



**UvA-DARE (Digital Academic Repository)**

**Case note: (Noot bij FISA-hof 18 november 2002)**

Asscher, L.F.

[Link to publication](#)

*Citation for published version (APA):*

Asscher, L. F., (2002). Case note: (Noot bij FISA-hof 18 november 2002), (JAVI- Juridische Aspecten Van Internet; No. 1).

**General rights**

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

**Disclaimer/Complaints regulations**

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <http://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.



# Noot bij FISA-hof 18 november 2002

LODEWIJK ASSCHER\* Op 18 november 2002 deed het Amerikaanse Foreign Intelligence

Surveillance court of Review een belangwekkende uitspraak. Dit geheime FISA-hof is een voortvloei-  
sel van de Foreign Intelligence Surveillance Act. Die wet regelt op welke voorwaarden Amerikaanse  
veiligheidsdiensten buitenlanders en Amerikanen mogen afluisteren en bespioneren in zaken van ter-  
rorisme en spionage.

In deze zaak vernietigt het Hof de uit-  
spraak van de lagere FISA-rechter over  
een verzoek van minister van Justitie  
Ashcroft om ruimere aftapbevoegdheden. De FISA-wet stamt uit 1978, en dus  
uit de Koude Oorlog.

Na de aanslagen van 11 september 2001  
is een reeks maatregelen genomen ter  
bestrijding van het terrorisme. Ashcroft  
diende ter uitvoering van deze maatregelen  
een reeks voorstellen in ter bestrijding  
van het terrorisme. De Anti Terrorism Act  
(ATA) en de PATRIOT-Act werden snel  
door het Congres aangenomen en breiden  
onder meer de bevoegdheid tot het  
opvragen van communicatiegegevens uit.  
De oude regelingen met betrekking tot  
verkeersgegevens zijn uitgebreid van de  
telefonie naar alle vormen van telecommu-  
nicatie waaronder het internet. Dit  
maakt het mogelijk om gebruikte web-  
adressen en de subject lines van e-mail-  
verkeer op te vragen. Weliswaar is hier-  
voor rechterlijke toestemming vereist,  
maar de rechter mag een dergelijk ver-  
zoek niet weigeren als de opsporings-  
autoriteit aangeeft de gevraagde gege-  
vens nuttig te achten in een onderzoek  
naar buitenlandse 'targets'. Bovendien  
maakt de PATRIOT-Act het mogelijk om  
veel eenvoudiger en in meer gevallen af  
te tappen in het kader van de FISA-wet-  
geving.

**Tappen na 9-11** | In de thans vernietigde  
uitspraak waren nadere eisen gesteld aan  
het verkrijgen van toestemming, die er  
met name op gericht waren dat de veilig-  
heidsdiensten niet met het oog op 'gewo-

ne' misdaadbestrijding gebruik zouden  
maken van hun bevoegdheden.

Nu het gaat om een geheime rechtbank  
waarvan alleen het vonnis openbaar is,  
heeft de regering feitelijk geen wederpar-  
tij in dit geding. In casu verzocht Ashcroft  
de rechter vast te stellen dat er geen  
nadere eisen aan het honoreren van een  
tapaanvraag gesteld mógen worden.

**Het communicatiegeheim in de VS** | De  
Amerikaanse Grondwet kent geen expli-  
ciet recht op privacy of communicatiege-  
heim. Wel bevat de constitutie in het  
Fourth Amendment een bepaling die het  
recht beschermt

'of the people to be secure in their per-  
sons, their houses, papers and effects  
against unreasonable searches and seizu-  
res, shall not be violated and no warrants  
shall issue, but upon probable cause, sup-  
ported by oath or affirmation, and particu-  
larly describing the place to be searched,  
and the persons and things to be seized'.

Het Fourth Amendment was een reactie  
op de zogenoemde general warrant  
(algemene last). In de Engelse koloniale  
tijd gingen officieren en politiebeambten  
zich gewapend met zo'n warrant te bui-  
ten aan roof, plundering en vernietiging  
van persoonlijke eigendommen. Om die  
reden werd in het Fourth Amendment de  
eis opgenomen dat een warrant aan  
bepaalde eisen dient te voldoen. Het  
Fourth Amendment beschermde oor-  
spronkelijk uitsluitend het huis, de eigen-  
dom, en de papieren tegen doorzoeking  
en inbeslagname en dus niet de latere  
vormen van elektronische communi-  
catie.<sup>1</sup>

De drooglegging van de jaren '20 en '30  
leidde tot een ongekende bloei van crimi-

naliteit en ook tot de ontwikkeling van  
revolutionaire nieuwe opsporingsmetho-  
den. De vergelijking met de verschijnselen  
rond de 'war on drugs' en de strijd tegen  
het terrorisme dringt zich op. In de zaak  
*Olmstead*<sup>2</sup> besteedde de Supreme Court  
aandacht aan de vraag of het afluisteren  
van telefonie onder het Fourth Amend-  
ment viel. Olmstead werd verdacht van de  
illegale verkoop van alcohol en werd  
afgeluisterd tijdens een gesprek vanuit  
een telefooncel. De Supreme Court vond  
geen bewijs van onrechtmatig binnen-  
dringen (*trespassing*) in het huis of kan-  
toor van de verdachte en meende dat het  
Fourth Amendment niet zo kon worden  
geïnterpreteerd dat telefoon er onder zou  
vallen, aangezien telefoon de stem via  
kabels buiten het huis brengt en dus  
nooit onder het Fourth Amendment kan  
vallen.

In zijn befaamde *dissenting opinion* geeft  
Justice Brandeis echter aan dat als de ont-  
wikkeling der technologie ertoe leidt dat  
veel individuen vertrouwelijk communi-  
ceren buiten het grondwettelijk bescherm-  
de gebied van het huis, dat ertoe moet  
leiden dat de Supreme Court ook de  
grenzen aan het overheidshandelen inter-  
preteert, rekening houdend met de ver-  
anderende omstandigheden. Volgens  
Brandeis moet het Fourth Amendment zo  
worden gelezen dat het die veranderingen  
kan opvangen, want:

'a principal to be vital must be capable of  
wider application than the mischief which  
gave it birth.'

Brandeis houdt in wezen een sterk pleidooi  
voor een meer techniekonafhankelijke  
benadering van het Fourth Amendment.

'Legislation, both statutory and constitu-  
tional, is enacted, it is true, from an expe-

\*Mr. L.F. Asscher is onderzoeker bij het  
Instituut voor Informatierecht van de Universiteit  
van Amsterdam. E-mail: asscher@ivir.nl



rience of evils, but its general language should not, therefore, be necessary confined to the form that evil had.’

In 1967 kreeg Brandeis alsnog gelijk en besloot de Supreme Court in de zaak *Katz*<sup>3</sup> dat ook het afluisteren zonder trespassing in strijd kon zijn met het Fourth Amendment.

### De bevoegdheden van veiligheidsdiensten

| Binnen het leerstuk van het communicatiegeheim nemen spionage- en veiligheidsdiensten een bijzondere plaats in.<sup>4</sup> De aard van het werk van veiligheidsdiensten maakt rechterlijke toestemming in de openbaarheid onpraktisch en zelfs een toetsing achteraf kan in sommige gevallen tot onwenselijke gevolgen leiden. Daarentegen is de inbreuk bij heimelijk en stelselmatige aftappen en meelesen des te groter als geen sprake is van openbare controle op het rechtmatig toepassen van die middelen en als degene wiens communicatie getapt is zich niet tot de rechter kan wenden om een uitspraak over de rechtmatigheid van de beperking. In Nederland wordt sinds de invoering van de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten (WIVD) over dergelijke zaken beslist door de minister van Binnenlandse Zaken, die weer verantwoording aflegt aan de geheime commissie voor binnenlandse veiligheid, artikel 25 lid 2 WIVD.

Als al te billijken valt dat aan aftappen door veiligheidsdiensten minder hoge eisen worden gesteld dan indien het gaat om de gewone misdaadbestrijding, dan is het van belang te zorgen dat niet onder het mom van terrorismebestrijding gebruik wordt gemaakt van de speciale bevoegdheden bij de gewone opsporing. Immers, dan zakt het niveau van bescherming over de gehele linie. Er moet dus een scheiding worden gemaakt tussen de informatie die wordt verkregen op grond van de FISA-bevoegdheden en andere informatie. In de Amerikaanse literatuur wordt gesproken van een *wall*, een muur tussen beide informatiestromen. Uiteraard moeten beide vormen van aftappen in overeenstemming zijn met de grondwettelijke ruimte.

De vereisten van het Fourth Amendment voorzien in een redelijkheidstoets en in een specificiteitstoets. De uitkomst van bovenstaande uitspraak maakt dat aan

die eisen niet of althans in mindere mate hoeft te worden voldaan bij opsporing in het kader van de strijd tegen het terrorisme. Daarbij doet het Hof een opvallende uitspraak in de richting van de Supreme Court. Dat laatste had namelijk bepaald dat de dreiging voor de samenleving niet het beslissende argument mag zijn in de beoordeling van de redelijkheid van een aftapbevel, het FISA-hof leest dat nu zo dat het weliswaar niet beslissend mag zijn maar wel cruciaal:

‘Although the Court cautioned that the threat to society is not dispositive in determining whether a search or seizure is reasonable, it certainly remains a crucial factor’.

Hoewel de eisen die in de nieuwe antiterrorismewetten gesteld worden wellicht niet voldoen aan de waarborgen van het Fourth Amendment, zo gaat het Hof verder, komen ze in elk geval dicht genoeg in de buurt. Het FISA-hof verwerpt de theorie van de muur tussen veiligheidstappen en gewone tapverzoeken. Spionage en terrorisme zijn immers misdrijven, dus het zou belachelijk zijn een dergelijk onderscheid te blijven maken, aldus het Hof. Organisaties als ACLU werd weliswaar toegestaan een *friend-of-the-court*-stuk in het geding te brengen maar ze mochten niet deelnemen aan de geheime rechtszitting zelf. Probleem is dat de burgerrechtenorganisaties ook niet de mogelijkheid hebben tegen deze uitspraak in beroep te gaan bij de Supreme Court. Dat kan alleen de staat zelf in de persoon van de heer Ashcroft en die kans is klein.

**Terroristen aan de Maas?** | Inmiddels is de scheiding tussen veiligheidsdiensten en Openbaar Ministerie ook in Nederland actueel na de vrijspraak door de Rechtbank Rotterdam van drie terrorisme verdachten.<sup>5</sup> De Rotterdamse rechter zet helder uiteen waarom er een muur tussen veiligheidsdienst en Openbaar Ministerie hoort te staan:

‘Hier [...] doet zich [...] de vraag voor of verdachte reeds op grond van de door de veiligheidsdienst aan het Openbaar Ministerie overgedragen inlichtingen door het Openbaar Ministerie als “verdachte in de zin van artikel 27, lid 1 Sv” kon worden aangemerkt. Deze vraag wordt door de rechtbank ontkennend beantwoord. De inlichtingeninwinning door de veiligheidsdienst is im-

mers niet geschied in het kader van een strafrechtelijk – en als zodanig met strafrechtelijke waarborgen omkleed – onderzoek met het doel bewijs tegen de verdachte te verzamelen, maar heeft plaatsgevonden in het kader van de aan genoemde dienst bij de WIV opgedragen taak, te weten het verzamelen van inlichtingen ten behoeve van de staatsveiligheid.’

Minister Donner van Justitie liet onmiddellijk weten een wetswijziging te overwegen als de uitspraak in hoger beroep niet vernietigd zou worden.

De FISA-zaak is voor Nederland om drie redenen van belang. In de eerste plaats roept zij de vraag op of in Nederland de afbakening tussen de bevoegdheden van de AIVD en de informatiebehoefte van het Openbaar Ministerie afdoende helder geregeld is. Een vraag die overigens ook al tijdens de IRT-enquête aan de orde kwam. In de tweede plaats is deze zaak van belang voor de voortdurende discussie over de digitale grondrechten in Nederland. Mijns inziens onderstreept de uitspraak het belang van een specifieke bepaling over de positie van de veiligheidsdiensten in het grondwettelijk communicatiegeheim van artikel 13 Grondwet. In de derde plaats vormt de uitspraak een concreet voorbeeld van de verschuiving tussen privacy en terrorismebestrijding sinds 11 september 2001. Het is daarbij de vraag in hoeverre ook de Nederlandse rechtsstaat gaat veranderen vanwege de strijd tegen het terrorisme. Weliswaar zijn vérgaande maatregelen noodzakelijk om de democratie te beschermen,

‘when the end justifies the means, the difference between terror and those fighting it, becomes increasingly indistinct.’

De links bij deze jurisprudentiebespreking vindt u op <<http://www.javisite.nl>>.

### Noten

- 1 Zie L.F. Asscher, *Communicatiegrondrechten*, Amsterdam: Cramwinckel 2002, Hoofdstuk 10.
- 2 *Olmstead vs. United States*, 277 US 438, 1928.
- 3 *Katz vs. US*, 389 US.
- 4 Zie hierover A.H. Ekker, ‘Het onderscheppen van telecommunicatie door de inlichtingen- en veiligheidsdiensten’, *Computerrecht* 2002-2, pp. 77-83.
- 5 Rechtbank Rotterdam, 18 decemer 2002.