Stichting Bits of Freedom
Postbus 10746
1001 ES Amsterdam

M +31 (0)6 5438 6680
E ot.vandaalen@bof.nl
W www.bof.nl

Leden van de Commissie Binnenlandse Zaken

Betreft
Kabinetsstandpunt rapport Staatscommissie Grondwet en aanpassing artikel 13 van de Grondwet

Datum
Amsterdam, 28 februari 2012

Geacht lid van de Commissie Binnenlandse Zaken,

1. Op 29 februari 2012 overlegt de Commissie Binnenlandse Zaken over de aanpassing artikel 13 van de Grondwet. De stichting Bits of Freedom komt op voor vrijheid en privacy op internet. Omdat de aanpassing van dit grondwetsartikel het communicatiegeheim kan versterken, maken wij graag van de gelegenheid gebruik om onze gedachten hierover met u te delen.

2. Kort samengevat zou het communicatiegeheim alle nieuwe vormen van communicatie moeten beschermen. Het zou zich niet alleen moeten richten op communicatie tussen twee personen maar ook tussen groepen. Het zou ook opgeslagen communicatie moeten beschermen. Verkeersgegevens zouden ook hieronder moeten vallen. Dat lichten we hieronder toe. Ook doen wij een voorstel voor een nieuwe grondwetsbepaling.

Kabinet zou ook artikel 7 en 10 Grondwet moeten aanpassen

3. De Staatscommissie Grondwet heeft geadviseerd om artikel 13 Grondwet aan te passen. Het huidige artikel 13 Grondwet biedt een zekere bescherming voor het “brief-”, “telefoon-” en “telegraafgeheim”. De Staatscommissie pleit om deze bepaling “techniekneutraal” te maken, zodat het communicatiegeheim wordt beschermd – ongeacht het medium waarmee wordt gecommuniceerd (zie par. 8.6 e.v.). Het kabinet heeft dit advies van de Staatscommissie overgenomen. Zij zal een voorstel tot herziening van dit grondwetsartikel voorbereiden. Bits of Freedom juicht dit toe.

4. De Staatscommissie adviseert echter ook om artikel 7 en 10 van de Grondwet aan te passen.

Ook deze artikelen zijn niet toegespitst op de uitdagingen van de digitale maatschappij, en passen bovendien niet bij internationale en Europese mensenrechtenverdragen. Bits of Freedom betreurt het dan ook dat het kabinet dit advies niet opvolgt.

> **Advies** De regering zou niet alleen artikel 13 Grondwet, maar ook artikel 7 en 10 Grondwet moeten aanpassen aan de digitale tijd.

Het communicatiegeheim moet alle nieuwe vormen van communicatie beschermen

5. De Staatscommissie merkt terecht op dat Nederlanders via veel meer dan de in artikel 13 Grondwet genoemde middelen communiceren. Het is niet mogelijk om hier een limitatieve opsomming van te geven, omdat de belangrijkste technologische infrastructuur – het internet – open is. Hierdoor zijn de afgelopen jaren talloze nieuwe communicatiemiddelen ontwikkeld: email, WhatsApp, Skype, videochat, Twitter, Google Wave etc. Het is niet te voorspellen wat voor communicatievormen zich in de toekomst zullen ontwikkelen. De grondwet zou dus alle nieuwe vormen van communicatie, ook die nog niet zijn uitgevonden, moeten beschermen.

> **Advies** Het communicatiegeheim zou ook nieuwe vormen van communicatie moeten beschermen.

Het communicatiegeheim moet communicatie tussen groepen beschermen

6. Een deel van de communicatie via nieuwe middelen speelt zich niet meer af tussen enkel ontvanger en verzender. Zo kan een bericht naar een groep van ontvangers worden verzonden, en kan een groep van personen gezamenlijk tegelijkertijd aan het chatten zijn. De bepaling moet erop gericht zijn om communicatie tussen niet alleen twee personen, maar ook communicatie tussen groepen personen hieronder te laten vallen.

> **Advies** Het communicatiegeheim zou ook de communicatie binnnen een groep van personen moeten beschermen.

Het communicatiegeheim moet ook opslag beschermen

7. Een belangrijk deel van de discussie over de reikwijdte van het communicatiegeheim gaat over de vraag of communicatie ook na transport (dus tijdens opslag) zou moeten worden beschermd. Als email bijvoorbeeld wordt verstuurd van A naar B, kan het eerst opgeslagen worden op de server van van de emaildienstverlener van B, totdat het door B eraf wordt gehaald en op zijn computer wordt opgeslagen. Het communicatiegeheim zou zich ook moeten uitstrekken tot opgeslagen gegevens, ook na transport, als die worden opgeslagen op de computer van de

ontvanger of de verzender. Op die manier wordt bijvoorbeeld ook gegarandeerd dat communicatie via social media zoals Facebook wordt beschermd. In dat geval staan deze gegevens immers permanent op de server van Facebook, en krijgen zowel verzender als ontvanger slechts tijdelijk toegang tot de communicatie op die server. Ook zou het analyseren van op een computer opgeslagen communicatie door middel van, bijvoorbeeld, spionagesoftware door het communicatiegeheim beschermd moeten worden.

> **Advies** Het communicatiegeheim zou ook de opslag van communicatiegegevens moeten beschermen.

Het communicatiegeheim moet ook verkeersgegevens beschermen

8. Verkeersgegevens zouden een integraal onderdeel van het communicatiegeheim moeten uitmaken. Verkeersgegevens zijn namelijk gevoelige gevens: het feit dát twee grote bedrijven veel met elkaar bellen om drie uur in de nacht, kan bijvoorbeeld al prijsgeven dat er vertrouwelijke overnamegesprekken zijn. Bovendien kunnen deze gegevens veel over een persoon vertellen: zo kan op basis van het bezoek van bepaalde websites al worden geconcludeerd dat iemand een bepaalde politieke of seksuele voorkeur heeft. Daarbij komt dat opsporingsdiensten privacyregels met betrekking tot privé-communicatie stelselmatig negeren en dat Nederland Europees koploper in de opvraging van telecomgegevens is. Bits of Freedom betreurt dan ook het advies van de Staatscommissie om verkeersgegevens buiten de reikwijdte van het communicatiegeheim te houden.

> **Advies** Het communicatiegeheim zou ook verkeersgegevens moeten beschermen.

Beperkingen slechts na rechterlijke toetsing

9. Bits of Freedom ondersteunt de keuze die is gemaakt in lid 2 sub a van de door Staatscommissie geadviseerde bepaling. In dit lid wordt beschreven dat beperking van het recht op het communicatiegeheim alleen mogelijk is als dit bij wet is voorzien en de rechter hiervoor een machtiging heeft gegeven. Dit betekent dat inbreuken door de overheid op het communicatiegeheim door de rechter worden getoetst.

10. Bits of Freedom heeft tegelijkertijd haar vraagtekens bij lid 2 sub b, waarin is bepaald dat in het belang van de nationale veiligheid een machtiging volstaat: hier is dus geen sprake van een rechterlijke toetsing. Het is de vraag of dit wenselijk is. Zo zijn de afgelopen jaren in de Verenigde Staten de internetverbindingen van honderdduizenden Amerikanen afgetapt zonder toetsing door de rechter in het kader van een vergaand geheim programma om internetverkeer op grote schaal te onderscheppen ten behoeve van de bestrijding van terrorisme (zie **bijlage**). Ook het Europees Hof voor de Rechten van de Mens (EHRM) in de zaak Klass benadrukt het belang van

rechterlijke toetsing bij inbreuken op het communicatiegeheim: “The Court considers that, in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge".[1] Hoewel het EHRM in 1978 nog een slag om de arm hield, lijkt een dergelijke terughoudendheid tegenwoordig veel minder op zijn plaats omdat surveillancetechnologie veel geavanceerder is geworden en de inbreuken op het communicatiegeheim dus veel ingrijpender. Dergelijke vergaande ingrepen op de persoonlijke levenssfeer moeten altijd door de rechter worden getoetst.

Advies Beperkingen op het communicatiegeheim moeten altijd door een rechter worden getoetst.

Nieuw voorstel: het telecommunicatiegeheim onschendbaar, rechterlijke toetsing

11. Uit het advies van de Staatscommissie blijkt dat de voorgestelde formulering die “vertrouwelijke communicatie” beschermt, onvoldoende bescherming biedt. De Staatscommissie maakt duidelijk dat met de door hun gekozen formulering bij de ontvanger afgeleverde, opgeslagen emails niet beschermd worden door het communicatiegeheim. Ook zouden verkeersgegevens niet hieronder vallen.

12. In plaats daarvan zou bepaald moeten worden dat ‘het telecommunicatiegeheim onschendbaar is’, waarbij de flexibele term “telecommunicatiegeheim” als koepelbegrip fungeert voor alle (huidige en toekomstige) vormen van elektronische communicatie.Ter vermijding van misverstanden zou in de toelichting moeten worden duidelijk gemaakt dat verkeersgegevens ook onder dit begrip vallen. Deze formulering wordt ook door Prof. Mr. Egbert Dommering geadviseerd (zie **bijlage**). Daarnaast zou duidelijk moeten worden gemaakt dat beperkingen op het communicatiegeheim altijd door een rechter moeten worden getoetst. Lid 2 sub b zou naar de mening van Bits of Freedom dan ook moeten komen te vervallen.

Nieuw voorstel Het telecommunicatiegeheim is onschendbaar, behalve in de gevallen bij de wet bepaald, op last van de rechter.

13. Bits of Freedom is vanzelfsprekend bereid om de bovenstaande opmerkingen verder toe te lichten wanneer daar behoefte aan bestaat.

Hoogachtend,

Ot van Daalen

1 Zie EHRM 6 september 1978, *Klass v. Germany*, par. 56.

Bijlage

De nieuwe Nederlandse Constitutie en de informatietechnologie

Bespreking van het rapport van de *Commissie Grondrechten in het digitale tijdperk*

Computerrecht 2000-4, p. 177-185

Door prof. mr. E.J. Dommering

Voorgeschiedenis

Eind mei van dit jaar heeft een Commissie met de titel ‘Grondrechten in het digitale tijdperk’ een rapport met een stevige studiebijlage[1] gepresenteerd die voorstellen bevat tot aanpassing van de bestaande grondrechten of invoering van nieuwe grondrechten ‘met het oog op de ontwikkelingen op het terrein van de informatie – en communicatietechnologie’, zoals het instellingsbesluit van 23 februari 1999 het formuleert. De Commissie stond onder voorzitterschap van de Leidse hoogleraar in de Encyclopedie tot de Rechtswetenschap en informaticarecht, Prof. Mr. H. Franken, telde negen leden met een diverse achtergrond lopend van het staatsrecht tot de stimulering van culturele producties en de politie,[2] en werd gesecondeerd door twee ambtelijke secretarissen en vier ambtelijke adjunct-secretarissen tezamen verbonden aan vier verschillende departementen.[3] Zij werd ingesteld nadat er in de Tweede en Eerste Kamer een principieel verschil van mening was ontstaan met de regering over het wetsontwerp tot wijziging van artikel 13 Gw, omdat daarbij door de regering onvoldoende zekerheid kon worden geboden dat e-mail voortaan onder het briefgeheim zou vallen.[4] De Eerste Kamer drong aan op het instellen van een studiecommissie en dat is dan deze Commissie geworden.

Het rapport bedraagt inclusief bijlagen 340 pagina’s, de studiebijlage 255 pagina’s. Het rapport heeft een zilverkeurig kaft met zilverkleurige nullen en enen als achtergrond witte titelletters op het omslag, moeilijk leesbare paginanummers van witte nummers op een zilverkleurig fond op een ongebruikelijke plaats aan de zijkant van de pagina’s, moeilijk leesbare wetteksten van witte letters in een zilverkleurig kader en onleesbare noten van zilveren 6 puntslettertjes op een witte pagina. Voor

deze vermoedelijk door de vereniging van opticiens gesponsorde vormgeving is blijkens het colofon (zilveren 8 puntsletter op wit) een zekere studio Tennekes te Amsterdam verantwoordelijk, zoals ik met behulp van een vergrootglas heb kunnen vaststellen. De blauwe studiebijlage kent deze inconveniënten niet.

Beperkingen opgelegd aan de Commissie

De Commissie kreeg als tijdspad opgelegd 1 mei 2000, hetgeen, zeker voor een zo grote commissie en de moeilijkheidsgraad van het onderwerp veel te kort is. Dat zij er toch in geslaagd is om binnen dit tijdspad een rapport af te leveren dat het gehele probleemveld analyseert verdient veel lof. Datzelfde geldt voor de onder voorzitterschap van Prof. A. Koekkoek[5] tot standgekomen studiebijlage waarin binnen een nog kortere periode een rechtsvergelijkend onderzoek is uitgevoerd naar de constituties, de relevante wetgeving en rechtspraak in Zweden, België, Frankrijk, Duitsland, de Verenigde Staten en Canada. De studiebijlage zal een blijvende waarde behouden als bronnenstudie, juist ook omdat zij verder gaat dan de grondwetsteksten.

Een tweede beperking was gelegen in de door de minister van Binnenlandse Zaken geformuleerde randvoorwaarde ‘zoveel mogelijk rekening te houden met bestaande wetgeving, bij de Staten Generaal ingediende wetsvoorstellen, aangekondigde wetsvoorstellen en naar de Staten Generaal gezonden beleidsnotities die raakvlak hebben met de taakopdracht van de Commissie’. Veelvuldig verwijst de Commissie ter ondersteuning van een argument dat juist kritische beoordeling of weerlegging van node had naar bestaande wetgeving.

Een derde beperking was gelegen in de interdepartementale verankering van de Commissie waarvan de sporen in het rapport waarneembaar zijn. De discussie over het door de regering voorgestelde artikel 13 Gw was met de Staten Generaal vrij hoog opgelopen waarbij de regering vanuit de Kamer wetenschappelijke publicaties kreeg tegengeworpen. Hoewel de Commissie op verschillende plaatsen open in discussie gaat met de wetenschap, treffen wij in het deel van het rapport dat over artikel 13 Gw handelt een toelichting aan die er op lijkt dat het betrokken departement alsnog ‘zijn gelijk wil halen’. Op pagina 160 van het rapport is dan plotseling sprake van ‘enkele scribenten’ die een destijds van de regering afwijkend standpunt vertolkten. Als geheel klinkt in dit deel van het rapport een zacht tandengeknars door. Het door de Commissie voorgestelde artikel 13 wijkt niet substantieel af van het door de Kamers verworpen voorstel, terwijl de analyse in de toelichting de

onbevangenheid mist die nodig is om een eerder voorstel nog eens kritisch te bekijken. Daarbij worden latere publicaties van ‘enkele scribenten’ gemist of onvolledig behandeld, laat staan weerlegd.[6]

Beperkingen die de Commissie zich heeft opgelegd

De Commissie behandelt in paragraaf 3.2 een aantal kenmerken van de grondwet die zij sober, open, codificerend, moeilijk veranderbaar en niet door de rechter te toetsen noemt. Alleen op het punt van de rechterlijke toetsing die de Nederlandse Grondwet in artikel 120 verbiedt kiest de Commissie in de grootst mogelijke meerderheid partij voor de opheffing van dit verbod. Het is immers door dit toetsingsverbod dat de Grondwet zich in het Nederlandse staatsbestel onvoldoende heeft ontwikkeld tot een open systeem van fundamentele normen, zoals bijvoorbeeld de Amerikaanse Constitutie die door de Amerikaanse hoogste rechter steeds aan de eisen van de tijd is uitgelegd en zoals bijvoorbeeld het EVRM dat door het EHRM telkens in het licht van de nieuwe maatschappelijke en technische ontwikkelingen wordt toegepast. Het is zelfs de vraag of wij een discussie over de noodzaak van ‘technologie neutrale’ grondrechten zouden hebben gehad als zich een constitutionele rechtspraak zou hebben kunnen vormen. Nu is die functie in de rechtspraktijk overgenomen door het EVRM, omdat in het Nederlandse monistische stelsel de Nederlandse rechter verplicht is directwerkend verdragsrecht toe te passen. Daardoor is de ‘verspreidingsjurisprudentie’ die de Nederlandse rechter onder artikel 7 Gw heeft gevormd (waarover hierna) goeddeels door artikel 10 EVRM ingehaald.

Juist nu de Commissie voor rechterlijke toetsing kiest is het merkwaardig dat zij zich overigens terughoudend opstelt en zich verschuilt achter de ‘soberheid’ en relatieve ‘onveranderbaarheid’ van de Grondwet. Zo wijst de Commissie de opneming in de Gw af van het criterium uit het EVRM dat beperkingen van grondrechten slechts zijn toegestaan voor zover die beperkingen ‘noodzakelijk zijn in een democratische samenleving’, omdat daarvan een verkeerde ‘uitstraling’ op de andere niet gewijzigde grondrechten zou uitgaan (p. 55-56). De opvatting van de Commissie dat dat onduidelijkheid zou geven naar andere niet gewijzigde grondrechten en naar de relatie tot de Europese norm is niet erg overtuigend, omdat het eerste is te ondervangen door een algemeen artikel met betrekking tot beperkingen op te nemen en de tweede opvatting miskent dat de verdragsstaten de vrijheid hebben (in wisselende graden van beleidsvrijheid al naar gelang de ‘margin of appreciation’ die het Hof hanteert) zelf de inhoud van deze norm te bepalen. Dat het een

nietszeggende norm zou zijn, zoals de voorzitter van de Commissie in de Staatscourant meedeelt,[7] mag de heersende opvatting in ambtelijk Den Haag zijn, maar is geen juiste weergave van de jurisprudentie van het Hof. De studiecommissie van de Vereniging voor Media en Communicarierecht stelt in haar advies van eind vorig jaar het opnemen van een materiële norm voor (kader 3).

De Commissie heeft zich nog een andere beperking opgelegd door af te zien van het opnemen van beperkingsdoeleinden, zoals die wel, en op goede gronden in het EVRM zijn opgenomen.[8] Tijdens de door de Commissie georganiseerde workshop was de meerderheid van de daar aanwezige deskundigen van oordeel dat overneming van de doelcriteria van het EVRM verreweg de beste oplossing was (rapport, p.102). Ook het in kader 4 opgenomen voorstel beval dit aan.[9] Onder verwijzing naar een niet gepubliceerde internetdiscussie met niet nader genoemde deskundigen worden deze ‘rubber paragraphs’ afgewezen. Vreemd genoeg maakt de Commissie dan de keuze dat de wetgever niet aan het noodzakelijkheidscriterium, maar –waar het de verspreiding betreft- aan enige geselecteerde doelcriteria, te weten: de openbare orde, de volksgezondheid en de veiligheid.

De Gw artikelen: algemene afbakeningsvraagstukken

Inleiding
De Commissie heeft een aantal grondrechten onderzocht, waarbij de artikelen 7 Gw (vrijheid van meningsuiting), 10 (privacy) en 13 Gw (het brief en telefoongeheim) het pièce de résistance vormen. Daarnaast heeft zij aanbevelingen gedaan over een nieuw openbaarheidsartikel en ook enige andere grondrechtartikelen op tijdsbestendigheid getoetst. Ik zal niet alle beschouwingen van de Commissie bespreken, maar mij concentreren op de artikelen 7 en 13 (mede in relatie tot 10). Wat de Commissie schrijft over openbaarheid kan slechts met instemming worden begroet, maar leidt niet tot een substantiële verandering van de Gw.

Openbare en niet openbare communicatie door middel van communicatiemiddelen
De Commissie staat in paragraaf 3.5.2 uitvoerig stil bij de convergentie van de (tele)communicatiemiddelen, kortgezegd hier op neerkomende, dat de telecommunicatiemiddelen steeds meer een multifunctioneel gebruik kennen waardoor openbare en privé vormen van communicatie, beeld, geluid en data door elkaar lopen. Het EHRM heeft in de (niet door de Commissie besproken) Autronic en Groppera-arresten de toegang tot de elektronische communicatiemiddelen expliciet onder de bescherming van artikel 10 lid 1 EVRM

gebracht en de ongeclausuleerde verwijzing naar een vergunningstelsel in het eerste lid aan een nauwkeurige noodzakelijkheidstest onderworpen.[10] In het wel door de Commissie besproken Antelecomarrest van de Hoge Raad[11] heeft de Raad de toegang tot de telecommunicatie-infrastructuur voor telefoondiensten aan artikel 10 EVRM getoetst met het argument dat de verschillende soorten communicatie niet meer zijn te onderscheiden. Men zou dus verwachten dat de Commissie de convergentie (toch wel bij uitstek het vraagstuk van het 'digitale tijdperk') aangrijpt door een aantal algemene toegangsnormen te ontwikkelen. Er is wel gesuggereerd dat de toegang tot de communicatiemiddelen begrepen zou kunnen worden in het 'verspreidingsrecht'[12] , maar ik ben met de studiecommissie van de VMC van oordeel dat het verspreidingsrecht dat aan het begin van de 20e eeuw door de HR is ontwikkeld tot het papieren tijdperk behoort: het gaat primair over uitdelen van pamfletten en opplakken van teksten.[13] Ik heb zelf een voorstel geformuleerd (zie kader 4) dat ook door de Commissie wordt besproken. Het gaat mij dan niet zozeer om het feit dat de Commissie dat voorstel niet heeft overgenomen (het was niet als een voorstel van wetgeving als een model voor de discussie bedoeld), als wel om de mistige (to put it mildly) argumentatie die de Commissie hanteert. Ik citeer enkele vlagen uit deze mistbank in het rapport (p. 66 en 67):

> 'Het moge juist zijn dat het verdeelvraagstuk dat uit de technische schaarste van communicatiemiddelen voortvloeit zich zowel voordoet bij openbare als niet-openbare communicatie, maar dat ziet er aan voorbij dat het verdeelvraagstuk in grondwettelijk perspectief alleen relevant is in relatie tot de vrijheid van meningsuiting (...). Technische schaarste bij besloten communicatie is in grondwettelijk opzicht niet relevant. Frequentieschaarste bij bijvoorbeeld telecommunicatie geeft weliswaar een verdeelvraagstuk, maar bij dat vraagstuk speelt het telefoongeheim geen rol.'

Dat was evenwel niet de vraag. Communicatiemiddelen kunnen voor alle mogelijke vormen worden gebruikt 'in deze turbulente tijden' (rapport, p. 153). Toegang tot die middelen is een essentiële voorwaarde voor de openbare communicatie en de communicatie tussen de burgers onderling en daarom achtte de HR artikel 10 EVRM op die toegangsvraag van toepassing. Die toegang kan maar in een beperkt aantal gevallen worden beperkt, namelijk wanneer er technische schaarste te verdelen valt zoals bij frequenties of wanneer economisch dominante machtsposities moeten worden gereguleerd en mijns inziens moet een constitutie in de 21e eeuw daarover een

uitspraak doen (zie het derde lid van de tekst in kader 4). De relatie tussen de economische orde en de orde van de grondrechten wordt steeds pregnanter, zoals Mortelmans onlangs aan de orde stelde.[14]

De Commissie had in dit opzicht lering kunnen trekken uit de door de studiegroep aangereikte buitenlandse wetteksten. De Franse wet 'relative à la liberté de la communication' bepaalt in artikel 1: 'L'établissement et l'emploi des installations de télécommunications sont libres'[15] De voorzitter van de Commissie verklaarde in de Staatscourant dat de commissie de grondwetsartikelen wilde laten aanvangen met een 'klaroenstoot'.[16] Mij dunkt dat die Franse tekst zo'n stoot is. In plaats daarvan: een nevelige stilte. Hierna zal ik laten zien dat het ook tot merkwaardige inconsistenties in het voorgestelde artikel 7 leidt.

Een voorbeeld dat illustreert dat dit tot wonderlijke resultaten leidt vormt de opmerking van de Commissie dat het actief storen van vertrouwelijke communicatie een inbreuk op dat recht vormt. Zij meent terecht dat de bevoegdheid die de minister van Verkeer & Waterstaat in artikel 3.10 Telecommunicatiewet krijgt om delen van een GSM net plat te leggen exorbitant is en aan rechterlijke controle moet worden onderworpen, omdat het om een inbreuk op de vertrouwelijke communicatie gaat (rapport, p. 168). Waarom zou dat niet ook gelden voor netten waarmee (semi) openbare communicatie wordt bedreven? Bij een meer integrale aanpak had die vraag toch ook bij openbare media gesteld moeten worden?

Privacy en andere privacyrechten (communicatiegeheim, persoonsgegevens, lichaam, huis)
In onze grondwet worden de verschillende aspecten van privacy onderscheiden: de persoonlijke levenssfeer (artikel 10 Gw), de integriteit van het lichaam (artikel 11 Gw), het huisrecht (artikel 12 Gw), het communicatiegeheim (artikel 13 Gw). De Commissie ziet alleen aanleiding voor artikel 13 Gw een wijzigingsvoorstel te doen. Dit voorstel heeft tot gevolg dat de communicatie die in de persoonlijke levenssfeer plaatsvindt uit het recht op de persoonlijke levenssfeer wordt gelicht en tezamen met het telefoongeheim als een afzonderlijk grondrecht wordt behandeld. Deze ongebruikelijke manoeuvre die geen recht doet aan het historisch gegroeide en de vergelijkbare beschermingen in de bestudeerde buitenlandse constituties, waar de Commissie overigens zo gevoelig voor is, leidt tot allerlei complicaties bij de afbakening van artikel 10 en artikel 13. Want wanneer is iets een vertrouwelijke communicatie? Waarom zou bij computerbestandonderzoek op afstand, het volgen van het inloggedrag op internet, het filmen van gedrag in de privé-sfeer, om maar een paar voorbeelden te noemen, een ander beperkingsregime moeten gelden dat bij het afluisteren

van gesprekken in de woning? Ik mis in het rapport een visie op de onderlinge samenhang tussen deze artikelen in het licht van 'deze turbulente tijden'. De woning is een glazen huis geworden waar zich allerlei op afstand toegankelijke elektronische informatiebestanden bevinden en waarvan de muren door nieuwe informatietechnieken transparant zijn geworden. Het communicatiegeheim dat ziet op getransporteerde gegevens gaat moeiteloos over in het opslaan van gegevens (de e-mailbox, de voice mail) in de privé-sfeer of in de sfeer van derden. De integriteit van het lichaam heeft in toenemende mate betrekking op persoonsgegevens (DNA, biometrie). Naar mijn mening vergt dat een integrale aanpak van de grondrechten die de privé-sfeer beschermen. Ook op dit punt geen klaroenstoten.

Horizontale werking
Bij alle artikelen wordt ingegaan op de werking van de grondrechten tussen burgers, in deze geprivatiseerde samenleving een steeds belangrijker onderwerp. De Commissie behandelt dit onderwerp bij de analyse terecht, maar doet er verder weinig mee. Zo missen wij een gedegen verantwoording hoe de inhoud van de grondrechten in geprivatiseerde verhoudingen kan worden gewaarborgd. Ik geef een paar voorbeelden. Iedereen roept dat het Internet geschikt is voor zelfregulering. Dat heeft voor – en nadelen. Inmiddels is er een Internet Content Rating Society (ICRA) opgericht die met behulp van steeds verfijndere filtertechnieken ratings voor zwarte lijsten voor inhoud opzet (niet sex naakt, wel medisch naakt, maar ook met betrekking tot onderwerpen die met de goede zeden niets te maken hebben). De ICRA wordt ondersteund door de Europese Commissie. Deze filtertechnieken gekoppeld aan geselecteerde zwarte lijst onderwerpen kunnen worden toegepast bij browsers of door servers van dienstenaanbieders (bilbliotheken, internetcafés), die alleen nog maar 'rated pages' doorgeven zonder dat de gebruiker er enige weet van heeft. In het Verenigd Koninkrijk is een Internet Watch Foundation (IWF) werkzaam die met succes haar invloed aanwendt om webpagina's van servers te doen verwijderen zonder dat de gebruiker daar iets tegen kan doen. De IWF heeft ook voor de Europese Commissie een rapport opgesteld.[17] Het gaat dus om door de overheid toegelaten en zelfs gestimuleerde geprivatiseerde censuur. Voor het briefgeheim geldt hetzelfde. E –mail verkeer binnen organisaties wordt op grote schaal gemonitord. De telecommunicatiebranche is op grote schaal geprivatiseerd. Hoe brief – en telefoongeheim van de gebruikers binnen deze verhoudingen nog zijn gewaarborgd is vrijwel geheel overgelaten aan de contractsvrijheid.

Het is een van de alarmerende ontwikkelingen van de elektronische informatiemaatschappij waar een Commissie

Digitale Grondrechten een constitutioneel antwoord op had moeten formuleren. De Commissie neemt daarover wel een standpunt in bij artikel 13, maar bij artikel 7 Gw op een onduidelijke manier. Blijkens pagina 105 van het rapport is zij zich wel bewust geweest van de nieuwe manipulatiemogelijkheden door het inbouwen van filters, maar dit inzicht wordt niet aangewend voor een grondwettelijke opdracht aan de wetgever censuur in private verhoudingen tegen te gaan. Het voorgestelde vierde lid van artikel 7 gaat eigenlijk alleen over meer overheidscontrole.

De afzonderlijke artikelen en de voorstellen van de Commissie (voor de oude en nieuwe tekst zie kaders 1 en 2)

Artikel 7
De Commissie adviseert terecht af te stappen van de eigenaardige media gebonden structuur van artikel 7 en het artikel te laten openen met een positieve niet technische formulering van het grondrecht. Ook wordt de uitsluiting van de grondwettelijke bescherming van de reclame terecht opgeheven. Bij nadere beluistering van deze klaroenstoot missen wij toch die noten, die de melodie van het VMC- voorstel zo veel welluidender maken (kader 3). Zo ontbreekt de (nieuws)garingsvrijheid omdat het veld te onoverzichtelijk zou zijn voor een regeling op grondwettelijk niveau (p. 98 van het rapport). Hoeveel fraaier is artikel 5 van de Duitse grondwet die zich bij het studiemateriaal van de Commissie bevond: ‘Jeder hat das recht sein Meinung in Wort, Schrift und Bild zu äusseren und zu verbreiten und sich aus algemein zugänglichen Quellen zu unterrichten.’

Artikel 7 eerste lid bezigt de termen ‘openbaren’ en ‘verspreiden’ waarmee beoogd wil zijn de verspreidingsjurisprudentie van de HR te sauveren. Deze jurisprudentie, hiervoor reeds kort aangeduid, is een onderscheid gaan maken tussen het ‘openbaren’ van een mening en het daarvan afgeleide (in het jargon: connexe) recht van ‘verspreiden’. Het eerste kon alleen door de formele wetgever worden beperkt (drukpersdelicten), het tweede ook door lagere regelgevers (plakverboden). Daarmee konden de gemeenten bij verordening optreden tegen plakken en pamfletten uitdelen, zolang een zelfstandig verspreidingsmiddel maar niet geheel gefrustreerd werd. Er moest binnen de gemeente dus altijd een muurtje om te plakken overblijven. Deze jurisprudentie was gebaseerd op artikel 7 Gw lid 1 en dus typisch drukpersjurisprudentie. Het leerstuk van het verspreidingsmiddel met zelfstandige betekenis werd bovendien ingehaald door de algemene noodzakelijkheidstoets van artikel 10 lid 2.[18] Bij

verspreiding van elektronische signalen speelde het geen rol. De gemeentelijke antenneverboden werden getoetst aan artikel 10 lid 2 EVRM. De Commissie licht nu beide begrippen uit de drukperscontekst) en gebruikt ze als algemeen aanknopingspunt voor de systematiek van de beperkingen in de voorgestelde leden twee en drie. Maar die begrippen passen niet in een elektronische omgeving, net zo min als openbaarmaken en verveelvoudigen uit het auteursrecht.[19] De Commissie heeft met dit probleem geworsteld, daartoe haar toevlucht nemend tot een teder gekoesterd voorbeeld uit het staatsrecht: de geluidswagen. De geluidswagen komt als middel van verspreiding van gedachten bij mijn weten alleen nog in derde wereld landen voor. In onze digitale delta hoor ik het gegalm tegen de gevels sporadisch, eenmaal in de maand als de chemocar rondtoetert dat iedereen zijn chemisch afval op de hoek van de straat moet komen inleveren. Welnu, de geluidswagen is een samenval van openbaarmaking (het getoeter door de microfoon) en verspreiding (hij rijdt). Maar het gaat niet alleen om staatsrechtelijke folklore want de Commissie zet het internet op een lijn met de geluidswagen. Het loont de moeite de Commissie hier zelf aan het woord te laten naar aanleiding van de kritiek van de VMC-Commissie dat het onderscheid gekunsteld is (rapport, p. 96):

> 'De Commissie realiseert zich dat het onderscheid tussen openbaarmaken en verspreiden niet altijd even scherp is en dat er vaak geen sprake is van twee activiteiten, maar van een samenval van twee momenten. Zo kan van een dergelijke samenval sprake zijn bij een medium als internet. In de 'off line' world kan gedacht worden aan een rijdende geluidswagen door de stad.'

Het draait nu om het tweede lid. Daar staat dat de openbaarmaking alleen kan worden beperkt 'bij wet' en geen voorafgaand verlof mag inhouden. 'Verspreiden' en 'ontvangen' daarentegen mogen krachtens de wet (dus bijvoorbeeld bij verordening mits de gedelegeerde wetgevende bevoegdheid steunt op een formele wet) worden beperkt in het belang van de openbare orde mits die beperking maar niet betrekking heeft op de inhoud van de denkbeelden. En er mag wel de eis van een voorafgaand verlof voor verspreiden en ontvangen worden opgenomen. Bij openbare orde denkt de Commissie (rapport, p. 110) aan het oude 'openbare orde' begrip van de verspreidingsjurisprudentie: 'de beveiliging van het verkeer, het voorkomen van wanordelijkheden, het handhaven van de nachtelijke rust in de nachtelijke uren en de bescherming van het stadsaanzicht en het landschapsschoon.' Met die passage over de geluidswagen nog in het geheugen vragen wij ons af wat dit voor het internet betekent. Het rapport zegt er op pagina 110 dit

over:

> 'Zoals hiervoor reeds ter sprake kwam, kan bij een samenval van het openbaren en verspreiden van informatie onder meer worden gedacht aan het rijden van een geluidswagen of het plaatsen van een home page op het internet. Op grond van bovenstaand voorstel bestaat zowel voor de formele wetgever als de lagere wetgever geen bevoegdheid de meningsuiting via internet aan een voorafgaand verlof te verbinden. Het belang van de openbare orde heeft immers betrekking op de fysieke ruimte, terwijl bovendien voorafgaand verlof niet op de inhoud van de uiting betrekking kan hebben'.

Wat betekent dit nu precies? Ik heb geprobeerd de consequenties te doordenken:

- Wat zegt artikel 7 in lid 2 nu precies over oprichting van elektronische communicatiemiddelen? Voor de drukpers gold in het oude artikel 7 Gw dat het verbod van voorafgaande verlof bij openbaren inhield dat er geen vergunningen mochten worden verlangd voor het oprichten van ondernemingen met betrekking tot 'drukpersproducten' (drukkerijen, uitgeverijen, leesbibliotheken). Door de samenval van openbaarmaken en verspreiden bij elektronische middelen is het verspreidingsregime mede van toepassing en kan er een voorafgaand verlof worden geëist. De inhoudelijke beperkingsgrond heeft echter betrekking op de fysieke openbare orde, waardoor de vraag rijst of door de voorgestelde regels de gehele telecommunicatiewetgeving niet in de lucht is komen te hangen. En wat is de consequentie als het openbare orde begrip toch wordt opgerekt?
- Wat betekent het artikel 7 lid 2 voor de drukpers? Is een journalist een openbaarder of een verspreider? Ik weet het niet: het onderscheid tussen openbaren en verspreiden was immers gekunsteld. Dus wel een mogelijkheid het beroep van journalist aan een vergunning te binden? Naar mijn mening is dit inderdaad de gedachtengang van de Commissie (rapport, p. 92-93). Daarmee worden de verworvenheden van drukpersjurisprudentie die een vergunningstelsel voor het drukpersbedrijf en beroep ongedaan gemaakt: voortaan geldt dat alle verspreidingsmiddelen (bedrijven, beroepen) aan een vergunning kunnen worden onderworpen.
- Is er een scherpe scheiding tussen fysieke openbare orde en elektronische communicatie mogelijk? De voetbaloorlogen tussen relschoppers worden gevoed met GSM spraak- en databerichten tussen de

> deelnemers en de 'leiders'. Het SMS berichten verkeer via mobiele toestellen neemt een enorme vlucht. Straks komt daar het 'wappen' (mobiel internetten) bij. Al dit verkeer heeft een (semi) openbaar karakter waarbij informatie vanuit centrale openbare punten ('hooligan' webpagina's) wordt opgehaald of aldaar wordt achtergelaten en via grote groepen wordt verspreid. Het gebruik kan enorme consequenties hebben voor de fysieke openbare orde, dus waarom zouden plaatselijke overheden niet vergunningstelsels voor het gebruik kunnen invoeren om het gebruik op bepaalde tijden en plaatsen te beperken? Uit pagina 93 van het rapport leid ik af dat de Commissie hier zonder veel omhaal kiest voor meer overheidsmacht.

Er is nog wel meer over deze bepalingen te zeggen, maar thans wordt het tijd de aandacht op het vierde lid te richten. Daar staat dat bij de wet regels kunnen worden gesteld over 'publieke mediadiensten' en dat daarbij algemene regels kunnen worden gesteld aan de algemene aard van de informatie die door deze diensten aan het publiek worden verspreid. In de toelichting (p. 113) lezen wij dat met 'publieke mediadiensten' wordt gedoeld op voor het publiek toegankelijke diensten, dus op alle openbare media. Laten wij de Commissie andermaal aan het woord:

> 'Bij regels omtrent pluriformiteit kan bijvoorbeeld worden gedacht aan invoering van een vergunningstelsel voor een bepaald soort mediadienst, waarbij vooraf in algemene zin wordt getoetst op eisen met betrekking tot de pluriformiteit van informatie die door middel van de publieke mediadiensten naar buiten wordt gebracht. In de huidige Mediawet is momenteel reeds voor publieke omroepinstellingen een zodanig stelsel neergelegd. Ook het stellen bij algemene maatregel van bestuur van voorschriften over de pluriformiteit van de informatie die via publieke mediadiensten naar buiten wordt gebracht, behoort tot de mogelijkheden.'

De lezer denkt eerst: Er staat niet wat er staat. Maar het staat er wel. De centrale overheid assumeert hier de bevoegdheid om voor *alle* media, of die nu subsidie ontvangen of niet, regels met betrekking tot de algemene inhoud te stellen, inclusief vergunningstelsels. Er hebben stormen gewoed in de perswereld over de ongrondwettigheid van publiekrechtelijke regelingen en persfusiecontrole regelingen[20] . De regels met betrekking tot de omroep worden steeds meer beperkt tot de publieke omroep (dus alleen de door de overheid gesubsidieerde omroep). Hoe kan het dat deze Commissie

met dit voorstel komt? De Commissie heeft klaarblijkelijk niet ingezien dat de vergunningsregel voor de omroep de uitzondering op de hoofdregel is dat voorafgaand verlof niet is toegestaan. Die uitzondering is men meer en meer gaan zien als een vergunning die betrekking heeft op de schaarste aan technische middelen en waarvan de uitoefening door de overheid aan strenge mededingingsnormen moet worden getoetst.

Artikel 10 en 13
Het privacy artikel uit de Gw ondergaat geen ingrijpende wijziging. Het gaat mij hier vooral om de verhouding tussen artikel 10 en 13. Ik zal daarom met artikel 13 beginnen en vanuit dat perspectief aangeven wat de verandering inhoudt.[21]

De Commissie heeft klaarblijkelijk gedacht dat artikel 13, net als artikel 7, moest beginnen met een niet technische formulering van de inhoud van het recht en dat is geworden: 'Iedereen heeft het recht om vertrouwelijk te communiceren'. Zoals ik hierna, kort zal uiteenzetten gaat mijn voorkeur uit naar een andere klaroenstoot, bijvoorbeeld artikel 10 van de Duitse grondwet: 'Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich'. Van mij zou het mogen zijn: Het briefgeheim en het telecommunicatiegeheim zijn onschendbaar. Dat pakt de papieren en alle vormen van elektronische overdracht en reserveert de eigen aard van het oude briefgeheim. Mijn bezwaren tegen de voorstellen van de Commissie laten zich als volgt samenvatten:

- Het telecommunicatiegeheim wordt ten onrechte op een lijn gesteld met het 'live gesprek', waarmee gedoeld wordt op het gesprek dat zonder technische hulpmiddelen wordt gevoerd (de Commissie – rapport p. 153- spreekt ook wel van 'directe' en 'indirecte' communicatie; ik vind de termen verwarrend, maar laat dat voor wat het is). Het post – en telecommunicatiegeheim gaan over geadresseerde gegevens die de zorg van derden worden toevertrouwd om deze op een aangegeven adres te bezorgen. Het geheim beoogt te verzekeren dat de geheimhouding van het begin tot het einde van de transportdienst is gegarandeerd en heeft op zichzelf niets met de aard van de geadresseerde communicatie te maken: het is het *geobjectiveerd geheim* van de transporteur, hetgeen iets anders is dan de *geobjectiveerde wil tot geheimhouding* van de verzender, zoals de Commissie schijnt te denken. Daarom dat dit geheim als zodanig beschermd moet worden in de nationale constituties. De tekst van artikel 5 van de ISDN richtlijn is een treffende illustratie van dit principe: 'De lidstaten garanderen het vertrouwelijke karakter van oproepen via het openbare telecommunicatie netwerk en openbare

telecommunicatiediensten'. Het gaat dus om het vertrouwelijke karakter van het *netwerk* en *de dienst*. De netwerk en dienstenaanbieder moeten de maatregelen nemen om de privacy veilig te stellen. Bij het 'live gesprek' zijn dat de gespreksdeelnemers zelf. Je kunt zelfs volhouden dat de voorgestelde bepaling een ontoereikende implementatie van artikel 5 van de ISDN richtlijn is.

- Het op een lijn stellen van het telecommunicatiegeheim met het gesprek in de privé-sfeer leidt tot allerlei afbakeningsvraagstukken. Ik verwijs naar hetgeen ik hiervoor opmerkte.
- Het criterium dat de Commissie voor 'vertrouwelijke communicatie' bezigt leidt tot rechtsonzekerheid, omdat de Commissie daarvoor uitgaat van een aan feiten en omstandigheden gekoppeld verwachtingspatroon van de deelnemers aan de communicatie, de zogenaamde 'reasonable expectation of privacy' (rapport, p. 163). Daarbij noemt de Commissie drie verschillende criteria, te weten de aard van het kanaal (beloten), adressering, de aard van de communicatie (gesloten envelop, encryptie, opschiften als 'vertrouwelijk'). De Commissie vermeldt niet welke omstandigheden voor het 'live gesprek' bepalend zijn voor de vertrouwelijkheid. In verband met dit verwachtingspatroon komt ook weer de geijkte briefkaart te voorschijn die niet onder het briefgeheim zou vallen. Dat is onjuist, omdat voor het lezen van de briefkaart door postsorteerder of besteller al een hindernis moet worden genomen die buiten de normale verrichting van de vertrouwelijke dienst valt: hij of zij behoeft immers alleen het adres te lezen.[22] Ik zie ook niet in waarom de briefkaarten zonder rechterlijke last naar het Openbaar Ministerie zouden mogen worden doorgezonden.
- Een controverse die is gebleven zijn de zogenaamde 'verkeersgegevens', dat zijn de gegevens die tijdens het transport worden gegenereerd of locatiegegevens (waar bevindt zich het GSM toestel). De Commissie plaatst deze, anders dan het EHRM buiten de bescherming van het communicatiegeheim (rapport, p. 159). De Commissie stelt dat deze gegevens beschermd worden door artikel 10 Gw. Daarover twee opmerkingen. Het is maar zeer de vraag of verkeersgegevens altijd kunnen worden aangemerkt als persoonsgegevens in de zin van artikel Gw.[23] Het zijn immers vaak alleen gegevens over data en tijdstippen van gegevensuitwisseling tussen twee randapparaten of locatiegegevens van een mobiel randapparaat. De tweede opmerking betreft het feit dat het beschermingsniveau van het

> communicatiegeheim en de op artikel 10 gebaseerde regelingen niet hetzelfde is. Dit is een plaats in het rapport waar niet verder wordt gediscussieerd, maar verwezen wordt naar de soepele praktijk die zich heeft gevormd onder bestaande wetgeving (waar de Commissie blijkens haar opdracht immers aan gebonden was) waarbij de opsporingsautoriteiten gemakkelijk aan deze gegevens kunnen komen.

Een verbetering is het feit dat de Commissie voorstelt om, in navolging van de Duitse grondwet, de notificatieplicht in het tweede lid op te nemen. Voorts wordt de eis van de rechterlijke last nu in het algemeen gesteld. De notificatieplicht houdt in dat iemand die wordt afgeluisterd daar zo spoedig mogelijk van in kennis moet worden gesteld. Toch neemt het voorgestelde derde lid een uitzonderingsbevoegdheid op ten behoeve van de nationale veiligheid (lees: de Binnenlandse Veiligheid Dienst), waarmee zij verder gaat dan de Duitse grondwet die de uitoefening van de uitzonderingsbevoegdheid onder politieke controle plaatst en ook verder gaat dan het EHRM die ten minste deze controle verlangt.[24] De Commissie neemt hier het door de regering tijdens de behandeling van de grondwetswijziging verdedigde, in de literatuur bestreden standpunt, zonder enige motivering over (rapport, p. 157). Er staat gewoon: ‘Deze uitzondering is conform de eerder genoemde jurisprudentie van het EHRM.’

De notificatieplicht wordt in de opzet van de Commissie ook uitgebreid tot het afluisteren in de privé-sfeer. Dat is zeker een verbetering. Zoals ik hiervoor heb uiteengezet is deze verhoogde rechtsbescherming mijns inziens uit te breiden tot alle ingrijpende inbreuken in de privé-sfeer waarbij het individu in verband met een opsporingsonderzoek of een onderzoek verbandhoudende met de nationale veiligheid in zijn of haar doen en laten wordt bespied. De Zweedse grondwet neemt dat als afzonderlijke categorie onder het privacyrecht op. Naar mijn mening zou artikel 10 op dit punt moeten worden aangepast.

Conclusie

Ik heb het rapport niet in extenso beproken en daarom onvoldoende recht kunnen doen aan de interessante beschouwingen over privacy en openbaarheid die het ook bevat. Ik heb mij moeten concentreren op de belangrijke artikelen 7 en 13 (in relatie tot 10). Ook op dit punt is het rapport, tezamen met de studiebijlage, het lezen zeer waard hoewel ik de keuzen die de Commissie heeft gemaakt en de conclusies waartoe zij is gekomen met kracht bestrijd. Het rapport laat zien hoe ingewikkeld het

probleem is en hoe moeilijk het is om technologie-onafhankelijke normen te ontwikkelen. Het rapport bevat ook veel waaruit blijkt dat de Commissie zich duidelijk bewust is geweest van de gevaren en mogelijkheden van de nieuwe informatietechnologie. Niettemin is de relatie tussen beschouwingen over dit onderwerp en voorgestelde wetteksten niet altijd duidelijk aanwezig en soms tegengesteld, in die zin dat de tekst niet aansluit op de beschouwingen.

Een belangrijke verbetering is dat de inhoud van de verschillende grondrechten nu in de grondwet is opgenomen. Onjuist acht ik dat het telefoongeheim en de communicatie in de privé-sfeer ('het gesprek') grondrechtelijk op een lijn worden gesteld. Het gaat om grondrechten die verschillende aspecten van de privacy beschermen: in het eerste geval de vertrouwelijkheid van de telecommunicatiedienst, in het tweede geval de vertrouwelijkheid van de privé-communicatie. Onjuist vind ik ook dat de Commissie de oprichting en exploitatie van de (multifunctionele) communicatiemiddelen niet in een afzonderlijke regel heeft willen vastleggen, temeer daar dit door de regeling van de verspreidings- en ontvangstvrijheid in artikel 7 lid 2 tot ingewikkelde interpretatievragen leidt. Onjuist vind ik in dit verband ook dat de Commissie een fundamentele discussie over de verhouding tussen de orde van de informatiegrondrechten en de economische orde uit de weg is gegaan. Zeer verwarrend vind ik de overplanting van de openbaarmaking en verspreidingscriteria uit de drukpersjurisprudentie naar een algemeen kader. Als denkexercitie vind ik het interessant omdat het aantoont dat 'technologieneutraal' ook niet alles is, maar de resultaten leiden tot grote rechtsonzekerheid. Het voorgestelde vierde lid van artikel 7 vind ik absoluut onaanvaardbaar, niet zozeer omdat de 'status aparte' van de omroep wordt opgeheven als wel omdat daarmee de weg wordt bereid naar de oprichting van een alles omvattend omroepbestel voor alle media. Dit voorstel wordt overigens in de toelichting geplaveid met goede bedoelingen, maar het leidt niettemin in de voorgestelde tekst tot een draconisch eindresultaat.

De controverse over het object van het telecommunicatiegeheim (vallen ook de verkeersgegevens er onder?) en de beperking ten behoeve van de nationale veiligheidsdiensten is gebleven. De Commissie brengt de discussie hierover ook niet veel verder. De Commissie mist een kans om een integrale beschermingslaag om de privé-sfeer heen te leggen om deze tegen alle mogelijke vormen van (elektronische of optische) inbreuk te beschermen. In het rapport mis ik ook een integrale aanpak van de problematiek van de horizontalizering van de gezagsverhoudingen: wel bij artikel 13 maar niet bij artikel 7.

Het rapport is een interessante en geconcentreerde bijdrage aan het debat, maar het verschaft de regering niet het instrumentarium een probleemloos voorstel aan de Tweede Kamer te doen. Als de regering deze voorstellen ongewijzigd overneemt heeft zij er ten opzichte van het vorige ontwerp alleen maar een aantal problemen bij gekregen. Dat de Commissie, na de parlementaire discussie die tot haar instelling heeft geleid, het risico heeft genomen om een voorzienbaar controversieel voorstel te doen begrijp ik overigens niet.

---

[1] Commissie Grondrechten in het digitale tijdperk, p/a postbus 20011, 2500 EA Den Haag, http://www.minbzk.nl/gdt, rapport en studiebijlage. *(terug naar tekst)*

[2] In de Commissie hadden, buiten de voorzitter, zitting: Prof. Dr. J. Arnbak, voorzitter van de OPTA en hoogleraar tele-infomatietechniek aan de TU Delft, prof.mr. M.A.P. Bovens, hoogleraar rechtsfilosofie en bestuurskunde aan de UvU, Mr. J.P.H. Donner, lid van de Raad van State, Mr. A.M. Gerritsma, directeur Stimuleringsfonds voor Nederlandse Culturele Omroepproducties, Prof. Mr. H.R.B.M. Kummeling, hoogleraar staatsrecht aan de UvU, prof. Mr. J.E.J. Prins, hoogleraar recht en informatisering aan de KUB, prof. Mr. H.J.de Ru, hoogleraar staatsrecht aan de VU, Prof. Mr. Dr. I.Th.M. Snellen, emeritus hoogleraar bestuurskunde aan de Erasmus Universiteit, Mr. P. Vogelzang, korpschef politieregio Utrecht. *(terug naar tekst)*

[3] Ministerie van Binnenllandse Zaken, Ministerie van Justitie, Ministerie van Verkeer en Waterstaat en Ministerie van Onderwijs, Cultuur en Wetenschap. *(terug naar tekst)*

[4] Ik verwijs naar E.J. Dommering, 'Geen telefoongeheim op elektronische snelweg', *Mediaforum* 1997-10, p. 142-147 en L.F. Asscher, *Constitutionele Convergentie van pers, omroep en telecommunicatie*, Deventer: Kluwer 2000 (Iterreeks nr. 26), p. 69 e.v. *(terug naar tekst)*

[5] De ondezoeksgroep, verbonden aan de KUB bestond uit mr. P. Zoonjens, Mr. F. Vlemminx, Mr. G.J. Leenknegt, Mr. Sj. Nouwt, Dr. B.J. Koops, H. van Schooten-van der Meer, Mr. R. Bos. *(terug naar tekst)*

[6] E.J. Dommering e.a., *Handboek Telecommunicatierecht*, Den Haag: SDU 1999, p. 602-605, L.F. Asscher a.w. noot 4, p. 58-63. *(terug naar tekst)*

[7] *Staatscourant* 24 mei 2000, nr 100, p. 5. *(terug naar tekst)*

[8] Voor de geschiedenis van het EVRM op dit punt, zie E.J. Dommering e.a., *Informatierecht, fundamentele rechten voor de informatiesamenleving*, p. 93. *(terug naar tekst)*

[9] E.J. Dommering, 'De Grondwet in de informatiesamenleving', in: M.C. Burkens e.a (red), *Gelet op de grondwet*, Deventer: Kluwer 1998, p. 111-121, L.F. Asscher, a.w. noot 4, p. 125. *(terug naar tekst)*

[10] EHRM 28 maart 1990, *NJ* 1991, 739, m.nt EAA en EHRM 22 mei 1990, *NJ* 1991, 740 m.nt. EAA. *(terug naar tekst)*

[11] HR 26 februari 1999, *NJ* 1999, 716, m.nt. EJD. *(terug naar tekst)*

[12] L.F. Asscher a.w. noot 4, p. 123. *(terug naar tekst)*

[13] Preadvies inzake een nieuwe tekst voor de artikelen 7 en 13 Gw van de studiecommissie VMC, *Mediaforum* 1999-11/12, p. i-viii. *(terug naar tekst)*

[14] K. Mortelmans, 'De toewijzing van radiozendtijd in Vlaanderen: enkele positieve en negatieve signalen voor Nederland', in: *Mediaforum* 2000-6, p.

192- 196. *(terug naar tekst)*

[15] Onderzoeksbijlage, p. 116. *(terug naar tekst)*

[16] Zie noot 7. *(terug naar tekst)*

[17] Action Plan on promoting safer use of the Internet, INCORE (Internet Content Rating for Europe), April 2000 (website DG XIII) en PREPACT, Review of European Third party filtering and rating software and services (www.idate.org). *(terug naar tekst)*

[18] Zie F. Kistenkas, *Vrije straatcommunicatie*, Deventer/Arnhem: Kluwer/Gouda Quint 1989. *(terug naar tekst)*

[19] Zie D.J.G Visser, *Auteursrecht op toegang*, Den Haag: Vuga 1997. *(terug naar tekst)*

[20] Ik verwijs voor een historisch overzicht naar G.A.I. Schuijt en A.J. Niewenhuis, in: Dommering e.a 2000, a.w. noot 8, hoofdstuk 8. *(terug naar tekst)*

[21] Het gaat om een herhaling van zetten. Ik heb de argumenten daarom summier weergegeven. Voor het volledige debat, zie de literatuuropgave in de noten 4 en 6. *(terug naar tekst)*

[22] Vgl. E.J. Dommering 1997, noot 4, p. 145. *(terug naar tekst)*

[23] Zie hierover G.N.M. Scarione-Gorgels, ' Hoofdstuk 11 van de Telecommunicatiewet, rijp voor revisie?', in: *Privacy & Informatie* 1999 nr. 5, p. 196-204; J. Nouwt, 'Privacy-aspecten van het Internet berichtenverkeer', in: *Privacy & Informatie* 2000, nr. 1, p. 15-23; G-J. Zwenne, 'Verkeersgegevens in de Telecommunicatiewet en de WBP', in: *Mediaforum* 200-5, p.152-157. *(terug naar tekst)*

[24] Zie E.J. Dommering 1997, noot 4, p. 146.

Geplaatst 30.06.2000

Bijlage

Related Issues

NSA Spying

NSA Spying FAQ

FAQ on NSA Spying (General Questions)

What is the NSA domestic spying program?

In October 2001, President Bush issued a secret presidential order authorizing the NSA to conduct a range of surveillance activities inside of the United States without statutory authorization or court approval, including electronic surveillance of Americans' telephone and internet communications. This program of surveillance continues through today and works with the cooperation of major

telecommunications companies.

In 2005, after the New York Times broke the story of the surveillance program, the President publicly admitted one portion of it -- warrantless surveillance of Americans believed to be communicating with people connected with terrorism suspects -- Senior Bush Administration officials later confirmed that the President's authorization went beyond the surveillance of terrorists and conceded that the program did not comply with the Foreign Intelligence Surveillance Act (FISA). The President, invoking a theory of limitless executive power to disregard the mandates of Congress, has reauthorized this warrantless surveillance more than thirty times, including after the Department of Justice found the program to violate criminal laws, and has indicated that he intends to continue doing so.

Shortly after the initial revelations, a whistleblower named Mark Klein came forward with evidence describing the specific AT&T facilities, including one on Folsom Street in San Francisco, where the handoff of customer communications is occurring. Mr. Klein's evidence confirmed what was already indicated by numerous newspaper reports and Congressional admissions — that the NSA is intercepting and analyzing millions of ordinary Americans' communications, with the help of the country's largest phone and Internet companies. EFF has brought two lawsuits to stop this illegal surveillance.

What do the cases claim about the interception of domestic communications of millions of Americans?

The cases allege that the government, in coordination with AT&T, intercepts communications (like phone calls and emails), and that AT&T illegally discloses communications records to the government.The core component of the surveillance is the government's nationwide network of sophisticated communications surveillance equipment, attached to the key facilities of telecommunications companies such as AT&T that carry Americans' internet and telephone communications.

Through this shadow network of surveillance devices, the government has acquired and continue to acquire the content of the phone calls, emails, instant messages, text messages and web communications, both international and domestic, of practically every American who uses the phone system or the internet in an unprecedented suspicionless general search through the nation's communications networks.

What do the cases claim about the communications records of millions of ordinary Americans?

The government has unlawfully solicited and obtained from telecommunications companies such as AT&T the complete and ongoing disclosure of the private telephone and internet transactional records of those companies' millions of customers, communications records indicating who the customers communicated with, when and for long, among other sensitive information. This transactional information is analyzed by computers in conjunction with the vast quantity of communications content acquired by government's network of surveillance devices, in what has been described as a vast data-mining operation.

How do the facts in EFF's *Hepting v. AT&T* and *Jewel v. NSA* cases relate to the warrantless spying that the President has admitted?

The cases allege that, in addition to eavesdropping on or reading specific communications that has been admitted, the government has indiscriminately intercepted the communications and obtained the communications records of millions of ordinary Americans. The government has admitted that it is engaging in more warrantless surveillance than it has specifically admitted. While we do not know for sure, one leading theory is that first the government intercepts all communications — including yours — and then targets certain communications for more in-depth analysis.

Is EFF challenging the surveillance of communications with members of Al Qaeda?

No. None of the plaintiffs in either EFF lawsuit, Hepting v. AT&T or Jewel v. NSA, have communicated with members of Al Qaeda. Instead, the lawsuit is about the dragnet surveillance of millions of ordinary Americans, like the plaintiffs, who have the right to go about their daily lives without the government intercepting their communications or rifling through the records of their communications.

Does the domestic spying program produce better results than FISA?

No. Reports have shown that the data from this wholesale surveillance did little more than commit FBI resources to follow up leads, "virtually all of [which], current and former officials say, led to dead ends or innocent Americans."

For instance:

> "We'd chase a number, find it's a school teacher with no indication they've ever been involved in international terrorism — case closed," said one former FBI official, who was aware of the program and the data it generated for the bureau. "After you get a thousand numbers and not one is turning up anything, you get some frustration."
>
> *— Lowell Bergman, et al, Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends, NY Times, Jan. 17, 2005.*

Wasting counter-terrorism resources on innocent school teachers makes America less free and no safer.

What's AT&T's role in the program?

EFF alleges that under the NSA domestic spying program, major telecommunications companies — and AT&T specifically — gave the NSA access to or information from their vast databases of communications records. This included information about their customers' calls and emails in the past, including all of those people who their customers have corresponded with. In addition, EFF

alleges that AT&T gave the government unfettered access to its over 300 terabyte "Daytona" database of caller information — one of the largest databases in the world.

Are ordinary American's communications included in the surveillance?

Yes. The lawsuit alleges that AT&T's has provided the government with unfettered access to the communications records of ordinary Americans whose communications go through the AT&T network. This includes AT&T customers, anyone who communicates with an AT&T customer, and individuals whose messages are simply carried over AT&T's networks.

Is the fight against warrantless spying on ordinary Americans a partisan issue?

No. EFF is a non-partisan organization and has consistently opposed illegal surveillance efforts, regardless of which party held the presidency. Indeed, the opposition to the domestic surveillance program has come from not just Democrats, but also leading conservatives. As David Keene, chairman of the American Conservative Union said, "This is not a partisan issue; it is an issue of safeguarding the fundamental freedoms of all Americans so that future administrations do not interpret our laws in ways that pose constitutional concerns."

Other leading conservatives who have spoken out on the domestic surveillance include:

- Former U.S. Rep. Bob Barr;
- Grover Norquist, president of Americans for Tax Reform;
- Paul Weyrich, chairman and CEO of the Free Congress Foundation; and
- Alan Gottlieb, founder of the Second Amendment Foundation.

What is AT&T's Daytona technology?

Daytona is a database management technology originally developed and maintained by the AT&T Laboratories division of AT&T, and used by AT&T to manage multiple databases. Daytona was designed to handle very large databases and is used to manage "Hawkeye," AT&T's call detail record (CDR) database. Daytona is also used to manage AT&T's huge network-security database, known as "Aurora." As of September 2005, all of the CDR data managed by Daytona, when uncompressed, totaled more than 312 terabytes.

What is AT&T's Hawkeye database?

Hawkeye is AT&T's call detail record (CDR) database, which contains records of nearly every telephone communication carried over its domestic network since approximately 2001. The records include the originating and terminating phone numbers and the time and length for each call.

What is AT&T's Aurora database?

Aurora is a network-security database that had been used to store Internet traffic data since approximately 2003. The Aurora database contains huge amounts of data acquired by firewalls, routers, honeypots and other devices on AT&T's global IP (Internet Protocol) network and other networks connected to AT&T's network.

How many calls go through AT&T?

By the end of 2004, on an average business day, AT&T Corp.'s network handled over 300 million voice calls as well as over 4,000 terabytes (million megabytes) of data. That's approximately 200 times the amount of data contained in all the books in the Library of Congress.

Where can I read more about the NSA surveillance program?

- Key news reports
- Federation of American Scientist's NSA page
- ACLU's NSA page

What is the National Security Agency?

The National Security Agency is a United States government intelligence agency that is responsible for the collection and analysis of foreign communications. According to the NSA site, it "coordinates, directs, and performs highly specialized activities to protect U.S. government information systems and produce foreign signals intelligence information."

- Official NSA website
- The National Security Archive's "The National Security Agency Declassified"
- Wikipedia entry on the NSA

What can I do to help?

Lawsuits take a tremendous amount of time, energy, and financial resources. The only way non-profits such as EFF can afford to pursue them are through the kind and generous donations of individuals such as you. If you believe in what we are fighting for, please consider donating to support our efforts.

FAQ on EFF's case against NSA (*Jewel v. NSA*)

- What is *Jewel v. NSA* about?
- What is the goal of the *Jewel v. NSA* lawsuit?
- What legal claims are being raised in the *Jewel v. NSA* lawsuit?
- Who is bringing the *Jewel v. NSA* lawsuit?
- Who is being sued?
- Why are the individuals being sued?
- How is this case different from the lawsuits that are challenging the surveillance of people who are believed to be

What is *Jewel v. NSA* about?

Jewel v. NSA challenges an illegal and unconstitutional program of dragnet communications surveillance conducted by the National Security Agency (NSA) and others in concert with major telecommunications companies like AT&T.

What is the goal of the *Jewel v. NSA* lawsuit?

The most important goal is to end the illegal surveillance, and to have it declared illegal and unconstitutional. The suit also seeks to further insure against future lawbreaking by seeking an award of damages for the five individual plaintiffs--not only from the government but also from the individual government officials responsible for creating and implementing the surveillance.

What legal claims are being raised in the *Jewel v. NSA* lawsuit?

- Violation of the Fourth Amendment to the Constitution
- Violation of the First Amendment to the Constitution
- Unlawful electronic surveillance or disclosure or use of information obtained by electronic surveillance in violation of 50 U.S.C. §1809.
- Unlawful interception, use or disclosure of Class communications in violation of 18 U.S.C. § 2511
- Unlawful solicitation and obtained disclosure of the contents of communications in violation of 18 U.S.C. § 2702(a)(1) or (a)(2)
- Unlawful solicitation and obtained disclosure of non-content records or other information in violation of 18 U.S.C. § 2702(a)(3)
- Violation of the Administrative Procedures Act
- Violation of the constitutional principle of separation of powers

Who is bringing the *Jewel v. NSA* lawsuit?

The lawsuit is brought by five people. The plaintiffs are ordinary Americans who all use AT&T as their communications provider, some for phone, some for internet. They bring some of their claims as individuals and others on behalf of all AT&T customers.

Who is being sued?

The lawsuit is against the United States government itself, a number of government agencies, as well as a number of current

and former agency officials who participated in or ordered the illegal surveillance. The claims on behalf of all AT&T customers seek a declaration that the surveillance is illegal and an injunction to stop it, while the individual plaintiffs also seek damages against all the defendants (except for the President, who the courts have ruled has absolute immunity against civil damages claims). The specific defendants are the United States, the National Security Agency, the Department of Justice, President George W. Bush, Vice President Dick Cheney, Cheney's Chief of Staff David Addington, NSA Director Keith B. Alexander, CIA Director Michael V. Hayden, Attorney General Michael B. Mukasey, former Attorneys General Alberto Gonzales and John D. Ashcroft, Director of National Intelligence Michael McConnell and former DNI John Negroponte.

Why are the individuals being sued?

The individuals are the architects and the operators of a massive illegal domestic surveillance program. Each of them swore to uphold the law and the constitution upon taking office, and had a responsibility to defend ordinary Americans from illegal surveillance, not perpetrate it.

Moreover, the Patriot Act made it more challenging to sue the government itself for past violations of the law, basically encouraging such suits to be brought against individual governmental officials rather than the government itself. Since the warrantless surveillance has now been going on for many years and may have changed in some ways over time, the claims against the individuals are the best way to ensure that the court rules on the legality of any past surveillance as well as ruling on the current surveillance. The damages claims against the individual government officials are only brought on behalf of the five individual plaintiffs, instead of the class.

How is this case different from the lawsuits that are challenging the surveillance of people who are believed to be communicating with members of Al Qaeda, like the one brought by the ACLU?

This lawsuit arises from the untargeted, warrantless surveillance of millions of ordinary Americans. The ACLU lawsuits challenge the targeted warrantless surveillance of specific individuals. Both the untargeted surveillance and the targeted surveillance are part of the same overall program. While portions of the warrantless wiretapping have been called the Terrorist Surveillance Program for public relations purposes, the government has admitted that this is not the full extent of the warrantless surveillance program authorized by the President.

How does this case relate to the case against AT&T or any of the other cases against telecommunications carriers?

These cases are two sides of the same coin. *Jewel v. NSA* is only against the government, not the telecommunications carriers. As a society built upon the rule of law, both the government and the carriers must be held responsible for the illegal program.

Does telecom immunity affect *Jewel v. NSA* case?

No. The immunity Congress passed only applies to telecommunications carriers, not the government. EFF believes that the immunity is unconstitutional and is fighting it in *Hepting v. AT&T* and the other telecommunications cases..

Why didn't you sue the government until now?

In 2006, suing AT&T looked like the fastest way to halt the illegal surveillance. Unfortunately, Congress interfered with the judicial process in our case by granting immunity to telecoms that participated in the warrantless wiretapping program. In response, we are opening up a new front in this battle. Our top priority is to stop the ongoing illegal surveillance as soon as possible, and to hold those responsible for the program to account.

FAQ on EFF's Case Against AT&T (*Hepting v. AT&T*)

What is EFF's lawsuit against AT&T, called *Hepting v. AT&T*, about?

EFF filed a class-action lawsuit against AT&T, accusing the telecom giant of violating the law and the privacy of its customers by collaborating with the National Security Agency (NSA) in its massive and illegal domestic spying program to wiretap and data-mine Americans' communications.

What is the lawsuit seeking?

EFF, on behalf of a nationwide class of AT&T customers, is suing to stop this illegal conduct and hold AT&T responsible for its illegal collaboration in the government's domestic spying program, which has violated the law and damaged the fundamental freedoms of the American public. The lawsuit requests an injunction and damages under the statute.

If the NSA did the illegal wiretapping and data-mining, why are you suing AT&T?

AT&T also violated the law, and the rights of its customers, by allowing and assisting with the illegal wiretapping and data-mining. The government's spying program would not be possible without AT&T's collaboration. AT&T should have been standing up for you and your privacy. In this country, we follow the law, we don't just follow orders.

EFF also has a case against the government, called *Jewel v. NSA*.

Why has EFF brought a class action against AT&T?

We believe that all AT&T customers have had their privacy violated by AT&T's actions. And importantly, bringing the case as a class action is the only sure way to make sure AT&T is prohibited from continuing these illegal actions. A class action ensures that an injunction against AT&T would apply throughout the country, not simply in the district in which the lawsuit was filed. Finally, we hope that the risk of serious statutory damages ($1,000 per subscriber under the ECPA and up to $10,000 per subscriber under the Telecom Act) will provide sufficient incentives for AT&T and the other telcos to push back on the feds with respect to this illegal program and in the future.

Who exactly is the case against?

Both AT&T Inc. and AT&T Corp. AT&T Inc. is the new name of SBC Communications, which acquired AT&T Corp. in November 2005. At closing, a wholly owned subsidiary of SBC merged with and into AT&T Corp., and thus AT&T Corp. became a wholly owned subsidiary of SBC. SBC adopted AT&T, Inc. as its name following completion of its acquisition of AT&T Corp.

Why is the case against both AT&Ts?

While the case focuses on the acts of AT&T Corp. (pre-merger), AT&T Inc. has begun a transition process designed to integrate the former SBC's telecommunications network with AT&T Corp.'s network, ultimately leading into unified networks. The lawsuit alleges that the facilities and technologies of the former SBC are being or will imminently be used to transmit the communications of AT&T Corp. customers, and will continue the violation of the privacy of its customers.

If the lawsuit succeeds, will the government still be able to surveil terrorists?

Yes. Wiretaps on terrorists are allowed under the law, and this lawsuit is not challenging the wiretap laws.

We have sued AT&T for breaking those laws — the telecommunications giant gave the government access to its communications switches and its huge databases of information on millions of ordinary Americans.

Those surveilled are AT&T customers who have not even been accused of affiliations with terrorists.

Americans can be both safe and free: if the government truly

believes it has cause to wiretap a suspect, it can order AT&T to provide information under FISA for up to 72 hours before going to the court. But AT&T has no business providing direct access to the communications of millions of ordinary Americans, without the checks and balances of Congress or the courts.

How many customers did AT&T have?

By the end of 2004, AT&T Corp. provided long distance service (including both stand-alone and bundled) to approximately 24.6 million residential customers, dropping from approximately 34.4 million customers at the end of 2003. Before the acquisition, AT&T Corp.'s bundled local and long distance service was available in 46 states, covering more than 73 million households.

How big is the new AT&T Inc.?

The new AT&T Inc. constitutes the largest telecommunications provider in the United States and one of the largest in the world. AT&T Inc. is the largest U.S. provider of both local and long distance services, serving millions of customers nationwide. AT&T Inc.'s international voice service carries more than 18 billion minutes per year, reaching 240 countries, linking 400 carriers and offering remote access via 19,500 points of presence in 149 countries around the globe. A point of presence is a facility where a long-distance carrier connects to a local telephone network.

Why are the first and fourth amendments at issue for AT&T?

Because AT&T is acting as the government's agent in the government's violation of the Bill of Rights. Accordingly, the lawsuit makes Constitutional claims in addition to alleging that AT&T violated the wiretap and telecommunications laws.

What about telecom immunity?

In response to the cases seeking to hold the telecoms accountable for their actions, the Bush Administration demanded that Congress give the telecoms retroactive immunity.

In July of 2008, Congress gave in to the president's demand, passing the FISA Amendments Act (FAA). In addition to expanding the executive's spying powers, the unconstitutional law allowed the Attorney General to file a certification designed to give immunity to the telecoms, and thereby to keep the courts from ruling that the warrantless wiretapping program was illegal. EFF is challenging the immunity law as unconstitutional.

Why are the FAA immunity provisions unconstitutional?

The FAA unconstitutionally attempts to take the factual and legal decisionmaking away from the courts for both statutory and constitutional claims. To the extent that the FAA purports to retain the court’s role in these cases, it does so only by turning the Court, and the process of adjudication, into a shadow-play of empty gestures hidden by Executive-controlled secrecy.

Could you be more specific?

While a full recital of the flaws in the FAA is beyond the scope of this FAQ, many of them are readily apparent:

- Congress violated the separation of powers by attempting to usurp judicial authority to decide the Fourth Amendment claims of millions of ordinary Americans who have been, and continue to be, subjected to dragnet surveillance for the past 7 years;
- Congress exceeded its constitutional authority by passing legislation that grants to the Executive the discretion to essentially dictate the outcome of specific, pending litigation;
- The statute improperly requires dismissal of claims of illegal surveillance between September 11, 2001 and January 17, 2007, based not on a judicial finding about the facts of the surveillance or the legality or constitutionality of the surveillance, but instead merely based on a "certification" from the Attorney General that that some unknown member of the Executive branch told the carriers that some undescribed surveillance was "lawful";
- The FAA denies due process to the plaintiffs by granting to the Executive, rather than the courts, the essential decisionmaking about their constitutional and statutory rights; and
- The FAA purports to grant to the Executive a unilateral right to require that the court keep secret not only the evidence, but its own decisions.