Rondetafelgesprek biometrische data in paspoorten

Tweede Kamer, vaste commissie voor Binnenlandse Zaken
woensdag 20 april 2011, 10.00 - 13.00u

10.00 - 11.30 ***Beleidsontwikkeling en uitvoering***

- Dhr. J. Grijpink, voormalig raadadviseur directie Algemene Justitiële Strategie V&J en hoogleraar RUU keteninformatisering in de rechtsstaat
- Dhr. A. Meijboom, CIO Politie Nederland
- Dhr. C. Meesters, voorzitter NVVB en projectdirecteur Burgerzaken en Basisregistratie gemeente Rotterdam
- Mw. L. De Leeuw, consulent IT & security (voormalig BPR)

11.30 - 12.00 ***Toezicht en controle***

- Mw. J. Beuving, collegelid CBP
- Dhr. H. Moraal, portefeuillehouder College van PG's

12.00 - 13.00 ***Onderzoek en reflectie***

- Dhr. A. Ruifrok, teamleider audio, beeldonderzoek en biometrie NFI
- Dhr. M. Snijder, CEO European Biometrics Group
- Dhr. R. Veldhuis, universitair hoofddocent Universiteit Twente
- Dhr. G. Munnichs, senior onderzoeker Rathenau Instituut
- Dhr. R. Van Renesse, security specialist (voormalig TNO)
- Mw. Q. Eijkman, senior onderzoeker CTC, Universiteit Leiden
- Dhr. V. Böhre, auteur WRR-webpublicatie "Happy Landings"

Woordelijk verslag door Privacy First (selectie van fragmenten):

De Leeuw: "Aan de toepassing van biometrie op paspoorten zijn enkele principiële bezwaren verbonden. De technologie dringt binnen in de persoonlijke levenssfeer en veroorzaakt een onbalans in de verhouding tussen burger en overheid. Dit is des te sterker zo wanneer biometrische kenmerken voor opsporingsdoeleinden worden opgeslagen in een centrale database."

Grijpink: "De 6 miljoen vingerafdrukken die we nu hebben, zijn die betrouwbaar? We weten het gewoon niet, omdat het niet gecontroleerd is. (…) Als de vingerafdrukken niet goed genoeg zijn voor de databank, mogen ze ook niet in het paspoort. Dus op het moment dat je zegt: "de kwaliteit is echt bagger", dan hadden ze nooit op het paspoort mogen staan. (…) Realiseer u dat biometrie een onrijpe technologie is en in een wapenwedloop terechtkomt tussen criminelen, burgers en overheden. (…) Ik zit al heel lang in dit dossier. De mensen die mij kennen, hier in de zaal, weten dat ik helemaal niet zo'n voorstander ben [van biometrie op reisdocumenten]. Voor mij had het niet gehoeven. Ik vind het veel te vroeg en veel te riskant.

Brussel heeft – voor mijn gevoel onnodig, onder druk van de Verenigde Staten – dat geaccepteerd. We hadden ook kunnen zeggen: “wie naar Amerika wil mag vrijblijvend en op vrijwillige basis biometrie op zijn paspoort laten zetten.” Dan waren we van een hele hoop ellende af geweest. Maar dat hebben we niet gedaan: we houden van grote stelsels die voor iedereen hetzelfde zijn. Wat dat betreft vallen we van de ene ellende in de andere. Ik ben dus niet een voorstander van biometrie op het paspoort. (…) Ik ben tegen een centrale databank omdat we daarmee geen controle zullen kunnen uitoefenen. Het ultieme doel van het voorkomen en verhelpen van identiteitsfraude kan daardoor niet worden gerealiseerd.”

Meijboom: “Ik stel vast dat er in de toekomst een steeds grotere waarde wordt gehecht aan een integer persoonsbeeld. Dat is in het belang van het optreden van de overheid, maar het is ook in het belang van betrokkenen. Identiteitsfraude is een onderwerp dat in de toekomst gaat spelen. Het tweede wat ik vaststel is dat de overheid bezig is om na te denken over het vraagstuk welke basisgegevens waar zouden moeten worden opgeslagen. (…) Voor de politie is in ieder geval van belang [onverstaanbaar] om het aantal biometrische gegevens in paspoorten te verbreden [slecht verstaanbaar], als het een identiteitsbewijs is dat we kunnen raadplegen, dat is het hoofddoel op dit punt. En dan gaat het om identiteitsfraude, en opsporing van criminaliteit valt dan terug op dat integere persoonsbeeld.”

Meesters: “[onverstaanbaar] het foutenpercentage van 21%. [onverstaanbaar] is er één gemeente die dat gedaan heeft. Dat is gebeurd in een periode van 12 oktober 2009 tot 7 november 2009. 448 reisdocumenten zijn er toen afgegeven. Bij het verifiëren van vingerscans bleek dat er bij 55 personen maar één vinger verifieerbaar was en bij 42 personen bleken géén vingers verifieerbaar te zijn. Vandaar dat percentage van 21%. Waarom heeft BZK steeds volgehouden: “het gaat goed”? Eigenlijk hebben we daar nooit een helder antwoord op gekregen; daar moet ik eerlijk in zijn. Er werden wel argumenten aangedragen van “dat betekent dat mensen dan opnieuw een document moeten aanvragen als blijkt dat het incorrect is en wie moet de kosten daarvoor dan betalen.” Echte goede argumenten hebben we nooit mogen vernemen.”

De Leeuw: “Naar mijn gevoel heeft het agentschap BPR – waar ik aan verbonden was in die tijd – zich een gesloten vesting getoond, welhaast een sekte. Wie daarmee van buitenaf contact kreeg kon niet vermoeden wat daar onder het [slecht verstaanbaar] [tapijt] werd verborgen. Nou, een aantal dingen. 1) Naar mijn gevoel is het onderzoek van meet af aan gedreven door politieke wenselijkheid. “Nederland, gidsland. Europese wil is wet.” [onverstaanbaar] Deze twee tezamen hebben geleid tot een cultuur van “niet denken, maar doen”. Vragen naar [onverstaanbaar]kwaliteit en communiceren daarover, vooral naar buiten toe en naar boven, werden taboe verklaard. De studie *naar* de haalbaarheid van de toepassing van biometrie op paspoorten verwerd op die manier tot een studie *van* de haalbaarheid. 2) Op de tweede plaats bepaalde externe adviesbureaus, soms niet altijd even terzake deskundig, waren boven kritiek verheven, maar vervulden desalniettemin een sleutelrol in het onderzoek naar de performance van de technologie. Andere, kwalitatief hoogwaardiger adviesbureaus functioneerden als een speelbal van eerdergenoemde adviesbureaus. Mijn eigen rol viel aanvankelijk samen met die van de projectleider. Al snel werd ik tot *persona non grata* bevorderd. Demotie en verandering van taakstelling werden gevolgd door een pseudo non-actiefstelling en dreiging met ontslag. 3) Ten derde. De communicatie met het centrale ministerie verliep via en werd volledig gecontroleerd door de directeur. Na enige opmerkingen mijnerzijds aangaande ervaringen inzake de performance van technologie bij een vergadering van de stuurgroep, ben ik voorgoed uit het gremium verwijderd. Mijn notities voor de directeur-generaal werden door de directeur herschreven of later ook aan mij

gedicteerd, ook waar het specifiek mijn expertise betrof. 4) Binnen het ministerie bevond ik mij in een [onverstaanbaar] isolement op een enkel klein gebaar of opdracht met meestal externe collega's na. Op een bepaald moment heb ik ook contact gezocht met een vertrouwenspersoon integriteit binnen het ministerie. Deze verklaarde mijn verhaal uit het feit dat er sprake zou zijn van *incompatibilité des humeurs*, een verstoorde arbeidsrelatie en dergelijke meer. In mijn bijzijn verklaarde hij plechtig dat niemand, maar dan ook niemand, buiten die kamer waar ik mij bevond daar ooit over zou horen. 5) In het kader van mijn studie aan de TIAS Business School heb ik een scriptie geschreven over de vraagstukken die in het kader van de haalbaarheidsstudie bleven liggen. Door enkele beroepsverenigingen is deze scriptie beloond met een [onverstaanbaar] *security award*. Het agentschap [BPR] heeft nooit belangstelling voor de scriptie getoond en het feit dat ik deze prijs had gewonnen leidde bij een latere manager van mij tot de opmerking "mijn nekharen gaan hiervan overeind staan". Ik heb nooit echt begrepen waarom. 6) Na vier jaar ambtenaarschap bij het ministerie heb ik mijn loopbaan voortgezet als consultant bij een professioneel bureau." (…)

Hennis-Plasschaert: "[onverstaanbaar] Ik wil graag weten of de heer Grijpink het beeld herkent zoals net is geschetst. [onverstaanbaar]"
Grijpink: "Daarover kan ik heel kort zijn: ja."

Meijboom: "Er mag geen twijfel bestaan over het integere persoonsbeeld. Dat integere persoonsbeeld is voor ons het absolute uitgangspunt. Dat los je niet op, wat ons betreft, door op het paspoort meer biometrische kenmerken te plaatsen waarvan deskundigen zeggen "het is twijfelachtig of…" Ik ben daar geen deskundige in. Het is ook niet zo dat de politie op straat als de identiteit van iemand moet worden vastgesteld of het paspoort wordt overhandigd, dan onmiddellijk even kijkt, waar dan ook... Het *mag* niet eens, maar het is ook technisch niet beschikbaar."

Beuving: "Ik kan het kort houden. Ter voorbereiding van de commissie hebben wij volstaan met het opsturen van ons wetgevingsadvies uit 2007 en de mededeling, de samenvatting die op onze website is gezet. Wij hebben dus al in 2007 een vrij kritisch en fundamenteel advies uitgedaan. Daar is wat mij betreft niets in veranderd. Als ik hier nu wat ter inleiding daar nog aan zou willen toevoegen, dan is het eigenlijk… dan laat ik misschien de wat meer diplomatieke formulering en de subtiele formuleringen… je moet soms zoeken in een wetgevingsadvies naar een aantal dingen die er absoluut in staan… die laat ik maar even los. En dan wil ik hier vooral zeggen: de centrale opslag is het grote risico. Eén van de grote nadelen van centrale opslag, of welk onderwerp dan ook, is waarvoor wij meestal waarschuwen: de *function creep*. Het bijzondere rond deze wet, en in die tijd het wetsvoorstel, is dat de *function creep* al bij voorbaat was ingebakken. En die ingebakken *function creep* is dat opsporingsdoel en daarnaast de eigenlijke, zuivere, primaire doelen zoals meteen al in het wetsvoorstel was voorzien. Ik vermoed sterk dat dat oneigenlijke doel er in feite toe geleid heeft dat men centrale opslag wilde. Want als je die onzuiverheid van doelen wegdenkt, als je daarvan gaat abstraheren, je haalt het opsporingsdoel eruit, je gaat naar de primaire besluiten, de eigenlijke doelen, dan zijn er volgens mij geen argumenten om tot centrale opslag te komen. Dan volstaat decentrale opslag, een decentrale opslag eventueel gecombineerd met een centrale verwijsindex. Al die andere doelen zijn dan waarschijnlijk heel goed daarmee te realiseren. En dan zeg ik er alleen nog wel bij dat het bij die decentrale opslag natuurlijk heel belangrijk is dat je gestandaardiseerde beveiligingsmaatregelen hebt. Dat overal in het land dezelfde maatregelen, dezelfde normen worden toegepast. Dan heb ik het nu nog niet gehad over biometrie. Het feit dat we met vingerafdrukken gaan werken juist om identiteitsfraude, een ander doel, maar een doel dat wel heel dicht aanzit tegen die eigenlijke doelen van een

paspoort, dat we die biometrie in het paspoort krijgen, vingerafdrukken in het paspoort. En ja, ik snap heel goed, in dat kader was dat opsporingsdoel natuurlijk zo vreselijk interessant, dat opsporingsdoel dat weer leidde tot die centrale opslag. En juist als je kijkt naar die vingerafdrukken zijn er wat mij betreft, wat betreft de opslag, drie smaken: 1) centrale opslag [onverstaanbaar], 2) decentrale opslag, en de andere variant is 3) alleen gebruiken in het paspoort zelf. Centrale opslag, daar zijn geen argumenten voor op het moment dat je het oneigenlijke doel van die opsporing eruit haalt. Dan blijft puur nog de vraag over of het dan decentrale opslag moet zijn. Kijk, je maakt een reisdocumentenadministratie, die zul je nodig hebben, dat zal wat mij betreft dan decentraal zijn, met die veiligheidsnormen waar ik het over had. Een decentrale reisdocumentenadministratie. En dan is de volgende vraag: gaan de vingerafdrukken in die reisdocumentenadministratie, gaan die in dat decentrale systeem, of volstaat het om ze te gebruiken in het paspoort. (…) De keuze voor het centrale systeem is wat mij betreft ingegeven door oneigenlijke gronden en oneigenlijke argumenten."

Moraal: "Voor het OM zijn in deze kwestie drie aspecten van belang. Dat is in de eerste plaats het gebruik van biometrische gegevens voor de identiteitsvaststelling in de strafrechtsketen. Het tweede is de opsporing en vervolging van fraude met dat soort gegevens. En in de derde plaats een centraal databestand als het gaat om opsporingsdoeleinden. (…) Als het gaat om het eerste is dat misschien wel de allerbelangrijkste voor ons: het integere persoonsbeeld in de strafrechtsketen. Wij kennen missers op dat punt, omdat in de strafrechtsketen de identiteit van mensen heeft gewisseld, mensen gebruik hebben gemaakt van valse identiteiten, mensen zijn gaan 'zitten' voor een ander. Zo kan ik u een aantal voorbeelden noemen waarbij de integriteit van de gegevens op de blauwe ogen werden geloofd. Die tijd hebben we denk ik inmiddels wel achter ons gelaten; in ieder geval moeten we die heel snel achter ons gaan laten. Er zijn allerlei ontwikkelingen met apparatuur en databases die de strafrechtsketen zelf aan het ontwikkelen is als het gaat om dat integere beeld van de persoon in de strafrechtsketen, waarbij dus mensen die in de strafrechtsketen komen – of dat nou bij de politie is, of dat het nou in een later stadium bij de zitting is, of in een later stadium bij de gevangenis is – worden gecheckt aan hun biometrische gegevens die zij op het lijf hebben, die in het paspoort staan en die bij ons in het systeem zitten. Geen misverstand daarover: dat is een systeem dat de strafrechtsketen zelf opbouwt en ook in beheer is bij de justitiële diensten, in dit geval in Almelo bij de justitiële informatiedienst. Het paspoort wordt nadrukkelijk daarbij gebruikt. Het biometrisch paspoort is daarbij dus van belang. Dat wordt ingelezen in dat systeem en wordt daar ook in vastgelegd. Maar de politie vermeldt méér in het systeem. Als u mij de vraag stelt: is daarvoor een centrale database nodig, dan is dat niet het geval, want die maken wij zélf in dit verband. En iedereen die aan het begin te maken krijgt met de politie en aan bepaalde criteria voldoet, die nemen wij op in dat systeem, zodat wij die persoon en iedereen die zich meldt als zijnde Jan Janssen kunnen controleren of dat inderdaad ook de heer Jan Janssen is. En daar hebben wij dus niet een nieuwe centrale database voor nodig. Dat is denk ik het belangrijkste als het gaat om het eerste aspect. Het tweede aspect, wat betreft de identiteitsfraude, daarvoor heb je nodig een goede vastlegging van de gegevens, dus het biometrisch paspoort is daar denk ik een hele belangrijke in [*sic*]. Terecht ook dat de nieuwe wetgeving nieuwe soorten van fraude ook vermeldt en strafbaar stelt, want het vervalsen van biometrische persoonsgegevens – dat op dit moment denk ik nog betrekkelijk weinig voorkomt – dat zal meer voorkomen. Een enkele keer zie je bij asielzoekers vingertoppenmutilatie, zoals dat heet, en de kans bestaat natuurlijk dat dat meer gaat voorkomen. De wetgever heeft hier in de nieuwe wetgeving aan gedacht. Het derde punt, dat is een databestand, of het paspoort zelf, het gebruik daarvan voor opsporingsdoeleinden. Dat is een lastig punt in die zin dat politie, het OM, maar vooral de politie, op dat punt natuurlijk ook al wel veel hebben. Hebben wij daarbij aan het paspoort veel? Dat hebben wij

wél, want de biometrische gegevens uit het paspoort zijn te vergelijken met de gegevens die de politie in het systeem heeft zitten en als je die vergelijkt dan kun je dat bij de opsporing gebruiken. Met name het gebruik van foto's zal daarbij van belang zijn. Een andere vraag is echter of een centrale database daarbij ook van heel groot nut kan zijn. Wij denken dat dat op dit moment nog beperkt is. U moet zich voorstellen dat bij de opslag in het paspoort één vinger wordt gescand en daar zijn – ik heb daar ook wel in het rapport van Böhre het nodige over gelezen – vraagtekens te zetten bij de kwaliteit daarvan. Dat in de eerste plaats. In de tweede plaats: er is maar één vinger, en op een plaats delict kun je er wel tien aantreffen. Dus het effect daarvan wordt op dit moment door ons als betrekkelijk ingeschat als je die centrale database hebt. Wat niet wil zeggen dat ie dus niet van nut is, want die is er wél, want je hebt wel die ene vinger en daar kun je wat mee. En je hebt een foto, en daar kun je ook bij identificatie, als het gaat om getuigengegevens, kun je daar wellicht wat mee. Dat dat in de toekomst kan veranderen als je daar meer en betere gegevens in opslaat en dat dat van nut kan zijn voor de opsporing, dat lijkt mij wel. Maar als u mij de vraag stelt: "hebben jullie op dit moment een zware behoefte aan een centrale database op dit punt?", dan moet ik zeggen, zoals ik net zei: dat nut is er, maar ik denk dat het nog beperkt is."

Beuving: "(…) Ik begrijp in ieder geval uit het rapport van Corien Prins dat bijvoorbeeld in de Eerste Kamer en zelfs de Raad van State, mensen met naam en toenaam genoemd ondertussen zeggen "hé, daar zijn we niet scherp genoeg geweest op dit onderwerp", dus ben ik in elk geval blij dat u ook in feite de herkansing daarin pakt. (…) Als het gaat om de vingerafdrukken in het paspoort, zou mijn voorkeur hebben: hou het bij de opslag in het paspoort en doe het zelfs niet decentraal, want je brengt het dan weer ergens buiten dat document zelf, en dat geeft altijd – al is het niet centraal, dat het grootste risico geeft, maar ook decentraal – het geeft áltijd weer risico's."

Ruifrok: "Mijn relatie met dit onderdeel is al gegeven: biometrie. Ik ben van daaruit ook betrokken geweest bij het *2b or not 2b*-project dat 6 jaar geleden is gedaan om een praktijktest uit te voeren voor het gebruik van biometrie in het paspoort. Daar werden wij later bij betrokken. En om aan te sluiten bij sommige opmerkingen die al eerder gemaakt zijn: er werd ons een beetje verzocht om een stempel van goedkeuring voor het gebruik van biometrie op die manier te geven. Laat betrokken gedurende het onderzoek, en dat was al vastgelegd. Voor onderzoek is het vaak heel erg belangrijk om alles vast te leggen wat fout gaat en niet wat goed gaat. Helaas is er weinig vastgelegd wat fout gaat en alleen gerapporteerd over wat goed gaat, en bij die rapportage is ook nog eens een keer een rapportagestijl gebruikt waar, wat gechargeerd gezegd: 'als je alles wat niet goed gaat niet meerekent, dan gaat het heel erg goed'. En als je dan kijkt naar welk percentage van de mensen goed geïdentificeerd konden worden op gezicht en/of vingerafdruk, dan hield je maar een kleine hoeveelheid over, waarbij het me niet zo heel erg verbaast dat er 21% fout gaat bij de huidige afname van vingerafdrukken bij de gemeentes. [slecht verstaanbaar] Als die kwaliteitscontrole niet goed is, dan voer je dus slechte data in. En als je dan later die data wilt vertrouwen, dan gaat het mis. Dus als je kwaliteitscontrole niet goed is, is dat een hele goede gelegenheid voor een kwaadwillende om in dat geval wel een stempel van goedkeuring op zijn identiteitsdocument te krijgen. Want dan zit iemand met het stempel 'dit is goed gecontroleerd' in het systeem, terwijl het niet goed ingevoerd is en, tot mijn grote verbazing, niet gecontroleerd wordt bij uitgifte. Dit is voor de crimineel hét moment om te zorgen dat hij een valse identiteit goed in het systeem kan krijgen. En dan zit ie gebakken."

Snijder: "Ja, die 21%, daar zit nog één addertje onder het gras, om het erger te maken, dat is namelijk welke drempelwaarden zijn bij die meting gebruikt. Is het een lage drempelwaarde,

dan is het bij een hoge drempelwaarde misschien wel 80%. [slecht verstaanbaar] Ik ben verheugd dat de Tweede Kamer het belang heeft onderkend van het heragenderen van het biometrisch paspoort. De redenen om daar verheugd over te zijn komen voor een belangrijk deel naar voren in het rapport 'Het biometrisch paspoort in Nederland: crash of zachte landing' dat ik vorig jaar in opdracht van de WRR heb geschreven. Ik noem enkele hoofdconclusies; het rapport zelf is nogal omvangrijk. De hoofdconclusies van mijn WRR-studie en de voor deze hoorzitting ingediende notitie zijn als volgt. Er is een discrepantie ontstaan tussen het geformuleerde beleid en de daadwerkelijke uitvoering. Met name de processen bij het aanvraag- en uitgifteproces kunnen de belofte van de beoogde maatregelen niet inlossen. De belofte was destijds maximaal 3 % volgens BZK, dus daar zitten we kilometers boven. En dan wil ik toch even aantekenen dat ik het eigenlijk shockerend vind dat deze cijfers boven tafel komen door het eigenlijk [onverstaanbaar] van de gemeente. Daar zakt mijn broek echt van af. Dit is mede veroorzaakt, deze discrepantie, door de enigszins oppervlakkige wijze waarop destijds studies en proeven zijn verricht, waardoor er in bepaalde opzichten een te rooskleurige rapportage aan de besluitvorming heeft kunnen plaatsvinden. Aanwezige externe en interne expertise is onvoldoende benut. Bepaalde risico's, onduidelijkheden en oplossingen die toen bekend waren zijn daardoor te weinig voor het voetlicht gebracht. Het is onduidelijk op welke afwegingen van techniek, organisatie, veiligheid en kosten het voorstel tot invoering van een centraal landelijk vingerafdrukkensysteem precies is gebaseerd. En welke partijen precies bij deze afwegingen betrokken zijn geweest. De mogelijkheid van een decentraal gemeentelijk verificatiesysteem is nooit serieus onderzocht. Een centrale landelijke database met vingerafdrukken is voor de meeste beoogde doelstellingen overbodig en zelfs onwenselijk. De enige doelstelling die het niet ondersteunt is de opsporingsfunctie: de 1:n zoekfunctie. In de huidige opzet is een centrale database voor een 1:n zoekfunctie technisch niet haalbaar. Er bestaat de kans dat er meer risico's worden geïntroduceerd dan zij problemen oplost. Het testen en certificeren van biometrie is verre van uitontwikkeld. Met name op het niveau van het *image* – dat is het plaatje van het gezicht en de vingerafdrukken dat wordt opgeslagen in het paspoort – bestaan nog geen leveranciersonafhankelijke testmethoden. Er wordt gesproken in de stukken naar de Kamer toe over een zogenaamde standaard die dat zou moeten garanderen. Die standaard garandeert iets anders. Die garandeert niet die kwaliteit. (…) Vanuit het perspectief van veiligheid en integriteit bestaan er steekhoudende en duurzame argumenten voor het op gemeentelijk niveau opslaan van de biometrische gegevens buiten het paspoort, met uitsluitend 1:1 verificatie als doel. 1:1 verificatie, dat is een decentraal verificatiesysteem op basis van vingerafdrukken, dus wel de aanvulling op de Europese richtlijn. Hierover zou ik het volgende willen opmerken. Vooralsnog lijkt de Europese verordening te kunnen vertrouwen op het breedst mogelijke draagvlak. Neem deze daarom als primair uitgangspunt voor de eerstvolgende stappen. Dat betekent dat de eerste prioriteit is het verkrijgen van een optimale kwaliteit en integriteit van in het paspoort opgeslagen biometrische gegevens, alvorens we eventueel definitief overgaan tot invoering van decentrale opslag als nieuw concept. Dat wil ik hier benadrukken, want dat is als concept nog helemaal niet bestudeerd. Het is een nieuw concept. We doen het nu, eigenlijk omdat we niet anders kunnen, maar het doel was altijd [slecht verstaanbaar]. Bij decentrale opslag als nieuw concept zal eerst bewezen moeten worden de processen rond de aanvraag- en uitgiftesystemen op orde te hebben. Ook een decentrale database op gemeentelijk niveau is gevoelig voor fraude en fouten. Daarom zullen voor deze nieuwe situatie eerst alle randvoorwaarden moeten worden vastgelegd. Zonder die randvoorwaarden zou op dit moment het opslaan van vingerafdrukken in welke database dan ook al snel leiden tot vervuiling en kans op fouten. Vanwege de afwezigheid van een controle-infrastructuur, zoals verificatie bij uitgifte, zullen bepaalde fouten en vormen van fraude niet eens aan het licht komen en stapelen de onzuiverheden zich

op. In eerste instantie dienen uitsluitend die data opgeslagen te worden die noodzakelijk zijn om het systeem te testen, te evalueren en te verbeteren. Voorkom leveranciersafhankelijkheid zoveel mogelijk. Alle nu opgebouwde databases kunnen de overgang naar een echte leveranciersonafhankelijke toekomst bemoeilijken en ook veel duurder maken; alles opnieuw gaan invoeren. Stel in de discussie rond de toepassing van biometrie eerst een duurzame en eenduidige doelomschrijving vast die door alle partijen wordt gedragen. Dat is een absoluut vereiste. Onduidelijke of veranderende doelstellingen kunnen elke gekozen oplossing laten resulteren in een desinvestering, onnodige maatschappelijke onrust of pijnlijke fouten. Biometrie is voor het leven. Voor een structurele toepassing ervan dienen burgers daarom te kunnen vertrouwen op een helder, duurzaam en betrouwbaar beleid voor de lange termijn. De kwaliteits- en integriteitsproblemen rond de biometrische gegevens vormen ook een supranationaal probleem waar op Europees niveau aan gewerkt wordt. Voorkomen moet worden dat Europese ontwikkelingen rond standaardisatie en wetgeving – let wel, de Europese Commissie is nu bezig met het bekijken of Nederland zich wel helemaal goed aan de regeltjes houdt, dus er kan ook zomaar een streep door de rekening gehaald worden – de Europese regelgeving en wetgeving ons in de wielen gaan rijden straks. Investeer daarom op dit moment met name in die onderdelen die daarmee in lijn danwel daarvan onafhankelijk zijn. Welke oplossingsrichting er ook wordt gekozen, de goede kwaliteit en integriteit van biometrische data in het paspoort zullen elk proces altijd ten goede komen. Dan sla ik een stuk over en kom ik tot een conclusie. Er is nog veel onbekend over biometrische toepassingen op grote schaal. De techniek is in diverse opzichten nog onvolwassen. Een stapsgewijze invoering van de techniek helpt ons te bepalen in hoeverre en op welke wijze de gekozen techniek en alles daaromheen ons kan ondersteunen in het bereiken van onze doelstellingen. Neem pas definitieve beslissingen over elke stap die verder gaat dan de Europese verordening als wij vanuit kennis, ervaring en onderzoek weten op welke kwaliteit, integriteit en interoperabiliteit we kunnen rekenen. Een goed doordacht, decentraal verificatiesysteem kan het aanvraag- en uitgifteproces significant verbeteren. Indien besloten wordt hierop over te gaan, dan is eerst een periode nodig voor het testen, evalueren en optimaliseren van het aanvraag- en uitgifteproces conform nader vast te leggen randvoorwaarden. En daarbij moeten we niet vergeten dat optrekken in Europees verband van belang is in verband met toekomstig overkoepelend beleid."

Veldhuis: "Wat ik in dit verband zou willen zeggen, is eigenlijk wat veel mensen al gezegd hebben. Ik wil iets zeggen over de effectiviteit van biometrische oplossingen en de veiligheid daarvan. En die zijn gekoppeld. De effectiviteit: hoe goed kun je nou zoeken in zo'n database? Iedereen is er hier wel van doordrongen dat biometrie fouten maakt. We hebben *false accepts* en *false rejects*, en al die fouten worden gekarakteriseerd door kansen. Die kansen, daar zit een *trade-off* tussen, afhankelijk van hoe je het systeem instelt kun je kiezen voor een hoge *false accept rate* en een lage *false reject rate*, dus dan laat je veel verkeerde personen toe maar de kans dat je iemand mist is niet zo groot, of omgekeerd. Die spelen een rol bij zo'n grote database, en die spelen een zwaardere rol naarmate die database groter gaat worden. Dus als u praat over een database met misschien 10 miljoen vingerafdrukken, zijn de problemen best groot. *False accepts*, die schalen min of meer lineair met een database, en als het heel groot wordt dan wordt dat wat minder, want als je begint met $1/10^{e}$ % voor 1:1 vergelijkingen dan [onverstaanbaar]. Die 21% in dit verband, die verbaast mij helemaal niet, en ik vermoed dat dat zelfs nog is van een redelijk kleine database, van zo'n 200.000 personen. Dus als de database groter wordt, dan wordt het probleem alleen maar groter. *False rejects*, dat is dus die *trade-off*, je kunt proberen dat aantal omlaag te krijgen of, anders gezegd, het aantal *near-matches*, de lijst van mensen die mogelijk zouden kunnen zijn kleiner te krijgen, door met de *trade-off* tussen *false-accepts* en *false rejects* te spelen, maar dan

neemt de kans dus toe dat je iemand niet vindt. Als dat iemand is die wel ten onrechte een paspoort heeft aangevraagd heb je wel een probleem, dus je hebt een gemaksprobleem ten opzichte van een veiligheidsprobleem. Daar moet je zorgvuldig mee omgaan. En mijn inschatting is op dit moment dat voor dit soort hele grote databases de techniek eigenlijk niet goed genoeg is om dat goed te doen. Standaard technologie voor vingerafdrukken, voor goede kwaliteit vingerafdrukken, haalt $1/10^{e}$ % *false accept rate* bijvoorbeeld bij 1% *false reject rate*, bij 1:1 vergelijking. En dan is het wel uit te rekenen, dat zal ik hier niet doen, waar we op uit gaan komen bij een database van 10 miljoen. En dan hebben we het nog over goede kwaliteit vingerafdrukken. Dat dus wat betreft de effectiviteit van het geheel. Dan kun je ook nog spreken over andere veiligheidsaspecten in deze context. En dan denk ik: of je nou praat over centrale of decentrale oplossingen [slecht verstaanbaar]. En ook een redelijk grote database als die van Den Haag, waar vermoedelijk uw vingerafdrukken in terecht zouden komen, is best een grote database. Als iemand met kwade bedoelingen daar bij zou kunnen, dan heeft hij heel veel informatie tegelijk. En zo'n database wordt niet beheerd door één persoon, daar zit een aantal personen omheen die allemaal bevoegdheden hebben en allemaal iets kunnen, en dat zijn allemaal mensen die verleidbaar zijn tot kwalijk gedrag. Sowieso aan alle opslag zit een veiligheidsrisico, en hier ook. Maar wat is hier aan de hand: als iemand hier bij kan komen, dan heeft hij ineens toegang tot, in het slechtste geval 10 miljoen vingerafdrukken, de gegevens van 10 miljoen personen, inclusief hun biometrische gegevens. Dat betekent in principe dat hij zou kunnen kijken naar die vingerafdrukken, hij zou valse vingerafdrukken kunnen maken, hij zou als het ware heel veel persoonsinformatie kunnen overnemen en vervolgens als één van u door de wereld kunnen gaan. Daarvan kunt u proberen dat tegen te gaan, maar die vingerafdruk, die is weg. Voor vingerafdrukken geldt: "once compromised, lost forever." Een nieuwe pincode kun je krijgen bij de bank, en nieuwe vingerafdrukken lukt niet. Dus daar zit een groot risico. In het kader daarvan zou ik de aandacht willen vestigen op nieuwe technologie die niet die effectiviteitsproblemen oplost – er blijven op dit moment fouten – maar die wel er voor zorgt dat wat je opslaat niet herleidbaar is tot de oorspronkelijke biometrie. Dus in plaats van het plaatje van de vingerafdruk sla je een code op. Die code heeft bovendien de eigenschap dat als hij *compromised* is hij opnieuw uitgegeven kan worden. En die code is niet of heel moeilijk herleidbaar tot de oorspronkelijke vingerafdrukken. Dus degene die dan bij die gegevens komt is niet in staat om het plaatje van die vingerafdrukken te genereren. Deze technologie is nog niet zo oud, is in ontwikkeling, is niet pasklaar om morgen zo'n database uit te rollen, maar verdient wel enig verder onderzoek als mogelijk enige oplossing om op een veilige manier grootschalig vingerafdrukken op te slaan."

Munnichs: "Wij zijn vrij kritisch over het gebruik van biometrie. We hebben eind vorig jaar een studie uitgebracht over het gebruik van databases. Daarin ontwaren we een algemeen patroon in de overgang naar databases. Het komt erop neer dat het steeds vanzelfsprekender lijkt om maar zoveel mogelijk gegevens op te slaan, vaak zonder dat precies duidelijk is welk doel daarmee gediend is en vaak met weinig aandacht voor de risico's die daarmee gepaard gaan. Als we tegen die achtergrond kijken naar de discussie over het biometrisch paspoort vallen de volgende zaken op: er lijken vraagtekens te kunnen worden geplaatst bij de opslag van biometrische gegevens in een nationale of gemeentelijke database. En voorzover ik begrijp lijkt die opslag niet nodig voor het primaire doel van *look-alike* fraude. Daarvoor volstaat 1:1 verificatie van de vingerafdrukken van de persoon met op het reisdocument opgeslagen gegevens. Ook opsporingsdoeleinden lijken onvoldoende legitimatie voor opslag van die gegevens in een database. De kwaliteit is dermate [onverstaanbaar]; de op het gemeentehuis opgeslagen vingerafdrukken volstaat daarvoor niet en het gebruik daarvan voor opsporingsdoeleinden leidt vooral tot vals-positieven. Dat heeft ook een forensisch expert van

de politie aan mij bevestigd. Daarnaast creëert opslag in databases nieuwe veiligheidsrisico's en een grotere kans op identiteitsfraude. En de negatieve gevolgen van vals-positieve uitkomsten of identiteitsfraude komen vooral op het bordje van de burger terecht, die nauwelijks in staat is om zich daartegen te verdedigen. Dat vormt een aantasting van zijn rechtspositie. Tenslotte vormt de opslag van biometrische gegevens in een database in die zin een vergaande maatregel omdat opslag – nu of in de toekomst – andersoortig gebruik van die gegevens mogelijk maakt. Daar wordt vaak aan gerefereerd met de term *function creep*. Opslag in een database is dan ook een grote stap die extra argumentatie behoeft, en 'gemak' vind ik daarvoor altijd een hele magere argumentatie. Al met al roept dit het beeld op dat we een grootschalige nationale database of een veelheid aan gemeentelijke databases aan het optuigen zijn waarmee nieuwe risico's worden geïntroduceerd zonder dat nu precies duidelijk is wat de baten ervan zijn. De overheid dient hierin uiteraard zorgvuldig te opereren en het lijkt ons dan ook wenselijk als er nog eens heel goed gekeken gaat worden naar het nut, de noodzaak en risico's van een nationale of gemeentelijke opslag van biometrische gegevens."

Van Renesse: "In overeenstemming met het onderwerp van deze sessie heb ik wat reflecties over mijn werk bij BPR. Ik heb in mijn carrière bij TNO – dat was van 1966 tot 2002 – in eerste instantie bij TNO en later als zelfstandig consulent, regelmatig opdrachten uitgevoerd voor het Agentschap [BPR]. En mijn ervaring is dat BPR geen prijs stelt op onafhankelijke, ongewenste inzichten betreffende de functionaliteit van biometrie of identiteitsdocumenten. Ik wil daarvan enkele voorbeelden geven. In oktober 1999 presenteerde TNO het in opdracht van BPR geschreven rapport *Quick-scan biometrie*, waarvan ik de auteur ben. Dat rapport geeft een uitgebreid overzicht van de problemen die moeten worden opgelost teneinde biometrie met succes te kunnen toepassen op identiteitsdocumenten. BPR was bepaald niet blij met dat rapport. Het had niet om problemen gevraagd. Ik verwijs voor nadere details naar het rapport *Crash of zachte landing*, paragraaf 8.3. Ik wist het toen nog niet, maar ik was toen toegetreden tot de club van *personi non grata*. In februari 2002 verliet ik TNO en begon als zelfstandig consulent voor documentbeveiliging. Ik bleef hierna nog werkzaam voor TNO om mijn kennis op het gebied van biometrie over te dragen. In juli 2002 deelde Ruud van Munster, projectleider biometrie bij TNO, mij echter mee dat TNO niet langer gebruik wilde maken van mijn diensten. BPR had TNO namelijk meegedeeld dat TNO niet bij het project *Biometrics against look-alike fraud in the next generation travel documents* zou worden betrokken wanneer ik lid van het projectteam zou zijn. In februari 2002 ook, werd ik door Interpol Nederland uitgenodigd een paper te presenteren op de 2002 Interpol-conferentie van 10 tot 12 april in Amsterdam. Ik diende mijn paper *Implications of biometrics on travel documents* begin maart in. De Interpol-conferentieorganisatie nam de dubieuze vrijheid mijn paper ongevraagd door te sturen naar BPR. Ik werd vervolgens verzocht op 13 maart 2002 te verschijnen voor mevrouw Ineke Ruiter en de heer Sjef Broekhaar van BPR. Het thema van het gesprek was hoe ik het in mijn hersens durfde te halen zo'n negatieve paper te willen presenteren terwijl minister Van Boxtel in de zaal zat. Tenslotte, in februari 2010 werd ik door BPR ingehuurd voor werkzaamheden op afroep. Tijdens mijn sollicitatiegesprek werd mij reeds meegedeeld dat het niet de bedoeling was dat de werkzaamheden werden verstoord door voortschrijdend inzicht. Tijdens de eerste werkbespreking werd mij voorts expliciet opgedragen niet schriftelijk te rapporteren. Alle rapportage diende mondeling te geschieden. Ja, ik moet speculeren: wat anders dan de letters van de WOB te omzeilen kan aan deze oekaze ten grondslag liggen? Maar dat is een persoonlijke speculatie. Mijn schriftelijk bezwaar hiertegen leidde ertoe dat ik binnen twee weken na aanvang van de werkzaamheden werd gewipt. Dit zijn enkele voorbeelden van de grondhouding van BPR met betrekking tot onafhankelijke en ongewenste inzichten. Ik acht het buitengewoon zorgelijk dat een

overheidsorgaan tracht ongewenste inzichten te onderdrukken bij het uitvoeren van haar projecten in plaats van deze, zo mogelijk, te weerleggen."

Eijkman: "Aangezien we het vandaag al best veel over effecten hebben gehad zal ik daar niet teveel over uitweiden en iets meer over het gebrek aan politieke *accountability*, rekenschap en de reactie van het maatschappelijk middenveld. Over het effect kan ik heel kort zijn: ik denk dat de 'terrorisme-kaart' niet te snel gespeeld moet worden. Bestrijding van terrorisme is heel belangrijk, alleen is het niet zo dat alle veiligheidsmaatregelen die de afgelopen jaren genomen zijn noodzakelijkerwijs terroristische aanslagen voorkomen [onverstaanbaar]. Daar ga ik verder niet over uitweiden omdat een aantal mensen daar eerder vandaag al op zijn ingegaan. Waar ik het eigenlijk over wil hebben in het hele dossier is, naar mijn idee, het gebrek aan politieke rekenschap. In zekere zin zijn we dat natuurlijk vandaag aan het doen, achteraf, en ik denk dat dat geheel ertoe heeft geleid dat het maatschappelijk middenveld zich zo sterk heeft gemobiliseerd in dit dossier. Als je kijkt wat er de afgelopen jaren is gebeurd, mensen zijn naar Europa gegaan, mensen zijn naar de Verenigde Naties – het Mensenrechtencomité – gestapt, voordat de Paspoortwet werd ingevoerd zelfs naar het Europese Hof voor de Rechten van de Mens. En voor iemand die persoonlijk meer dan 10 jaar heeft meegedraaid in de mensenrechtenwereld in Nederland zijn dat hele extreme maatregelen. Ik denk dat dat te verklaren is door het gebrek aan transparantie in het voortraject, die leidde eigenlijk tot gebrek aan kennis, zowel bij Kamerleden maar ook bij de media, waardoor ook geen vragen, geen kritische vragen werden gesteld. Ik denk dat het verhaal van de heer Van Renesse, ik hoor ook een aantal andere mensen, ik denk dat politici zich moeten realiseren dat dat neveneffecten heeft. Eén van die neveneffecten is dat als die wet eenmaal is ingevoerd, dat dan de maatschappij 'opstaat'. En ik denk eigenlijk dat dat een grotere vraag is waar deze Kamercommissie misschien over moet nadenken in dit dossier: hoe leggen we eigenlijk rekenschap af, zowel naar de Tweede Kamer als ook naar de maatschappij. En dan creëer je dus weerstand, en daarom zitten we hier vandaag, los even van alle biometrische discussies. Als ik het heb over de heftige mobilisatie, dan spreek ik met name over het oneigenlijke doel waar mevrouw Beuving het ook over had. De Europese verordening ging om het voorkomen van identiteitsfraude. Eigenlijk is via de achterdeur ook een opsporingsregister, met allerlei voorwaarden weliswaar… en op zich is daar niks mis mee als we dat willen als maatschappij, als onderzoeker kan ik daar ook niks over zeggen. Maar dan moet je eigenlijk een apart wetgevingstraject starten daarover en dan moeten we met z'n allen de discussie aangaan: willen we om de staatsveiligheid te beschermen of om terrorisme te bestrijden of voor opsporing, willen we dan een nationale database met biometrische kenmerken? En dan moet je daar een aparte discussie over starten, maar niet via de achterdeur van Europa een opsporingsregister, onder allerlei voorwaarden, maar met het risico van *function creep*. Dus dat wilde ik eigenlijk in deze discussie meegeven, deze reflectie. *Last but not least*, mijn persoonlijke standpunt is eigenlijk dat een centraal opsporingsregister, of dat nou decentraal is of niet, er niet moet komen. Er moet een aparte discussie komen in Nederland of we dat willen of niet, en dat is uiteindelijk aan jullie om dat te beslissen. De grotere vraag is misschien ook: hoe worden Europese verordeningen ingevoerd in Nederland? Is het democratisch tekort in Europa nu eigenlijk niet terug in de Tweede Kamer?"

Böhre: "Het biometrische-paspoortdossier werd door de WRR omschreven als een *black box* dossier. Zij hadden er eerder ook zelf onderzoek naar gedaan en het bleef schimmig; het bleef het karakter van een *black box* houden. Mede om die reden zijn Max Snijder en ik ingeschakeld om te proberen om daar toch wat meer licht op te kunnen werpen, op dat dossier. Dat hebben wij met alle mogelijke middelen geprobeerd. Zelf had ik weliswaar eigenlijk alleen maar toegang tot internetbronnen en kon ik maar heel weinig mensen

interviewen, tot mijn grote spijt. Ik hoop dat deze meeting een eerste aanzet gaat vormen, ook in parlementair opzicht, maatschappelijk opzicht, het is natuurlijk al langer aan de gang, om nu echt eens een keer wat fundamentele vragen met elkaar te gaan bediscussiëren. En dan heb ik het niet alleen maar over techniek en over veiligheid en over de manier van opslag, wel of geen *hashing*-technieken en dat soort dingen. Ik heb het over fundamentele vragen, over privacy, over transparantie, over accountability, identiteit, effectiviteit en efficiëntie, maar ik zou zelf voornamelijk de nadruk willen leggen op privacy en keuzevrijheid. Dat gaat tenslotte de burger aan, en ik denk dat we daar vooral met z'n allen op zouden moeten focussen, op het perspectief van de burger. En dan kan ik heel kort herhalen wat er de afgelopen anderhalf jaar is gebeurd. Dat is natuurlijk dat mensen pas nadat de wet was aangenomen daarmee werden geconfronteerd, in het algemeen. Bijna niemand had er ooit van gehoord. Ik zelf moet ook bekennen dat ik ook pas vlak voor aanname in de Eerste Kamer op de hoogte raakte van het feit dat überhaupt die wet zou worden aangenomen. Ik kom zelf ook uit de mensenrechtenwereld, was ook actief bij het Nederlands Juristen Comité voor de Mensenrechten, sinds kort werk ik voor Privacy First en voor het Platform Bescherming Burgerrechten. Het NJCM heeft toen dus de kans gegrepen om linea recta de boel aan te kaarten bij het VN-Mensenrechtencomité in Genève. Dat heeft destijds ook tot maatschappelijke discussie geleid, voor het eerst dus, in het aanlooptraject van 10 jaar, vond er tóen pas maatschappelijke discussie over die wet plaats, nádat hij was aangenomen, zónder stemming door de Eerste Kamer. Dat is natuurlijk eigenlijk te gek voor woorden, bij zo'n draconische wet, met doeleinden als opsporing en vervolging, terrorismebestrijding, rampenbestrijding, inlichtingenwerk in binnen- en buitenland. De meesten van die doelen zijn vrijwel onbesproken gelaten in de Tweede Kamer. Dat verbaast mij tot op de dag van vandaag. Mijn punt wat ik hier vandaag wil maken is: kijk vooral nu naar de toekomst. Ik denk dat we het er met zijn allen over eens kunnen zijn dat het een puinhoop is, zowel in wetgevend opzicht als in maatschappelijk opzicht als in technisch opzicht, hoe het nu is vormgegeven, ik denk dat het een drama is. En mijn punt zou zijn: schaf per direct de decentrale opslag af en ga je zuiver focussen op de implementatie van de Europese verordening, daar kunnen we immers niet onderuit als Nederland op dit moment, al kun je over de verordening ook vragen stellen, maar dat is dan voor de toekomst op Europees niveau. Ik vind dat biometrie vrijwillig zou moeten zijn, dat de burger zelf een keuze zou moeten hebben of hij wel of niet zijn vingerafdrukken zou willen afstaan. En wat de infrastructuur betreft, ik zou zeggen, richt het op verificatie in plaats van identificatie, dus geen opsporing, ook niet dat het mogelijk wordt. Het punt wat moet worden gevraagd hier, is als je bijvoorbeeld een *hashing*-techniek zou willen invoeren, in hoeverre is dat dan nog bruikbaar voor identificatie c.q. opsporingsdoeleinden? Anders zijn we nog net zo ver van huis met zijn allen als eerder, misschien. Mijn voorkeur gaat dan nu uit naar het Duitse model, dus alleen opslag in de chip in het document, en niet decentraal, en zéker niet centraal, omdat die twee opties denk ik grotendeels dezelfde risico's inhouden, zeker op lange termijn, qua verschuivende doeleinden. (...) Onlangs is u een overzicht toegezonden door minister Donner, over de implementatie van de verordening in heel Europa. Daarover wil ik een opmerking maken: dat biedt een momentopname. Wat je moet weten als Tweede Kamer om je daar goed een oordeel over te kunnen vormen is de ontwikkeling door de tijd heen. Wat niet uit het document van Donner blijkt is dat de laatste jaren sprake is, of schijnt te zijn, van een ontwikkeling van centrale naar decentrale opslag. Een aantal landen die in eerdere tabellen een paar jaar geleden nog stonden genoteerd als hebbende een centrale opslag, hebben inmiddels een decentrale opslag, voorzover ik weet. En dat blijkt dus niet uit de tabel van Donner."