Cloud diensten in hoger onderwijs en onderzoek en de USA Patriot Act

Dr. J.V.J. van Hoboken, Mr. A.M. Arnbak & prof. Dr. N.A.N.M. van Eijk,

m.m.v. mr. N.P.H. Kruijsen

Instituut voor Informatierecht

Universiteit van Amsterdam

http://www.ivir.nl

september 2012

Versie 1.1 (spelfout naam en titel van mr. Kruijsen en opmaakfout pagina 32 verwijderd).

Instituut voor Informatierecht
Faculteit der Rechtsgeleerdheid
Universiteit van Amsterdam
Kloveniersburgwal 48
1012CX Amsterdam
http://www.ivir.nl
t +31 (0)20 525 3406

Management samenvatting

De overgang naar cloud computing levert de nodige vragen op. Een van de terugkerende vragen is of deze overgang consequenties heeft voor de toegang tot gegevens door buitenlandse overheden. Daarbij wordt typisch verwezen naar de Amerikaanse overheid en de zogenaamde Patriot Act, die het mogelijk zou maken dat gegevens van Nederlandse gebruikers van cloud diensten worden opgevraagd vanuit de VS. Deze notitie beantwoordt in opdracht van SURFdirect[1] de vraag in hoeverre dat het geval is, vanuit het perspectief van de kennisinstellingen in Nederland. Verder onderzoekt deze notitie de vraag hoe het beste omgegaan zou moeten worden met dit risico.

Er kan worden vastgesteld dat de Patriot Act een symboolfunctie is gaan spelen in het debat. Daarom wordt in deze notitie niet alleen gekeken naar deze specifieke wetgeving uit 2001, maar naar het bredere juridisch kader in de VS en Nederland voor wat betreft de toegang tot gegevens in het kader van strafvordering en nationale veiligheid. De notitie plaatst het vastgestelde juridische risico vervolgens in breder perspectief door te kijken naar de organisatie van de vertrouwelijkheid en veiligheid van gegevens in het algemeen. Op basis van de gemaakte analyse worden tenslotte aanbevelingen gedaan voor geïnformeerde besluitvorming in de sector.

Het antwoord op de gestelde vraag naar de mogelijkheden op toegang tot gegevens in de cloud voor justitie en veiligheidsdiensten in de VS is tegelijk simpel en complex. Wetgeving in de Verenigde Staten en Nederland zorgt ervoor dat politie, justitie of veiligheidsdiensten linksom of rechtsom een mogelijkheid hebben om gegevens van kennisinstellingen en betrokkenen op te vragen. De overgang naar cloud computing brengt hier in beginsel geen verandering in. Indien gebruik gemaakt wordt van een cloud dienst die onder Amerikaanse jurisdictie valt bestaat er de mogelijkheid dat gegevens direct in de VS bij de betreffende onderneming worden opgevraagd. Indien er geen jurisdictie is, bestaat de mogelijkheid dat gegevens worden opgevraagd via samenwerking met Nederlandse justitie of veiligheidsdiensten, bij een cloud dienst of bij de instelling zelf. Het voorkomen dat enige toegang plaatsvindt is gezien deze stand van zaken in elk geval juridisch niet mogelijk en garanties op dat punt zijn dus ook niet te geven.

Tegelijkertijd bestaan er significante verschillen tussen de mogelijkheden tot toegang door Amerikaanse autoriteiten. Zo is er in het geval dat gegevens direct opgevraagd kunnen worden bij de cloud dienst onder Amerikaanse wetgeving zeer beperkte rechtsbescherming voor Nederlandse gebruikers van deze dienst, terwijl zulke rechtsbescherming wel geldt in het geval

[1] SURFdirect is onderdeel van SURF, de ICT-samenwerkingsorganisatie voor het hoger onderwijs en onderzoek.

van bevragingen onder Nederlandse wetgeving. De Amerikaanse constitutionele waarborgen op het gebied van bevragingen door de Amerikaanse overheid zijn niet van toepassing op Nederlandse gebruikers van de cloud. En de rechtsbescherming in specifieke Amerikaanse wetgeving ziet voornamelijk op Amerikaanse burgers en ingezetenen.

De betreffende Amerikaanse wetgeving biedt tegelijkertijd ruime mogelijkheden gegevens uit de cloud op te vragen, een mogelijkheid die in het geval van veiligheidsdiensten erg laagdrempelig is te noemen. Het gaat daarbij nadrukkelijk niet slechts om de Patriot Act uit 2001, maar om een complex en dynamisch geheel aan bevoegdheden van de Amerikaanse overheid op het gebied van opsporing en nationale veiligheid. Buiten het schetsen van het wettelijk kader, is er gezien het karakter van het handelen van deze diensten in de praktijk geen zicht te krijgen op de werkelijke bevragingen van gegevens vanuit de VS. Ondernemingen zullen typisch geen enkele mededeling kunnen doen over de vraag of bevragingen plaatsvinden. Wel is te verwachten dat het opvragen van gegevens uit de cloud door overheden zal toenemen. Het gebrek aan aandacht in de VS voor de belangen van vertrouwelijkheid van gegevens van niet-Amerikanen maakt de situatie er vanuit Nederlands perspectief niet beter op. Het verdient opmerking dat het gaat om een onderwerp dat reeds op de agenda is geplaats in het Nederlandse parlement, alsmede in Brussel bij het Europese Parlement, de Europese Commissie en de Artikel 29 Werkgroep voor gegevensbescherming.

Deze notitie concludeert dat het voor de instellingen zaak is om zicht te krijgen en blijven hebben op de verschillende modaliteiten van toegang door justitie en veiligheidsdiensten en de daarmee samenhangende risico's voor kennisinstellingen goed in kaart te brengen. Het verdient aanbeveling deze observatie deel te laten uitmaken van een algemene maatschappelijke kosten-baten analyse, waarin alle op het spel staande belangen op het gebied van de informatiehuishouding worden meegenomen. Daarbij moet gedacht worden aan de belangen van informatieveiligheid, en vertrouwelijkheid, de privacy van betrokkenen, alsmede de voor de instellingen karakteristieke belang van de academische vrijheid en het gevaar van chilling effects op het gedrag van betrokkenen. Het is aan te bevelen binnen de sector een risicoanalyse te maken op basis van een categorisering van de verschillende soorten gegevens die het onderwerp zou kunnen worden van bevragingen. Voor gegevens waarvoor het risico onaanvaardbaar wordt geacht dat deze daadwerkelijk in handen zouden kunnen komen van een buitenlandse overheid, zonder dat daarover enige transparantie bestaat, zouden alternatieven ontwikkeld kunnen worden binnen de sector.

Dat toegang door overheden plaatsvindt is uiteraard geen nieuw gegeven. De te maken afwegingen bij de overgang naar cloud computing kunnen voortbouwen op binnen de instellingen bestaande protocollen, voorlichting en afwegingen ten aanzien van daadwerkelijke bevragingen. Het onderwerp dient bij het aangaan van cloud diensten besproken te worden en

voorkomen moet worden dat op dit punt schijnzekerheden worden geboden door cloud providers. De mogelijkheid dat bevragingen vanuit het buitenland plaatsvinden is geen risico dat door middel van contractuele waarborgen kan worden uitgesloten en Nederlandse wetgeving op het gebied van privacy is ook geen waarborg. De vraag of een onderneming onder Amerikaanse jurisdictie valt, hetgeen al snel het geval is, dient door de betreffende onderneming zelf en overtuigend beantwoord te kunnen worden. Het is een hardnekkige misvatting dat er geen jurisdictie bestaat onder Amerikaans recht als de gegevens niet op Amerikaans grondgebied zijn opgeslagen. Het criterium in dit kader is of de cloud provider structureel activiteiten binnen de VS ontplooit, bijvoorbeeld door een vestiging te hebben, of onderdeel te zijn van een in de VS gevestigde onderneming die controle heeft over de betreffende gegevens.

Door de overgang naar cloud diensten zal in beginsel sprake zijn van een vermindering van de autonomie van de instellingen ten aanzien van de omgang met bevragingen. Daarom dient goed gekeken te worden naar de specifieke risico's bij bepaalde categorieën van gegevens, waaronder de vraag of er gegevens zijn waarvoor dit gebrek aan autonomie onaanvaardbaar is. Verantwoordelijken binnen de instellingen dienen verder te beseffen dat het geen probleem betreft dat na een enkele besluitvormingsronde van tafel is. Het betreft een onderwerp dat een heldere plaats dient te krijgen in de doorlopende besluitvorming over cloud computing in de sector. Er dient op hoog niveau meegedacht te worden over alternatieven die betere rechtsbescherming zouden kunnen bieden. De gedachtevorming over een nationale cloud kunnen hier een uitkomst bieden. Er kan vanuit de sector input geleverd worden voor het politieke debat over de ruime jurisdictie en toegang die de Amerikaanse overheid zich toebedeelt. En er dient voorkomen te worden dat lock-in het onmogelijk maakt dat voortschrijdend inzicht kan leiden tot nieuwe besluitvorming over dit complexe onderwerp.

Inhoudsopgave

1. Inleiding en vraagstelling

1.1 Cloud diensten en de Patriot Act

Er is de laatste jaren volop discussie over de vraag naar de juridische implicaties van cloud computing. Dit debat is ook relevant voor de hoger onderwijs- en onderzoekssector, gezien de lopende ontwikkelingen rondom cloud computing in de sector. Gezien de rol van SURF, de ICT-samenwerkingsorganisatie voor het hoger onderwijs en onderzoek en opdrachtgever van dit onderzoek, bestaat bij haar de behoefte een goed beeld te hebben van het bestaande juridisch kader. Zo kan zij haar rol in de discussie omtrent de besluitvorming over het aangaan van cloud dienstverlening door kennisinstellingen zo effectief mogelijk spelen.[2] Het gaat daarbij om een breed scala aan cloud diensten waaronder e-mail, doc-sharing, en contacts.[3]

Een belangrijk aspect in de discussie is de vraag of de informatieveiligheid en de vertrouwelijkheid van gegevens bij de overgang naar cloud computing gewaarborgd blijft. Wat zijn de gevolgen voor de privacy, de bescherming van persoonsgegevens en de informatieveiligheid indien gegevens van studenten, onderzoekers en bestuurders niet langer binnen een eigen ICT-omgeving worden beheerd, maar terecht komen in een door een derde, mogelijk buitenlandse partij aangeboden elektronische omgeving? Staat de Nederlandse en Europese privacywetgeving toe dat dit soort gegevens door een Amerikaanse aanbieder – de belangrijkste aanbieders van clouddiensten zijn van Amerikaanse origine - worden opgeslagen buiten Europees grondgebied, waar minder strenge regels gelden ten aanzien van de bescherming van persoonsgegevens?[4] En bestaat de mogelijkheid dat de aanbieder van de betreffende dienst door buitenlandse overheidsdiensten wordt verplicht om gegevens over te dragen aan buitenlandse overheden in verband met strafrechtelijk onderzoek of de nationale veiligheid? En als dit het geval is, hoe dienen die mogelijkheid en de daarmee samenhangende risico's dan beoordeeld te worden?

Deze notitie spitst zich toe op die laatste twee vragen: wat is de consequentie van de overgang naar cloud computing voor toegang tot gegevens voor buitenlandse veiligheidsdiensten en strafrechtshandhavers en wat zijn de risico's daarvan voor instellingen voor hoger onderwijs en onderzoek (hierna: de kennisinstellingen) in Nederland? Er is op dit moment in het bijzonder discussie en onduidelijkheid over de betekenis van de bestaande wet- en regelgeving in de Verenigde Staten. De discussie wordt dan in het bijzonder beheerst door de vraag naar de betekenis van de zogenoemde 'Patriot Act'. Deze, alsmede vergelijkbare wettelijke bepalingen in de VS, zoals de 'Foreign Intelligence Surveillance Act', scheppen de mogelijkheid dat gegevens van Nederlandse gebruikers van cloud diensten worden opgevraagd door Amerikaanse overheidsdiensten. Als gevolg van deze mogelijkheid is

[2] Zie bijvoorbeeld SURF, 'Privacy en Security in de Cloud', http://www.surfsites.nl/cloud/wat-is-cloud/privacy-en-security-in-de-cloud/. Zie ook SURFNET 2010.

[3] In deze notitie wordt aangesloten bij de gangbare definitie van cloud computing van het NIST: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Zie NIST 2011, p.2.

[4] Hier is in opdracht van SURF onderzoek naar gedaan door TILT. Zie TILT 2011. Zie ook Article 29 Working Party 2012.

de Patriot Act een veel voorkomende verwijzing in de discussies over de cloud. Dat geldt voor discussies in de media, in de politiek, en in beleidskringen in Nederland, maar ook daarbuiten zoals bij kennisinstellingen die onderhandelen over cloud computing contracten. Het is gezien deze discussies van belang om zicht te hebben op deze juridische bepalingen, zodat een heldere inschatting gemaakt kan worden van de risico's voor de privacy van eindgebruikers en informatieveiligheid van de opgeslagen gegevens. Deze studie beoogt deze helderheid te verschaffen in een discussie waarin grote behoefte bestaat aan een overzicht van de daadwerkelijke feiten en risico's.

1.2 Vraagstelling

Deze notitie richt zich op de vraag naar de consequenties van de Patriot Act (USA PATRIOT Act) en de daaruit voortvloeiende risico's voor de privacy, de informatieveiligheid en vertrouwelijkheid ten gevolge van cloud computing bij kennisinstellingen. Gezien de inhoud van de Patriot Act gaat het om de vraag naar de bevoegdheden van overheidsinstanties (in het bijzonder Amerikaanse) om toegang te krijgen tot gegevens in de cloud in verband met de strafrechtelijke handhaving en de nationale veiligheid. Dit is een andere vraag dan de hierboven genoemde problematiek met betrekking tot de naleving van het Europese en Nederlandse recht met betrekking tot de bescherming van persoonsgegevens.

Om een goed antwoord te kunnen geven op de vraag of de informatieveiligheid en privacy van gebruikers in het kader van cloud computing voldoende blijft gewaarborgd, zijn een aantal zaken van belang. Ten eerste dient opgemerkt te worden dat de Patriot Act een bepaalde symboolfunctie is gaan spelen in het publieke debat, maar dat er in de praktijk sprake is van een complexer samenspel van juridische bevoegdheden en waarborgen in de Amerikaanse wetgeving in het kader van de toegang tot gegevens voor strafvordering en nationale veiligheidsdoeleinden. Gezien deze complexiteit dient een studie naar de betekenis van een bepaald juridisch instrument zoals de Patriot Act zich uit te strekken tot het geheel aan vergelijkbare normen in de betreffende nationale wetgeving. De zorgen in Europa over de toegang tot cloud gegevens zijn verder gezien de op het spel staande handelsbelangen voor de betrokken Amerikaanse industrie niet onopgemerkt gebleven.[5] Dit zorgt er voor dat een deel van de informatievoorziening op dit gebied gekleurd is door het strategisch belang de bestaande zorgen weg te nemen.[6]

Ten tweede is het niet slechts de vraag wat de implicaties en risico's zijn van dat specifieke wettelijk kader voor cloud computing, maar ook in hoeverre deze risico's verschillen al naar gelang de modaliteit van de betreffende diensten. Daarbij spelen een reeks van vragen over het bestaan van jurisdictie en de relevantie van de geografische locatie waar de data worden opgeslagen. Dit zijn vragen die in het debat over cloud computing en de Patriot Act nadrukkelijk een rol spelen.[7] Zijn de risico's voor de privacy en informatieveiligheid daadwerkelijk kleiner bij alternatieven voor diensten van bedrijven als Google en Microsoft, als bijvoorbeeld gegevens worden opgeslagen op Nederlands of Europees grondgebied? Wat is de waarde van contractuele waarborgen in dat kader? In hoeverre maakt het voor de besproken

[5] Zie bijvoorbeeld Rauf 2011.

[6] Zie bijvoorbeeld Kennard 2012 En recentelijk, Hogan Lovells 2012 (een advocatenkantoor voor de cloud industrie).

[7] Zie bijvoorbeeld Baker 2011; Bruins 2011, p. 48; Betlem 2012.

bepalingen verschil indien de aanbieder een Amerikaanse (hoofd)vestiging heeft? En wat zijn de voordelen van een Europese- of strikt Nederlandse organisatie van cloud diensten voor het Nederlands hoger onderwijs en onderzoek?

Ten derde is het van belang om de betreffende risico's voor de informatieveiligheid en privacy in een breder perspectief te plaatsen. Het is daarbij uitdrukkelijk de vraag of er in onevenredige mate aandacht wordt besteed aan de risico's samenhangend met de Patriot Act. Andere nationale staten, inclusief Nederland kennen daarmee vergelijkbare bepalingen voor toegang tot gegevens in het kader van strafrechtelijke handhaving en nationale veiligheid. En vanuit het perspectief van de informatieveiligheid verdienen andere aan cloud computing verbonden risico's en afhankelijkheden mogelijk net zoveel aandacht. Een breder inzicht in deze risico's en afhankelijkheden is noodzakelijk om te komen tot goed geïnformeerde beleidsvorming omtrent cloud computing die rekening houdt met de mogelijkheid dat gegevens kunnen worden opgevraagd door buitenlandse overheden.

1.3 Opbouw van de notitie

Deze notitie zal gezien het bovenstaande bestaan uit drie delen, alsmede een conclusie met aanbevelingen. Het eerste deel (paragraaf 2) betreft een beschrijving en uitleg van de Patriot Act en vergelijkbare relevante wetgeving in de VS. Daarbij wordt ook aandacht geschonken aan de constitutionele waarborgen voor privacy en vertrouwelijkheid van gegevens in de VS (*Fourth Amendment*) en het dynamische karakter van het bestaande wettelijke kader, zoals recente ontwikkelingen op het gebied van cybersecurity wetgeving duidelijk maken. En er wordt een korte schets gegeven van het bestaande wettelijk kader in Nederland voor de bevraging van cloud providers, alsmede een aantal voorbeelden van wetgeving in andere Europese landen.

Het tweede deel (paragraaf 3) bespreekt de betekenis van het beschreven Amerikaanse wettelijk kader voor de bevraging van cloud providers in het kader van strafvordering en nationale veiligheid voor de afname van cloud diensten vanuit Nederland. Daarbij wordt eerst een beoordeling gegeven van de bestaande mogelijkheden tot toegang van Amerikaanse autoriteiten tot cloud data van buitenlandse kennisinstellingen in zowel sfeer van buitenlandse inlichtingen alsmede de strafvorderlijke sfeer. Deze mogelijkheden worden in context geplaatst door kort een vergelijking te maken met het wettelijk kader in Europa en Nederland. Vervolgens wordt de betekenis van het bestaande juridisch kader voor de praktijk inzichtelijk gemaakt aan de hand van drie scenario's. In deze scenario's is steeds sprake van een bevraging door overheidsinstanties van gegevens uit de cloud. In de scenario's komen de verschillende cloud varianten en de betekenis van deze varianten voor de mogelijkheden tot bevraging, de rechtsbescherming van betrokkenen.

Het derde deel van deze notitie (paragraaf 4) beantwoordt de vraag hoe de risico's van de bestaande mogelijkheden in de Amerikaanse wetgeving door kennisinstellingen in Nederland in juridische zin ingeschat dienen te worden. Bij de beantwoording van deze vraag wordt nadrukkelijk aandacht besteed aan de wijze waarop de beschreven problematiek in het bestaande kader voor de bescherming van de vertrouwelijkheid van gegevens ingebed moet worden.

1.4 Verantwoording

Het onderzoek voor deze notitie is door het Instituut voor Informatierecht (IViR, Universiteit van Amsterdam, www.ivir.nl) uitgevoerd in opdracht van SURF Digital Rights Expertise Community (SURFdirect), onderdeel van SURF, de ICT-samenwerkingsorganisatie voor het hoger onderwijs en onderzoek. Het IViR hanteert bij het verrichten van onderzoek in opdracht van derden de uitgangspunten zoals neergelegd in de door de KNAW opgestelde verklaring van wetenschappelijke onafhankelijkheid.[8] Het project is uitgevoerd door dr. J.V.J. van Hoboken, mr. A.M. Arnbak, prof. dr. N.A.N.M. van Eijk met medewerking van N. Kruijssen. Het onderzoek is gedaan op basis van literatuuronderzoek.

[8] http://www.knaw.nl/content/Internet_KNAW/actueel/bestanden/wetenschappelijke_onafhankelijkheid.pdf

2. Cloud computing en gegevensvordering vanuit de VS: het juridisch kader

Deze paragraaf beschrijft het Amerikaanse juridische kader voor gegevensvordering met betrekking tot cloud computing. Eerst wordt een algemeen beeld geschetst van de Amerikaanse constitutionele waarborgen voor de privacy bij overheidstoegang tot gegevens (*Fourth Amendment*) en de door het *United States Supreme Court* ontwikkelde doctrines ten aanzien van de bescherming die het *Fourth Amendment* biedt. Daarna wordt stilgestaan bij de wetgeving die overheidsinstanties toegangsbevoegdheden bieden, zoals de Patriot Act, de Foreign Intelligence Surveillance Act (FISA), de bepalingen uit de recente FISA Amendments Act van 2008 (FAA) en relevante bepalingen buiten de sfeer van de inlichtingendiensten, zoals de Electronic Communications Privacy Act (ECPA) en de recent voorgestelde Cyber Intelligence Sharing and Protection Act (CISPA). Tenslotte wordt een breder perspectief geboden op het juridisch kader voor gegevensvordering met betrekking tot cloud computing, door kort stil te staan bij vergelijkbare wetgeving in Europese landen en Nederland in het bijzonder, en de hier geldende constitutionele waarborgen op het gebied van de toegang tot gegevens in de cloud door de overheid.

2.1 Constitutionele bescherming in de Verenigde Staten

In het *Fourth Amendment* van de *Bill of Rights* in de Amerikaanse grondwet is het recht op bescherming tegen onredelijke doorzoekingen en inbeslagnames neergelegd:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[9]

In *Katz v. United States* heeft het *Supreme Court* bepaald dat deze bescherming situaties omvat waarin iemand een 'reasonable expectation of privacy' heeft.[10] De zogenaamde *Third Party Doctrine* levert echter vervolgens een belangrijke beperking op ten aanzien van deze bescherming.[11] Deze doctrine houdt in dat wanneer men persoonlijke informatie overdraagt aan een derde partij, zoals een financiële dienstverlener, men in beginsel geen redelijke verwachting op privacy kan hebben.[12] De constitutionele bescherming van het *Fourth Amendment* komt daarmee te vervallen in situaties waarin gegevens door derde partijen worden beheerd. De *Third Party Doctrine* wordt door commentatoren problematisch geacht voor de Internet omgeving, omdat het afstaan van gegevens inherent is aan het gebruik van het internet. Op grond van de doctrine, komt iemand die zijn gegevens afstaat aan een elektronische dienstverlener, zoals een Internet Service Provider (ISP), in beginsel niet langer een beroep toe op een constitutioneel gewaarborgde 'reasonable expectation of privacy'.[13]

[9] United States Constitution, Bill of Rights, Adopted 1791.
[10] *Katz v. United States*, 389 U.S. 347, 361 (1967).
[11] *Katz v. United States*, 389 U.S. 347, 361 (1967). Zie ook *United States v. Miller*, 425 U.S. 435, 443 (1976).
[12] Zie ook Solove 2004, p. 200-209.
[13] Voor een discussie, zie Kerr 2004, p. 3.

Van belang in het kader van deze studie is verder dat de bovengenoemde bescherming uit het *Fourth Amendment* alleen door Amerikaanse burgers kan worden ingeroepen, alsmede door buitenlanders die zodanige banden met de Verenigde Staten hebben ontwikkeld dat ze deel uitmaken van de Amerikaans samenleving. Zoals het *Supreme Court* in de zaak *United States v. Verdugo-Urquidez* het stelt:

> There is [...] no indication that the Fourth Amendment was understood by contemporaries of the Framers to apply to activities of the United States directed against aliens in foreign territory or in international waters.[14]

Dat betekent dat Nederlandse of andere buitenlandse 'gebruikers' van Amerikaanse cyberspace, die verder geen banden met de VS onderhouden, geen bescherming van het *Fourth Amendment* toekomt.[15] In de Amerikaanse literatuur is vervolgens veel discussie over de vraag wat deze bescherming voor Amerikaanse burgers precies inhoudt. Aangezien deze bescherming voor Europeanen in beginsel echter niet geldt is deze discussie voor deze studie dus in beginsel niet relevant.[16] Het *Supreme Court* geeft in haar rechtspraak aan dat (met het *Fourth Amendment*) vergelijkbare bescherming via andere politieke wegen zal moeten worden afgedwongen maar niet kan worden afgeleid uit de Amerikaanse grondwet:

> If there are to be restrictions on searches and seizures which occur incident to such American action, they must be imposed by the political branches through diplomatic understanding, treaty, or legislation.[17]

Er moet op grond van het bovenstaande worden geconcludeerd dat het *Fourth Amendment* geen rol van betekenis speelt bij de vraag of Amerikaanse overheidsinstanties toegang kunnen krijgen tot gegevens van gebruikers van cloud diensten vanuit Nederland, als die diensten onder Amerikaanse jurisdictie vallen.

De vraag welke diensten onder Amerikaanse jurisdictie vallen is beantwoord in de Amerikaanse rechtspraak, onder meer in rechtspraak over toegang tot gegevens bij buitenlandse banken met activiteiten in de VS. Zodra er sprake is van 'activiteiten binnen de grenzen van de Verenigde Staten', is het Amerikaanse recht in beginsel van toepassing.[18] Indien een onderneming een vestiging in de VS heeft kan er vanuit gegaan worden dat er jurisdictie bestaat, maar ook in andere complexere gevallen kan jurisdictie bestaan. Een recent rapport over cloud computing vat het als volgt samen:

> The United States [...] takes the position that it can use its own legal mechanisms to request data from any Cloud server located anywhere around the world so long as the Cloud service provider is subject

[14] *United States v. Verdugo-Urquidez*, 494 U.S. 259, 267 (1990).

[15] Zie Banks, p. 1656-1657.

[16] Zie bijvoorbeeld Banks, voetnoot 23 en bijbehorende tekst ("The Constitution continues to provide a baseline. The Fourth Amendment Warrant Clause applies to electronic surveillance conducted for foreign intelligence purposes within the United States if the surveillance involves U.S. persons who do not have a connection to a foreign power.").

[17] *United States v. Verdugo-Urquidez*, 494 U.S. 259, 275 (1990).

[18] *United States v. Bank of Nova Scotia*, 740 F.2d 817 (11th Cir. 1984). In deze uit 1984 daterende zaak bepaalde de *US Supreme Court* dat de plaats van dataopslag niet doorslaggevend is: "*The foreign origin of the subpoenaed documents should not be a decisive factor.*" Het principe van extra-territoriale jurisdictie wordt ook elders toegepast, bijvoorbeeld in Australië. Zie *Bank of Valletta PLC v. National Crime Authority* [1999] FCA 1099.

> U.S.jurisdiction: that is, when the entity is based in the United States, has a subsidiary or office in the United States, or otherwise conducts continuous and systematic business in the United States.[19]

De locatie waar de mogelijk op te vragen gegevens door een dienstverlener worden opgeslagen is dus in elk geval niet leidend voor de beantwoording van de vraag of een dienstverlener onder Amerikaanse jurisdictie valt en als gevolg daarvan geconfronteerd zou kunnen worden met de uitoefening van wettelijke bevoegdheden inzake toegang tot gegevens van gebruikers van deze dienstverlener.

Naar aanleiding van de Nederlandse parlementaire discussie over biometrische gegevens bij het bedrijf Morpho is de minister van Binnenlandse Zaken op basis van een advies van de Landsadvocaat tot een vergelijkbare conclusie gekomen. Er bestaat een mogelijkheid tot het vorderen van gegevens vanuit de VS indien de activiteiten van de betreffende onderneming in de VS een continu en systematisch karakter hebben. Ook bestaat die mogelijkheid ten aanzien van gelieerde ondernemingen met activiteiten in de VS, indien deze ondernemingen bezit, bewaring, of controle hebben over de betreffende gegevens.[20]

2.2 Wettelijk kader VS bevoegdheden tot toegang (Patriot Act, FISA, FAA, ECPA, SCA)

2.2.1 Introductie

De Amerikaanse wet- en regelgeving kent een reeks specifieke bepalingen die overheidsinstanties bevoegdheden geven tot het verkrijgen van toegang tot gegevens. Hieronder volgt een overzicht van de wetgeving en bepalingen die het meest relevant zijn vanuit de Nederlandse context en de voorwaarden en rechtsbescherming die bij deze bepalingen wordt geboden door de Amerikaanse wet- en regelgeving.

Het betreft een complex en uitgebreid geheel aan wetgeving voor de uitoefening van dwangmiddelen in het kader van de strafvordering en nationale veiligheid. Daarbij moet worden opgemerkt dat een groot deel van de betreffende bepalingen de eisen weerspiegelen die op grond van de Amerikaanse grondwet gelden voor het verkrijgen van inlichtingen over *Amerikaanse* burgers of ingezetenen. In sommige gevallen, zoals de ECPA, heeft de Amerikaanse wetgever het ontbreken van duidelijke constitutionele bescherming voor de privacy en vertrouwelijkheid van communicatie gecompenseerd door het stellen van wettelijke grenzen.

Achtereenvolgens wordt stilgestaan bij de Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act), de FISA (Foreign Intelligence Surveillance Act), de FAA (FISA Amendments Act van 2008) en de ECPA (Electronic Communications Privacy Act).

2.2.2 De Patriot Act

De Patriot Act werd in 2001 aangenomen in de nasleep van 9/11, en wordt vaak gezien als de wet die als gevolg heeft dat “gegevens die door een Amerikaans bedrijf worden beheerd, altijd opgevraagd kunnen

[19] Zie Hogan Lovells 2012, p. 5.

[20] Tweede Kamer 2011-2012, 31 734, nr. 8, p.2.

worden door de Amerikaanse overheid".[21] Deze zienswijze is een sterk vereenvoudigde weergave van de juridische stand van zaken in de Verenigde State. De Patriot Act is geen zelfstandige wetgeving maar in feite een veelomvattende wetswijziging. Het bevat op sommige punten een vereenvoudiging van de toen bestaande procedures tot het opvragen van data bij bedrijven, zoals het later besproken artikel 50 USC 1861.[22] De Patriot Act kende echter zelf weinig nieuwe bevoegdheden toe en moet hoofdzakelijk worden opgevat als een kaderregeling die tal van andere, oudere wetten op verschillende wijzen amendeerde.[23] De Patriot Act en de wetten die deze amendeerde zijn verder sinds 2001 een aantal keer gewijzigd en sommige delen ervan - met bevoegdheden die voorzien waren van een zogenaamde 'sunset clause' - zijn verlengd.[24] De laatste verlenging vond plaats op 26 mei 2011.[25]

De voor deze studie belangrijkste bepalingen uit de Patriot Act behelzen een aanpassing van de Foreign Intelligence Surveillance Act (FISA) en de Electronic Communications Privacy Act (ECPA). De FISA ziet op de verkrijging van buitenlandse inlichtingen (*foreign intelligence*) door middel van aftappen, doorzoekingen en bevragingen van gegevens in het kader van de bescherming van de nationale veiligheid. De ECPA ziet op het aftappen en verkrijgen van gegevens bij elektronische communicatie diensten in het kader van de strafrechtelijke handhaving. Na de wijzigingen van de FISA door de Patriot Act vonden recentelijk twee andere belangrijke wijzigingen van de FISA plaats: de Protect America Act (PAA) van 2007 en in 2008 de FISA Amendment Act 2008 (FAA). Bij deze laatste wijziging is er een specifieke bepaling toegevoegd die ziet op het opvragen van gegevens van ´niet-Amerikaanse personen verblijvend in het buitenland´.

In het vervolg wordt beschreven onder welke voorwaarden toegang tot gegevens door een Amerikaanse overheidsinstantie tot de wettelijke mogelijkheden behoort. Een analyse van de verdere verwerking en uitwisseling van deze gegevens en de specifieke overheidsinstanties en functionarissen die daarbij een rol spelen gaat de reikwijdte van deze studie te buiten. Daarbij moet ook worden opgemerkt dat er maar beperkt informatie beschikbaar is over de afhankelijkheden en samenwerking tussen en de overlappende taakstellingen van de betrokken verantwoordelijken en organisaties, zoals de Attorney General, de Director of National Intelligence, de NSA, the US Marshals en de FBI. De Washington Post

[21] Zie Whittaker 2011. De Patriot Act is ook meermalen in de Nederlandse parlementaire discussies op deze wijze aangehaald. Zie bijvoorbeeld *Kamerstukken II* 2010/11, 3516 (Kamervragen lid Elissen (PVV) over Europese data die beheerd wordt door Amerikaanse bedrijven). *Kamerstukken II 2*010/11, 3514 (Kamervragen lid Schouw (D66) over het artikel 'Amerika graait in Europese clouddata'). *Kamerstukken II* 2010/11, 3515 (Kamervragen lid Gesthuizen (SP) over het door Google verstrekken van internetdata aan Amerikaanse autoriteiten). Zie ook Udo de Haes 2011.

[22] Zo maakte Patriot Act, Title II, Section 220, het mogelijk via de federale rechter een nationaal opsporingsbevel te verkrijgen, waar voorheen meerdere bevelen nodig waren per staat. Zie Department of Justice 2005, p. 59.

[23] Zie Kerr 2003, p. 607-608.

[24] het betreft bijvoorbeeld de *USA PATRIOT Improvement and Reauthorization Act of 2005*, de *USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006*, *An Act To Extend Expiring Provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005*, de *FISA Sunsets Extension Act of 2011* en de *USA PATRIOT Sunsets Extension Act of 2011*.

[25] The PATRIOT Sunsets Extension Act of 2011 (H.R. 514) Pub. L. 112-14 (26 mei 2011).

heeft recentelijk een studie gepubliceerd van het complexe samenspel tussen de bij de veiligheid betrokken instanties in de VS.[26]

2.2.3 De Foreign Intelligence Surveillance Act (FISA) en de FISA Amendment Act 2008 (FAA)

Binnen het Amerikaanse wettelijk kader faciliteert de Foreign Intelligence Surveillance Act (FISA) het verkrijgen van buitenlandse inlichtingen (50 USC 1801-1885c) door de Amerikaanse overheid.[27] De Patriot Act heeft de bevoegdheden uit deze wet op enkele plaatsen gewijzigd. Hetzelfde geldt voor de FISA Amendments Act (FAA) in 2008.[28] Deze laatste wet is van bijzonder belang in het kader van deze studie. De FAA voorziet namelijk in een nieuwe regeling voor de bevoegdheid tot het verkrijgen van gegevens van niet-Amerikaanse personen verblijvend in het buitenland door Amerikaanse overheidsdiensten die buitenlandse inlichtingen vergaren ten behoeve van de nationale veiligheid. Deze regeling is te vinden in onderdeel 702 van de FAA en het daarmee ingevoerde artikel 50 USC 1881a (in het hoofdstuk 'aanvullende bevoegdheden voor personen buiten de VS') en wordt hieronder toegelicht. Daarna wordt stilgestaan bij een aantal overige bevoegdheden uit de FISA die vanuit de vraagstelling van deze studie relevant zijn.

De betekenis van artikel 50 USC 1881a vanuit Nederlands perspectief is het beste te begrijpen door te kijken naar een combinatie van drie elementen. Ten eerste de reeds besproken constitutionele bescherming van Amerikanen en het ontbreken van deze bescherming voor niet-Amerikaanse personen verblijvend in het buitenland. Ten tweede de achtergrond van de FISA, namelijk het voorzien in toezicht op het vergaren van inlichtingen vanwege de mogelijkheid dat daarbij de grondrechten van Amerikanen in het geding zou kunnen komen. En ten derde de recente wijzigingen van de FISA (door de FAA) in reactie op het aftappen zonder rechterlijk bevel van communicatie van Amerikanen door de regering Bush.

De oorspronkelijke FISA is een wet uit 1978. Het voert een wettelijk kader in voor het vergaren van buitenlandse inlichtingen door middel van *electronic surveillance.* De FISA werd ingevoerd als reactie op het misbruik van dergelijk handelen door Amerikaanse inlichtingendiensten. De wet kan worden opgevat als een compromis tussen twee belangen. Aan de ene kant het faciliteren van de verkrijging van buitenlandse inlichtingen door de Amerikaanse overheid in verband met de bescherming van de Amerikaanse nationale veiligheid. En aan de andere kant het voorzien in de geldende constitutionele bescherming bij het verkrijgen van buitenlandse inlichtingen, aangezien en voor zover deze gericht zou kunnen zijn op communicatie van Amerikanen.[29]

Het was dus niet het doel van FISA Europeanen of andere buitenlanders te beschermen tegen interceptie van hun communicatie door Amerikaanse veiligheidsdiensten. En het is ook nooit de

[26] Zie The Washington Post 2011.
[27] Voor een bondig overzicht van het bepaande in de FISA, zie CRS 2007.
[28] En de Protect America Act uit 2007 die is vervangen door de FAA.
[29] Zie Banks 2007, p. 1216-1233.

bedoeling geweest om het aftappen van communicatie van buitenlanders niet-verblijvend op Amerikaans grondgebied door middel van de FISA aan banden te leggen.[30]

De FAA uit 2008 en het bepaalde in artikel 50 USC 1881a is de uitkomst van een recentere discussie in de VS omtrent het aftappen zonder rechterlijk bevel (*warrantless wiretapping)* door de NSA ten tijde van de Bush regering. De regering Bush had Amerikanen afgeluisterd zonder daarvoor en rechterlijk bevel te verkrijgen. De New York Times had hierover bericht vanaf het einde van 2005.[31] Het debat spitste zich toe op de vraag of er sprake was geweest van het ongrondwettelijk afluisteren van *Amerikaanse* burgers onder het mom van de vergaring van buitenlandse inlichtingen.

In reactie op de ontstane maatschappelijke weerstand en het pleidooi van de betrokken overheidsdiensten dat de FISA procedures geen effectieve middelen boden, heeft de Amerikaanse wetgever met de Protect America Act (PAA) in 2007 en de FAA - die de PAA verving - de FISA gemoderniseerd en deze controversiële activiteiten wettelijk geregeld. Op dit moment vindt in het Amerikaanse parlement een discussie plaats over het verlengen van de betreffende wetgeving, die anders aan het einde van 2012 zal komen te vervallen.[32] De American Civil Liberties Union (ACLU), een burgerrechtenbeweging in de VS, is van mening dat de FAA in strijd is met de Amerikaanse grondwet.[33] Overigens is de FAA, voor zover het gaat om het vergaren van buitenlandse inlichtingen over buitenlanders verblijvend in het buitenland, in de Verenigde Staten niet controversieel.[34] De discussie in de VS is er op gericht dat bij gebruik van bevoegdheden tot het afluisteren en verkrijgen van gegevens over mensen in het buitenland *Amerikanen* in hun grondrechten zouden kunnen worden aangetast.

2.2.4 Vergaring van gegevens over niet-Amerikaanse personen in het buitenland: artikel 50 USC 1881a

Artikel 50 USC 1881a is het geëigende middel voor Amerikaanse inlichtingen- en veiligheidsdiensten om inlichtingen over niet-Amerikaanse personen verblijvend in het buitenland te vergaren.[35] Deze bepaling regelt dat een speciale rechtbank, de *Foreign Intelligence Surveillance Court* (FISC), dergelijke vergaring van inlichtingen toetst in het geval betrokken Amerikaanse overheidsdiensten daarvoor de assistentie van elektronische communicatiediensten nodig hebben. Zoals blijkt uit de definities in art. 50 USC 1881 zijn de betreffende bevoegdheden van toepassing op verschillende soorten elektronische communicatie diensten, waaronder telecommunicatiediensten, elektronische communicatiediensten en *remote computing services*.[36] *Remote computing services* zijn aan het publiek aangeboden diensten op het gebied van de opslag en bewerking van gegevens met behulp van een elektronisch communicatie systeem.[37] De definitie omvat dus diensten op het gebied van cloud computing. De FAA is, in

[30] Zie Blum 2009, p. 278-279.

[31] Zie Risen & Lichtblau 2005. Voor een overzicht, zie Banks 2010, p. 1641-1643. Zie ook Blum 2009; Sims 2006.

[32] Zie bijvoorbeeld The Washington Post 2012.

[33] Zie ACLU 2008.

[34] Zie Blum, p. 295-296.

[35] Voor een bondige uitleg over deze bepaling door de Amerikaanse overheid zelf, zie Clapper and Holder 2012.

[36] Art. 50 USC 1881 (4).

[37] Art. 18 USC 2711 (2) bepaalt als volgt: “the term “remote computing service” means the provision to the public of computer storage or processing services by means of an electronic communications system”.

tegenstelling tot FISA, technologie neutraal.[38] Het maakt onder de FAA dus niet langer uit via welke technologie de onderschepte data wordt getransporteerd, zowel open transmissie via de ether met satelliet als gesloten transmissie via optische kabels vallen binnen de reikwijdte van deze bepaling.

Het initiatief voor de vergaring van gegevens op basis van 50 USC 1881a ligt bij de *Attorney General* en de *Director of National Intelligence*. Zij zijn op basis van deze bepaling bevoegd tot het gezamenlijk autoriseren van het onderwerp maken van onderzoek van niet-Amerikaanse personen verblijvend in het buitenland voor het vergaren van buitenlandse inlichtingen. De autorisatie kan voor een jaar gegeven worden. Er moet wel sprake zijn van goedkeuring vooraf door de FISC (art. 50 USC 1881a(i)(3)), tenzij sprake is van spoedeisende omstandigheden (art. 50 USC 1881a(c)(2)).

Niet voor elk individueel gebruik van de bevoegdheid in art. 50 USC 1881a is aparte gerechtelijke goedkeuring van de FISC nodig. De goedkeuring door het FISC is gericht op jaarlijkse certificeringen door de *Attorney General* en de *Director of National Intelligence*, die de doelen van de verkrijging van buitenlandse inlichtingen identificeren. In vergelijking met de situatie vóór de invoering van de FAA is dit een verzwakking van de procedurele waarborgen voor niet-Amerikaanse personen verblijvend in het buitenland. Voor het in werking treden van deze wet moest de Amerikaanse overheid per individueel geval het redelijke vermoeden (*probable cause*) aantonen dat het doel van de vergaring een buitenlandse mogendheid (*foreign power*) of een functionaris daarvan betrof, en op basis daarvan per geval goedkeuring van de FISC verkrijgen.[39] Dit betekende in de praktijk dat de Amerikaanse overheid in dit soort gevallen niet-Amerikaanse personen verblijvend in het buitenland dezelfde rechtsbescherming toekende als personen in de VS, terwijl de Amerikaanse grondwet geen bescherming vergt:

> Although FISA' s original procedures are proper for electronic surveillance of persons inside this country, such a process for surveillance of terrorist suspects overseas can slow, or even prevent, the Government's acquisition of vital information, without enhancing the privacy interests of Americans. Since its enactment in 2008, section 702 [50 USC 1881a] has significantly increased the Government's ability to act quickly.[40]

De meeste waarborgen bij art. 50 USC 1881a zijn gericht op het voldoen aan de constitutionele bescherming van Amerikaanse ingezetenen en Amerikaanse personen in het buitenland. Zo is het toezicht van de FISC erop gericht dat i) de bevoegdheid wordt gebruikt voor niet-Amerikaanse personen verblijvend buiten de VS, ii) dat de beperking ten aanzien van de rechtmatigheid van de verkrijging van geheel binnenlandse communicatie wordt nageleefd, en iii) dat de opgestelde procedures voor het gebruik van de bevoegdheid door de Amerikaanse overheid in overeenstemming zijn met het *Fourth Amendment*. De rechterlijke toetsing door de FISC levert dus eigenlijk geen rechtsbescherming op voor niet-Amerikaanse personen verblijvend in het buitenland.

Er zijn wel materiële beperkingen die voor niet-Amerikaanse personen verblijvend in het buitenland relevant geacht kunnen worden. De belangrijkste is dat – voor niet-Amerikaanse personen verblijvend in

[38] Zie ook Ohm 2010.

[39] Clapper and Holder 2012, p. 4.

[40] Clapper and Holder 2012, p. 4.

het buitenland – de vergaring van gegevens op basis van art. 50 USC 1881a gericht moet zijn op het verkrijgen van buitenlandse inlichtingen (*foreign intelligence information*).[41] De wettelijke definitie van dit begrip is echter ruim. Het omvat informatie met betrekking tot een buitenlandse mogendheid of regio in verband met de nationale defensie, nationale veiligheid of de handelingen met betrekking tot de buitenlandse zaken van de VS.[42]

Het verkrijgen van zodanige buitenlandse inlichtingen hoeft verder niet het primaire doel te zijn bij het gebruik van deze bevoegdheid. Het is voldoende als het verkrijgen van dergelijke inlichtingen een belangrijk doel is.[43] Deze toets is met de invoering van de FAA minder streng geworden.[44]

> In addition, non-U.S. person targets do not have to be suspected of being an agent of a foreign power nor, for that matter, do they have to be suspected of terrorism or any national security or other criminal offense, so long as the collection of foreign intelligence is a significant purpose of the surveillance.[45]

Ook is met de FAA de eis komen te vervallen dat het doel van het gebruik van de bevoegdheid bestaat uit het vergaren van informatie over een buitenlandse mogendheid (*foreign power*), zoals een terrorist of buitenlandse spion, zoals gedefinieerd in art. 50 USC 1801(a). Het is voldoende dat sprake is van gerichtheid op niet-Amerikaanse personen verblijvend in het buitenland. De vergaring van gegevens hoeft evenmin gericht te zijn op specifieke verdachte personen, maar kan gericht zijn op algemenere en andersoortige doelen zoals NGOs, media organisaties of geografische regio's in het buitenland.[46] Oftewel, het doel zou kunnen bestaan uit het vergaren van informatie over een onderzoeksgroep op een bepaalde universiteit in Nederland.

Ten gevolge van het karakter van de wetgeving zijn over de specifieke inzet van de bevoegdheid weinig details beschikbaar. De details met betrekking tot de inzet van de bevoegdheid in art. 50 USC 1881a zijn niet openbaar.[47] Naast het toezicht door het FISC is sprake van verplichte halfjaarlijkse interne rapportages over de vergaring van gegevens op basis van art. 50 USC 1881a. Deze rapportages zijn echter geheim en worden alleen gestuurd aan de speciale commissie voor de nationale veiligheid in het Amerikaanse parlement en de FISC.[48] De openbare rapportage verplichting in de FISA strekt zich niet uit tot getallen over de inzet van art. 50 USC 1881a. Door deze openbare rapportages wordt bijvoorbeeld wel bekend hoe vaak gebruik gemaakt is van de bevoegdheid om toegang te krijgen tot bedrijfsgegevens

[41] Voor de definitie van *foreign intelligence information,* zie 50 USC 1801(d).

[42] De ACLU stelt bijvoorbeeld dat het kan gaan om "journalists, human rights researchers, academics, and attorneys [..]Think [...] of an academic who is writing about the policies of the Chávez government in Venezuela, [...]. Zie ACLU 2008.

[43] 50 U.S.C. sec. 1804(a)(6)(b). Zie ook Seamon & Gardner 2005, p. 324.

[44] Voor een bespreking, zie Baldwin & Koslosky 2011, p. 719-720.

[45] Banks 2010, p.1646.

[46] Voor een uitgebreide discussie, zie Banks 2010.

[47] Voor een Nederlandse uitgave met besprekingen over de inrichting van het toezicht op inlichtingen diensten, zie Review Committee on the Intelligence and Security Services 2007.

[48] Zwaar geredigeerde versies van deze rapportages zijn wel openbaar geworden ten gevolge van verzoeken op basis van de Amerikaanse wet op de openbaarheid van bestuur en zijn op internet te vinden. Zie bijvoorbeeld Attorney General and Director of National Intelligence 2010.

(*business records*, art. 50 USC 1861) van bedrijven in de VS.[49] Ten aanzien van het gebruik van de bevoegdheid in art. 50 USC 1881a kan slechts worden afgegaan op de beschikbare wetenschappelijke literatuur. Zoals de gezaghebbende rechtswetenschapper Banks het inschat:

> Although details of the implementation of the program authorized by the FAA are not known, a best guess is the government uses a broad vacuum-cleaner-like first stage of collection, focusing on transactional data, where wholesale interception occurs following the development and implementation of filtering criteria. Then NSA engages in a more particularized collection of content after analyzing mined data.[50]

Gezien het bovenstaande kan de volgende conclusie worden getrokken met betrekking tot de betekenis van art. 50 USC 1881a voor gegevensvordering in het kader van cloud computing Het betreft een wettelijke procedure die brede, programmatische vergaring van gegevens zonder verdenking mogelijk maakt ten aanzien van buitenlandse personen in het buitenland. De vergaring hoeft niet gericht te zijn op specifieke personen en of de specifieke inhoud van hun communicatie maar moet bijdragen aan het vergaren van buitenlandse inlichtingen.[51] De bevoegdheid kan worden aangewend tot cloud computing diensten opererend in de VS en biedt voor de betrokken Amerikaanse overheidsdiensten een wettelijke mogelijkheid om op grote schaal gegevens over niet-Amerikaanse burgers, verblijvend in het buitenland, te vergaren. De Amerikaanse grondwet staat hier niet aan in de weg.

2.2.5 Overige relevante bepalingen in de FISA

Naast de situatie van niet-Amerikaanse personen in het buitenland, kent de FISA een lange reeks specifieke bevoegdheden voor het aftappen van communicatie (art. 50 USC 1801-1812), het uitvoeren van fysieke doorzoekingen (art. 50 USC 1821-1829) en de inbeslagname van tastbare voorwerpen en het verkrijgen van business records (art. 50 USC 1861). Zoals reeds opgemerkt zijn de betreffende bepalingen er mede op gericht te voorzien in de constitutionele bescherming voor Amerikaanse personen, bescherming die in het geval van niet-Amerikaanse personen verblijvend in het buitenland ontbreekt.

Art. 50 USC 1861 in zijn huidige vorm is een voortvloeisel van de Patriot Act en biedt de mogelijkheid voor de FBI om bedrijfsgegevens op te vragen met betrekking tot een onderzoek naar spionage en terrorisme van zowel niet-Amerikaanse als Amerikaanse personen. De reikwijdte van deze bepaling is dus beperkter dan art. 50 USC 1881a dat ziet op de vergaring van buitenlandse inlichtingen in bredere zin. Als het een Amerikaanse persoon betreft, mag het onderzoek zich niet uitsluitend richten op activiteiten die beschermd zijn door de vrijheid van meningsuiting en vereniging (First Amendment). Voor niet-Amerikaanse personen kan dat echter wel. Bij deze activiteiten kan bijvoorbeeld gedacht worden aan het bezoeken van politieke of religieuze bijeenkomsten of het schrijven over bepaalde politieke of religieuze onderwerpen. In tegenstelling tot art. 50 USC 1881a hoeft er bij deze bepaling

[49] Voor het kalenderjaar 2011 betreft het een aantal van 205 keer. Zie Department of Justice 2012. De verplichting tot openbaarmaking van deze gegevens volgt uit art. 50 USC 1862(c)(1).
[50] Banks 2010.
[51] Zie Banks 2010.

overigens geen betrokkenheid te zijn van een elektronische communicatiedienst. De bevoegdheid zou zich evenwel nog steeds kunnen richten op een aanbieder van een cloud dienst.

De tegenwoordig geldende procedure en mogelijkheden van art. 50 USC 1861 zijn door de Patriot Act aangepast en een aantal waarborgen is door de Patriot Act verzwakt.[52] De FBI hoeft niet meer aan te tonen dat er een redelijke verdenking is maar het is voldoende als gesteld wordt dat er sprake is van een terrorisme of spionage onderzoek. De personen, waarop het onderzoek gericht is, hoeven geen link te hebben met een buitenlandse mogendheid. Art. 50 USC 1861(d) biedt verder de mogelijkheid tot het opleggen van zogenaamde 'gag'-orders: verplichtingen voor bedrijven het gebruik van de bevoegdheid door overheidsinstanties geheim te houden.

2.2.6 De Electronic Communications Privacy Act (ECPA) en de Stored Communications Act (SCA)

De Electronic Communications Privacy Act (ECPA) en de Stored Communications Act (SCA) die daar deel van uitmaakt (18 USC 2701-2711) reguleren de overheidstoegang tot elektronische communicatie in het kader van het onderzoek naar en de vervolging van criminaliteit door Amerikaanse justitie, politie en andere betrokken diensten.[53] Deze federale wetgeving biedt een tegenwicht voor het ontbreken van constitutionele bescherming op grond van de reeds besproken *Third Party Doctrine*. Ze voorziet in procedures voor bevragingen en stelt wettelijke grenzen aan het aftappen van communicatie en het vergaren van gegevens in de elektronische communicatiesector. Het verbiedt ook de vrijwillige verstrekking van deze gegevens door betrokken diensten. Zoals eerder genoemd heeft de Patriot Act enkele wijzigingen aangebracht in de ECPA. Het betreft wetgeving die al een aantal decennia oud is en waarvan gesteld wordt dat deze geen duidelijkheid meer biedt in het huidige, veel complexer geworden landschap van elektronische communicatiediensten.

> It is unlikely that anyone could provide a definitive opinion about the privacy protections available for information in the cloud against a government or other demand for disclosure.[54]

In het kader van cloud computing gaat het met name om opgeslagen data. De SCA is daarom het meest relevant. De bepalingen ten aanzien van het aftappen van communicatie (Titel I van de ECPA) zien op het onderscheppen van communicatie in de transportfase en zullen verder niet behandeld worden.

De SCA biedt de mogelijkheid voor politie en justitie om opgeslagen communicatie en gegevens over gebruikers van elektronische communicatiediensten en remote computing services op te vragen.[55] Er wordt een verschil gemaakt tussen communicatiediensten en remote computing services en een verschil voor wat betreft de duur van dataopslag. De sterkste rechtsbescherming is aanwezig in het geval het een communicatiedienst betreft en de inhoud van de communicatie die wordt opgevraagd door politie

[52] Zie Rubel 2007.

[53] Zie Kerr 2004.

[54] Gellman 2009.

[55] Er is recentelijk geprocedeerd in de VS over de toegang tot de persoonsgegevens en prive berichten van een Nederlands burger bij Twitter. Zie U.S. District Court, Eastern District of Virginia, Memorandum Opionion, Case 1:11-dm-00003-TCB-LO, Document 85, Filed 11/10/11,https://www.eff.org/sites/default/files/filenode/MemorandumOpinion1353.

of justitie minder dan 180 dagen oud is. In dat geval is er een rechterlijk bevel (*warrant)* nodig om de gegevens op te vragen en moet een redelijke verdenking worden aangetoond bij ieder individueel geval van bevraging (18 USC 2703(a)).

Voor *remote computing services* gelden twee verschillende procedures. Er is een procedure voor het opvragen van de inhoud (18 USC 2703(b)) en een procedure voor het opvragen van gegevens over de gebruiker en het gebruik van de betrokken dienst (18 USC 2703(c)), zoals diens identificerende gegevens of de gebruikte nummers, zoals het IP-adres van een internet gebruiker.[56] Er moet aangetoond worden dat er een redelijke verwachting is dat de opgevraagde gegevens relevant zullen zijn voor een lopend strafrechtelijk onderzoek.

Zoals genoemd beperkt de SCA de mogelijkheid van Internet Service Providers (ISPs) om vrijwillig gegevens te verstrekken aan de overheid (art. 18 USC 2702). Er geldt echter een uitzondering op deze regel voor zogenaamde verkeersgegevens en abonneegegevens, zoals e-mailadressen en IP-adressen.[57] Daarnaast mogen niet-openbare ISPs, bijvoorbeeld universiteitsnetwerken, wel vrijwillig gegevens verstrekken, zowel inhoudelijke als niet-inhoudelijke informatie.[58]

In de meeste gevallen zal data opgeslagen in de cloud de bescherming van de ECPA en de SCA genieten, maar wat deze bescherming precies is en of zij toereikend is vanuit het oogpunt van de bescherming van privacy is onderwerp van debat.[59] Het is een voortdurend onderwerp van juridische procedures in hoeverre opgeslagen communicatie en data bij elektronische communicatie diensten de bescherming van het *Fourth Amendment* geniet. In *US v. Warshak* oordeelde rechters van het *Sixth Circuit* in hoger beroep dat iemand die e-mails opslaat op de servers van een derde wel degelijk kan rekenen op een 'reasonable expectation of privacy'.[60] In *Rehberg v. Paulk* oordeelde het *Eleventh Circuit* echter dat opgeslagen e-mails geen grondwettelijke Fourth Amendment bescherming genieten.[61] De *Supreme Court* heeft zich over de kwestie nog niet uitgelaten. Tegelijkertijd blijft het zo dat indien degene van wie gegevens worden opgevraagd geen Amerikaanse persoon is en niet in de VS verblijft, de bescherming van het *Fourth Amendment* niet ingeroepen kan worden.

Het moet tenslotte opgemerkt worden dat het wettelijk kader voor de vergaring en verstrekking van gegevens aan de Amerikaanse overheid niet statisch is, maar het onderwerp van voortdurende wijzigingen en politiek debat. Het antwoord op de in deze studie voorliggende vragen kan als gevolg hiervan dus op belangrijke punten wijzigen. Eind 2011 is bijvoorbeeld het CISPA wetsvoorstel (Cyber Intelligence Sharing and Protection Act) geïntroduceerd in het Amerikaanse parlement.[62] CISPA ziet op informatie-uitwisseling tussen Amerikaanse bedrijven en de overheid in het geval van cyberaanvallen.

[56] Voor een uitgebreidere bespreking van de bevoegdheden in de SCA, zie Kerr 2004.
[57] 50 U.S.C. sec. 2703(c). Zie Kerr 2004, p. 22-24.
[58] 50 U.S.C. sec. 2702(b) en 2702(c).
[59] Zie bijvoorbeeld Dempsey 2006.
[60] *Warshak v. United States*, 490 F.3d 455 (6th Circuit 2007).
[61] *Rehberg v. Paulk*, 529 F.3d 892 (11th Circuit 2007).
[62] Cyber Intelligende Sharing and Protection Act (CISPA) H.R. 3523 (19 april 2012).

De bescherming die ECPA biedt tegen de vrijwillige verstrekking van gegevens door elektronische communicatiediensten aan de overheid zou door CISPA worden aangetast.[63]

2.3 Wetgeving en constitutionele bescherming in Europa

Om het Amerikaanse wettelijk en constitutioneel kader in perspectief te plaatsen wordt hier kort stilgestaan bij vergelijkbare wetgeving en grondrechtelijke bescherming in Europa. De VS is zeker geen unicum als het gaat om het toekennen van bevoegdheden aan overheidsdiensten op het gebied van justitie, politie en nationale veiligheid. Toch zijn er ook een aantal verschillen, die vanuit de rechtsbescherming relevant geacht moeten worden.

In algemene zin geldt in Europa de privacybescherming van artikel 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens ("EVRM") van de Raad van Europa en de artikelen 7 en 8 van het recentere Handvest van de grondrechten van de Europese Unie (Handvest). Deze grondrechten op Europees niveau normeren het handelen van overheden en bedrijven jegens eenieder die zich in de jurisdictie bevindt en hebben daarmee een universeel karakter.[64] Ze beschermen het recht op privé-leven en het recht op vertrouwelijkheid van communicatie *ongeacht burgerschap, afkomst of verblijfsplaats*, hetgeen een belangrijk verschil is met de grondrechtelijke bescherming door het *Fourth Amendment* in de VS.

> Artikel 8 EVRM
>
> 1. Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
>
> 2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Het afluisteren, onderscheppen of opvragen van opgeslagen communicatie en de daarop betrekking hebbende gegevens maakt inbreuk op dit grondrecht, maar kan geoorloofd zijn als aan de door het Europese Hof ontwikkelde criteria is voldaan. Een inbreuk op art. 8 lid 1 EVRM moet een inbreuk een "legitiem belang" dienen, "bij wet voorzien" en "noodzakelijk in een democratische samenleving" zijn. Op basis van artikel 8 EVRM legt het Europees Hof voor de Rechten van de Mens in talloze uitspraken aan Europese overheden de verplichting op om bevoegdheden en waarborgen in het kader van overheidstoegang tot gegevens en de inhoud van communicatie in wetgeving te verankeren.[65] Vaste argumenten van het Hof zijn dat de samenleving zich moet kunnen informeren omtrent privacy

[63] Zie Electronic Frontier Foundation 2012.

[64] Nederland is zowel deel van de Europese Unie (waarvoor zowel het Handvest als het EVRM van kracht is) als de Raad van Europa, waar ook niet EU lidstaten zoals Turkije, Rusland en Oekraïne deel van uitmaken.

[65] Zie bijvoorbeeld EHRM 1 juli 2008 (Liberty *v. UK)*', §62-§69.

inbreuken door overheidsinstanties, dat deze instanties het publieke belang van een gegevensvordering nauwkeurig dienen te rechtvaardigen en dat burgers zich tegen de consequenties van overheidstoegang moeten kunnen verdedigen. Een tweede opmerkelijk verschil is gezien het bovenstaande dat privacy beperkingen in de Europese rechtsorde wettelijk geregeld moeten worden, waar in het Amerikaanse stelsel privacybescherming - in de gevallen dat het Fourth Amendment geen bescherming biedt - slechts aanwezig is als deze bij wet geregeld is (vgl. de ECPA).

De Europese Unie kent regels op het gebied van justitiële samenwerking, maar laat het stellen van bevoegdheden op het gebied van strafvordering en nationale veiligheid vooralsnog aan de lidstaten. Voor het Verdrag van Lissabon , waarbij....,waren vorderingsbevoegdheden in juridische zin het exclusieve domein van de lidstaten, maar met het de inwerkingtreding van dit verdrag is het stellen van vorderingsbevoegdheden op Europees niveau wel mogelijk geworden.

Tot op heden heeft de Europese wetgever geen regels gesteld op het gebied van cloud computing en vorderingscriteria voor nationale overheden. De herziening van de data protectie richtlijn is interessant in dat kader. Waar in uitgelekte versies van de nieuwe Regulering strikte regels opgenomen waren met betrekking tot het vorderen van cloud gegevens door buitenlandse overheidsinstanties,[66] zijn deze regels in de uiteindelijk gepubliceerde versie van de regulering afgezwakt.[67] De betreffende wetgeving bevat ook de bepalingen met voorwaarden over de uitvoer van persoonsgegevens buiten de EU, die een belangrijke rol spelen in de discussie over het juridisch kader voor het aangaan van cloud computing in Europa. Het volgen van deze ontwikkelingen in de EU is daarom van belang, aangezien de Europese wetgever dus mogelijk nadere regels zou kunnen stellen met betrekking tot de bescherming van gegevens van Europeanen in de cloud en tot een betere afstemming zou kunnen komen tussen vorderingsmogelijkheden en de algemene regels met betrekking tot de verwerking van persoonsgegevens. De Artikel 29 Werkgroep, het overleg tussen de Europese privacy toezichthouers, merkt hierover het volgende op:

> Access to personal data for national security and law enforcement purposes: It is of the utmost importance to add to the future Regulation that controllers operating in the EU must be prohibited from disclosing personal data to a third country if so requested by a third country's judicial or administrative authority, unless this is expressly authorized by an international agreement or provided for by mutual legal assistance treaties or approved by a supervisory authority. […] The Working Party is concerned by this gap in the Commission proposal as it entails a considerable loss of legal certainty for the data subjects whose personal data are stored in data centres all over the world. For that reason, the Working Party would like to stress the need to include in the Regulation the obligatory use of Mutual Legal Assistance Treaties (MLATs) in case of disclosures not authorised by Union or Member States law.[68]

Vooralsnog zijn de regels voor het vorderen van gegevens bij cloud diensten in Europa echter te vinden in de verschillende nationale wettelijk kaders. Bestudering van deze wettelijke kaders in de verschillende

[66] Het ging om art. 42 lid 3 van de betreffende gelekte tekst. Zie European Commission 2011.

[67] Zie European Commission 2012, onderdeel 132 van de preambule.

[68] Article 29 Working Party 2012, p. 23.

landen laat zien dat er in andere Europese landen wettelijke vorderingsmogelijkheden bestaan die op vergelijkbaar zijn met de bevoegdheden van Amerikaanse autoriteiten zoals hierboven uiteengezet. Zo wordt sinds 1 januari 2009 in Zweden op grond van nieuwe FRA-regelgeving al het grensoverschrijdende telefoon en internetverkeer gemonitord. De wet werd aangenomen in het kader van het antiterrorisme beleid en de Zweedse autoriteit die deze surveillance uitvoert heeft daarvoor geen rechterlijk bevel nodig. In het Verenigd Koninkrijk is onlangs wetgeving met vergaande nieuwe bevoegdheden voor de overheid om gegevens over internet communicatie op te kunnen vragen voorgesteld in het parlement (Communications Data Bill).[69] Deze wettelijke regels in Zweden en Engeland zijn overigens nog niet door een rechter getoetst aan de criteria van het EVRM.

2.4 Gegevensvordering in Nederland

Net als in de VS moet ook in Nederland onderscheid gemaakt worden tussen toegang tot gegevens voor de inlichtingendiensten (AIVD en MIVD) enerzijds, en toegang voor politie en justitie anderzijds. Voor de inlichtingendiensten is de Wet op de inlichtingen en veiligheidsdiensten 2002 (Wiv 2002) leidend. Deze wet regelt de activiteiten van de AIVD (Algemene Inlichtingen en Veiligheidsdienst) en de MIVD (Militaire Inlichtingen en Veiligheidsdienst). Op grond van art. 64 lid 2 aanhef en onder a van deze wet is de Commissie van Toezicht betreffende de Inlichtingen en Veiligheidsdiensten (CTIVD) belast met het toezicht op deze diensten.

De Wiv 2002 geeft de AIVD en MIVD de bevoegdheid tot het verwerken van persoonsgegevens van een breed scala aan personen (art. 13 Wiv 2002) en biedt verschillende bepalingen met betrekking tot het vergaren van inlichtingen. Art. 25 lid 1 geeft de bevoegdheid tot het met een technisch hulpmiddel *gericht* aftappen, ontvangen, opnemen en afluisteren van *elke vorm* van gesprek, telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk, ongeacht waar een en ander plaatsvindt. Volgens art. 27 lid 1 Wiv 2002 zijn de AIVD en de MIVD bevoegd tot het met een technisch hulpmiddel *ongericht* ontvangen en opnemen van *niet-kabelgebonden* telecommunicatie. In het toezichtsrapport inzake de inzet van SIGNIT (*signals intelligence*) door de MIVD stelt de CTIVD dat in een aantal gevallen toestemming is verleend voor de gerichte interceptie dan wel selectie van gegevens van een bepaalde breed geformuleerde categorie van personen en organisaties, en dat deze werkwijze niet in overeenstemming is met de WIV 2002.[70]

De bevoegdheden tot toegang voor justitie en politie is geregeld in het Wetboek van Strafvordering. Op 16 juli 2005 is de Wet bevoegdheden vorderen gegevens (Wbvg) in werking getreden. Deze wet kent de bevoegdheid toe om bepaalde gegevens te vorderen van derden in het kader van het strafrechtelijk onderzoek. Een vordering kan gericht zijn op identificerende gegevens, andere dan identificerende gegevens, toekomstige gegevens en/of gevoelige gegevens. Ook bevat de wet de bevoegdheid tot het vorderen medewerking te verlenen bij het ontsleutelen van versleutelde gegevens. Deze dwangmiddelen zijn neergelegd n het Wetboek van Strafvordering (art. 126nc-126nh en art. 126uc-126uh). Voor wat betreft de mate van rechtsbescherming geldt een getrapt stelsel: naar mate de

[69] Zie bijvoorbeeld Bernal 2012.

[70] Zie CTIVD 2011, paragraaf 7.2.2. en 8.3.3.

categorie gegevens ingrijpender is, gelden zwaardere voorwaarden. Zo is bijvoorbeeld voor het vorderen van identificerende gegevens geen tussenkomt van de Officier van Justitie vereist, en kunnen de gegevens door een gewoon opsporingsambtenaar worden opgevraagd.

De bevoegdheden uit de Wbvg kunnen ook ingezet worden om gegevens te vergaren over personen anders dan de verdachte, indien dit nodig is in het belang van het onderzoek. Gegevens kunnen worden gevorderd van een ieder die daarvoor redelijkerwijs in aanmerking komt. En in beginsel kan een ieder van wie gegevens bewaard en verwerkt worden doelwit van gegevensvordering zijn. De bevoegdheden op grond van de Wbvg zijn dus breed. In beginsel zijn derden verplicht de gevorderde gegevens te verstrekken. In het geval niet aan een gegevensvordering wordt voldaan kan dit een strafbaar feit opleveren op grond van het niet opvolgen van een ambtelijk bevel/vordering (art. 184 Sr). In art. 126bb lid 1 Sv is verder nog een notificatieregeling opgenomen. Dit houdt in dat, indien de situatie het toelaat, aan de verdachte/betrokkene schriftelijk mededeling wordt gedaan over het inzetten van de bevoegdheden uit de Wbvg. Identificerende gegevens zijn uitgesloten van deze notificatieregeling.

De Nederlandse overheid heeft verder ook de wettelijke mogelijkheid gecreëerd, mede door middel van gesloten verdragen met andere staten (waaronder de VS), dat gegevens over Nederlandse burgers worden opgevraagd ten behoeve van onderzoek door buitenlandse justitie of veiligheidsdiensten. Het gaat hier bijvoorbeeld om zogenaamde wederzijdse rechtshulp in strafzaken op basis waarvan justitie en politie hun bevoegdheden kunnen aanwenden ten dienste van een buitenlandse overheid zoals bijvoorbeeld de Amerikaanse. Indien Amerikaanse overheidsdiensten geen jurisdictie hebben ten aanzien van een in Nederland opererende dienst kunnen zij op basis van dergelijke overeenkomsten een verzoek doen tot rechtshulp. Deze overeenkomsten zijn vanuit internationaalrechtelijk perspectief het geëigende middel voor buitenlandse overheden om toegang te krijgen van gegevens over Nederlanders.[71] In het geval van een cloud provider (of gelieerde onderneming) met continue systematische activiteiten in de VS is er volgens de Amerikaanse wet echter geen duidelijke verplichting om ten aanzien van de toegang tot gegevens over Nederlanders gebruik te maken van deze middelen. De Amerikaanse overheid claimt in dat soort gevallen in beginsel immers gewoon zelf jurisdictie, zoals besproken in paragraaf 2.1. Dit laat de mogelijkheid van een betere afstemming op dit punt middels internationale verdragen uiteraard onverlet.

Verder bestaat er op grond van artikel 59 WIV 2002 de mogelijkheid dat Nederlandse veiligheidsdiensten vrijwillig gegevens verstrekken aan buitenlandse inlichtingendiensten en op het verzoek van buitenlandse diensten van bevriende naties, zoals de VS, ondersteuning verzorgen. Deze ondersteuning kan bestaan uit het inzetten van speciale bevoegdheden zoals aftappen en het opvragen van gegevens bij Nederlandse organisaties of bedrijven. De CTIVD schrijft recentelijk dat de betrokken Nederlandse dienst daarbij de inzet van deze bevoegdheden zelfstandig dient te toetsen aan de Nederlandse voorwaarden. Maar uit hetzelfde rapport van de CTIVD blijkt dat deze toetsing in de

[71] Voor een bespreking en aanbevelingen op dit punt zie Brown & Korff 2012. Zie ook Westmoreland 2012.

praktijk niet altijd goed plaatsvindt en dat op het gebied van SIGINT structureel sprake is van het leveren van ondersteuning op basis van zogenaamde 'Memoranda of Understanding'.[72]

[72] CTIVD 2011, p. 59-60.

3. Implicaties wettelijk kader gegevensvordering VS bij afname cloud diensten

Om de juridische analyse inzichtelijk te maken voor de praktijk, worden hieronder de belangrijkste conclusies op een rij gezet. Verder worden drie scenario's beschreven van de mogelijkheid van verkrijging van data opgeslagen in de cloud. Paragraaf 4 staat vervolgens stil bij de uitwerking van deze juridische conclusies over het juridisch kader in de Verenigde Staten en plaatst risico's van gegevensvordering in de context van andere juridische overwegingen die spelen bij de afname van cloud diensten.

Het bovenstaande overzicht van het wettelijk kader en de grondrechtelijke bescherming in de VS geeft blijk van een mogelijkheid tot toegang van Amerikaanse autoriteiten tot cloud data van buitenlandse kennisinstellingen in de strafvorderlijke sfeer en een laagdrempelige mogelijkheid tot toegang tot gegevens in de sfeer van Amerikaanse inlichtingendiensten. Art. 50 USC 1881a springt daarbij het meest in het oog, vanwege de beschreven mogelijkheden en het achterliggende gebrek aan rechtsbescherming voor niet-Amerikaanse personen verblijvend in het buitenland. De bepaling maakt het in beginsel mogelijk gegevens en communicatie van grote groepen Nederlanders te vergaren, als zij gebruik maken van cloud diensten die activiteiten hebben in de VS, zonder dat daar informatie over beschikbaar komt voor de afnemers of de individueel betrokkenen. Deze vergaring van gegevens hoeft verder niet uitsluitend gericht te zijn op buitenlandse inlichtingen. Zij kan al plaatsvinden wanneer het belangrijkste doel is dat dit uiteindelijk buitenlandse inlichtingen zal opleveren.[73]

Scenario 1: Gegevens van studenten

In het kader van een vak van een interdisciplinaire masteropleiding Digitale Media van een Nederlandse universiteit schrijven studenten in teams papers over de mogelijkheid de vertrouwelijkheid van klokkenluiders te garanderen bij websites zoals Wikileaks. De docent van het vak staat bekend als internationaal expert op het gebied van het gebruik van cryptografische technieken door journalisten en activisten. Bij een avondseminar tijdens de cursus zijn ontwikkelaars van een nieuwe Wikileaks site op bezoek die interesse tonen in de door de studenten ontwikkelde ideeën. De betrokken universiteit maakt gebruik van de cloud diensten van een grote Amerikaanse dienstaanbieders voor het groot deel van de beschikbare ICT voorzieningen voor studenten, zoals de opslag van documenten, email en elektronische leeromgeving.

De fysieke locatie van de servers waar de Amerikaanse dienstaanbieders hun data opslaan is niet relevant voor de vraag of Amerikaanse regelgeving het opvragen van de gegevens van de studenten mogelijk maakt. Op grond van art. 50 USC 1881a kunnen de bevoegde Amerikaanse autoriteiten, zoals de NSA, in beginsel toegang krijgen bij de cloud provider tot de betreffende gegevens van de gehele studentenpopulatie van de betreffende universiteit, bijvoorbeeld in het kader van het vergaren van buitenlandse inlichtingen over de bedreigingen voor de buitenlandse zaken van de Verenigde Staten.

[73] Voor een recente bespreking van nationale veiligheidsproblematiek door de *Director of National Intelligence*, zie Clapper 2012.

Er is verder in de VS geen sprake van constitutionele waarborgen voor Nederlandse gebruikers van cloud diensten die onder Amerikaanse jurisdictie vallen, omdat het *Fourth Amendment* niet van toepassing is. Allereerst zijn cloud providers aan te merken als derden, waardoor voor de gebruikers van deze diensten de 'reasonable expectations of privacy' onder de *Third Party doctrine* komen te vervallen. Bovendien strekken Amerikaanse constitutionele waarborgen zich niet uit tot buitenlanders die zich niet in de VS bevinden. In dat opzicht genieten Nederlandse gebruikers van cloud diensten vanuit Amerikaans juridisch perspectief dezelfde grondrechtelijke bescherming als Noord-Koreanen.

Verder is de fysieke locatie van servers in beginsel niet relevant voor de bevoegdheden van de Amerikaanse autoriteiten gezien het feit dat jurisdictie bestaat ten aanzien van een onderneming indien er sprake is van activiteiten in de Verenigde Staten met een continu en systematisch karakter, zoals bijvoorbeeld een vestiging. Zoals eerder opgemerkt is het bestaan van een directe koppeling tussen jurisdictie en de locatie van opslag een onjuiste maar breed gedragen opvatting in het debat. Het is een opvatting die in verschillende onderzoeksrapporten terugkeert, zoals de studie over cloud computing van het gezaghebbende European Network and Information Security Agency (ENISA), het EU agentschap op het gebied van informatie veiligheid.[74]

Scenario 2: Bestuurlijke informatie in e-mails

Het bestuur van een grote Nederlandse Hogeschool is in gesprek over samenwerking en uitwisselingen met een aantal technische universiteiten in de Golf-Regio. Om de samenwerking verder vorm te geven wordt de hulp ingeschakeld van een Amerikaanse consultant. De bestuurlijke e-mails met de betrokken buitenlandse partners van de Hogeschool zijn opgeslagen in de UCloud, een clouddienst van UniSer. Data in de UClowd worden enkel op servers in Nederland opgeslagen. UniSer, de in Nederland gevestigde aanbieder van deze cloud, biedt naast de UCloud ook een clouddienst aan in de VS, UcalCloud, met een vestiging en datacenters in Utah.

Dat de e-mails in dit scenario op servers in Nederland worden opgeslagen, is niet relevant voor het bereik van de Amerikaanse regelgeving voor de verkrijging van deze gegevens. Dat UniServe ook diensten in de VS aanbiedt wel. Zou het dit niet doen, dan hebben de Amerikaanse autoriteiten in beginsel geen directe toegang in het kader van de vergaring van buitenlandse inlichtingen. In een dergelijk geval kan om de hulp van de Nederlandse veiligheidsdienst worden verzocht. In het geval er een strafrechtelijk onderzoek zou spelen naar de Amerikaanse consultant, dan kunnen de bestuurlijke emails op drie manieren in handen kan komen van Amerikaanse autoriteiten: (1) door vrijwillige verstrekking door UCalCloud; niet-openbare ISPs, bijvoorbeeld universiteitsnetwerken, kunnen vrijwillig gegevens verstrekken aan justitie, zowel inhoudelijk als niet-inhoudelijk. Het kan zijn dat hier contractueel beperkingen aan zijn gesteld. (2) door een verzoek op grond van art. 18 USC 2703. Als er sprake is van een niet-openbare ISP is de SCA niet van toepassing (50 USC sec. 2711 jo. 50 USC sec. 2703), en kunnen de gegevens met een gewone subpoena worden opgevraagd. (3) via een rechtshulpverzoek van Amerikaanse justitie aan Nederlandse justitie om de gegevens op te vragen bij Ucloud, of bij de betreffende Hogeschool zelf.

[74] De ENISA studie gaat uit van de opvatting dat de opslag locatie bepalend is voor de vraag naar jurisdictie. Zie ENISA 2009, p. 84.

Bij de specifieke bepaling uit de FISA (art. 50 USC 1881a) gelden nauwelijks voorwaarden en beperkingen die een betekenisvolle rem vormen op de gegevensvordering van cloud data van buitenlandse gebruikers. Daarbij komt dat het afbrokkelende onderscheid tussen justitie en veiligheidsdiensten in de VS alsmede het feit dat het vergaren van inlichtingen niet langer het primaire doel maar een belangrijk doel van de inzet van de bevoegdheid hoeft te zijn. Zo kunnen de opgevraagde en verzamelde gegevens in beginsel ook terecht komen bij instanties die zijn belast met de opsporing van strafbare feiten. Oftewel, niet alleen de student die een bedreiging zou kunnen vormen voor de Amerikaanse nationale veiligheid, maar ook de student die te goeder trouw via de e-mail afspreekt met een door de Amerikaanse autoriteiten gevolgde verdachte van handel in drugs.

Scenario 3: Onderzoekgroep en data nucleair wetenschappelijk onderzoek

Een onderzoeksgroep aan een Nederlandse technische universiteit doet onderzoek naar nieuwe ontwikkelingen op het gebied van nucleaire technologie. De verzamelde data voor het onderzoek staan sinds kort op de EUcloud, een EU brede clouddienst voor en door universiteiten. De servers van deze cloud staan in Duitsland. EU cloud is een private organisatie opgericht. Na enige tijd verkeert EUcloud in financiele moeilijkheden. Het zet zichzelf te koop gezet en wordt uiteindelijk overgenomen door een grote speler in de markt met vestigingen in de VS. Een andere kandidaat was een cloud provider met een hoofdkantoor China.

In het geval dat er geen enkele link bestaat tussen de EUcloud, de TU Delft en de VS, hebben de Amerikaanse autoriteiten niet direct toegang tot deze onderzoeksdata. Het is wel mogelijk dat Amerikaanse inlichtingendiensten in het kader van onderlinge contacten over proliferatie indirect gegevens verkrijgen van bevriende Europese diensten, waaronder de AIVD. Bij de uitoefening van bevoegdheden door deze diensten, bijvoorbeeld bij het screenen of verzamelen van inlichtingen over personen voorzien het EVRM en het Handvest van de Grondrechten van de EU in grondrechtelijke rechtsbescherming. Na de overname heeft de VS in beginsel wel jurisdictie. Het is niet mogelijk contractueel afspraken te maken om de bevraging van gegevens door justitie of veiligheidsdiensten onmogelijk te maken. Dit is wel mogelijk ten aanzien van de rechtspositie als klant bij eventuele overnames, bijvoorbeeld als dit leidt tot de mogelijkheid van toegang tot de data vanuit andere jurisdicties.

De EU laat de wettelijke regeling van vorderingsbevoegdheden vooralsnog over aan de lidstaten. Nationale veiligheid en opsporing zijn breed erkende uitzonderingsgronden op privacy en dataprotectie in Nederland en andere Europese lidstaten, die ruime vorderingsbevoegdheden in principe kunnen legitimeren. Een groot verschil met de Verenigde Staten is dat de vorderingsbevoegdheden binnen de lidstaten van de Europese Unie binnen de grenzen moeten blijven van breed geformuleerde fundamentele rechten. Het EVRM en het recent in werking getreden EU Handvest van de Grondrechten vereisen individuele rechtsbescherming (zoals een eerlijk proces) en een bepaalde mate van transparantie en verantwoording met betrekking tot aftappen en gegevensvordering. Een bijkomend verschil tussen de constitutionele kaders in de EU en de VS, is dat de Europese grondrechtenverdragen een universeel (voor eenieder geldend, ongeacht nationaliteit) karakter hebben, waar niet-Amerikaanse ingezetenen in het wettelijk kader in de VS nauwelijks bescherming genieten. Op de derde plaats is

reeds opgemerkt, dat privacy beperkingen in Europa wettelijk vastgelegd moeten worden, waar privacybescherming in de Verenigde Staten geen gegeven is. In de VS is het gezien de beperkte gelding van het *Fourth Amendment* vaak andersom. Daar is de privacybescherming in specifieke contexten bij wet geregeld worden, zoals in het geval van de ECPA.

Deze overeenkomsten en verschillen tussen de Amerikaanse en Europese jurisdicties in het kader van cloud computing en gegevensvordering, leiden allereerst tot de constatering dat er geen juridische garanties bestaan voor de vertrouwelijkheid van informatie in de cloud. Indien er voor politie of justitie of veiligheidsdiensten in Nederland of van een bevriende natie aanleiding is om toegang te zoeken tot gegevens, bestaat hier linksom of rechtsom de mogelijkheid toe. Wordt data opgeslagen bij cloud providers die activiteiten ontplooien in de Verenigde Staten, dan is de stelling verdedigbaar dat het geldende juridisch kader in de VS voor nagenoeg alle denkbare situaties de mogelijkheid biedt aan Amerikaanse autoriteiten om direct bij de provider gegevens op te vragen.

Terwijl in beide jurisdicties de vorderingsmogelijkheden aanwezig zijn, geniet data opgeslagen in cloud omgevingen die volledig losgekoppeld zijn van 'activiteiten in de Verenigde Staten' een aanvullende rechtsbescherming op basis van het EVRM en het EU Handvest. Het zal echter in de praktijk niet altijd makkelijk zijn te achterhalen of een cloud aanbieder of een van zijn ketenpartners activiteiten in de VS ontplooit met een continu en systematisch karakter, zoals bijvoorbeeld een vestiging. Tegelijkertijd is het duidelijk dat dit voor veel internationaal opererende dienstaanbieders op het gebied van cloud computing het geval zal zijn en dat deze situatie ten gevolge van overnames elk moment zou kunnen veranderen. De genoemde aanvullende rechtsbescherming in het geval van diensten die niet onder de jurisdictie van de VS vallen vormt in de Europese en Nederlandse context een rem op de vormgeving van te vergaande bevoegdheden tot gegevensvordering en het verdere gebruik van deze gegevens in de veiligheidsketen.

4. Risico's

4.1 Gegevensvordering uit de cloud: theorie en praktijk

In de vorige paragraaf is aan de orde gekomen dat er geen juridische waarborgen bestaan om de vertrouwelijkheid van cloud data te garanderen met betrekking tot toegang door Amerikaanse overheid als de betreffende cloud provider 'activiteiten in de Verenigde Staten' ontplooit. Gaat het om gegevens van niet-Amerikanen, dan is er bovendien geen sprake van enig inzicht in hoe vaak, door welke instantie en met welke reden cloud data gevorderd worden door de Amerikaanse overheid. De motieven van gegevensvordering zijn over het algemeen het verwerven van inlichtingen en de (met steeds minder waarborgen omkleedde) opsporing van strafbare feiten. Maar het is te verwachten dat initiatieven op het gebied van cybersecurity, zoals CISPA met haar ruime definities en toepassingsbereik, eerder zullen leiden tot een verruiming van de toegangsbevoegdheden en de vorderingsfrequentie van cloud data.

In haar uitgebreide rapportage over de voordelen en risico's van cloud computing, oordeelde ENISA al in 2009 dat het risico van gegevensvordering vanuit andere jurisdicties hoog is.[75] Hierbij dient te worden opgemerkt, dat ENISA in 2009 nog uitging van de relevantie van de fysieke locatie van gegevens voor de vorderingsmogelijkheden van overheidsinstanties. Op basis van het hiervoor beschreven regels met betrekking tot jurisdictie is deze fysieke locatie in de Amerikaanse context echter in beginsel irrelevant gebleken. De mitigatie van dit risico is daarmee dus nog complexer geworden.

De praktische vervolgvraag van het hoge risico en de complexere mitigatie, is natuurlijk hoe vaak de gegevens daadwerkelijk gevorderd worden. Het feit dat een vordering van gegevens bij een cloud provider mogelijk is, betekent uiteraard niet dat deze gegevens daadwerkelijk zullen worden opgevraagd. Deze praktische vraag is echter niet goed in te schatten, laat staan te beantwoorden, aangezien rapportageverplichtingen in het geval van buitenlandse vorderingen niet bestaan. Er kan daarom geen kwantitatief beeld geschetst worden van de vorderingspraktijk, noch kunnen trends van de vorderingspraktijken worden beschreven voor zover het de vergaring van gegevens bij internationaal opererende cloud aanbieders betreft. Het verdient opmerking dat het strikt in eigen beheer houden van gegevens het voordeel heeft dat in beginsel wel inzicht zal bestaan in het aantal vorderingen dat plaatsvindt naar deze gegevens, aangezien de vorderingen in dat geval aan de eigen instelling zullen zijn gericht. In andere gevallen kan desalniettemin door middel van enkele conceptuele observaties een beeld geschetst worden van de vorderingspraktijk vandaag de dag en in de toekomst.

Gegevensvordering van cloud data speelt al een steeds belangrijkere rol bij de vergaring van inlichtingen en binnen de opsporing. En het is te verwachten dat het belang van toegang tot cloud data voor de hele veiligheidsketen in de toekomst verder zal toenemen. Zonder volledigheid na te streven, worden enkele ontwikkelingen hier aangestipt. Allereerst stijgt het gebruik van cloud diensten spectaculair, waardoor meer relevante informatie alleen in via de cloud in handen gekregen kan worden. Analysemethoden

[75] ENISA 2009, p. 45-46.

worden tegelijkertijd steeds krachtiger, waardoor het voor autoriteiten steeds interessanter wordt om grote hoeveelheden data te doorzoeken op patronen, bijvoorbeeld van verdacht gedrag.

Op de tweede plaats zullen, in aanvulling op deze endogene (aan cloud computing inherente) ontwikkelingen, exogene factoren het belang van cloud data voor de vergaring van inlichtingen en strafvordering doen toenemen. Zo komt de effectiviteit van andere veelgebruikte vorderingsmogelijkheden onder toenemende druk. Dit geldt bijvoorbeeld voor het aftappen van elektronische communicatie. Al in 2005 benadrukte een evaluatierapport van de Nederlandse Telecommunicatiewet dat door "diverse technische en marktontwikkelingen de effectiviteit en efficiëntie van de aftapbaarheidswetgeving af neemt".[76] De marktontwikkelingen laten decentralisatie en explosieve toename van aanbieders van elektronische communicatie zien, terwijl de technische aspecten destijds zagen op pakket-geschakelde informatieoverdracht (in plaats van circuit-geschakeld), die aftapbaarheid slechts mogelijk maakt bij de eindpunten in het netwerk, dat wil zeggen vlakbij de eindgebruiker. Omdat er niet op enkele punten in het netwerk, maar op veel meer punten afgeluisterd dient te worden, is deze vorm van aftappen kostbaar - dit geldt in gelijke zin voor gegevensvordering.

Een andere belangrijke ontwikkeling is de wijde beschikbaarheid en standaard ingezette encryptie op real-time communicatie. Daarbij kan gedacht worden aan het gebruik van encryptie bij Web browsing en e-mailverkeer. Waar conventionele telecomaanbieders nu wettelijk verplicht zijn hun netwerk in te richten om gegevensvordering en tappen te faciliteren, zorgt deze *end-to-end* encryptie ervoor dat deze vormen van communicatie niet of nauwelijks waarneembaar zijn voor een telecomoperator of internet netwerk provider. Voor veel webmail aanbieders is HTTPS communicatie tegenwoordig de standaard, zodat communicatie onderweg van de ene eindgebruiker naar de andere niet of nauwelijks effectief getapt kan worden, behalve bij de aanbieders zelf.[77] De Amerikaanse privacy deskundige Swire beschrijft deze ontwikkeling en stelt dat dientengevolge de aandacht van inlichtingen- en opsporingsdiensten in de online omgeving naar cloud providers zal verschuiven, omdat de op hun servers opgeslagen informatie toegankelijk gemaakt wordt voor eindgebruikers en commerciële exploitatie en derhalve niet langer versleuteld is. Dit geldt voor alle vormen van cloud computing voor het publiek, of het nu VoIP, webmail, E-Commerce, banking of andere toepassingen betreft.[78] Een mogelijke consequentie van een dergelijke ontwikkeling is dat in toenemende mate zal worden overgegaan tot versleuteling van de informatie zelf.

Voor wat betreft het aantal bevragingen, maakt de Amerikaanse wetenschapper Banks onderscheid in de verschillende stadia van het communicatieproces. Zijn inschatting is dat de Amerikaanse overheid voor de verzameling van gegevens een brede 'stofzuigerbenadering' hanteert voor opgeslagen gegevens en dat de NSA de verzamelde gegevens vervolgens analyseert.[79] Swire noemt in dit verband recente berichtgeving rondom een nieuw analysecentrum van de NSA, dat in potentie alle communicatie die verband heeft met de Verenigde Staten verzamelt, filtert op patronen, en vervolgens verder kan

[76] TILT & Dialogic 2005, p. 67-69.
[77] Zie Swire 2012 p. 7-10.
[78] Zie Swire, p. 10
[79] *Supra*, note 46.

analyseren.[80] Deze door experts geschetste ontwikkelingen kunnen gezien het ontbreken van officiële informatie onmogelijk worden bevestigd, noch ontkracht. Maar uit de ontwikkelingen kan wel de verwachting afgeleid worden, dat de toegang tot cloud data van Amerikaanse instanties zal blijven toenemen.

4.2 Significante risico's, significante kanttekeningen

In algemene zin brengt deze notitie aan het licht dat kennisinstellingen met afname van cloud diensten van providers die 'activiteiten in de Verenigde Staten' ontplooien niet in juridische zin de vertrouwelijkheid en veiligheid van data in de cloud kunnen garanderen. Contractuele afspraken noch algemene juridische waarborgen kunnen deze voor kennisinstellingen onwenselijke situatie veranderen. Daarmee vormt afname van cloud diensten in dit specifieke opzicht een inperking van de autonomie, beschikkingsmacht en informatiepositie van kennisinstellingen en bestaat er een gevaar dat de intellectuele vrijheid van medewerkers en studenten in het Nederlands hoger onderwijs en onderzoek in het geding komt. Het ontbreken van een mogelijke garantie op de vertrouwelijkheid van informatie kan de reputatie van instellingen aantasten. Er ontstaan gezien de overgang naar een cloud computing omgeving onbedoeld nieuwe mogelijkheden voor de Amerikaanse overheid toegang te verkrijgen tot informatie (*function creep*). En er bestaat een permanente dreiging dat dergelijke toegang daadwerkelijk plaats heeft en aldus afbreuk doet aan de mate waarin men wil en kan communiceren (chilling effect).

Deze constatering heeft concrete gevolgen. Zo zullen kennisinstellingen niet in de positie verkeren, om hun medewerkers of studenten in te lichten in het geval van een concrete gegevensvordering, laat staan hun medewerkers al in dat stadium van een inlichtingen- of opsporingsonderzoek door Amerikaanse autoriteiten te beschermen. Waar data in de eigen informatiehuishouding verwerkt worden, zullen dergelijke onderzoeken tenminste in een vroeg stadium bekend zijn bij kennisinstellingen. Individuele excessen of de mogelijke surveillance van een onderzoeksgroep, zoals uiteengezet in de scenario's in paragraaf 3, zullen kennisinstellingen in verlegenheid brengen en mogelijk hun reputatie aantasten. Zo kan cloud computing de maatschappelijke verantwoordelijkheid van kennisinstellingen onder druk zetten.

Verder dienen kennisinstellingen zich te realiseren, dat er op het punt van de bevragingen door buitenlandse overheidsdiensten geen vertrouwensband met de cloud provider zal kunnen ontstaan. Kennisinstellingen zullen immers nooit precies weten hoe cloud providers de data verder verwerken in het kader van gegevensvordering door overheidsinstellingen en of cloud providers op dit gebied zelfs verregaand samenwerken met deze instanties.[81] Deze asymmetrie in de informatiepositie is een risico en bemoeilijkt zorgvuldig geïnformeerde besluitvorming over de afname van cloud diensten. Het is bijvoorbeeld maar de vraag of kennisinstellingen ooit een volledig beeld krijgen van de activiteiten (in de

[80] Zie Swire, p. 8. Zie ook Bradford 2012.

[81] Recent voorbeeld is de uitspraak van het District Court Virginia in EPIC vs NSA over de samenwerking van Google met de NSA. Volgens de uitspraak hoeven Google, noch de NSA, samenwerking te bevestigen noch te ontkrachten. Zie *EPIC v. NSA*, 11-5233 (6th Circuit 2012), http://www.wired.com/images_blogs/threatlevel/2012/05/EPIC-v.-NSA-DC-Cir.-2012.pdf. Zie verder Kravets 2012.

Verenigde Staten) van de cloud provider, haar ketenpartners, of cloud data bij verwijdering door eindgebruikers daadwerkelijk (bij alle ketenpartners) van de server wordt verwijderd en wat er met de data gebeurt ingeval van faillissement, overname of gewenste ontbinding van de overeenkomst. De providers hebben immers geen belang, noch een verplichting om deze asymmetrie weg te nemen. Bovendien moet rekening gehouden worden met de situatie dat cloud providers niet in staat zijn te goeder trouw een antwoord (laat staan een garantie) te geven bij dergelijke complexe vragen. Dit is met name het geval als een cloud provider alleen software aanbiedt en voor de opslag en verwerking van cloud data gebruik maakt van de infrastructuur van derden.[82]

De risico's van gegevensvordering in verband met een migratie door SURF en andere Nederlandse kennisinstellingen naar 'de cloud' zijn significant. Tegelijkertijd kunnen er kanttekeningen geplaatst worden. Zonder volledigheid na te streven, zien deze kanttekeningen op informatiebeveiliging in het algemeen en (de praktijk rondom) gegevensvordering en cloud computing in het bijzonder.

Een kennisinstelling kan met betrekking tot gegevensvordering van oordeel zijn dat gegevensvordering door overheidsinstantie nauwelijks problematisch is met betrekking tot een aantal categorieën data. In welke mate vormt de gegevensvordering van ongevoelige gegevens en openbare informatie een risico voor kennisinstellingen of eindgebruikers? Deze vraag zet aan tot een belangrijke afweging in het kader van de afname van cloud computing, namelijk welke categorieën data kennisinstellingen en eindgebruikers als gevoelig beoordelen. Oftewel, welke factoren zorgen ervoor dat onzichtbare en bijkans ongecontroleerde overheidstoegang een risico vormt voor kennisinstellingen? Deze vraag staat los van de beoordeling over de wenselijkheid van zulke toegang, maar is des te nijpender gezien de juridische stand van zaken en de veronderstelde voordelen van cloud computing voor kennisinstellingen.

Een tweede kanttekening inzake de mogelijkheid van bescherming tegen risico's samenhangend met het gebruik van 'de cloud' ziet op de eindgebruikers. Immers, een kennisinstelling kan op zichzelf beslissen om geen gebruik te maken van cloud diensten. Maar als een eindgebruiker communiceert met een derde partij wiens communicatie wel met behulp van een cloud provider wordt verwerkt, vervalt deze bescherming die lokale dataverwerking biedt in belangrijke mate. Het komt zelden voor dat de wijze waarop gegevens bij een derde worden verwerkt (of er bijvoorbeeld sprake is van een Amerikaanse cloud provider) bekend is bij een eindgebruiker. Zo zijn vele universiteiten in het buitenland voor de verwerking van communicatie- en opslagdata vrij geruisloos overgestapt op cloud computing, niet zelden van Amerikaanse providers. En als de verwerking iets bredere bekendheid geniet, bijvoorbeeld bij de Universiteit van Cambridge die al wat langer gebruik maakt van cloud diensten van Google,[83] dan is het nog maar de vraag of deze omstandigheid communicatie en zelfs samenwerking met wetenschappers die gebruik maken van de (buitenlandse) cloud diensten in de weg zal staan. Toch kunnen door de ene kennisinstelling bewust beschermde gegevens via deze route alsnog onder de

[82] Zogenaamde SaaS-providers (Software as a Service), in vergelijking met IaaS (Infrastructure as a Service). Zie voor een nadere toelichting SURFNET 2010, p. 3-4.

[83] Zie University of Cambridge 2012.

beschreven regimes toegankelijk worden voor overheidsinstanties. Dergelijke routes vormen een reële beperking op de mogelijkheid van bescherming van gegevens tegen gegevensvordering in de cloud.

Binnen een risicoanalyse van de afname van cloud diensten door kennisinstellingen, dient gegevensvordering gezien de in deze studie gemaakte analyse een rol te spelen. Maar welke plaats gegevensvordering in een lange lijst van aan informatiebeveiliging gerelateerde risico's dient te nemen, is in de praktijk moeilijk te bepalen. Datalekken, daadwerkelijke verwijdering en interoperabiliteit van encryptie-standaarden zijn immers niet alleen relevante beveiligingsrisico's waar het gaat om (on)rechtmatige toegang door overheden, maar vormen op zichzelf mogelijk nog significantere risico's voor kennisinstellingen, alsmede voor de privacy en informatieveiligheid van eindgebruikers. Weliswaar beoordeelt de reeds aangehaalde studie van ENISA overheidstoegang in de hoge risico-categorie, toch valt het buiten het bereik van deze studie om deze kwestie te beoordelen. Dat neemt niet weg, dat kennisinstellingen aan de risico's van gegevensvordering van in de cloud opgeslagen informatie serieus dienen te overwegen.

5. Conclusie en aanbevelingen

5.1 Conclusie

Wat is de betekenis van de Patriot Act voor de mogelijkheid dat gegevens in de cloud vanuit Nederlandse kennisinstellingen worden opgevraagd door de Amerikaanse overheid. Dat is de vraag die aan deze notitie ten grondslag ligt.

Vooraf moet worden opgemerkt dat de Patriot Act een symboolfunctie is gaan spelen in het debat over de vraag of de vertrouwelijkheid en veiligheid van informatie in de cloud voldoende gewaarborgd blijft. De Patriot Act uit 2001 heeft bevoegdheden tot het vergaren van gegevens door Amerikaanse veiligheidsdiensten en Justitie aangescherpt. In werkelijkheid is de Patriot Act echter slechts een complex onderdeel in een nog veel complexer en dynamisch geheel aan bevoegdheden voor gegevensvordering binnen het Amerikaanse rechtssysteem. Alleen op basis van een analyse van dit grotere geheel kan een zinnige discussie gevoerd worden over de betekenis en relevantie van de mogelijkheid van gegevensvordering vanuit de VS voor Nederlandse kennisinstellingen.

Als vanuit het perspectief van de Nederlandse afnemer van een cloud dienst gekeken wordt naar dit juridisch kader in de VS kunnen de volgende conclusies getrokken worden. Ten eerste bestaat er in de VS geen constitutionele bescherming bij de vergaring van gegevens van niet-Amerikaanse personen verblijvend in het buitenland. Alle geldende rechtsbescherming dient als gevolg daarvan wettelijk te zijn vastgelegd. De geldende wettelijke rechtsbescherming bij de verschillende vorderingsbevoegdheden blijkt vervolgens sterk gericht op de rechten van Amerikanen.

Ten aanzien van buitenlandse (lees Nederlandse) gebruikers in de cloud bestaan ruime mogelijkheden voor de Amerikaanse overheid om gegevens op te vragen. De in 2008 ingevoerde specifieke bepaling voor het opvragen van gegevens van niet-Amerikaanse personen buiten de VS springt het meest in het oog door de ruime mogelijkheden die het biedt en masse gegevens op te vragen. Ook in het kader van strafrechtelijk onderzoek bestaan bevoegdheden in de VS voor het opvragen van gegevens bij cloud providers. Er dient wel sprake te zijn van jurisdictie, maar daarvan is in beginsel al sprake bij cloud providers met een vestiging of anderszins continue en systematische activiteiten in de VS. Het is een misvatting dat de Amerikaanse overheid bij het uitoefenen van deze bevoegdheden alleen jurisdictie heeft als het gaat om gegevens die zich fysiek bevinden op Amerikaans grondgebied.

Het is verder zo dat Europese en Nederlandse privacy regels (zoals de Wbp) uiteindelijk niet aan de uitoefening van deze bevoegdheden door de Amerikaanse overheid in de weg kunnen staan. Hetzelfde geldt voor contractuele afspraken. Waar deze in andere gevallen uitkomt bieden ten aanzien van het juridisch inkaderen van risico's, is het niet mogelijk de mogelijkheid van bevragingen door justitie of veiligheidsdiensten juridisch in te perken. Vanuit internationaal rechtelijk perspectief, en vanuit het belang op vertrouwelijkheid van informatie vanuit het perspectief van de kennisinstellingen wringen deze conclusies wel. Uiteindelijk kan hier echter alleen op internationaal niveau een daadwerkelijke oplossing voor worden gevonden.

In concrete zin is er weinig te zeggen over de vraag hoe vaak de Amerikaanse overheid gebruik zal maken van de besproken mogelijkheden. Er is weinig tot geen transparantie over het gebruik van de betreffende bevoegdheden en er zal vaak een geheimhoudingsverplichting gelden voor betreffende cloud aanbieders, ook richting de direct betrokkenen. Dit leidt er toe dat het erg lastig is het daadwerkelijke risico in te schatten dat gegevens daadwerkelijk worden opgevraagd. Tegelijkertijd kan wel de verwachting uitgesproken worden dat bevragingen van cloud providers een steeds belangrijker wapen in het arsenaal van opsporings- en veiligheidsdiensten zullen zijn. Gezien het gebrek aan transparantie over gegevensvorderingen kan de ontwikkeling richting cloud computing tot een vermindering van autonomie leiden. In de situatie dat de gegevens bij een kennisinstelling in eigen beheer zijn ontstaat er wel een beeld van de hoeveelheid bevragingen en bestaat er eventueel ook een mogelijkheid zich juridisch tegen een bevraging te verzetten.

Het feit dat de Amerikaanse overheid de besproken mogelijkheden heeft gegevens op te vragen bij in de VS opererende cloud providers is op zich geen unicum. Ook Nederlandse en andere Europese landen kennen in beginsel vergelijkbare bevoegdheden. En deze bevoegdheden worden tevens ingezet ten behoeve van andere landen, zoals de VS, indien deze geen jurisdictie hebben met betrekking tot de gezochte gegevens. Uit officiële rapportages van de CTIVD lijkt op te maken dat soms te makkelijk van deze mogelijkheid gebruik wordt gemaakt. Een belangrijk verschil is dat in Europa aanvullende grondrechtelijke bescherming geldt op basis van het EVRM en dat bevoegdheden en de uitoefening daarvan zich dient te houden aan de door dit mensenrechtenverdrag gestelde grenzen van proportionaliteit. Ook is het te verwachten dat de grondrechtelijke belangen van Nederlandse ingezetenen een nadrukkelijkere rol zullen spelen binnen de verantwoordingsmechanismen van Nederlandse overheidsdiensten, zoals de verantwoording van de inlichtingendiensten aan het Nederlandse parlement en de CTIVD.

5.2 Aanbevelingen

Het besproken juridisch kader, de risicoanalyses van onder meer ENISA en de geschetste beleidsontwikkelingen, geven aanleiding om de mogelijkheid van gegevensvordering vanuit de VS serieus te nemen. Het is evident dat het risico van gegevensvordering door overheidsinstanties in bredere zin helder op de agenda dient te worden geplaatst. Allereerst is goed geïnformeerde besluitvorming uiteraard essentieel. De mogelijkheid dat gegevens vanuit Nederland worden opgevraagd door de Amerikaanse, een andere buitenlandse, of de Nederlandse overheid zal bij alle in Nederland opererende cloud aanbieders aanwezig zijn. Er dient realistisch met deze mogelijkheid omgegaan te worden en het onderwerp dient met leveranciers goed besproken te worden. Aspecten die daarbij aan de orde kunnen komen voor wat betreft de VS zijn onder andere of de aanbieder onder Amerikaanse jurisdictie valt, of delen van de dienstverlening worden uitbesteed aan derden (bijvoorbeeld voor het maken van back ups), hoe het verwijderen van gegevens in de cloud is georganiseerd en wat er gebeurt met de in de cloud verwerkte data in het geval van faillissement of overname van de cloud provider of bij ontbinding van de overeenkomst. Indien juist om redenen van het ontbreken van Amerikaanse (of andere buitenlandse) jurisdictie gekozen wordt voor een bepaalde

cloud aanbieder, is het aan te bevelen een specifieke contractuele beperking op te nemen ten aanzien van een overname die daar verandering in zou kunnen brengen.

Het is verder aan te bevelen een goede risicoanalyse te maken op basis van een categorisering van de verschillende soorten gegevens die het onderwerp zou kunnen worden van bevragingen. Op basis van een dergelijke interne analyse binnen de kennisinstelling kunnen keuzes gemotiveerd worden en indien nodig besproken met direct betrokkenen. Voor informatie en gegevens waarvoor het risico dat deze daadwerkelijk in handen komen van een Amerikaanse veiligheidsdienst zonder dat daarover enige transparantie bestaat te groot wordt geacht, zouden alternatieven ontwikkeld kunnen worden binnen de sector. Een goed doordachte in juridisch ingerichte nationale cloud voor de onderwijs- en onderzoekssector zou naar verwachting betere waarborgen kunnen bieden tegen het risico dat in onevenredige mate toegang verkregen wordt tot gegevens door een buitenlandse overheid.

De meeste kennisinstellingen zullen reeds beschikken over in meer of mindere mate geformaliseerde protocollen voor de omgang met gegevensvordering door de Nederlandse politie, justitie, of veiligheidsdiensten. Deze protocollen en de daaraan ten grondslag liggende overwegingen kunnen bij de beleidsvorming over het aangaan van cloud diensten en het risico dat daarmee gegevens beschikbaar komen voor buitenlandse overheden een belangrijke rol spelen. Uniformiteit van protocollen en de toepassing ervan is van wezenlijk belang, ook wanneer er meer nationale oplossingen wordt nagestreefd. Zo zou vrijwillige gegevensverstrekking – de basis voor willekeur en ondermijning van vertrouwen – niet moeten voorkomen. Een verdere versterking van een dergelijk verbod op regelgevend niveau kan daarbij een goed middel zijn.

Waar waterdichte juridische waarborgen tegen ongewenste gegevensvordering uit het buitenland ontbreken kunnen technische beschermingsmaatregelen toch in enige betekenisvolle bescherming voorzien. Zo kan bij goed ontworpen decentrale en gefragmenteerde opslag voorkomen worden dat alle gegevens in een keer makkelijk kunnen worden opgevraagd. En uiteraard dient de mogelijkheid overwogen worden om gebruik te maken van versleuteling. Daarbij moet aangetekend worden dat versleutelingstechnieken voor veel daadwerkelijke gebruikers mogelijk tot te veel complexiteit zouden kunnen leiden. Voor de omgang met bijzonder gevoelige gegevens dient echter ook binnen een cloud context goede instructies aan gebruikers gegevens te worden, net zoals dat in een traditionelere ICT omgeving binnen de instelling het geval dient te zijn. Differentiatie naar de aard van de gegevens en de wijze waarop gegevensstromen plaats vinden kan daarbij wenselijk zijn om proportionaliteit en effectiviteit te waarborgen.

Kortom, de implementatie van cloud computing dient bij kennisinstellingen, gezien hun bijzondere maatschappelijke rol, onderdeel te zijn van een integrale maatschappelijke kosten/baten-analyse. Daarin dienen niet-ICT-gerelateerde aspecten die samenhangen met de veiligheid en vertrouwelijkheid van informatie voldoende aandacht te krijgen (academische vrijheid, reputatie, chilling effect).

De verschillende mogelijkheden voor de Amerikaanse overheid om gegevens op te vragen bij cloud providers is geen statisch gegeven, maar zijn voortdurend onderwerp van debat en wijziging. Datzelfde geldt als de problematiek breder wordt getrokken dan slechts de relatie met de VS. De autonomie van

de kennisinstellingen ten aanzien van de informatiehuishouding dient te worden gewaarborgd en lock-in situaties moeten worden voorkomen. Het blijven nadenken en bijdragen aan alternatieven voor bestaand aanbod is daarom van groot belang. Voortschrijdend inzicht dient vertaald te kunnen worden naar heronderhandeling van aangegane overeenkomsten. Het garanderen van een realistische exit strategie is in dit verband even relevant als het garanderen van een back up van gegevens en garanties ten aanzien van de daadwerkelijke verwijdering van gegevens.

Aangezien de besproken juridische problematiek zich buiten het beslissingsveld van de betrokkenen in de sector bevindt, verdient het aanbeveling dat de sector een duidelijk standpunt ontwikkelt richting de politiek. De bescherming van privacy en vertrouwelijkheid van gegevens in het kader van cloud computing staat op dit moment op de politieke agenda in de EU. Daarbij wordt ook gedebatteerd over betere waarborgen ten aanzien van de vordering van gegevens uit de cloud door niet-Europese overheden. Ook in de VS is overigens op dit moment debat over de bevoegdheid die het mogelijk maakt gegevens op te vragen van niet-Amerikaanse personen in het buitenland. De belangen bij vertrouwelijkheid van gegevens van deze personen zijn in dat debat in het geheel nog niet aan de orde gekomen.

Cloud computing kent net als iedere nieuwe technologie haar kansen en bedreigingen. Waar de kansen evident zijn, kunnen de bedreigingen ondergesneeuwd raken of kan de informatie daarover juist vertroebelen in maatschappelijke discussies. De maatschappelijke discussie over de Amerikaanse Patriot Act en de betekenis hiervan voor het aangaan van cloud diensten lijkt tot nog toe een voorbeeld van dat laatste. Kennisinstellingen zijn bij uitstek in de positie om hier verantwoordelijkheid te nemen.

Bronnenlijst

ACLU, 'Why the FISA Amendments Act is Unconstitutional', 5 februari 2008, http://www.aclu.org/files/images/nsaspying/asset_upload_file578_35950.pdf.

Michael Armbrust et al., *Above the Clouds: A Berkeley View of Cloud Computing*, Technical Report No. UCB/EECS-2009-28, 10 februari 2009, http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

Article 29 Working Party, Opinion 05/2012 on Cloud Computing, 01037/12/EN, WP 196, 1 July 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

Attorney General and the Director of National Intelligence, Semiannual Assessment of Compliance witb Procedures and Guidelines Issued Pu rsuant to Section 702 of tbe Foreign Intelligence Surveillance Act, Reporting Period: June 1, 2009 -November 30, 2009,

May 2010, http://www.fas.org/irp/agency/doj/fisa/sar-may10.pdf.

Jennifer Baker, Europe cloud vendors cleaning up with data protection fears, Techworld, 5 December 2011, http://news.techworld.com/security/3322757/europe-cloud-vendors-cleaning-up-with-data-protection-fears/

Fletcher N. Baldwin & Daniel R. Koslosky, 'Mission Creep in National Security Law', 114 West Virginia Law Review 2011.

James Bamford, Big Brother is Listening, Atlantic Magazin, April 2006, http://www.theatlantic.com/magazine/archive/2006/04/big-brother-is-listening/4711/?single_page=true

William Banks, The Death of FISA, 2007, http://www.minnesotalawreview.org/wp-content/uploads/2011/11/Banks_Final.pdf

William C. Banks, 'Programmatic Surveillance and FISA: Of Needles in Haystacks' Vol. 88 (2010) Texas Law Review 7, 1633-1667.

Paul Bernal, 'The Draft Communications Bill and the ECHR', UK Constitutional Law Group, 11 juli 2012, http://ukconstitutionallaw.org/2012/07/11/paul-bernal-the-draft-communications-bill-and-the-echr/.

Rutger Betlem, 'Hoe veilig zijn min data eigenlijk in de cloud?', Expertpanel, Het Financieele Dagblad, 25 juni 2012.

Stephanie C. Blum, 'What Really Is at Stake with The FISA Amendment Act of 2008 and Ideas for Future Surveillance Reform', 18 Public Interest Law Journal, 2009.

J. Bradford, 'The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)', Wired.com, 15 maart 2012, http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1.

Ian Brown and Douwe Korff, 'Digital Freedoms in International Law', Global Network Initiative, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2085342.

Ronald Bruins, 'Wet- en regelgeving kan cloudaanbieders helpen', Cloudworks, Mei 2011, www.cloudworks.nu/uploads/CW4-los-low.pdf.

James R. Clapper, Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence, 31 January 2012, http://intelligence.senate.gov/120131/clapper.pdf.

James R. Clapper and Eric H. Holder, Letter to John Boemer, Harry Reid, Nancy Pelosi and Mitch McConnell, 8 February 2012, http://www.dni.gov/electronic_reading_room/dni_ag_letter.pdf

CRS, 'The U.S. Foreign Intelligence Surveillance Court and the U.S. Foreign Intelligence Surveillance Court of Review: An Overview',

24 January 2007, http://www.fas.org/sgp/crs/intel/RL33833.pdf.

CTIVD, Toezichtsrapportage inzake de inzet van SIGINT door de MIVD, CTIVD nr. 28, 23 augustus 2011.

James X. Dempsey, 'The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age', Statement before the Senate Committee on the Judiciary, 22 september 2010, https://www.cdt.org/files/pdfs/20100922_jxd_testimony_ecpa.pdf.

Department of Justice, 'USA PATRIOT Act: Sunsets Report', April 2005, http://www.justice.gov/olp/pdf/sunsets_report_final.pdf.

Deptartment of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence In Criminal Investigations (2009), p. 115-116, http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

Department of Justice, Report submitted pursuant to sections 107 and 502 of the Foreign Intelligence Surveillance Act, 30 April 2012, http://www.justice.gov/nsd/foia/foia_library/2011fisa-ltr.pdf.

Electronic Frontier Foundation, 'Cybersecurity Bill FAQ: The Disturbing Privacy Dangers in CISPA and How To Stop It', 15 april 2012, https://www.eff.org/deeplinks/2012/04/cybersecurity-bill-faq-disturbing-privacy-dangers-cispa-and-how-you-stop-it.

European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Version 56, 29 November 2011 (Leaked Draft), http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf.

European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012, COM(2012) 11 final, 2012/0011 (COD).

European Network and Information Security Agency, 'Cloud Computing Risk Assessment' (Rapport 2009) http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

European Network and Information Security Agency, 'Security and Resilience in Governmental Clouds - Making an Informed Decision' (Rapport 2011) http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/

Anna Fielder et al. , Cloud Computing, Study, Directorate General for Internal Policies, IP/A/IMCO/ST/2011, 18 May 2012.

Robert Gellmann, 'Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing', World privacy Forum, 23 February 2009, http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

William E. Kennard, United States Ambassador to the European Union, Remarks at the 2012 European Cloud Computing Conference, 12 March 2012, http://useu.usmission.gov/kennard_032112.html.

Orin S. Kerr, 'Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't' 97 Northwestern University Law Review 2003.

Orin S. Kerr, 'A User's Guide to the Store Communications Act - and a Legislature's Guide to Amending It', 27 George Washington Law Review 2004.

David Kravets, Court Upholds Google-NSA Relationship Secrecy, Wired.com, 11 mei 2012, http://www.wired.com/threatlevel/2012/05/google-nsa-secrecy-upheld/.

Hogan Lovells, A Global Reality: Governmental Access to Data in the Cloud, A Hogan Lovells White Paper, Washington, DC, 23 May 2012, http://www.hldataprotection.com/uploads/file/Hogan%20Lovells%20White%20Paper%20Government%20Access%20to%20Cloud%20Data%20Paper%20%281%29.pdf.

NIST, Mell, P. & Grance, T., The NIST Definition of Cloud Computing, 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Paul Ohm, 'The Argument Against Technology-Neutral Surveillance Laws', 88 Texas Law Review 1685, 2010.

David Saleh Rauf, PATRIOT Act clouds picture for tech, Politico, 29 November 2011, http://www.politico.com/news/stories/1111/69366.html.

Review Committee on the Intelligence and Security Services, *Accountability of intelligence and security agencies and human rights*, The Hague, 2007.

James Risen & Eric Lichtblau, Bush Lets U.S Spy on Callers Without Courts, The New York Times, 16 December 2005, http://www.nytimes.com/2005/12/16/politics/16program.html.

A. Rubel, 'Privacy and the USA Patriot Act: rights, the value of rights, and autonomy', 26 Law and Philosophy 119, 2007.

Paul Schwartz, Reviving Telecommunications Surveillance Law, 75 University of Chicago Law Review, 2008, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1116783.

Richard H. Seamon & William D. Gardner, 'The PATRIOT Act and the Wall between Foreign Intelligence and Law Enforcement', 28 Harvard Journal of Law and Public Policy 2005.

John Cary Sims, What NSA is Doing… and Why It's Illegal, 33 Hastings Constitutional Law Quarterly 101, 2006.

Daniel J. Solove, The Digital Person, New York: NYU Press, 2004.

SURFNET, Cloud Security, Checklist en de te stellen vragen, December 2010, http://www.surfnet.nl/Documents/rapport_201012_Cloud_Security_checlist_v1.0.pdf.

Peter R. Swire, 'From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud', 12 April 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2038871.

David Teneyuca, 'Internet Cloud Security: The Illusion of Inclusion', Information Security Technical Report (2011).

The Washington Post, Top Secret America, 2011, http://projects.washingtonpost.com/top-secret-america/.

The Washington Post, 'Oregon senator blocks five-year extension of surveillance law', 11 juni 2012.

TILT & Dialogic, Aftapbaarheid van telecommunicatie, Een evaluatie van hoofdstuk 13 Telecommunicatiewet, Tilburg, november 2005, http://www.dialogic.nl/documents/2004.59-0535.pdf.

TILT, 'De wolk in het onderwijs, Privacy aspecten bij cloud computing services', Surfnet, Kennisnet, 2011, http://www.surf-academy.nl/media/Seminar%20Privacy/De_wolk_in_het_onderwijs_feb2011[1].pdf

Andreas Udo de Haes, 'Amerika graait in Europese clouddata', Webwereld, 1 juli 2011, http://webwereld.nl/nieuws/107156/amerika-graait-in-europese-clouddata.html.

University of Cambridge, University Computing Service, Introduction to Google Apps @ Cambridge, 2012, http://www.ucs.cam.ac.uk/googleapps.

U.S. District Court, Eastern District of Virginia, Memorandum Opionion, Case 1:11-dm-00003-TCB-LO, Document 85, Filed 11/10/11,https://www.eff.org/sites/default/files/filenode/MemorandumOpinion1353.pdf.

Van Doorne, Rand Europe & Verdonck Kloosters & Associates, Cloud Computing, Fundament op Orde, Eindrapportage, 2012.

Kate Westmoreland, Sharing Evidence across Borders: the Human Rights Challenge, 2012 (forthcoming).

Zack Whittaker, Microsoft admits Patriot Act can access EU-based cloud data, ZDNet, 28 June 2011,

http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225.