

## **Verslag workshop 'Bewaarplicht Verkeersgegevens'**

Datum: Vrijdag 24 september 2004, 14:00-17:00.  
Locatie: Oudemanhuispoort, Amsterdam  
Organisatie: Instituut voor Informatierecht (IViR) en XS4ALL Internet B.V.  
Deelnemers: 27

### *14:00-14:05 Judith van Erve (XS4ALL) - Welkomstwoord*

Judith van Erve, public affairs officer van XS4ALL, heet de aanwezigen welkom. Ze deelt mee dat Nico van Eijk, de oorspronkelijke middagvoorzitter, helaas door de griep is geveld. Gelukkig was Remy Chavannes van Stibbe zo genereus hem te vervangen. Judith vertrouwt erop dat het een inspirerende middag wordt en geeft het woord aan Remy.

### *14:05-14:10 Remy Chavannes (Stibbe) - Opening*

Remy Chavannes, advocaat bij Stibbe te Amsterdam, opent de middag. Hij betreurt dat niemand van Justitie aanwezig wil zijn tijdens de workshop en zal daarom soms de rol van 'advocaat van de duivel' op zich nemen. Volgens Remy gaat het tijdens deze middag vooral om de volgende vragen: Wat is het probleem waarvoor de bewaarverplichting van verkeersgegevens in het leven wordt geroepen? Hoe belooft deze bewaarplicht dit probleem eigenlijk op te lossen? Welke moeilijkheden veroorzaakt de bewaarplicht echter? Wat is hiervoor een mogelijke oplossing? En welk plan kunnen de deelnemers daarvoor opstellen? Remy stelt Anton Ekker voor als eerste spreker en geeft hem het woord.

### *14:10-14:30 Anton Ekker (IViR) – De bewaarplicht verkeersgegevens: achtergrond en inhoud.*

Anton Ekker is als projectonderzoeker verbonden aan het Instituut voor Informatierecht te Amsterdam en werkt momenteel aan een proefschrift over anonimiteit en uitingsvrijheid. Anton schreef ook een artikel in het Parool van 3 juli 2004 over de bewaarplicht. Anton verzorgt deze middag een algemene inleiding op het onderwerp, waarbij hij o.a. de achtergrond en inhoud van het voorstel behandelt.

De bewaarverplichting van verkeersgegevens staat al sinds 2002 op de wensenlijstjes van de Europese opsporingsdiensten. Na de aanslagen in Madrid van 11 maart 2004 heeft de Raad van Europa een lijst met anti-terroristische maatregelen opgesteld waarop de bewaarplicht eveneens te vinden is. Op 28 april jongstleden werd bovendien een voorstel tot een bewaarplicht ingediend bij de Raad van Europa door Groot-Britannie, Frankrijk, Ierland en Zweden.

Anton zet uiteen welke verkeersgegevens onder de regeling kunnen vallen. Het bewaren van factureringsgegevens, gegevens over transmissie en een aantal overige gegevens zal betekenen dat bijvoorbeeld te achterhalen is wanneer iemand belde, met wie, hoe lang, welke internetsite diegene bezocht en welke zoektermen hij/zij gebruikte in een zoekmachine. De privacygevoeligheid hiervan vloeit voort uit het feit dat verkeersgegevens kunnen worden gekoppeld aan allerlei verschillende soorten persoonsgegevens zoals abonneegegevens en gebruikersgegevens. Verkeersgegevens kunnen daardoor ook veel zeggen over de inhoud.

Het voorstel dat door de vier lidstaten is ingediend betreft volgens Anton niet alleen verkeersgegevens maar eigenlijk alle gegevens die samenhangen met gebruik van tele communicatiediensten. De twee (!) definities die in het voorstel zijn opgenomen lijken álles te omvatten. In art. 1 van het voorstel is de definitie van gegevens:

'verkeersgegevens, locatiegegevens, abonneegegegevens en gebruikersgegevens'. Terwijl in art. 2 gegevens worden gedefinieerd als 'gegevens die nodig zijn voor opsporing en identificatie van de bron, met inbegrip van personalia e.d. en die nodig zijn voor identificatie van routing en bestemming, tijdstip, de datum en de duur, de telecommunicatie, communicatieapparatuur en locatie'.

De verplichting tot bewaren van de gegevens komt te rusten op aanbieders van openbare elektronische communicatienetwerken en -diensten. De bewaartermijn is volgens het voorstel gesteld op ten minste 12 maanden en ten hoogste 36 maanden na de productie. Een lidstaat kan besluiten af te wijken indien het de genoemde bewaarperiodes niet aanvaardbaar vindt. Onduidelijk is of dit laatste betekent dat listaten ook kunnen besluiten géén bewaarplicht in te voeren. Dit zou de nationale implementatie van groot belang maken.

De technologieën waarvan de gegevens bewaard moeten worden volgens het voorstel zijn legio. Van vaste en mobiele telefonie tot internetprotocollen als e-mail en voice-over IP. Zeer opvallend is dat zelfs 'toekomstige technologische ontwikkelingen' onder de werkingssfeer vallen.

Het voorstel is gebaseerd op een kaderbesluit binnen de derde pijler van de EU (politiële en justitiële samenwerking in strafzaken). Dit is een intergouvernementele besluitvormingsprocedure wat o.a. betekent dat het Europees parlement slechts om advies wordt gevraagd. Een kaderbesluit maakt consultatie door nationale parlementen mogelijk, al is de Nederlandse gang van zaken dat alleen de praktische details door het parlement kunnen worden ingevuld.

Het besluit dient met éénparigheid van stemmen te worden aangenomen. Op Europees niveau is vastgesteld dat het besluit voor juni 2005 moet zijn aangenomen. Alleen Duitsland en Griekenland maken nog bezwaar. Nederland is sinds het Nederlands EU-voorzitterschap niet meer tegen het voorstel.

Als Anton de toetsing van het voorstel aan art. 8 EVRM behandelt blijkt te meer hoe precair het voorstel is. Uit jurisprudentie van het Europese Hof voor de Rechten van de Mens over privacy en telecommunicatie blijkt dat telefoonverkeer valt onder het begrip 'correspondentie' van artikel 8 EVRM (Klass). 'Metering records' en het gekozen telefoonnummer vallen eveneens onder artikel 8 EVRM (Malone). Anton eindigt dan ook met een top vijf van bezwaren tegen de bewaarplicht: 1e Het voorstel is te ruim en te vaag geformuleerd. Het voorstel is niet beperkt tot bepaalde categorieën van personen. Dit levert een breuk op met bestaande privacybeginselen. 2e De proportionaliteit van het voorstel is onvoldoende onderbouwd. 3e De behandeling in de derde pijler geeft onvoldoende democratische legitimatie. 4e Het doel van het voorstel is handhaving van strafrecht maar de privacyrisico's manifesteren zich ook in andere contexten. Het kan een stuwmeer van gegevens opleveren dat een potentieel doelwit voor hackers en dataminers vormt. Er ontstaat gevaar voor cybercrime. 5e De kosten zullen hoog zijn en de technische haalbaarheid is nog niet bewezen.

Maurice Wessling (Bits of Freedom) vraagt zich af of er door het voorstel tegelijkertijd met de bewaarplicht ook een vergaarplicht ontstaat of dat slechts een bewaarplicht wordt ingesteld van de gegevens die al vergaard worden. Volgens dhr. Kaspersen (Vrije Universiteit Amsterdam) gaat het niet om een vergaarplicht, want dan zou de tekst van het voorstel anders moeten luiden.

De dagvoorzitter benadrukt nogmaals dat de grote vraag is welk probleem men met de bewaarplicht tracht op te lossen. Hij stelt voor om over te gaan naar de lezing van Sjoera Nas en introduceert haar. Sjoera krijgt het woord.

*14:30-14:50 Sjoera Nas (Bits of Freedom) – Verslag van de publieke consultatie in Brussel van 21 september 2004.*

Sjoera Nas werkt voor de onafhankelijke stichting Bits of Freedom die opkomt voor privacy en digitale burgerrechten.

Sjoera behandelt tijdens haar lezing de publieke consultatie over de bewaarplicht die de directoraten generaal 'Justitie en Binnenlandse Zaken' en 'Informatiemaatschappij' van de Europese Commissie organiseerden op 21 september 2004. Dit was een open workshop waaraan iedereen mocht deelnemen. Twee derde van de inzendingen was afkomstig van vertegenwoordigers uit de telecomindustrie en één derde van zgn. 'civil societies'. Er waren geen inzendingen of commentaar van opsporingsautoriteiten. Een vertegenwoordiger van het Spaanse telecombiedrijf Telefonica kon tijdens de workshop melden dat bij hen alleen 'jonge' gegevens werden opgevraagd. Telefonica heeft nooit gegevens hoeven verstrekken die ouder waren dan drie maanden, zelf niet na de aanslagen in Madrid. Dit sterkt de gedachte dat een bewaarverplichting van een jaar op zijn minst onnodig is. De conclusie van de workshop is dat meer onderzoek nodig is naar 'data-preservation' en dat de bewaartermijn korter moet worden.

In samenwerking met de Europese digitale burgerrechten organisatie EDRi heeft Bits of Freedom een verklaring laten opstellen tegen de bewaarplicht verkeersgegevens. Deze is ondertekend door talloze privacy voorvechters en vele andere organisaties uit de hele wereld. De verklaring noemt de voorgenomen bewaarplicht 'invasive, illusory, illegal en illegitimate'.

Het voorstel is 'illegal', omdat een bewaarplicht in strijd is met art. 8 EVRM. Het voorstel is bovendien 'invasieve' omdat er op Internet geen onderscheid mogelijk is tussen inhoud en meta-informatie. De informatie die bij telefonie uit de verkeersgegevens verkregen wordt is vrij simpel. Bij Internet zijn de verkeersgegevens echter veel meer verweven met informatie over de inhoud. Deze inhoudelijke informatie legt dan ook reeds de intenties van een gebruiker bloot. Indien iemand bijv. uit simpele interesse in Google de zoektermen 'terrorisme' en 'bommen maken' intypt kan diegene reeds als verdacht worden aangemerkt. Ook is het voorstel 'illusory' omdat verkeersgegevens niet 100% accuraat zijn. Als laatste noemt de verklaring het voorstel 'illegitimate' omdat het op ondemocratische besluitvorming stoelt.

Over het on-democratische aspect van het voorstel merkt dhr. Patijn (wetgevingsjurist) op dat het Nederlandse parlement de Nederlandse regering kan dwingen een negatief advies uit te brengen in de Europese besluitvorming. Sjoera benadrukt nogmaals dat het erg opvallend is dat sinds het EU-voorzitterschap van Nederland de regering ineens niet meer tegen het voorstel is.

Sjoera brengt het rapport naar voren dat door Bits of Freedom is verkregen met een beroep op de Wet Openbaarheid van Bestuur (WOB). Uit dit rapport van de Politie Rijnmond blijkt dat twee derde van alle onderzoeken ook succesvol zou kunnen worden afgerond zonder dat er überhaupt enige verkeersgegevens beschikbaar zouden zijn. Bovendien blijkt uit het rapport dat slechts in 2% van de gevallen alle opgevraagde gegevens ouder zijn dan een half jaar.

De politie Rijnmond vindt echter dat de inbreuk die ze maakt op de privacy door het opslaan van verkeersgegevens veel minder vergaand dan de inbreuk die ze maakt als ze verdachten bijv. moet volgen. Bits of Freedom is het hier niet mee eens en stelt dat het gelegitimeerder is om inbreuk te maken op de privacy van een verdachte dan de privacy van alle burgers.

Sjoera rond haar verhaal af en de middagvoorzitter stelt de derde spreker voor.

*14:50-15:10 Bernard Hulsman (CBP) – Juridische en privacy aspecten van een bewaarplicht verkeersgegevens.*

Bernard Hulsman is senior beleidsmederker bij het College Bescherming Persoonsgegevens (CBP). Het CBP stelt zich op verschillende punten actief op in het debat omtrent de bewaarplicht. Het CBP is lid van de 'art. 29 werkgroep', een verband van verschillende toezichthouders, die zich bezig houdt met de uitleg van de Europese richtlijnen over privacy en over elektronische communicatie. Het CBP heeft bovendien een adviserende taak bij wetgeving over privacy. Hierbij richt zij zich onder meer op het waarborgen van grondrechten in de digitale samenleving. Als laatste heeft het CBP ook als taak het toezicht op de naleving van privacy-regels. Het CBP onderzoekt hiertoe bijv. of de regels worden nageleefd en bemiddelt bij inzage in gegevens.

Volgens Bernard Hulsman is het doel van het CBP een bewaarplicht zo te omkleden met waarborgen dat het belang van de privacy bewaard blijft. Het CBP ziet privacy dus niet 'als pasgevalen sneeuw die niet betreden mag worden'. Het gaat om de waarborgen die zulke regelingen omgeven. Bij de bewaarplicht verkeersgegevens vraagt het CBP zich echter af of dit haalbaar is.

Uit rechtspraak van het Europees Hof van de Rechten van de Mens blijkt dat reeds het enkele verzamelen van gegevens niet onschuldig is. Het potentiële gebruik van die gegevens is een aantasting van de persoonlijke levenssfeer, niet alleen het daadwerkelijke gebruik. Ook verdienen verkeersgegevens volgens het Hof bijzondere bescherming met het oog op het recht vertrouwelijk te communiceren. Maatvoering bij 'secret services' is bovendien noodzakelijk voor het ontzien van onverdachte personen. Volgens het CBP is het EVRM het belangrijkste middel om de juiste afwegingen te maken omtrent de voorwaarden die de regeling moet omgeven. De waarborgen bij de bewaarplicht zullen moeten bestaan uit een notificatieplicht, een inzagerecht en een toetsingsrecht door de verdediging bij evt. rechtszaken.

Dhr. Hulsman merkt op dat gegevensbescherming niet alleen ten dienste staat van privacy. Dataproductie raakt ook andere belangen zoals het verbod van discriminatie, het recht op een eerlijk proces, het recht om vertrouwelijk te communiceren en het ontzien van bijzondere belangen zoals die van de advocatuur en gezondheidszorg.

Het standpunt van de 'art. 29 werkgroep' en het CBP is dan ook dat zij zich tegen een algemene bewaarplicht verzetten wegens strijd met art. 8 EVRM. Het CBP sprak zich eerder uit tegen art. 13.4 Telecommunicatiewet, dat reeds een gevaarlijk precedent bleek. Het CBP zal in oktober 2004 komen met een opinie over de bewaarverplichting.

Dhr. Hulsman sluit af met een citaat van Corien Prins (Universiteit Tilburg): 'Het fundamentele punt ligt dan ook niet bij de individuele opsporingsbevoegdheid, maar bij de optelsom van alle geïntroduceerde bevoegdheden. We moeten af van een situatie waarin iedere bevoegdheid afzonderlijk wordt bediscussieerd'. Dhr. Hulsman

wil de aanwezigen aansporen die optelsom te maken. Niet alleen van de bevoegdheden, maar ook van de grondrechten die in het geding komen met een 'bewaarplicht van alles'.

Er wordt een pauze ingelast.

*15:30-15:50 Bert-Jaap Koops (TILT) – Strafvordelijk kader van een bewaarplicht verkeersgegevens.* Bert-Jaap Koops is universitair hoofddocent aan het Tilburgs Centrum voor Recht, Technologie en Samenleving Institute for Law, Technology and Society (TILT) van de Universiteit van Tilburg. Bert-Jaap doet onderzoek naar de gevolgen van informatie- en communicatietechnologie voor het recht, in het bijzonder voor het strafrecht en reguleringsvraagstukken. Daarnaast besteedt hij aandacht aan juridische aspecten van informatiebeveiliging. Vandaag gaat zijn lezing over het strafvordelijk kader van een bewaarplicht.

Het vorderen van verkeersgegevens staat sinds 1926 in de wet. Artikel 126n Sv bepaalt sinds 2000 de regeling in Strafvordering. Per 1 september 2004 zijn wijzigingen opgetreden door de inwerkingtreding van de 'Wet vorderen gegevens telecommunicatie' en het 'Besluit vorderen gegevens telecommunicatie'. Op grond van art. 126n Sv mag de Officier van Justitie gegevens vorderen die bij AMVB (in deze het 'Besluit vorderen gegevens telecommunicatie') zijn aangewezen. Of naast vele andere gegevens URL's ook onder deze AMVB vallen is onduidelijk. Volgens de Memorie van Toelichting is dit wel het geval, maar URL's niet worden genoemd in het Besluit. Bert-Jaap vindt dat URL's niet onder het begrip verkeersgegeven zouden moeten vallen.

Op basis van art. 13.2a Telecomwet (Tw) is ten aanzien van de verkeersgegevens een meewerkplicht voor de telecomaانبeiders in het leven geroepen. In 13.4 Tw is dit geregeld voor de gebruikersgegevens. Via het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) kunnen de gegevens worden opgevraagd door onder meer justitie.

Bernard Hulsman (CBP) merkt op dat de regeling van de meewerkplicht en het CIOT als doel had databases aan te leggen bij de verschillende telecomaانبeiders zodat justitie individuele opvragingen zou kunnen doen. Het wordt nu echter steeds meer een centrale database met het gevaar van datamining. Kaspersen merkt echter op dat het CIOT technisch zo is ingericht dat slechts individuele opvragingen mogelijk zijn.

Bert-Jaap behandelt vervolgens de bewaarplicht in een algemene strafvordelijke context waarbij hij een aantal algemene kenmerken van het strafrecht vergelijkt met de bewaarplicht. Zo is strafrecht primair reactief en is het bedoeld als 'ultimum remedium'. Deze kenmerken zijn bij de bewaarplicht niet terug te vinden. Bovendien worden bij de bewaarplicht verantwoordelijkheden van de overheid overgeheveld naar bedrijf en burger. Een deel van de opsporingstaak van de overheid wordt bij de bewaarplicht neergelegd bij bedrijven. Bert-Jaap constateert een algemene tendens tot verstrafrechtelijking van de maatschappij. In principe is het zo dat iemand pas 'verdachte' is als hij verdacht is. Een bewaarplicht geldt echter voor iedereen en een ieder komt hiermee dus eerder in aanraking met justitie. Sjoera Nas (Bits of Freedom) merkt in dit kader op dat het EU-voorstel niet spreekt over een bewaarplicht in het belang van alleen terrorismebestrijding, maar over opsporing in het algemeen. Dit terwijl het voorstel juist wel onder het mom van terrorismebestrijding wordt gepresenteerd.

Bert-Jaap stelt voor verschillende regimes in te voeren voor verschillende soorten van privacy-inbreukmakende gevoelige gegevens. De 'verkeersgegevens' die bij internet gegenereerd worden zeggen veel meer over de inhoud dan de verkeersgegevens in telefonie, en locatiegegevens zijn ook privacy-gevoeliger dan traditionele verkeersgegevenscom.telecom. Door verschillende regelingen te treffen kan de privacy bij de opslag van de verschillende gegevens gewaarborgd blijven.

Bert-Jaap rondt af met een aantal discussiepunten. De dagvoorzitter stelt voor deze te bewaren voor na de laatste spreker.

*15:50-16:15 Simon Hania (XS4ALL) – Technische (on)mogelijkheden van een bewaarplicht verkeersgegevens.*

Simon Hania is technisch directeur van XS4ALL en in die hoedanigheid eindverantwoordelijk voor de kwaliteit en veiligheid van de technische dienstverlening aan de abonnees, inclusief alle daarvoor ingezette ICT-middelen. Simon behandelt vandaag de technische mogelijkheden en moeilijkheden van een bewaarplicht verkeersgegevens.

Simon zet met een verhelderend plaatje uiteen waar de gegevens ontstaan in het verkeerstraject van internet. Hij legt uit dat een provider alleen die gegevens kan opslaan van iemand die op een website kijkt die op de server van de desbetreffende provider draait. Indien bijvoorbeeld een XS4ALL-klant een website bekijkt bij een andere provider kan XS4ALL daarover nauwelijks gegevens vastleggen. Pas als die XS4ALL-klant een website bekijkt die bij XS4ALL zelf draait kan XS4ALL de verkeersgegevens vastleggen. Zo ontstaat er dus bij de verschillende providers een enorme berg van gegevens over klanten van andere providers.

Om een bronbestemmingsanalyse te kunnen doen (wie heeft met wie op welk tijdstip gecommuniceerd) moeten 5,4 miljard 'pakketjes' met informatie per uur vastgelegd worden. Volgens Simon is er op dit moment geen techniek voorhanden die dit mogelijk maakt en zal dit in de nabije toekomst ook niet mogelijk worden.

Een veelvoorkomende misvatting is volgens Simon dat de vastlegging betrouwbaar kan plaatsvinden. Bij het vastleggen van enorme hoeveelheden gegevens raakt er wel eens wat zoek of worden verschillende gegevens niet goed aan elkaar gekoppeld. Dit brengt het grote gevaar met zich dat op basis van verkeerde gegevens conclusies worden getrokken. Bovendien werkt het niet zo dat door eerst maar eens van alles vast te leggen, achteraf altijd de benodigde info terug te vinden is. Er moet eerst veel meer duidelijk worden over de manier van vastleggen. Zoeken naar 'een speld in een hooiberg' is absoluut een eufemisme als het gaat om verkeersgegevens.

Voor providers zal de bewaarplicht een enorme impact hebben. Het is dus niet juist dat providers nu al zoveel vastleggen dat een bewaarplicht geen impact zal hebben. De kosten van opslag zijn nog niet te overzien. Simon ziet voor de toekomst vooral ook een probleem wat betreft de opleiding van mensen bij justitie. Er zijn op dit moment te weinig mensen die überhaupt weten wat mogelijk is en wat niet. Wat betreft de technische (on)mogelijkheden is het voorstel voor de invoering van een bewaarplicht duidelijk niet goed onderzocht.

De dagvoorzitter stelt voor om over te gaan naar de discussie.

### *16:15-16:45 Discussie*

Sjoera Nas (Bits of Freedom) benadrukt nogmaals dat er een verschil is tussen de gegevens afkomstig van telefonie en die van internet. Bij internet is er geen onderscheid te maken tussen de inhoud en het 'verkeers'gegeven op zich. Bovendien bewaren telefonie-aanbieders nu al veel gegevens, terwijl internetproviders dat niet doen. Simon Hania (XS4ALL) merkt op dat het huidige opslaan door internetproviders op dit moment onvolledig is. Dat kan tot slechte en onbetrouwbare gegevens leiden, die niet als bewijs kunnen worden gebruikt. Volgens Dhr. Patijn (wetgevingsjurist) zijn de gegevens echter niet alleen als bewijs bedoeld, maar vooral ook als 'intelligence'. De informatie die eruit is af te leiden kan gebruikt worden om verder bewijsmateriaal te vinden. Dhr. Kaspersen (Vrije Universiteit Amsterdam) merkt bovendien op dat getuigen ook per definitie onbetrouwbaar zijn dus dat het argument van onbetrouwbaarheid van de gegevens niet zo sterk is.

Anton Ekker (IViR) ziet een gevaar in de cumulatie van de toenemende regelingen die inbreuk maken op de privacy. Voor de langere termijn is het van groot belang om deze tendens in de gaten te houden. De bewaarplicht van verkeersgegevens wordt volgens hem te veel vanuit alleen het privacy-oogpunt belicht. Het gaat echter om het geheel van verschillende regelingen die inbreuk maken op meerdere grondrechten.

Judith van Erve (XS4ALL) zegt dat de uitbreiding van de bevoegdheden tot opvraging betekent dat een steeds grotere groep personen gegevens mogen opvragen. Er is echter slechts een beperkte kring mensen die weet waar het echt over gaat. Hierdoor worden gegevens door bijv. de politie verkeerd geïnterpreteerd. Judith vertelt een anekdote uit de praktijk waarbij de politie mailheaders verkeerd om las, waardoor het slachtoffer van bedreiging via e-mail juist werd gezien als de dader.

Simon Hania ziet in dit licht vooral een probleem wat betreft de opleiding van de opsporingsautoriteiten. Men weet er gewoon te weinig van. Volgens Dhr. Kaspersen is dit echter geen argument tegen het invoeren van een bewaarplicht, aan het opleidingsprobleem is relatief makkelijk wat te doen.

De dagvoorzitter, Remy Chavannes (Stibbe), gooit de knuppel in het hoenderhok door te zeggen dat het probleem met de bewaarplicht wordt opgelost als de Staat de kosten op zich neemt. De providers zullen dan een stuk minder moeilijk doen. Bovendien is XS4ALL misschien zo netjes om zo min mogelijk gegevens te bewaren, maar andere providers bewaren vast meer, onder andere voor marketingdoeleinden. Zulke grote problemen kan het dus niet opleveren voor de providers. Alex Bik (BIT B.V.) heeft echter onderzoek gedaan voor de NLIP, de branchevereniging van de Internetproviders, en daaruit blijkt volgens Alex dat providers eigenlijk best netjes zijn op dit punt. Bovendien zijn de meeste gegevens helemaal niet bruikbaar voor marketingdoeleinden.

Dhr. Patijn zegt dat de ervaring in het verleden de overheid ertoe heeft gebracht dit soort zaken bij het bedrijfsleven zelf neer te leggen. In het verleden zijn overheden vaak beduvelend met enorme rekeningen. Bovendien weet de overheid ook niet hoe het moet dus laten ze het over aan de providers. Zij zijn de deskundigen en kunnen de kosten het beste marginaliseren. Volgens dhr. Kaspersen is het verstandig om de operationele kosten van de bewaarverplichting bij de overheid onder te brengen zodat ook de overheid op de kosten zal letten. De kosten voor de opslag zelf kunnen dan door de providers worden betaald. Bert-Jaap Koops (TILT) ziet ook het belang van een goede verdeling van infrastructurele kosten (providers) en operationele

kosten (overheid). Maurice Wessling (Bits of Freedom) merkt op dat de operationele kosten waarschijnlijk heel laag zullen zijn, want het opvragen van de gegevens is heel makkelijk. Simon Hania zegt dat dit echter helemaal ligt aan de manier van opslaan.

Remy Chavannes vraagt zich af wat er nu moet gaan gebeuren. Welke rol is weggelegd voor het parlement? Remy acht de volgende zaken van belang. Het inzagerecht moet beperkt worden tot het doel van bestrijding van internationale criminaliteit en terrorisme, de bewaarplicht moet beperkt blijven tot gegevens die al bewaard worden, de wijze van bevraging moet vooraf worden gedefinieerd en de noodzaak van de regeling moet beter naar voren worden gebracht door de overheid.

Dhr. Kaspersen vindt dat er vooral eerst gezegd moet worden: 'Niet doen!'. Er zitten teveel klemmen en angels aan de praktische invoerbaarheid volgens hem. Bovendien er zijn nog teveel vragen die niet in het Kaderbesluit besproken worden. Het voorstel is eigenlijk net een ongestuurde bom. Dhr. Patijn merkt op dat het allemaal gaat om informatiemacht. De opslag van gegevens zal een precedent zijn voor de toekomst. Het kan alleen maar erger worden met alle creditcards, biometrie en RFID van deze tijd. Volgens dhr. Patijn is het een ziekte en zaait het uit. Jurjen Pen (de Roos & Pen advocaten) zegt dat hét slagwoord in de politiek 'transparantie' is. Straks zullen steeds meer gegevens opvraagbaar zijn en juist door die transparantie moet je er tegen zijn. We stappen straks in een wereld waar je niet wilt leven volgens dhr. Pen.

Bert-Jaap Koops vraagt zich af wat nu de beste strategie is. Het principiële argument tegen een bewaarplicht, inbreuk op de privacy, slaat bij de meeste mensen niet aan, dus er moet iets anders bedacht worden. Marijke Vos (GroenLinks) denkt ook dat de principiële discussie niet te winnen is binnen het huidige klimaat. Vooral de praktische argumenten tegen een bewaarplicht zullen naar voren moeten worden gebracht. Marijke Vos ziet het echter somber in dat de Nederlandse regering een negatief advies zal uitbrengen. Dat is echter geen argument om niet te blijven vechten. Ook Dhr. Kaspersen is voor actief verzet tegen de bewaarplicht. Hij stelt voor om contact op te nemen met de Duitsers omdat zij een groot constitutioneel probleem hebben met de bewaarplicht. Dat probleem met hun grondwet biedt goede mogelijkheden voor verzet.

#### *16:45:16:50 Afsluiting*

Remy Chavannes bedankt alle aanwezigen voor hun bijdrage. Judith van Erve bedankt allereerst Remy voor zijn voortreffelijk dagvoorzitterschap. Ook de andere sprekers worden hartelijk bedankt voor hun inspanningen. Iedereen is uitgenodigd voor de afsluitende borrel.