Aan: TWEEDE KAMER DER STATEN-GENERAAL
Aan de leden van de vaste Kamercommissie JBZ-zaken
T.a.v. de griffier
Postbus 20018
2500 EA 's-Gravenhage

Amsterdam, 30 augustus 2005

Betreft: Nieuwe ontwikkelingen bewaarplicht verkeersgegevens

Geachte Kamerleden,

Namens het ISPO, het internet service providers overleg, willen wij graag uw aandacht vragen voor een aantal nieuwe ontwikkelingen in het dossier 'bewaarplicht verkeersgegevens'.

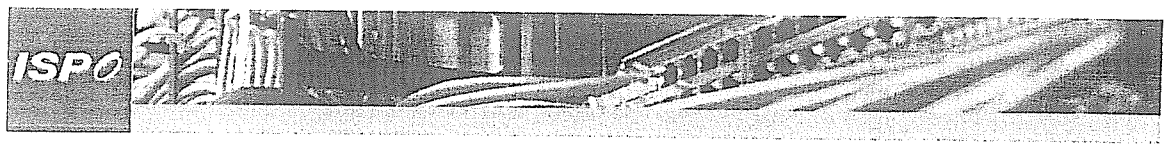
Op dinsdagmiddag 6 september 2005 spreekt u opnieuw over het voorgestelde Kaderbesluit van de ministers van Justitie, om verkeersgegevens minimaal 1 en maximaal 4 jaar verplicht te laten bewaren door de aanbieders van internet en telefoondiensten, voor de opsporing, vervolging en bestraffing van misdrijven in de breedste zin des woords.

Graag maken wij u attent op het feit dat de Europese Commissie op korte termijn een eigen Richtlijnvoorstel bekend maakt. Een concept van dit Commissie voorstel is te lezen via: http://www.edri.org/docs/EUcommissiondataretentionjuly2005.pdf

Het ISPO is van mening dat het voorstel een verbetering met zich meebrengt ten opzichte van het ontwerp kaderbesluit van de JBZ ministers. In de eerste plaats omdat de Commissie kiest voor behandeling in de eerste pijler, met volledig meebeslissingsrecht van het Europese Parlement. Ten tweede lijkt in het voorstel het soort gegevens dat opgeslagen moet worden, beperkter te zijn dan in eerdere voorstellen. Tot slot voorziet het voorstel van de Commissie in een 'vergoeding voor additionele kosten'. Deze uitgangspunten zien wij als een veel beter begin van de discussie over een eventuele bewaarplicht dan de procedure die tot nu toe door de JBZ-ministers is gevolgd.

Echter, ISPO heeft nog steeds een aantal zeer zwaarwegende bezwaren tegen het huidige voorstel van de Commissie.

Ten eerste zijn nut en noodzaak van de bewaarplicht nog steeds niet aangetoond. Op dit moment ligt er nog steeds een Kamermotie die minister Donner verbiedt verdere stappen in Europees verband te nemen tot dat nut en noodzaak van een bewaarplicht zijn vastgesteld. Het Erasmus rapport toont de nut en noodzaak in het geheel niet aan. Met het Erasmus rapport,



waarover wij u op 11 juli al een brief stuurden, is de minister hier niet in geslaagd. In tegendeel. Het rapport maakt juist duidelijk dat de politie in 'vrijwel alle gevallen' probleemloos toegang had tot de gevraagde verkeersgegevens. En uit de rest van Europa zijn geen onderzoeken bekend die een vergelijkbare vraagstelling hadden, noch enig ander openbaar overtuigend bewijs van nut en noodzaak. Toch heeft de JBZ-raad in informeel overleg al besloten hoe dan ook op 12 oktober een unanieme beslissing te willen nemen over de bewaarplicht verkeersgegevens. Voor zowel het voorstel van de JBZ-Raad als dat van de Europese Commissie geldt dat nut en noodzaak dienen te worden vestgesteld voordat verdere besluitvorming in Europ over de bewaarplicht plaatsvindt.

Ten tweede vreest ISPO dat de sector in Nederland er met de invulling van het begrip vergoeding van additionele kosten uit de richtlijn bekaaid gaat afkomen. De overheid hanteert op dit moment een normbedrag voor gegevensverstrekking van €6,56. Dit is niet eens afdoende om administratieve en personeelskosten te dekken, laat staan dat de benodigde investeringen worden vergoed.

Ten derde zijn wij van mening dat de soorten gegevens die aanbieders moeten opslaan onvoldoende duidelijk zijn gedefinieerd. Het lijkt erop dat internetaanbieders niet alle gegevens over internetverkeer hoeven op te slaan, maar slechts verkeergegevens over communicatie tussen personen. Dit wordt echter onvoldoende duidelijk uit de definities.

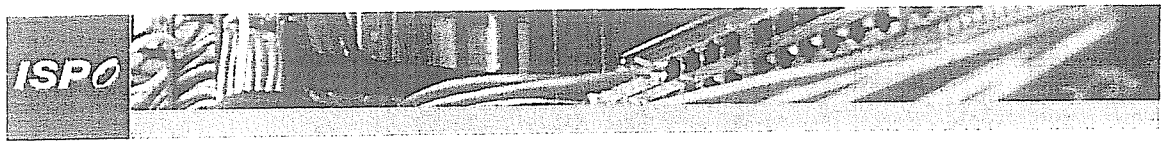
Zoals u uit onze bijgaande brief aan de Europese Commissie kunt lezen, vinden wij dus dat ook het Commissie-voorstel niet tegemoet komt aan de bezwaren van de sector. Overigens worden bezwaren van Nederlandse aanbieders door vrijwel alle Europese aanbieders van elektronische communicatiediensten gedeeld. Wij willen u in dat verband wijzen op bijgevoegd position paper van een groot aantal Europese organisaties.

Wij hopen dat u de bezwaren die u eerder aan de orde heeft gesteld opnieuw indringend aan de minister wilt voorleggen en instemming aan verdere besluitvorming wilt onthouden zolang de besluitvorming over de voorgestelde maatregelen niet langs democratische weg plaatsvindt, nut en noodzaak niet zijn aangetoond en de sector niet afdoende wordt gecompenseerd.

Hoogachtend,

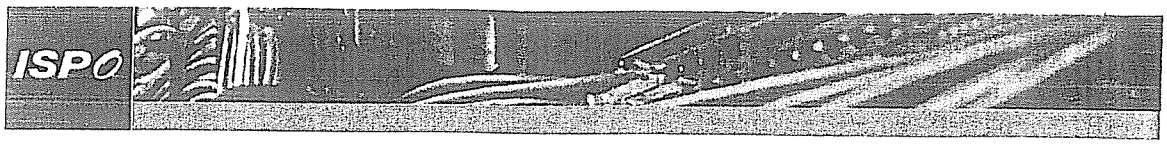
Namens ISPO,

Judith van Erve
XS4ALL Public Affairs
020-3987683
Judith@ispo.nl
www.ispo.nl



Bijlagen:

- Brief van ISPO aan Europese Commissie d.d. 30 augustus 2005.
- Joint statement to the Informal Justice Council,
8 & 9 September 2005, on Communications Data Retention



Her Excellency Viviane Reding
European Commission
Commissioner for Information Society and Media
Rue de la Loi 200 B-1049 Brussels - Belgium

His Excellency Franco Frattini
European Commission
Vice President and Commissioner for Justice, Freedom and Security
Rue de la Loi 200 B-1049 Brussels - Belgium

cc: Members of the LIBE and Industry committees of the European Parliament

Amsterdam, August 30, 2005

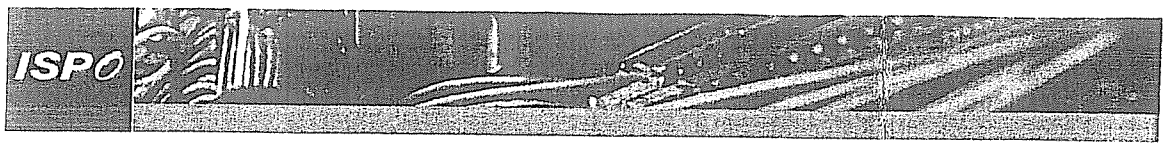
Regarding: commentary Dutch ISP's on EC proposal on data retention

Dear Mr Frattini, Mrs Reding,

On behalf of ISPO, the Dutch internet provider platform, we kindly ask your attention for some first comments on the draft Commission proposal for a Directive on data retention. We are well aware this proposal is still in consultation and has not been finalized yet, but feel it is appropriate to send our reflections before September 2005. We expect the negotiations between Commission, Council and Parliament to rapidly reach momentum around the informal JHA Council of 8 september 2005, and are concerned the specific problems of the internet industry might be overlooked.

We are pleased to see the Commission insists on a first pillar directive procedure. We are also pleased the Commission insists on reimbursement of 'additional costs' for the industry, caused by the obligation to retain data without any business purpose. We also see a clear difference in length of storage periods between the Commission proposal and the last UK-prepared version of the JHA proposal for a framework decision. However, we cannot help but notice the same lack of evidence for the benefits of traffic data retention. We will gladly oblige with the proposal to collect statistics on the use of retained data and present these annually to the Commission, but would have expected this information had already been collected by law enforcement agencies as the start of a debate about the necessity of creating a Directive on mandatory data retention.

In fact, as far as we know, the research conducted by the Rotterdam Erasmus University into the usefulness and necessity of data retention is the only public research in Europe into such statistics. But instead of providing a convincing argument for any period of mandatory data retention, this report concludes that law enforcement 'in virtually all cases' could obtain all the data they requested. For a detailed analysis of the Erasmus report, we kindly refer you to the attached document.



The Netherlands do not have any mandatory data retention law, with the single exception of a specific obligation (an administrative decree) on providers of pre-paid mobile telephony services to store caller location data for 3 months, in order to be able to trace the identity of a pre-paid caller. Because a possible European framework decision on this issue would have such a grave financial and operational impact on the telecommunications industry, the Dutch Parliament has forbidden the Minister of Justice to take any further steps in the European Union leading to mandatory data retention until the need for and benefits of data retention have been proven. In our opinion, this same argument applies to a Commission directive proposal.

On the issue of cost reimbursement, we are very concerned about the phrasing of the definition of additional costs. So far, the Dutch government has transferred all costs related to law enforcement unilaterally to the industry. The Dutch Telecommunication Law only prescribes reimbursement for the personnel and administrative costs of executing law enforcement orders, but none of the very high infrastructural and incremental costs. On 1 April 2005, government has unilaterally, without any consultation with the industry, lowered the standard reimbursement fee for personnel costs to the unrealistically low amount of 13 euro per wiretapping order and 6,56 euro for the execution of an order to retrieve traffic data. Given the immense expected costs of implementing data retention, and the repeated intention of the Dutch Minister of Justice not to reimburse any additional costs, we are deeply concerned about our future economic viability and ability to develop new services.

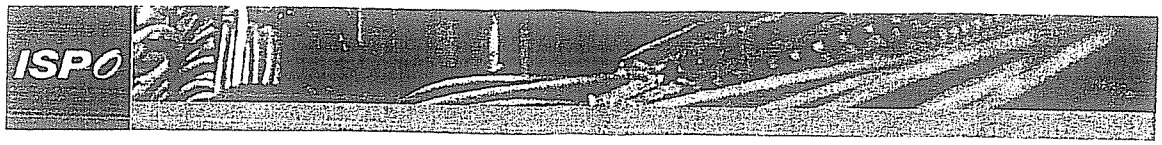
A further issue of concern for ISPO is the fact that the annex of the guideline proposal that specifies the types of data to be retained does not provide a clear-defined scope for the data retained. This is especially the case for data necessary to trace and identify the destination of a communication. ISPO assumes that only person-to-person communication is within the scope of these type of data. ISPO strongly urges the Commission to use a definition that strictly limits the scope data to be retained.

With the Commission we wholeheartedly agree that innovation in the IT-sector is the engine of the European economy. Given the rapid replacement of traditional telecommunication services by IP-based services, we are afraid any seemingly modest list of data, will continuously be subjected to expansion. The proposed 'flexible list' and decision mechanism behind closed doors strike us as the biggest flaw in the Commission proposal. If the purpose is to create a balance between human rights and law enforcement demands, any shift in this balance should be properly debated in the European Parliament and should never bind national parliaments.

Sincerely,

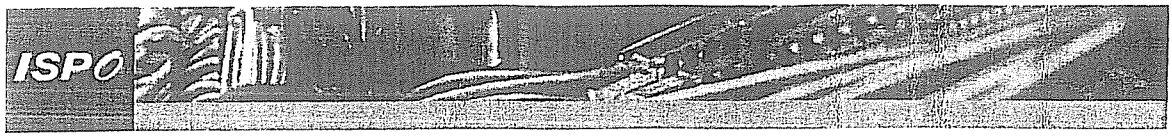
on behalf of ISPO,

Judith van Erve
XS4ALL Public Affairs
+31 20 3987683
judith@ispo.nl
www.ispo.nl



Addition:

Commentary on the Erasmus Study by ISPO.



Commentary of ISPO on the Erasmus study

A similar commentary has been sent to the members of cabinet of The Netherlands and the relevant committees in the Upper and the Lower Houses of the Dutch Parliament on July 2005 .

The Erasmus study clearly states that because of the lack of substantial data, the researchers were not able to establish a representative survey. Therefore several officers of the department of justice and the police department have been interviewed to take into account their experiences regarding the use of traffic data in the investigation and prosecution of crime. The conclusion of the report is that one has not been able to estimate whether data retention measures would be useful or necessary to prevent or investigate acts of terrorism or crime. We feel this is accurate since the report reflects no more than a wish-list of the police and justice departments. The report also carries several misconceptions with regard to techniques and practices of the internet. In this commentary we would like to address some of them. We hope that more technical insight will enhance the believe that extensive data retention for internet traffic data is not the solution to terrorism and crime.

Research method

In our view, the study in no way supports the usefulness and necessity of a general obligation to retain data. Not for telephony, but certainly not for the internet. Rather than presenting an unequivocal, concrete, quantifiable added value of specific historic internet traffic data as a burden of evidence in legal cases involving serious crime, the report presents a list of wishes drawn up by unidentified 'police internet experts'.

The added value of available traffic data

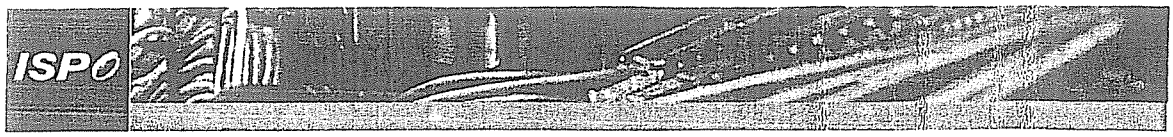
The study takes the position that there are only a few completed criminal cases available and that, for that reason, it has not been possible to answer the question of whether historic traffic data has been shown to have a direct or indirect importance with regard to evidence in criminal cases. The report is based on 65 cases which were pre-selected by the commissioning party - in other words, this was by no means a random representative sample. Although the study demonstrates that cases have been solved in which traffic data played a role, it leaves a great many questions unanswered: were there alternatives to the traffic data, did traffic data play an essential role in detection and prosecution?

Substantiation of the expansion of the obligation to retain data

In the providers' opinion, the report really falls down regarding the question of whether an expansion of the obligation to retain data would have had a positive effect on the course of the criminal investigation. The report uses the following example in support of a longer obligation to retain data.

In one of the cases investigated, the National Investigation Unit came across a completed drug shipment into which an extensive investigation had already been carried out. If the historic traffic data had been available at that moment covering a period of one year, in relation to the main suspect, it would have been possible, in all probability, to link the drug shipment in question with this suspect.

It will be clear that this observation on its own offers extremely weak substantiation of a far-reaching measure such as an expansion of the obligation to retain data. The other cases highlighted actually demonstrate that, for a large number of cases, there is no need whatsoever for an obligation to retain data. As the researchers argue that the usefulness and necessity of an obligation to retain traffic data cannot be demonstrated on the basis of these cases,



supplementary interviews were held with police and ministry of justice employees, who were involved in the cases referred to above and therefore cannot be objective.

The report says the following about the research method used:

"It is very much the question as to whether conclusions can be drawn, from the study into dossiers in which traffic data is lacking, regarding the effect that the presence of the traffic data would have had on the collection of evidence." (p.33)

and then:

"*No scientifically substantiated opinion can therefore be given with regard to the necessity on the part of the police... Furthermore, it is also the case that Internet Service Providers do not retain traffic data for the purpose of invoicing.*" (p.34)

Further conclusions of the Erasmus report

What is clear from the report is that crime investigators need clarity and unequivocalness regarding the obligation to retain data, so that they know what they can demand from the providers. It goes without saying that this observation cannot form a substantiation of the obligation to retain data. A possible solution to this would be to retain data for a short period.

It is also assumed in the report that demands by crime investigators would be more considered and specific if there were an obligation to retain data for a period of one year. This assumption is based on a presumption, and has not been proved by any research or fact. This assumption is, in fact, contradicted by the statement in the study that crime investigators would prefer to request a standard set of data. Requesting a standard set of data is anything but a considered and specific demand, and in the case of a longer obligation to retain data would only result in requests for more data.

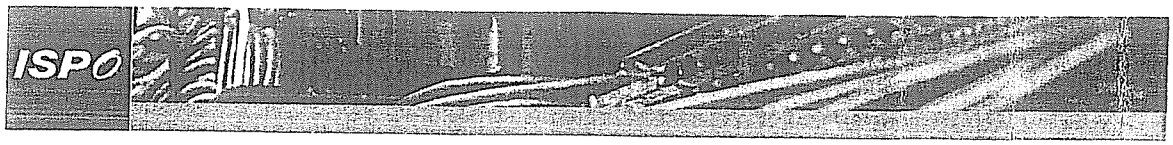
Additionally, the usefulness of a longer period of retention is debatable, given that the report shows that the collection of (extremely) large quantities of information is usually not important to solving a concrete criminal case. This is due to the limited manpower in the area of processing and analysis of the data and the political pressure to take on a large number of cases, which automatically results in limited time to carry out a study (p.39).

The only conclusion the Erasmus report could reach was that the usefulness and necessity of an obligation to retain data remains utterly unproven:

"*It has therefore not been possible to answer the question of whether historic traffic data is of direct or indirect importance to evidence in criminal cases.*" (p.37)

and:

"It must be stated emphatically that the question of whether an obligation to retain data for a specific period is desirable was only addressed in the study from the point of view of the requirements of criminal investigators." (p.37)



Technical impact

It also became apparent that the Erasmus report contains a large number of misunderstandings about the technical and practical feasibility. Up to now, these aspects have remained underexposed, partly because providers have barely been able to consult with the ministerial departments involved. A vivid example of this is the fact that

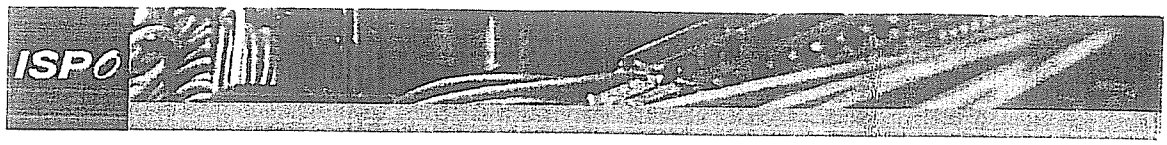
"The police have indicated that the possibilities currently offered under Section 126n/u of the Dutch Code of Criminal Procedure may not provide sufficient leads for crime investigation in future. In addition, experts have indicated that increasing use is being made of proxy servers located abroad. It is therefore important that rules be drawn up at the international level regarding obligations on retaining this data." (p.35).

An obligation to retain internet data is totally pointless if technical limitations such as these are not taken into account. You will find a more detailed explanation of the technical limitations in Appendix 1.

Economic impact

The economic damage that this poorly thought-out proposal will have on the entire sector, if all the 'wishes' in the report are granted, is incalculable. We expect that a small access and hosting provider, with approximately 1 GBit per second in data traffic, will need 1 Petabyte of storage space per year. On the basis of concrete quotations for a single provider, the initial investment will be approximately €7.5 million. In addition to this, there will be structural depreciation costs of €210,000 per month and operational costs of between €25,000 and €35,000 per month for staff and infrastructure (operational management, technical investigation and legal support, accommodation space, cooling and power requirements). For medium-large providers, these costs must be multiplied by a factor of 8, and for large providers by no less than a factor of 15. The cost estimate in the KPMG report of November 2004 is therefore inadequate. It only takes account of storage capacity, and not retrieval, security, etc. In addition, the quantity of Internet traffic on which KPMG has based its estimate has, in the meantime, increased by a factor of three, so that the costs of an obligation to retain data have also increased proportionately.

The sector has already had to make considerable investments in making and keeping its networks and services available for wiretapping. The Erasmus report shows that little or no use is made of the possibilities to tap individual suspects on the internet. While use of the Internet has increased explosively since 2002, this has apparently not resulted in court cases in which direct traffic data has played a convincing role as direct evidence. The lack of use of the current powers must not form a reason for the unlimited expansion towards powers to systematically monitor all Internet users.



Conclusion

We draw three conclusions from the Erasmus report:

1. The recommendation that an obligation to retain data for one year could be useful is in no way substantiated by the study.
2. Mr Donner, the Dutch Minister of Justice, has no insight whatsoever into the consequences of the obligation to retain data on Internet Service Providers, and appears to be deaf to the valid arguments of both the telephony and ISP sectors.
3. An obligation to retain data in the EU is pointless; the criminal investigation authorities will only be satisfied with a worldwide registration of each person's communication behaviour.

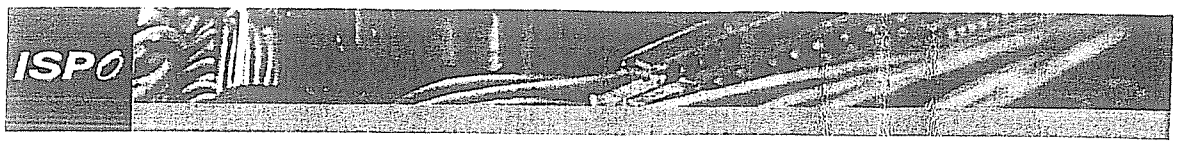
Another of our points is that it is amazing that the economic impact remains totally underexposed. At the very least, an impact analysis should be carried out into the economic effects of an obligation to retain data. This should at least include a calculation of what the consequences would be of an economic flight abroad of the current webhosting activities of Dutch and other European companies. An impact assessment should also be drawn up into the consequences of the argument put forward by Minister Donner that communication providers should not be compensated in any way for these investments, and therefore of the sharp increase in fees charged to consumers and a possibly dramatic reduction in freedom of choice.

The Upper and Lower Houses of the Dutch Parliament, as well as the European Parliament, have previously spoken out against the proposed obligation to retain data, due to the lack of substantiation of the usefulness, necessity and costs. In our eyes, this report does not add any value to this debate. The usefulness, necessity and proportionality of the obligation to retain data have still not been proven.

This is why we are urgently asking you not to approve any further steps in the European negotiations on this proposal before a further study into usefulness, necessity and proportionality, and before an economic analysis has demonstrated that the obligation to retain data has an added value, and that the economic damage is limited.

Appendix (1):

1 - Technical appendix



Appendix 1 - Technical supplement

Reliability of data

The internet providers cannot guarantee the accuracy and completeness of traffic data, or a correct traceability of an individual. This is a direct consequence of the extremely large data flows, which are continually at the limit of the technical possibilities, the de facto unreliable transport and processing mechanisms used, and the fact that logging data is primarily solely intended for technical diagnostics of the systems, and the services supplied through them.

The technology in this area is and remains extremely fallible. The current situation is, however, sufficient for the corporate objectives of the Internet providers. Another aspect is that traffic data can very easily be misinterpreted, as has been demonstrated in practice. This is partly due to the lack of sufficiently broadly accepted international standards in the area, as a result of which several hundred different storage formats are in use among Dutch Internet providers, each with its own specific interpretation of the stored data elements. The use of traffic data, referred to on p. 17, to get suspects to confess during an interview, or to identify them in court as 'apparently mendacious witnesses' is therefore, in our opinion, surrounded by extremely serious risks regarding correct and honest legal process.

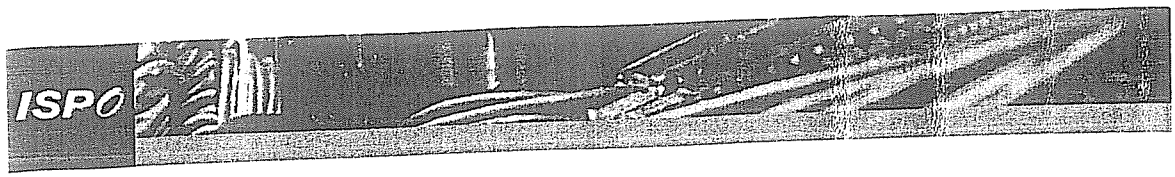
Technical impossibilities

It is indicated, for example, that what are known as A and B analyses must be able to be carried out on IP numbers. This means that an Internet provider must register for each customer which IP number is making contact with the computer(s) of the customer, and with which IP number the customer is making the connection.
Providers have no corporate objective whatsoever to record such a hyper-detailed profile for each customer, and do not see any physical means of recording it, other than by setting up a tap on the full content of all the traffic of each customer. The 'content' would then have to be removed from this tap. Such a tap would also contain all unwanted contacts established with a computer through the internet, such as port scans, viruses and spam.

In addition, a registration would also have to be made of how often and how intensively he or she uses external internet services such as Skype (free Voice over IP software), MSN (a Microsoft chat-like messenger service) and peer-to-peer exchange services such as KaZaa. But such software is positioned between the receiver and the sender. The provider therefore almost never sees the direct connection between the actual receiver and sender.

In the case of Skype, software that enables telephony over the internet, many people make use of what are known as supernodes (without being aware of this), to enable traffic to be sent to a different user, because the user's own private or business network does not permit direct external contacts for reasons of security, for example. Each PC on the internet with such software can call itself a supernode. (Again without the user knowing it). If the connection can be established directly, the call is established directly, but if this is not possible, the software immediately offers the use to a 'network hub'. As telephone calls are made on a public network, Skype uses heavy encryption as standard - 256 bit AES encryption. This keeps the volume of the communication at an even level as standard, so that the provider has no idea of the volume of the call or the number of parties involved.

MSN has a similar construction. All the chat traffic goes through MSN servers and not directly between the receivers. Only when exchanging files and webcam images can two people establish a direct connection between one another, but then only after an invitation is sent via the central server. Moreover, if one of the parties involved does not permit a direct connection (for security reasons), the exchange of files can be taken over by the central server. If criminal investigators are interested in information about the MSN use of a suspect, they would therefore initially have to approach this service, which is established in the US.



Internet as an international medium

The report almost totally ignores another technical development which would make an obligation to retain data in the Netherlands and the EU a disastrous undertaking. The internet is a global network, with innumerable useful internet services located outside Europe, such as anonymisation services such as TOR (http://tor.eff.org/) or the use of encryption techniques and tunnel methods to move data traffic outside the EU and thereby avoid the obligation to retain data. On p.35 of the report, it is suggested that the EU should put pressure on the rest of the world to ensure that all the communication behaviour of all internet users throughout the world be stored.

"The police have indicated that the possibilities currently offered under Section 126n/u of the Dutch Code of Criminal Procedure may not provide sufficient leads for crime investigation in future. In addition, experts have indicated that increasing use is being made of proxy servers located abroad. It is therefore important that rules be drawn up at the international level regarding obligations on retaining this data."

An obligation to retain data in the EU is therefore pointless; the criminal investigation authorities will only be satisfied with a worldwide registration of each person's communication behaviour.