwit mogen zijn van inlichtingenvergaring. Het mag ook geen verrassing zijn dat de wettelijke basis voor het mandaat en de bevoegdheden van de inlichtingendiensten zeer sterk uiteenloopt.[270]

Het toezicht op de inlichtingendiensten verschilt ook sterk per lidstaat, maar wel kan over het algemeen gesteld worden dat het in de lidstaten ontbreekt aan voldoende toezicht. Daarbij is er vooral een gebrek aan coördinatie tussen de verschillende toezichtsorganen (uitvoerende macht, parlementair toezicht en toezicht van expertgroepen). Bovendien lijkt de Europese norm dat toezichtsorganen slechts beperkte toegang hebben tot relevante informatie en documentatie van de inlichtingendiensten. Als voorbeeld kunnen parlementaire onderzoekscommissies in de meeste lidstaten informatie opvragen bij de inlichtingendiensten of de uitvoerende macht, maar kunnen die informatie niet opeisen.[271]

---

[268] Ewen MacAskill, 'UK setting bad example on surveillance, says UN privacy chief' (versie 9 maart 2016), http://www.theguardian.com/world/2016/mar/09/uk-setting-bad-example-on-surveillance-says-un-privacy-chief (13 mei 2016).
[269] Geciteerd via: Europees Bureau voor de grondrechten, 'Surveillance by intelligence services', 24.
[270] Ibidem, 27.
[271] Ibidem, 57-58.

Lidstaten, en de Unie zelf, proberen ondertussen door middel van 'technologische soevereiniteit' de mogelijkheid voor de NSA om surveillance toe te passen in Europa te beperken.[272] Zo heeft de gedachte gespeeld om een 'Europees internet' in te stellen waarbij data niet meer langs internetservers in de VS zou worden gestuurd. In februari 2014 opperde Angela Merkel, bondskanselier van Duitsland, het idee om een Europees communicatienetwerk op te zetten.[273] Een ander idee uit de Duitse koker was het instellen van een 'niet-spionage eis' voor bedrijven die meedingen in het binnenhalen van veiligheidsgevoelige contracten. Door het akkoord gaan met die eis verplichten zij zichzelf ertoe om geen informatie door te geven aan een buitenlandse overheid. De Duitse overheid kreeg echter de nodige kritiek te verduren voor deze 'vorm van protectionisme'.[274] Bovendien komen met deze voorstellen de waarden van internetneutraliteit en een open en vrij internet in het geding.[275] Daarom kan er binnen de EU beter werk gemaakt worden van voorstellen voor betere dataencryptie ter bescherming tegen ongewenste surveillance.[276]

Het nastreven van 'datalocalisatie', oftewel het lokaal opslaan van data, lijkt dan ook niet de beste oplossing om surveillance door buitenlandse inlichtingendiensten tegen te gaan. Datalocalisatie kan surveillance juist makkelijker maken aangezien logistieke problemen voor inlichtingendiensten afnemen: alle data is gecentreerd op één plek. Daarnaast is de kans ook aanwezig dat door datalocalisatie de veiligheidsmaatregelen, die genomen worden om de data te beschermen, zwakker worden. De bedrijven die de data opslaan voelen namelijk niet de noodzaak om de veiligheidsmaatregelen continu te verbeteren onder druk van wereldwijde concurrentie. Bovendien was hierboven al geconcludeerd dat de kans zeer reëel is dat lokale inlichtingendiensten de opgeslagen data delen met een partnerdienst in een ander land.[277] Het toepassen van datanationalisme ten behoeve van de privacy en veiligheid is dan ook een stelling waar vraagtekens bij gezet kunnen worden. Zeker omdat landen die datalocalisatie nastreven ook nog eens relatief vaak het slachtoffer worden van cybercrimes.[278]

Het punt om data beter te beveiligen is ondertussen, uit angst voor het verlies van klanten, opgepakt door technologiebedrijven. Zij zijn na de verontwaardigde reacties van consumenten op de

[272] Zie voor een overzicht van de voorstellen: Tim Maurer e.a., 'Technological Sovereignty: Missing The Point? An Analysis of European Proposals after June 5, 2013' (Rapport Global Public Policy Institute en New America's Open Technology Institute, z.p. 2014) 28-29.
[273] BBC News, 'Data protection: Angela Merkel proposes Europe network' (versie 15 februari 2014), http://www.bbc.com/news/world-europe-26210053 (11 mei 2016).
[274] Anthony Dworkin, Surveillance, privacy, and security, 5.
[275] Tim Maurer e.a., 'Technological Sovereignty: Missing the Point?', 22-23.
[276] Ibidem, 22.
[277] Anupam Chandler en Uyên P. Lê, 'Data Nationalism', *Emory Law Journal* 64 (2015) 3, 677-739, 717-718.
[278] Chandler en Lê, 'Data Nationalism', 718-721.

onthullingen van Snowden aan de slag gegaan om effectievere encryptie te realiseren. Zo haalde Google in oktober 2014 het nieuws met de claim dat het bedrijf een onbreekbare vorm van encryptie had weten te installeren.[279]

Het is interessant om te concluderen dat, wanneer men kijkt naar de EU en de EC, er sinds de onthullingen van Snowden er op grote schaal wordt opgeroepen om de internationale mensenrechten en privacy te respecteren. Tegelijkertijd wordt, door middel van de nieuwe privacyregelgeving, ook gewerkt aan het bevorderen van de Europese economische belangen. Daarbij wordt het gebruik van Big Data als een belangrijke economische kans voor Europa gezien.[280] Het is duidelijk dat persoonlijke informatie tegenwoordig een belangrijk economisch (ruil)middel is. Het is echter diezelfde die een risico vormt voor EU-burgers wanneer inlichtingendiensten er over kunnen beschikken en het is daarom ook verontrustend dat het sleutelbegrip nationale veiligheid niet overal in Europa wordt gebruikt of überhaupt hetzelfde betekent, terwijl inlichtingendiensten onder het mom van diezelfde nationale veiligheid allerlei mogelijkheden hebben om zichzelf toegang te verschaffen tot Big Data.[281] Dit vormt dus op zijn zachtst gezegd een interessante tegenstelling, waar nog eens als complicerende factor bij komt dat het toezicht op de Europese inlichtingendiensten vaak ondermaats is.

3.3 De rechterlijke macht aan het woord

De rechterlijke machten in Europa en de VS hebben zich niet stil gehouden in de discussies die zijn los gebarsten rondom surveillance en privacy. In de VS en Europa hebben verschillende rechtbanken hun oordeel uitgesproken over onder andere de legitimiteit van de surveillanceprogramma's van inlichtingendiensten, de regels omtrent de opslag van data en de afspraken voor dataverkeer tussen de VS en de EU.

Hierdoor positioneert de rechterlijke macht zich als een belangrijke speler in de discussie rondom veiligheid en privacy. Zodoende is de rechterlijke macht een drijfkracht voor wat betreft het hervormen van de relatie tussen het individu en de staat. Deze relatie is, mede door de veranderingen in het veiligheidslandschap, namelijk aan verandering onderhevig. In naam van veiligheid, en de drang

[279] CBC News, 'Google claims it installed unbreakable encryption after NSA spying' (versie 23 oktober 2014), http://www.cbc.ca/news/business/google-claims-it-installed-unbreakable-encryption-after-nsa-spying-1.2810773 (11 mei 2016).
[280] Zie Europese Commissie, 'Factsheet: The EU Data Protection Reform and Big Data' (maart 2016). Beschikbaar via http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf (12 mei 2016); Carrie Coredo, 'The President's Comments on European Privacy Claims and A Look Back at the LIBE Committee Report on Government Surveillance' (versie 19 februari 2015), https://www.lawfareblog.com/presidents-comments-european-privacy-claims-and-look-back-libe-committee-report-government (12 mei 2016).
[281] Europees Bureau voor de grondrechten, 'Surveillance by intelligence services', 25-26.

om veiligheidsrisico's het liefst compleet uit te sluiten, worden immers tegenwoordig veel zaken in de samenleving uit het oog van veiligheidsbeleid binnen het veiligheidsdomein ondergebracht.[282] Het toepassen van massasurveillance komt hier dan ook uit voort.

Door inmenging van de rechtelijke macht in de veiligheid-privacy tegenstelling wordt over het algemeen het belang van privacy als een wettelijk principe benadrukt om de hervorming van de relatie tussen het individu en de staat aan te pakken. Daarbij geeft Valsamis Mitsilegas, hoogleraar Europees strafrecht aan de Queen Mary Universiteit te Londen, aan dat privacy op vijf manieren van belang kan zijn:

> *In focusing on the impact of surveillance on the individual as a whole, rather than focusing on the protection of specific categories of personal data; in emphasizing the need to protect private life and personal data as fundamental rights, rather than attempting to provide a mere regulatory framework for the use and processing of personal data; in challenging the justification and practices of the collection of personal data by the state and the private sector per se, rather than merely setting limits on the processing, use and transfer of such data ex post, after it has been collected; in addressing the challenges of profiling individuals resulting from the maximization of the collection, and access to, personal data and the interlinking of databases; and last, but not least, in focusing on the reconfiguration of the relationship of trust between the citizen and the state which a permanent and generalized surveillance regime entails.*[283]

Wat betreft deze punten hebben rechters zich overigens al in diverse rechtszaken uitgesproken voordat überhaupt de surveillanceprogramma's via Snowden aan het licht kwamen. Het aanvankelijk geheime *Terrorism Surveillance Program* werd in december 2005 namelijk bij het grote publiek bekend na berichtgeving in de *New York Times*.

Na deze onthulling werden in de loop der jaren diverse rechtszaken aangespannen waarin vraagtekens geplaatst bij de bevoegdheid van de Amerikaanse overheid onder FISA en de *Patriot Act*.[284] De rechtszaken werden echter in het algemeen door de rechters verworpen aangezien de

[282] Mitsilegas, 'The Value of Privacy in an Era of Security', 104.
[283] Ibidem, 107.
[284] Er werden ook verschillende rechtszaken gevoerd tegen telecomproviders die de privacy van hun klanten zouden hebben geschonden door samen te werken met de NSA bij het uitvoeren van elektronische surveillance. Hierop werd door het Congres sectie 802 van de *FISA Amendments Act* ingebracht. Hiermee werd aan deze bedrijven achteraf immuniteit toegekend zodat ze niet meer vervolgd konden worden.

eisers, in de ogen van de rechters, geen aantoonbaar belang wisten aan te tonen. Eén van de dergelijke zaken was *Clapper v. Amnesty International USA*. Deze zaak werd in juli 2008 opgestart door een groep mensenrechtenadvocaten. De achterliggende gedachte was dat surveillance onder sectie 702 hun grondwettelijke rechten schond en aangezien de eisers beroepsmatig geregeld contact hadden met buitenlanders er een 'objectieve redelijke kans bestond dat hun communicatieverkeer verzameld zou worden onder sectie 702 in de toekomst'. Hierdoor hadden ze kostbare maatregelen moeten nemen om de vertrouwelijkheid van hun communicatieverkeer te kunnen waarborgen.[285]

Uiteindelijk bepaalde het Hooggerechtshof in februari 2013 dat ondanks het feit dat de overheid door de geheime onderdelen van de wetgeving de enige partij is die weet welke communicatie onderschept is, derde partijen geen aantoonbaar belang hebben om de wet aan te vechten. Ze kunnen immers niet aantonen dat ze schade hebben geleden. Het Hooggerechtshof bepaalde daarmee dat het feitelijke bestaan van geheime surveillance geen aantoonbaar juridisch belang rechtvaardigt. Hierdoor is het niet in feite niet mogelijk om geheime surveillanceprogramma's juridisch aan te vechten zonder enige vorm van onthulling van geheime informatie.[286]

Hiermee hanteert het Amerikaanse Hooggerechtshof een andere visie dan het EHRM. Juist vanwege het geheime karakter van surveillance erkent het EHRM over het algemeen juist het belang van eiser(s), zelfs wanneer bewijs ontbreekt die kunnen aantonen dat de geheime surveillance op de eiser(s) gericht was. Alleen al het bestaan van wetgeving die geheime surveillance toestaat, wordt door het EHRM gezien als een inbreuk op de rechten van een individu onder artikel 8 van het EVRM.[287] In de loop der jaren heeft het EHRM verschillende testen ontwikkeld om te bepalen of een bepaalde vorm van surveillance toelaatbaar is. Daarbij is het simpele feit dat de surveillance in overeenstemming is met de nationale wetgeving niet afdoende. Het EHRM beoordeelt de mate van proportionaliteit en de garanties tegen misbruik. Daarnaast beoordeelt het Hof de vorm, reikwijdte en duur van de genomen maatregelen; de redenen voor het toepassen; de bevoegdheden van de relevante autoriteiten en de mogelijkheid om te stoppen met de vorm van surveillance onder de nationale wetgeving.[288]

De onthullingen van Snowden hebben tot nu toe nog niet tot heel ander beeld geleid wat betreft de uitspraken van Amerikaanse rechters. Er lopen bij verscheidene rechtbanken echter rechtszaken over de wettelijke geldigheid van grootschalige surveillanceprogramma's. Tot op heden zijn verschillende lagere rechtbanken tot tegenstrijdige conclusies gekomen, maar heeft het

[285] Adam D. Moore (red.), *Privacy, security and accountability: ethics, law and policy* (Londen 2016) 213-214.
[286] Moore (red.), *Privacy, security and accountability*, 214.
[287] Ibidem, 210.
[288] Ibidem, 210-211.

Hooggerechtshof nog geen uitspraak gedaan over de houdbaarheid van grootschalige surveillanceprogramma's met betrekking tot het Vierde Amendement.[289]

Binnen de EU hebben het Hof van Justitie van de Europese Unie en het EHRM in de afgelopen jaren jurisprudentie neergezet die in theorie van grote invloed is voor de overeenstemming, of het ontbreken ervan, van nationale surveillancewetgeving met de Europese regelgeving.

Op basis van artikel 8 van het Handvest van de Grondrechten van de EU verklaarde het Hof van Justitie in 2014 de Europese richtlijn voor dataretentie uit 2006 ongeldig. Deze richtlijn verplichtte telecomproviders om tot twee jaar communicatiegegevens te bewaren.[290] Volgens het Hof was het verplicht opslaan van gegevens echter in strijd met het recht op bescherming van persoonlijke informatie doordat er bij de opslag van gegevens geen onderscheid werd gemaakt tussen de verschillen tussen gegevens, de redenen waarom gegevens werden opgeslagen en het ontbreken van objectieve en onafhankelijke criteria die bepalen wanneer autoriteiten toegang hebben tot de data. Hierdoor ging de richtlijn voorbij aan het principe van proportionaliteit.[291]

De uitspraak van het Hof betekende dus dat gegevens niet meer verplicht opgeslagen hoefden te worden met als gevolg dat de inlichtingendiensten van lidstaten geen toegang meer hadden telefoon- en internetgegevens. Daarom voerde het Verenigd Koninkrijk noodwetgeving in waarmee telecomproviders alsnog verplicht werden om telefoon- en internetgegevens 12 maanden te bewaren.[292] Het ongeldig verklaren van de richtlijn door het Hof betekende een duidelijk signaal dat opgeslagen data niet zonder meer kan worden gebruikt: *"The fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the persons concerned a feeling that their private lives are the subject of constant surveillance."*[293]

Anderhalf jaar later, in oktober 2015, was het Hof van Justitie wederom kritisch over een Europese dataregeling. Deze keer betrof het de *Safe Harbour*-overeenkomst met de VS voor het uitwisselen van persoonsgegevens. De overeenkomst, die in 2000 tot stand kwam, voorzag in het afgeven van garanties voor vergelijkbare privacybescherming bij Amerikaanse bedrijven ten opzichte van Europese burgers en bedrijven. Na de onthullingen van Snowden bleek echter dat in de

[289] Ibidem, 234.
[290] De richtlijn werd in 2006 door de Europese Commissie ingevoerd als reactie op de terroristische aanslagen in Madrid van 2004 en Londen van 2005.
[291] Carly Nyst, 'The Growing Divide Between European Governments and Regional Courts on Surveillance' (versie 16 maart 2016), https://www.justsecurity.org/29990/growing-divide-european-governments-regional-courts-surveillance/#more-29990 (13 mei 2016).
[292] Anthony Dworkin, Surveillance, privacy, and security, 4.
[293] Europees Hof van Justitie, 'Press Release No 54/14: The Court of Justice declares the Data Retention Directive to be invalid' (8 april 2014). Beschikbaar via http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf (13 mei 2016).

overeenkomst geen afspraken waren opgenomen die surveillance door de Amerikaanse overheid konden beperken. In de overeenkomst stond namelijk dat (Amerikaanse) bedrijven zich aan de Amerikaanse wetgeving moesten houden, ook al zouden ze daarmee de afspraken schenden die onder de *Safe Harbour*-overeenkomst waren overeengekomen. Hierdoor was het voor een Europeaan niet mogelijk om Facebook aan te klagen als het bedrijf vanwege het PRISM-programma van de NSA persoonlijke gegevens zou doorspelen aan de inlichtingendienst. Omdat de *Safe Harbour*-overeenkomst dus geen beperkingen oplegde aan Amerikaanse surveillance bepaalde het Hof dat de overeenkomst de Europese wetgeving schond.[294] In de uitspraak benadrukte het Hof overigens ook dat de Europese nationale wetgevingen voor de inlichtingendiensten in toenemende mate niet in overeenstemming waren met de Europese afspraken.[295]

Er vallen twee kanttekeningen te maken. Ten eerste is Facebookdata van Europeanen onder Amerikaanse wetgeving beter beschermd als het op een server in de VS is opgeslagen in plaats van op een server in de EU. Wanneer data namelijk in de VS is opgeslagen, kan het alleen door de NSA verzameld worden als die dienst over een bevelschrift van de FISC beschikt.[296] Wanneer de gegevens van niet-Amerikaanse burgers buiten de VS zijn opgeslagen hoeft de NSA niet over een gerechtelijk bevelschrift te beschikken om de gegevens te verzamelen. Bovendien zijn de beperkte privacyregels voor buitenlanders onder PPD-28 alleen aan toezichtsorganen onderhevig binnen de uitvoerende macht.[297] Daarnaast heeft de NSA, ten opzichte van Europese landen, in relatief opzicht meer te maken met wettelijk toezicht op het handelen van de dienst dan partnerdiensten in de EU.[298]

Ook het EHRM heeft zich begin 2016 uitgesproken tegen surveillance. Het Hof oordeelde in de zaak *Szabó and Vissy v. Hungary* dat de Hongaarse surveillancewet in strijd is met het recht op privacy van het EVRM. Het Hof ging specifiek in op het gevaar van nieuwe surveillancetechnologieën en het feit dat de ontwikkeling van wettelijke waarborgen zeer waarschijnlijk geen gelijke tred houden met de ontwikkelingen op technologisch vlak. Daarnaast benadrukte het Hof het belang van het versterken

[294] Timothy Edgar, 'Schrems v. Data Protection Commissioner: Some Inconvenient Truths The European Court of Justice Ignores' (versie 6 oktober 2015), https://lawfareblog.com/schrems-v-data-protection-commissioner-some-inconvenient-truths-european-court-justice-ignores (13 mei 2016).
[295] Carly Nyst, 'The Growing Divide Between European Governments and Regional Courts on Surveillance' (versie 16 maart 2016), https://www.justsecurity.org/29990/growing-divide-european-governments-regional-courts-surveillance/#more-29990 (13 mei 2016).
[296] Uiteraard kunnen er ook vraagtekens worden gesteld bij de onafhankelijkheid van FISC.
[297] Timothy Edgar, 'Schrems v. Data Protection Commissioner: Some Inconvenient Truths The European Court of Justice Ignores' (versie 6 oktober 2015), https://lawfareblog.com/schrems-v-data-protection-commissioner-some-inconvenient-truths-european-court-justice-ignores (13 mei 2016).
[298] Timothy Edgar, 'Why Should We Buy Into The Notion That The United States Doesn't Care About Privacy?' (versie 23 oktober 2015), https://www.lawfareblog.com/why-should-we-buy-notion-united-states-doesnt-care-about-privacy (13 mei 2016); Center for Democracy and Technology, 'National Security Standards by Country', https://govaccess.cdt.info/standards-ns-country.php (13 mei 2016).

van noodzakelijke waarborgen ten opzichte van massasurveillance: de noodzaak van een geïndividualiseerde verdenking, een strikte noodzakelijkheidstest en de geschiktheid van ministeriële autorisatie op dit gebied.[299]

Het is nu de vraag hoe deze situatie zich in de toekomst verder zal ontwikkelen. In februari 2016 bereikten de EU en de VS een nieuwe overeenkomst voor de uitwisseling van data. Deze overeenkomst, getiteld *Privacy Shield*, moet uiteindelijk nog worden goedgekeurd door het Hof van Justitie. Als de overeenkomst daadwerkelijk wordt goedgekeurd is het nog maar de vraag of de Europese databeschermingsautoriteiten en rechtbanken er mee akkoord gaan. Tegelijkertijd kan dan ook de vraag worden gesteld in hoeveel EU-lidstaten de nationale privacywetgeving afdoende is. Binnen de EU valt het uitwisselen van data tussen bedrijven namelijk onder de Europese wetgeving, maar dat geldt niet voor de nationale surveillance van lidstaten. Dus is de vraag of Europese datastromen naar bijvoorbeeld Frankrijk, het Verenigd Koninkrijk en Hongarije – landen met verregaande wetgeving voor massasurveillance – gestopt zouden moeten worden als die landen geen EU-lidstaten waren.[300]

Daarnaast is er een trend zichtbaar van het tot stand komen van nieuwe surveillancewetgeving in de EU-lidstaten, terwijl het Europese Hof van Justitie en het EHRM zich steeds meer uitspreken over surveillance-aspecten, en dus nationale veiligheidsonderwerpen, binnen lidstaten. Mogelijk gevolg hiervan zou wel eens kunnen zijn dat nationale lidstaten de uitspraken van het EHRM en het Hof van Justitie aan hun laars gaan lappen vanwege grote politieke belangen.[301]

3.4 Surveillance, privacy en metadata

De onthullingen van Snowden hebben het grote publiek niet alleen de relevantie van metadata laten zien, maar ook het belang van metadata voor overheden. Data mining is al sinds de jaren ’90 in opkomst. Sinds die tijd is de hoeveelheid opgeslagen online data steeds meer toegenomen, terwijl de kosten voor opslag en analyseren van die data zijn gedeeld. Zowel private partijen als de overheid hebben hier dankbaar gebruikt van gemaakt om efficiënter en goedkoper te kunnen werken. Sinds 11

[299] Europees Hof voor de Rechten van de Mens, *Szabó and Vissy v. Hungary*, no. 37138/14, 12 januari 2016. Beschikbaar via http://hudoc.echr.coe.int/eng?i=001-160020.
[300] Jennifer Baker, ‘A clash of EU privacy standards’ (versie 13 februari 2016), http://www.politico.eu/article/chash-over-data-protection-standards-privacy-safe-harbor-europe/ (13 mei 2016).
[301] Carly Nyst, ‘The Growing Divide Between European Governments and Regional Courts on Surveillance’ (versie 16 maart 2016), https://www.justsecurity.org/29990/growing-divide-european-governments-regional-courts-surveillance/#more-29990 (13 mei 2016).

september 2001 wordt data mining steeds meer door de overheid gebruikt om informatie te vergaren over terroristen en andere criminelen.[302]

Data mining heeft zich ook gemanifesteerd in de werkwijzen van inlichtingendiensten. Dit roept echter problemen op. Zo maakten de onthullingen van Snowden duidelijk dat het verschil in privacy in de relatie tussen de staat en de burger enerzijds en een bedrijf en de klant anderzijds aan het vervagen is. Als klant kan je namelijk wel toestemming geven aan een bedrijf voor het gebruik van persoonlijke gegevens, maar doordat bedrijven meewerken aan de programma's van de NSA kan je tegelijkertijd dus ook je gegevens hebben afgestaan aan de overheid.

Vanwege de enorme omvang aan data waar analisten van inlichtingendiensten over beschikken, wordt niet alle beschikbare informatie gelezen. In plaats daarvan worden relaties tussen data gevisualiseerd. Daarbij is er sprake van een enorm onderzoeksveld vol met verdenkingen. Door het in bulk verzamelen van data en vervolgens het visualiseren van die gegevens lijkt het onmogelijk om met zekerheid het verschil tussen binnenlandse personen en buitenlanders vast te stellen. Wettelijke vereisten beperken daarbij het functioneren van het systeem en daardoor lijkt het dat inlichtingendiensten over het algemeen van mening zijn dat de wetgeving moet worden aangepast, in plaats van het systeem.[303]

Ook de inhoud van het begrip nationale veiligheid verandert hierdoor. Nationale veiligheid gaat immers niet alleen over het nationale aspect als het gaat om verzamelen en analyseren van gegevens: data gaat de landsgrenzen over. Het belang van surveillance voor de nationale veiligheid of de openbare orde wordt dan ook veelvuldig benadrukt. Zo wordt in veel Europese landen wetgeving doorgevoerd om de mogelijkheden van inlichtingendiensten om (grootschalige) surveillance toe te passen. Uiteraard is het naleven van de nationale wetgeving door inlichtingendiensten, de aanwezigheid van afdoende toezicht en het respecteren van mensenrechten van belang om de privacy van burgers te waarborgen.

Het recht op privacy dient tegenwoordig in feite als een middel om de verspreiding van surveillance in de samenleving – als gevolg van de verweven processen van transnationalisatie, digitalisatie en privatisering – te temperen.[304] Dat is ook noodzakelijk aangezien metadataprogramma's van inlichtingendiensten door problemen op het gebied van de wetgeving, privacy en transparantie de waarden van privacyrechten ondermijnen. Een belangrijke les van de onthullingen van Snowden is het gekweekte begrip voor het potentieel en de mogelijke valkuilen van

[302] Slobogin, 'Government Data Mining and the Fourth Amendment', 317-318.
[303] Zygmunt Bauman e.a., 'After Snowden: Rethinking the Impact of Surveillance', 125.
[304] Ibidem, 126.

metadata. Het is echter zeer onwaarschijnlijk dat met de onthullingen van Snowden alle informatie over Big Data boven water is. Voor beleidsmakers, die de handelingsruimte voor de inlichtingendiensten bepalen, is het daarom van belang om de nadelen van Big Data goed in kaart te brengen: wetgeving loopt immers achter op de actualiteit.

4 Conclusie

Eind 19e eeuw definieerden de Amerikanen Samuel Warren en Louis Brandeis privacy als het recht om alleen gelaten te worden. De achterliggende gedachte van Warren en Brandeis was dat de Amerikaanse overheid niks te maken had met het leven van individuele burgers. Tegenwoordig is de rol van privacy in de samenleving van een andere aard. Persoonlijke informatie is in de afgelopen decennia een uiterst waardevol ruilmiddel geworden. Bedrijven verschaffen (gratis) diensten in ruil voor informatie en ook de overheid gebruikt persoonlijke gegevens om de dienstverlening te verbeteren en uit te breiden. De aantrekkelijkheid van (persoonlijke) informatie is ook toegenomen door hogere toegankelijkheid tot metadata. De opkomst van (elektronische) communicatiemiddelen, en de mogelijkheid om grote hoeveelheden data op te slaan hebben daar aan bijgedragen.

Uit diverse onthullingen, onder andere van de *New York Times* in 2005 als Snowden in 2013, werd duidelijk dat inlichtingendiensten in de VS en Europa metadata van telefoonverkeer en elektronisch internetverkeer verzamelen. Daarbij werken de diensten samen met commerciële bedrijven, zoals telecomproviders. Vanwege nationale veiligheidsbelangen en het minimaliseren van risico's hebben overheden de surveillancepraktijken gelegitimeerd, of zijn ze dat van plan. Wat dat betreft is de tijdsgeest van de 21ste eeuw sterk veranderd in vergelijking met de revolutionaire tijdsgeest aan het einde van de 18e eeuw. Het opgeven van vrijheid voor veiligheid, zoals Franklin zei, is iets wat tegenwoordig in zekere mate gemeengoed is.

De onthullingen van Snowden hebben de uitvoerende mogendheden in de VS en de EU desondanks onder druk gezet om stelling te nemen tegen de veelal geheime vormen van surveillance. De overheden benadrukken echter het belang van geheimhouding rondom de programma's in de naam van de nationale veiligheid. Tegelijkertijd erkennen de overheden ook wel het belang van goede regelgeving en toezicht.

In de VS heeft het Witte Huis na Snowden werk gemaakt van meer openheid aangaande de inlichtingendiensten, onder meer door het vrijgeven van bepaalde geheime documenten, en de beperking van bevoegdheden van de inlichtingen – door de *USA Freedom Act*, alhoewel telefoonmetadataprogramma onder Sectie 215 van de *Patriot Act* veel minder nuttige informatie opleverde dan het verzamelen van internetdata onder Sectie 702 van FISA. Tegelijkertijd ziet de realiteit er naar uit dat Europese landen – onder druk van terroristische dreigingen en toenemende instabiliteit – alleen maar meer bevoegdheden aan de inlichtingendiensten toekennen.

In dezelfde periode voert de Commissie strengere regelgeving omtrent databescherming door, sprak haar afschuw uit over de praktijken van de NSA en stond voor het recht op privacy van European. De EU heeft echter geen zeggenschap zaken aangaande nationale veiligheid en de nationale

inlichtingendiensten. In overeenstemming met de Europese regelgeving zijn er binnen de nationale wetgeving namelijk verschillende uitzonderingsposities voor inlichtingendiensten opgenomen met betrekking tot de privacyregels. De Commissie kan blijven oproepen om veranderingen door te voeren, bijvoorbeeld het aanscherpen van de regels of het organiseren van inlichtingenwerk op Europees niveau, maar vormt daarmee een roepende in de woestijn. Eerder nog kan worden gesteld dat in Europa op dit moment een beweging zichtbaar is die te vergelijken is met de beweging in de VS na 11 september 2001: simpelweg meer bevoegdheden naar inlichtingen- en veiligheidsdiensten. Overigens is het gebruik van inlichtingen binnen de EU zeer ondoorzichtig en is er over het delen van inlichtingen wellicht nog minder bekend. Zonder de aanwezigheid van sterk, onafhankelijk toezicht zal er waarschijnlijk dus niets veranderen. Het realiseren van verbeterde toezicht was dan ook één van de redenen waarom Snowden besloot om naar buiten te treden.

Ondertussen beschikken bedrijven over een potentiële goudmijn voor inlichtingen- en veiligheidsdiensten. In dit digitale tijdperk worden consumenten immers uitgebreid gevolgd door bedrijven in ruil voor gratis communicatiediensten. Mochten inlichtingendiensten toegang hebben tot die gegevens, dan maakt krachtige privacybescherming geen verschil meer.

Amerikaanse en Europese rechters kijken ondertussen totaal verschillend naar de claims van overheden betreffende de geheimhouding in naam van de nationale veiligheid. Amerikaanse rechtbanken zijn zeer terughouden met het toekennen van wettelijke claims tegen de hang naar geheimhouding van de overheid zonder dat er sprake is van een aantoonbaar belang. Het EHRM staat dergelijke claims wel toe en stelt overheden ook aansprakelijk voor geheime surveillance. Het spreekt overigens voor zich dat het EHRM een andere relatie heeft tot de overheden van EU-lidstaten dan de relatie die het Amerikaanse Hooggerechtshof heeft tot het Witte Huis. Desondanks kunnen er voor de duidelijk zowel in de VS als in Europa vraagtekens worden gesteld bij de wettelijke houdbaarheid van de surveillanceprogramma's.

Het feit dat mensen tegenwoordig zelf vrijwillig informatie afstaan aan derden, betekent dat privacy niet meer draait om het recht om alleen gelaten te worden, maar in de kern om bescherming van persoonlijke informatie. Vandaar dat het belang van databescherming zowel in Europa als de VS wordt erkend. Het probleem met privacy draait tegenwoordig echter om de vraag wie toegang heeft tot die informatie. Zolang dat onduidelijk is, is het beeld dat we met constante surveillance te maken hebben gegrond. Waar die veranderingen gestart zullen worden is nog maar de vraag. In de VS liggen de grondrechten namelijk sterk verankerd in de grondwet en het doorvoeren van veranderingen is daarom aan het Hooggerechtshof. Het is in de VS daarom wachten tot het Hooggerechtshof een eigentijdsere interpretatie aan het Vierde Amendement gaat geven, terwijl er meer Europa meer partijen en belanghebbenden aanwezig zijn die een verandering kunnen teweeg kunnen brengen. Het

zijn achter de nationale lidstaten die de bevoegdheden van de inlichtingendiensten verruimen en de Commissie die langs de zijlijn toe moet kijken. Een verandering zal ook in Europa waarschijnlijk bij de rechterlijke macht beginnen.

Bibliografie

AD.nl. *Hollande's coalitie tegen IS krijgt steeds meer vorm.* 26 november 2015. http://www.ad.nl/ad/nl/1013/Buitenland/article/detail/4195814/2015/11/26/Hollande-s-coalitie-tegen-IS-krijgt-steeds-meer-vorm.dhtml (geopend januari 15, 2016).

Angwin, Julia, en Jeff Larson. *The NSA Revelations All in One Chart.* 30 juni 2014. https://projects.propublica.org/nsa-grid/ (geopend maart 27, 2016).

Arrest in zaak C-632/14 Maximillian Schrems/Data Protection Commissioner. C-362/14 (Hof van Justitie van de Europese Unie, 6 oktober 2015).

Ashiagbor, Diamond, Nicola Countouris, en Ioannis Lianos. *The European Union after the Treaty of Lisbon.* Editor: Diamond Ashiagbor, Nicola Countouris, & Ioannis Lianos. Cambridge: Cambridge University Press, 2012.

Atkin, Michelle Louise. „The Future of Privacy in Post-9/11 America." *International Journal of Intelligence Ethics* 4, nr. 2 (2013): 13-47.

Baker, Jennifer. *'A clash of EU privacy standards'.* 13 februari 2016. http://www.politico.eu/article/chash-over-data-protection-standards-privacy-safe-harbor-europe/ (geopend mei 13, 2016).

Bamberger, Kenneth A, en Deirdre K Mulligan. „Privacy on the Books and on the Ground." *Stanford Law Review* 63, nr. 2 (2011): 247-316.

Barnett, Randy E. „Why the NSA Data Seizures Are Unconstitutional." *Harvard Journal of Law and Public Policy* 38, nr. 1 (2015): 3-20.

Bauman, Zygmunt, et al. „After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8, nr. 2 (2014): 121-144.

Bazan, Elizabeth B, Gina Marie Stevens, en Brian T Yeh. *Government Access to Phone Calling Activity and Related Records: Legal Authorities.* Congressional Research Service Report, Damascus: Penny Hill Press, 2007.

BBC News. *'Data protection: Angela Merkel proposes Europe network'.* 15 februari 2014. http://www.bbc.com/news/world-europe-26210053 (geopend mei 11, 2016).

Bedoya, Alvaro. *Executive Order 12333 and the Golden Number.* 9 oktober 2014. https://www.justsecurity.org/16157/executive-order-12333-golden-number/ (geopend april 20, 2016).

Beuth, Patrick. *Wie der BND das Netz überwacht.* 18 juni 2013. http://www.zeit.de/digital/datenschutz/2013-06/internet-ueberwachung-bnd (geopend april 25, 2016).

Big Brother Watch and Others v. United Kingdom. 58170/13 (Europees Hof voor de Rechten van de Mens, 30 september 2013).

Bignami, Francesca. „Privacy and Law Enforcement in the European Union: The Data Retention Directive." *Chicago Journal of International Law* 8, nr. 1 (2007): 233-255.

Bigo, Didier, et al. „National Programmes for Mass Surveillance op Personal Data in EU Member States and their Compatibility with EU Law.” Rapport Europees Parlement, Brussel, 2013.

Borger, Julian. *GCHQ and European spy agencies worked together on mass surveillance.* 1 november 2013. http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden (geopend april 25, 2016).

Brown, Ian, Morton H Halperin, Ben Hayes, Ben Scott, en Mathias Vermeulen. *Towards Multilateral Standards for Surveillance Reform.* Discussion Paper, Oxford : Oxford Internet Institute, 2015.

Byman, Daniel, en Benjamin Wittes. *Reforming the NSA. How to Spy after Snowden.* 17 april 2014. https://www.foreignaffairs.com/articles/united-states/2014-04-17/reforming-nsa (geopend maart 26, 2016).

Byström, Nomi. *'Finland: New surveillance law threatens fundamental rights'.* 6 oktober 2015. https://edri.org/finland-surveillance-law-threatens-fundamental-rights/ (geopend mei 13, 2016).

CBC News. *'Google claims it installed unbreakable encryption after NSA spying'.* 23 oktober 2014. http://www.cbc.ca/news/business/google-claims-it-installed-unbreakable-encryption-after-nsa-spying-1.2810773 (geopend mei 11, 2016).

Center for Democracy and Technology. *'National Security Standards by Country'.* sd. https://govaccess.cdt.info/standards-ns-country.php (geopend mei 13, 2016).

Chandler, Anupam, en Uyên P. Lê. „Data Nationalism.” *Emory Law Journal* 64, nr. 3 (2015): 677-739.

Clarke, Conor. „Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp? Ex Parte Proceedings and the FISC Win Rate.” *Stanford Law Review Online* 66, nr. 125 (2014): 125-133.

Clarke, Richard A, Michael J Morell, Geoffrey R Stone, Cass R Sunstein, en Peter Swire. *The NSA Report: Liberty and Security in a Changing World.* Princeton: Princeton University Press, 2014.

Commissie burgerlijke vrijheden, justitie en binnenlandse zaken. „Electronic mass surveillance of EU citizens.” Onderzoeksrapport Europees Parlement, Brussel, 2013.

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten. „Jaarverslag 2014-2015.” Jaarverslag, Den Haag, 2015.

Coredo, Carrie. *'The President's Comments on European Privacy Claims and A Look Back at the LIBE Committee Report on Goverment Surveillance'.* 19 februari 2015. https://www.lawfareblog.com/presidents-comments-european-privacy-claims-and-look-back-libe-committee-report-government (geopend mei 12, 2016).

Departement van Justitie. *FISA 101: Why FISA Modernization Amendments Must Be Made Permanent.* sd. https://www.justice.gov/archive/ll/index.html (geopend maart 29, 2016).

Deskundigeverklaring Ian Brown 'Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK'. 581780/13 (Europees Hof voor de Rechten van de Mens, 27 september 2013).

Donohue, Laura K. „Bulk Metadata Collection: Statutory and Constitutional Considerations.” *Harvard Journal of Law and Public Policy* 37, nr. 1 (2014): 757-900.

Donohue, Laura K. „Section 702 and the Collection of International Telephone and Internet Content.” *Harvard Journal of Law and Public Policy* 38, nr. 1 (2015): 117-265.

Doucet, Lyse. *Paris Attack: From 9/11 to 1/11.* 12 januari 2015. http://www.bbc.com/news/world-europe-30786552 (geopend januari 15, 2016).

Dover, Robert. „From CFSP to ESDP: the EU's Foreign, Security, and Defence Policies.” In *European Union Politics*, door Michelle Cini, & Nieves Pérez-Solórzano Borragón, 239-257. Oxford: Oxford University Press, 2010.

Dworkin, Anthony. „Surveillance, privacy and security: Europe's confused response to Snowden.” Beleidsmemo European Council on Foreign Relations, 2015.

Edgar, Timothy. *'Schrems v. Data Protection Commissioner: Some Inconvenient Truths The European Court of Justice Ignores'.* 6 oktober 2015. https://lawfareblog.com/schrems-v-data-protection-commissioner-some-inconvenient-truths-european-court-justice-ignores (geopend mei 13, 2016).

—. *'Why Should We Buy Into The Notion That The United States Doesn't Care About Privacy?'.* 23 oktober 2015. https://www.lawfareblog.com/why-should-we-buy-notion-united-states-doesnt-care-about-privacy (geopend mei 13, 2016).

Electronic Privacy Information Center. *Foreign Intelligence Surveillance Act (FISA).* 28 maart 2016. https://epic.org/privacy/surveillance/fisa/ (geopend maart 28, 2016).

Erwin, Marshall Curtis. *Intelligence Issues for Congress.* Congressional Research Service Report, Damascus: Penny Hill Press, 2013.

Etzioni, Amitai. „NSA: National Security vs. Individual Rights.” *Intelligence and National Security* 30, nr. 1 (2015): 100-136.

Europa Nu. *'Bescherming van persoonsgegevens in Europa'.* 10 mei 2016. https://www.europa-nu.nl/id/vhkejco8liwc/bescherming_van_persoonsgegevens_in (geopend mei 10, 2016).

Europees Bureau voor de grondrechten. *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Mapping Member States' legal frameworks.* Europees Bureau voor de grondrechten, 2015.

Europees Hof van Justitie. „Press Release No 54/14: The Court of Justice declares the Data Retention Directive to be invalid.” *http://curia.europe.eu.* 8 april 2014. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf (geopend mei 13, 2016).

Europese Commissie. „e-Library Migration and Home Affairs.” *http://ec.europa.eu.* 28 april 2015. http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf (geopend januari 31, 2016).

—. *EU Charter of Fundamental Rights.* 8 januari 2016. http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm (geopend januari 31, 2016).

—. „European Commission calls on the U.S. to restore trust in EU-U.S. data flows.” *europa.eu.* 27 november 2013. europa.eu/rapid/press-release_IP-13-1166_en.pdf (geopend januari 23, 2016).

—. „'European Commission calls on the U.S. to restore trust in EU-U.S. data flows'." *http://europe.eu.* 27 november 2013. http://europa.eu/rapid/press-release_IP-13-1166_en.pdf (geopend mei 10, 2016).

—. „'Factsheet: The EU Data Protection Reform and Big Data'." *http:ec.europa.eu.* Maart 2016. http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf (geopend mei 12, 2016).

—. „'Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU'." *http://ec.europe.eu.* 27 november 2013. http://ec.europe.eu/justice/data-protection/files/com_2013_847_en.pdf (geopend mei 9, 2016).

—. „Rebuilding Trust in EU-US Data Flows." *http://ec.europe.eu.* 27 november 2013. http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf (geopend mei 10, 2016).

Executive Office of the President. „Big Data: Seizing Opportunities, Preserving Values." Rapport Het Witte Huis, 2014.

Fidler, David P. *The Snowden Reader.* Editor: David P Fidler. Bloomington: Indiana University Press, 2015.

Finn, Peter, en Ellen Nakashima. *'Obama defends sweeping surveillance efforts'.* 7 juni 2013. https://www.washingtonpost.com/politics/obama-defends-sweeping-surveillance-efforts/2013/06/07/2002290a-cf88-11e2-9f1a-1a7cdee20287_story.html (geopend mei 9, 2016).

Finn, Peter, en Sari Horwitz. *U.S. charges Snowden with espionage.* 21 juni 2013. https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html (geopend januari 16, 2016).

Fiveash, Kelly. *'EU ministers respond sleepily to Viv Reding's 'Snowden wake-up call' on data protection'.* 9 juni 2014. http://www.theregister.co.uk/2014/06/09/viv_reding_justice_council_of_ministers_data_protection/ (geopend mei 11, 2016).

Follorou, Jacques, en Franck Johannès. *'Révélations sur le Big Brother français'.* 7 juli 2013. http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html (geopend mei 3, 2016).

Friedman, Lawrence M. *The Human Rights Culture: A Study in History and Context.* New Orleans: Quid Pro, LLC, 2011.

Gellman, Barton, en Ashkan Soltani. *'NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say'.* 30 oktober 2013. https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (geopend mei 9, 2016).

Goidel, Kirby, Craig Freeman, en Brian Smentkowski. *Misreading the Bill of Rights: Top Ten Myths Concerning Your Rights and Liberties.* Santa Barbara: Praeger, 2015.

Goitein, Elizabeth. *'Overseas Surveillance in an Interconnected World'.* 17 maart 2016. https://www.justsecurity.org/29994/overseas-surveillance-interconnected-world/#more-29994 (geopend mei 9, 2016).

González Fuster, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Heidelberg: Springer, 2014.

Graham, Megan. *Adding Some Nuance on the European Court's Safe Harbor Decision.* 7 oktober 2015. https://www.justsecurity.org/26651/adding-nuance-ecj-safe-harbor-decision/ (geopend januari 23, 2016).

Grimmett, Richard F. *Authorization for Use of Military Force in Response to the 9/11 Attacks (P.L. 107-40): Legislative History.* Congressional Research Service Report, Damascus: Penny Hill Press, 2007.

Gutwirth, Serge, et al. „D1: Legal, social, economic and ethical conceptualisations of privacy and data protection .” Rapport PRESCIENT project, 2011.

Gutwirth, Serge, Ronald Leenes, en Paul de Hert. *Reforming European Data Protection Law.* Editor: Serge Gutwirth, Ronald Leenes, & Paul de Hert. Dordrecht: Springer, 2015.

Gutwirth, Serge, Ronald Leenes, Paul de Hert, en Yves Poullet. *European Data Protection: Coming of Age.* Editor: Serge Gutwirth, Ronald Leenes, Paul de Hert, & Yves Poullet. Dordrecht: Springer, 2013.

—. *European Data Protection: In Good Health?* Editor: Serge Gutwirth, Ronald Leenes, Paul de Hert, & Yves Poullet. Dordrecht: Springer, 2012.

Herman, Michael. *Intelligence power in peace and war.* 10th. Cambridge: Cambridge University Press, 2010.

Het Europees Parlement en de Raad van de Europese Unie. „Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.” *EUR-Lex.* sd. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046 (geopend april 29, 2016).

Het Witte Huis. „Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.” Rapport White House Office , Washington, 2012.

—. „Presidential Policy Directive/PPD-28.” *www.whitehouse.gov.* 17 januari 2014. www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf (geopend mei 9, 2016).

—. *Remarks by the President in a Press Conference.* 9 augustus 2013. https://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference (geopend mei 9, 2016).

In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]', Amended Memorandum Opinion. BR 13-109 (Foreign Intelligence Surveillance Court, Washington, D.C. 19 juli 2013).

Keller, Josh, Alicia Parlapiano, David E. Sanger, en Charlie Savage. *'Obama's Changes to Government Surveillance'.* 17 januari 2014. http://www.nytimes.com/interactive/2014/01/17/us/nsa-changes-graphic.html (geopend mei 9, 2016).

Kobrin, Stephen J. „Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance." *Review of International Studies* 30, nr. 1 (2004): 111-131.

Kuner, Christopher. „Data Nationalism and its discontents." *Emory Law Journal Online.* 2015. http://law.emory.edu/elj/elj-online/volume-64/responses/data-nationalism-its-discontents.html (geopend januari 23, 2016).

Lederman, Marty, en Steve Vladeck. *'The Constitutionality of a FISA "Special Advocate"'.* 4 november 2013. https://www.justsecurity.org/2873/fisa-special-advocate-constitution/ (geopend mei 9, 2016).

Lee, Newton. *Counterterrorism and Cybersecurity: Total Information Awareness.* 2nd. New York: Springer, 2015.

Liberty and Others v. the United Kingdom. 58243/00 (Europees Hof voor de Rechten van de Mens, 1 juli 2008).

Linder, Douglas O. *Constitutional Limitations on the Judicial Power: Standing, Advisory Opinions, Mootness, and Ripeness.* 6 januari 2015. http://law2.umkc.edu/faculty/projects/ftrials/conlaw/caseorcontroversy.htm (geopend april 4, 2016).

Lucas Jr., George R. „NSA Management Directive #424: Secrecy and Privacy in the Aftermath of Edward Snowden." *Ethics & International Affairs* 28, nr. 1 (2014): 29-38.

Lui, Edward C, Andrew Nolan, en Richard M Thompson II. *Overview of Constitutional Challenges to NSA Collection Activities.* Congressional Research Service Report, Damascus: Penny Hill Press, 2015.

MacAskill, Ewen. *'UK setting bad example on surveillance, says UN privacy chief'.* 9 maart 2016. http://www.theguardian.com/world/2016/mar/09/uk-setting-bad-example-on-surveillance-says-un-privacy-chief (geopend mei 13, 2016).

Manach, Jean-Marc. *'Frenchelon: la DGSE est en « 1ère division »'.* 2 oktober 2010. http://bugbrother.blog.lemonde.fr/2010/10/02/frenchelon-la-dgse-est-en-1ere-division/ (geopend mei 2, 2016).

Maurer, Tim, Isabel Skierka, Robert Morgus, en Mirko Hohmann. *Technological Sovereignty: Missing The Point? An Analysis of European Proposals after June 5, 2013'.* Beleidsnota, Global Public Policy Institute; New America's Open Technology Institute, 2014.

McAskill, Ewen, en James Ball. *'UN surveillance resolution goes ahead despite attempts to dilute language'.* 21 november 2013 . http://www.theguardian.com/world/2013/nov/21/un-surveillance-resolution-us-uk-dilute-language (geopend mei 11, 2016).

Mitsilegas, Valsamis. „The Value of Privacy in an Era of Security: Embedding Constitutional Limits on Preemptive Surveillance." *International Political Sociology* 8, nr. 1 (2014): 104-108.

Moïsi, Dominique. *Charlie Hebdo. Un 11-Septembre de la France?* 9 januari 2015. http://www.ouest-france.fr/debats/editorial/charlie-hebdo-un-11-septembre-de-la-france-3103540 (geopend januari 15, 2016).

Moore, Adam D. *Privacy, security and accountability: ethics, law and policy.* Editor: Adam D. Moore. Londen: Rowman & Littlefield International, 2016.

Muiznieks, Nils. *'Europe is Spying on You'.* 27 oktober 2015. http://www.nytimes.com/2015/10/28/opinion/europe-is-spying-on-you-mass-surveillance.html (geopend mei 11, 2016).

National Security Agency. *SIGINT Frequently Asked Questions.* 15 januari 2009. https://www.nsa.gov/sigint/faqs.shtml#sigint4 (geopend maart 28, 2016).

NOS. *'Onderzoek naar rol AIVD, MIVD'.* 3 juli 2013. http://nos.nl/artikel/525332-onderzoek-naar-rol-aivd-mivd.html (geopend mei 3, 2016).

Nyst, Carly. *'The Growing Divide Between European Governments and Regional Courts on Surveillance'.* 16 maart 2016. https://www.justsecurity.org/29990/growing-divide-european-governments-regional-courts-surveillance/#more-29990 (geopend mei 13, 2016).

O'Mara, Nadia. *'UK Government Introduces Revised Investigatory Powers Bill in Parliament'.* 2 maart 2016. https://www.justsecurity.org/29668/uk-government-introduces-revised-investigatory-powers-bill-parliament/ (geopend mei 13, 2016).

Omtzigt, Pieter. „Mass surveillance." Rapport Parlementair Assemblée Raad van Europa, Straatsburg, 2015.

Pengelly, Martin. *NSA listed Merkel among leaders subject to surveillance - report.* 29 maart 2014. http://www.theguardian.com/world/2014/mar/29/nsa-merkel-leaders-surveillance-documents-snowden (geopend januari 19, 2016).

Priest, Dana. *'Help From France Key in Covert Operations'.* 3 juli 2005. http://www.washingtonpost.com/wp-dyn/content/article/2005/07/02/AR2005070201361.html (geopend mei 3, 2016).

Privacy and Civil Liberties Oversight Board. „Recommendations Assessment Fact Sheet." *https://www.pclob.gov.* 5 februari 2016. https://www.pclob.gov/library/Recommendations_Assessment_FactSheet_20160205.pdf (geopend mei 9, 2016).

Privacy and Civil Liberties Oversight Board. *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act.* Privacy and Civil Liberties Oversight Board, 2014.

Prosser, William L. „Privacy." *California Law Review* 48, nr. 3 (1960): 383-423.

Rainie, Lee, en Mary Madden. *Americans' Privacy Strategies Post-Snowden.* 16 maart 2015. http://www.pewinternet.org/2015/03/16/Americans-Privacy-Strategies-Post-Snowden/ (geopend maart 26, 2016).

Rascoff, Samuel J. „Presidential Intelligence." *Harvard Law Review* 129, nr. 3 (2016): 633-716.

Reding, Viviane. „Letter to US Attorney General Eric Holder.” *Europees Parlement.* 10 juni 2013. http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/p6_ltr_holder_/p6_ltr_Holder_en.pdf (geopend mei 9, 2016).

—. „Press Release Archive for June 2013.” *Europese Commissie.* 24 maart 2016. http://ec.europa.eu/ireland/press_office/media_centre/june2013_en.htm#12 (geopend april 25, 2016).

—. *Press Release Archive for June 2013.* 24 maart 2016. http://ec.europa.eu/ireland/press_office/media_centre/june2013_en.htm#12 (geopend april 25, 2016).

—. *'PRISM scandal: The data protection rights of EU citizens are non-negotiable'.* 22 oktober 2015. http://europe.eu/rapid/press-release_SPEECH-13-536_en.htm (geopend mei 9, 2016).

Regan, Priscilla M. „Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows.” *Journal of Social Issues* 59, nr. 2 (2003): 263-282.

Richardson, Bradford. *Ex-CIA Director: Snowden should be 'hanged' for Paris.* 19 november 2015. http://thehill.com/blogs/blog-briefing-room/260817-ex-cia-director-snowden-should-be-hanged-for-paris (geopend januari 15, 2016).

Rijksoverheid. *'Geen onbelemmerde toegang tot internet en telefoon voor AIVD en MIVD'.* 21 juni 2013. https://www.rijksoverheid.nl/actueel/nieuws/2013/06/21/geen-onbelemmerde-toegang-tot-internet-en-telefoon-voor-aivd-en-mivd (geopend mei 3, 2016).

Roessler, Beate, en Dorota Mokrosinska. *Social Dimensions of Privacy: Interdisciplinary Perspectives.* Editor: Beate Roessler, & Dorota Mokrosinska. Cambridge: Cambridge University Press, 2015.

Sanger, David E. *'U.S. Privacy Panel Backs N.S.A.'s Internet Tapping'.* 2 juli 2014. http://www.nytimes.com/2014/07/03/world/privacy-board-backs-nsa-program-that-taps-internet-in-us.html (geopend mei 9, 2016).

Savage, Charlie. *'Watchdog Report Says N.S.A. Program is Illegal and Should End'.* 23 januari 2014. http://www.nytimes.com/2014/01/23/us/politics/watchdog-report-says-nsa-program-is-illegal-and-should-end.html?_r=0 (geopend mei 9, 2016).

Schneier, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* New York: W. W. Norton & Company, 2015.

Seifert, Jeffrey W. *Data Mining and Homeland Security: An Overview.* Congressional Research Service Report, Damascus: Penny Hill Press, 2008.

Servenay, David. *'Terrorisme: pourquoi Alliance Base a fermé à Paris'.* 24 mei 2010. http://rue89.nouvelobs.com/2010/05/24/terrorisme-fermeture-dalliance-base-a-paris-152349 (geopend mei 3, 2016).

Shane, Scott. *'No Morsel Too Minuscule for All-Consuming N.S.A.'.* 2 november 2013. http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?pagewanted=2&_r=0 (geopend mei 9, 2016).

Sharp, Tim. *Right to Privacy: Constitutional Rights & Privacy Laws.* 12 juni 2013. http://www.livescience.com/37398-right-to-privacy.html (geopend januari 23, 2016).

Singer, Natasha. *White House Proposes Broad Consumer Data Privacy Bill.* 27 februari 2015. http://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data-privacy-bill.html (geopend januari 23, 2016).

Slobogin, Christopher. „Government Data Mining and the Fourth Amendment." *The University of Chicago Law Review* 75, nr. 1 (2008): 317-341.

—. *Privacy at Risk: The New Government Surveillance and the Fourth Amendment.* Chicago: Chicago University Press, 2007.

Sloot, Bart van der. „Privacy in het post-NSA tijdperk." *Nederlands Juristenblad* 17 (2014): 1172-1179.

Spiegel Online. *'Spying Fallout: German Trust in United States Plummets'.* 8 november 2013. http://www.spiegel.de/international/germany/nsa-spying-fallout-majority-of-germans-mistrust-united-states-a-932492.html (geopend mei 9, 2016).

Stalla-Bourdillon, Sophie, Joshua Phillips, en Mark D Ryan. *Privacy vs. Security.* Springer, 2014.

Szabó and Vissy v. Hungary. 37138/14 (Europees Hof voor de Rechten van de Mens, 12 januari 2016).

The Economic Times. *CIA Director John Brennan blasts Edward Snowden in wake of Paris attacks.* 18 november 2015. http://articles.economictimes.indiatimes.com/2015-11-18/news/68382544_1_paris-attacks-edward-snowden-islamic-state-group (geopend januari 16, 2016).

The Economist. *Liberty's lost decade.* 3 augustus 2013. http://www.economist.com/news/leaders/21582525-war-terror-haunts-america-still-it-should-recover-some-its-most-cherished (geopend januari 17, 2016).

—. „Get off of my cload ." *The Economist*, 10 oktober 2015: 59-60.

The Local. *'Denmark wants to watch everything you do online'.* 29 januari 2016. http://www.thelocal.dk/20160129/denmark-eyes-massive-online-surveillance-of-citizens (geopend mei 13, 2016).

The Member States of the European Union. „Charter of Fundamental Rights of the European Union." *EUR-Lex.* 26 oktober 2012. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (geopend januari 31, 2016).

The Technology and Privacy Advisory Committee. *Safeguarding Privacy in the Fight Against Terrorism.* Rapport The Technology and Privacy Advisory Committee, Washington: Ministerie van Defensie, 2004.

Toh, Amos, Faiza Patel, en Elizabeth Goitein. „Overseas Surveillance in an Interconnected World." Rapport Brennan Center for Justice, New York, 2016.

United Sates v. United States District Court. 70-153 (Het Amerikaans Hooggerechtshof, 19 juni 1972).

United States v. United States District Court. 70-153 (United States Supreme Court, 19 juni 1972).

Villasenor, John. *What You Need to Know about the Third-Party Doctrine.* 30 december 2013. http://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/ (geopend januari 23, 2016).

Vladeck, Stephen I. „The FISA Court and Article III.” *Washington and Lee Law Review* 72, nr. 3 (2015): 1161-1180.

Washington Post. *NSA slides explain the PRISM data-collection program.* 10 juli 2013. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (geopend maart 26, 2016).

Weber and Saravia v. Germany. 54934/00 (Europees Hof voor de Rechten van de Mens, 29 juni 2006).

Whitman, James Q. „The Two Western Cultures of Privacy: Dignity Versus Liberty.” *The Yale Law Journal* 113, nr. 6 (2004): 1151-1223.

Witzleb, Normann, David Lindsay, Moira Paterson, en Sharon Rodrick. *Emerging Challenges in Privacy Law: Comparative Perspectives.* Editor: Normann Witzleb, David Lindsay, Moira Paterson, & Sharon Rodrick. Cambridge: Cambridge University Press, 2014.