Hartelijk dank voor de uitnodiging om deel te nemen aan deze bijeenkomst over de praktijken, gevolgen en wettelijke kaders rondom transnationale surveillance door inlichtingendiensten in de elektronische communicatieomgeving. De bestaande wettelijke kaders in de Verenigde Staten en de gevolgen daarvan voor de vertrouwelijkheid van cloud data, de autonomie en cybersecurity van cloud afnemers en de privacy van eindgebruikers hebben wij – met onze collega Prof. dr. Nico van Eijk – inmiddels in een tweetal publicaties[1] beschreven. In deze studies constateerden wij reeds voor de recente publicaties door The Guardian en anderen dat de bestaande brede wettelijke mogelijkheden in de VS, met name in §1881a (section 702) van de Amerikaanse Foreign Intelligence Surveillance Act ('FISA'), voor grootschalige surveillance waarschijnlijk navolging zullen krijgen in de praktijk. Dit leidde al het afgelopen jaar tot wereldwijde media-aandacht,[2] hernieuwde zorgen rondom het biometrische paspoort en het EPD,[3] en daaropvolgend twee presentaties van ons onderzoek in het Europees Parlement. In de afgelopen weken blijken onze constateringen zorgwekkend dichtbij de waarheid te liggen, in het bijzonder met het oog op het PRISM programma van de Amerikaanse inlichtingendienst NSA en het TEMPORA programma van de Engelse inlichtingendienst GCHQ in nauwe samenwerking met de NSA.

In deze notitie vatten wij de belangrijkste conclusies van ons onderzoek samen in een reeks stellingen, daarbij voortbouwend op de recente berichtgeving en ontwikkelingen:

- Surveillance door een inlichtingendienst vanuit het ene land, van burgers in een ander land is niet nieuw, maar de transitie richting cloud computing zorgt voor een ongekende toename van zulke transnationale surveillance mogelijkheden.

- Cloud data kunnen gevoelige persoonlijke informatie, overheidsinformatie, bedrijfsinformatie en vertrouwelijke communicatie omvatten. Daarmee is cloud surveillance een kwestie van de privacy van burgers, maar in belangrijke mate ook een probleem voor overheden, bedrijven, media en andere organisaties.

- De Amerikaanse Grondwet biedt geen bescherming voor niet-Amerikaanse personen of organisaties die niet in de V.S. verblijven. De FISA amendering in 2008 heeft plaatsgevonden om grootschalige surveillance zonder betekenisvolle waarborgen van deze groep mogelijk te maken. De waarborgen zijn er slechts om 'toevallige bijvangst' van gegevens van Amerikaanse personen en organisaties te minimaliseren. Europese datasubjecten komt geen bescherming toe, net als alle overige buitenlandse datasubjecten. De invulling van de zeer ruime definitie van 'foreign intelligence information' in de praktijk wordt ook niet rechterlijk getoetst.

[1] Van Hoboken, Joris V. J., Arnbak, Axel and Van Eijk, Nico, Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad (May 30, 2013). Available at SSRN: http://ssrn.com/abstract=2276103. J.V.J. van Hoboken, A.M. Arnbak, N.A.N.M. van Eijk, met medewerking van N.P.H. Kruijsen, 'Cloud diensten in hoger onderwijs en onderzoek en de USA Patriot Act', rapport in opdracht van SURF, september 2012. Engelse vertaling: Van Hoboken, Joris V. J., Arnbak, Axel and Van Eijk, Nico, Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act (November 27, 2012). Available at SSRN: http://ssrn.com/abstract=2181534.

[2] Bijv.: http://www.cbsnews.com/8301-205_162-57556674/patriot-act-can-obtain-data-in-europe-researchers-say/

[3] Bijv.: http://nos.nl/video/429087-toezicht-op-gegevens-in-een-cloud-is-hard-nodig.html en http://nos.nl/video/446392-vs-kan-toegang-tot-epd-krijgen.html

- PRISM valt waar het niet-Amerikanen betreft strikt juridisch gezien binnen de mogelijkheden van het Amerikaanse recht, maar levert strijd op met art. 8 van het Europees Verdrag voor de Rechten van de Mens, o.m. gezien het ontbreken van een heldere, specifieke juridische basis voor dergelijke praktijken en het brede karakter van de surveillance, zonder wettelijke waarborgen en afweging van proportionaliteit. Lidstaten bij het EVRM, Nederland inclusief, dienen op basis van hun positieve verplichtingen op te treden tegen dergelijke overmatige surveillance van burgers vanuit het buitenland.

- Voor de beoordeling van de schade voor afnemers van cloud computing diensten, voor de naleving en het voortbestaan van grondrechten van Europese en Nederlandse ingezetenen en voor de democratische rechtsorde is het cruciaal dat er een nauwkeurig inzicht komt in de aard en omvang van de PRISM en TEMPORA surveillance programma's. Het in het leven roepen van nationale en internationale onderzoekscommissies met brede bevoegdheden is geboden.

- In de praktijk delen inlichtingendiensten gegevens met elkaar op een 'quid pro quo' basis – voor wat hoort wat. Dit geeft diensten een prikkel om steeds meer data te vergaren, om zo hun informatiepositie ten opzichte van partners te versterken. Een belangrijke vraag is dus welke verdere waarborgen nodig zijn om te voorkomen dat Europese inlichtingendiensten lokale toegangscriteria kunnen omzeilen door te profiteren van de brede mogelijkheden in het buitenland.

- Veel commerciële cloud aanbieders bieden versleutelde verbinding aan voor het transport van gegevens, maar hebben een economische prikkel om cloud data vervolgens op te slaan in een te ontsleutelen vorm, zodat de deze data doorzocht kan worden – bijvoorbeeld voor het aanbieden van advertenties. Het is voor afnemers/gebruikers van het grootste belang om te weten in hoeverre de sleutels voor zowel het transport als de opslag van cloud data gedeeld worden met veiligheidsdiensten. Niet in de laatste plaats omdat zowel de NSA als de Britse GCHQ expliciet de ruimte nemen voor politieke en economische spionage.

- In onze studies staan vier mogelijke juridische oplossingsrichtingen centraal: het beperken van surveillance i) in V.S. wetgeving; ii) in het internationale recht; iii) in het Europees recht, in het bijzonder dataprotectie-recht en iv) door het versterken van toezicht op transnationale surveillance op nationaal niveau. Wij concluderen dat juridische oplossingen ingewikkeld te realiseren zijn, gezien het transnationale karakter van de surveillance. Bij dataprotectie geldt als inherente beperking, dat veel cloud data geen persoonsgegevens betreffen. Gezien de enorme belangen die op het spel staan, zien wij versterkt toezicht op transnationale surveillance en samenwerking door inlichtingendiensten, ook in Nederland, op de korte termijn de meest urgente oplossingsrichting, gepaard gaande met het instellen van een betekenisvolle nationale en internationale onderzoekscommissie met een breed mandaat.