



Eerste Kamer der Staten-Generaal
Commissie voor de JBZ-raad
Postbus 20017
2500 EA Den Haag

Verzonden per post en e-mail: griffie@eerstekamer.nl

Amsterdam, 20 juni 2005

Betreft: ontwerp kaderbesluit bewaarplicht verkeersgegevens

Geachte commissie-leden,

In uw commissie is verschillende keren gesproken over het ontwerp kaderbesluit voor een bewaarplicht voor verkeersgegevens. Naar aanleiding van de meest recente JBZ raad begin juni hebben de ondergetekende aanbieders begrepen dat het kaderbesluit voor het bewaren van verkeersgegevens niet in één keer maar in fases zal worden ingevoerd. Het is hierbij niet duidelijk geworden of deze verplichting door middel van besluitvorming in de eerste pijler of de derde pijler zal worden opgelegd.

Ondanks dit 'compromis' blijven aanbieders zéér bezorgd over de mogelijke inhoud van de besluitvorming en de gevolgde procedures. De belangen van de sector en die van consumenten lijken hierbij ernstig te worden geschaad. Omdat de besluitvorming ondoorzichtig blijft, is het voor ons van het grootste belang dat de geldende bezwaren van de sector – aanbieders van internet én telefonie - bij u bekend zijn. Graag brengen wij deze overwegingen en bezwaren in deze brief onder uw aandacht in het kader van het mondelinge overleg van de commissie met Minister Donner op 28 juni.

Uitstel betekent geen afstel

Besluitvorming over de bewaarplicht kan pas plaatsvinden op het moment dat er inzicht is over de nut, noodzaak, proportionaliteit en kosten van de bewaarplicht. Een eventuele fasering van de bewaarplicht doet daar niets aan af als dat betekent dat gegevens toch bewaard moeten worden, alleen pas later. De principiële bezwaren die al vele malen aan de orde zijn geweest blijven dus onverkort van kracht. Hiervoor verwijzen wij korthedshalve naar een brief van een groot aantal aanbieders van 13 december 2004 die als bijlage bij deze brief is toegevoegd.

Kosten van de bewaarplicht

Aanbieders zullen hoge kosten moeten maken om te voldoen aan de bewaarplicht. Zo worden gegevens over internet- en e-mailverkeer en over niet beantwoorde telefoonoproepen gewoonlijk niet opgeslagen omdat deze gegevens niet nodig zijn ten behoeve van normale bedrijfsvoering zoals facturatie.¹ Daarnaast valt te verwachten dat het aantal aanvragen van de autoriteiten fors zal toenemen en daardoor de administratieve en personele lasten: het ontwerp kaderbesluit maakt immers het 'grensoverschrijdend' opvragen van verkeersgegevens mogelijk.

Aanbieders zullen op meerdere fronten tot aanzienlijke investeringen worden gedwongen als gevolg van deze bewaarplicht. De huidige opslagcapaciteit van marktpartijen is immers niet afdoende. Partijen moeten investeren in apparatuur voor opslag van gegevens, maar ook in additionele software om gegevens te kunnen opzoeken en zullen er investeringen moeten worden gedaan in beveiliging van de data evenals in goed opgeleid personeel. Marktpartijen achten een dergelijke last voor de telecomsector volstrekt disproportioneel als niet alle gemaakte kosten worden vergoed.

Deze bezwaren zijn niet of nauwelijks onderzocht, ondanks het feit dat de sector hier meermalen om heeft verzocht. Desondanks is er per 1 april j.l. zonder enig overleg met aanbieders en zonder adequate toetsing van administratieve lasten een nieuwe kostenregeling in werking getreden die ook van toepassing zal zijn op het verstrekken van gegevens in het kader van de nieuwe bewaarplicht. De gangbare vergoedingen die tussen aanbieders en Justitie waren overeengekomen, zijn in deze nieuwe regeling op basis van normvergoedingen gedecimeerd. Als een aanbieder hogere kosten maakt dan de zeer lage normvergoedingen, dan kan hij deze alleen via een zeer bewerkelijk proces declareren. Zeer waarschijnlijk zal dan slechts een beperkt deel van de kosten worden vergoed. Een vergoeding van initiële investeringen is in deze regeling überhaupt niet aan de orde.

Aanbieders vragen zich af hoe het Ministerie van Justitie een ordentelijke uitvoering van de bewaarplicht door aanbieders kan garanderen zonder dat aanbieders worden vergoed voor alle investeringen en personele en administratieve kosten die zij maken. De bestaande kostenregeling moet daarom worden aangepast en uitgebreid met een vergoedingsregeling voor investeringen.

Geen overleg tussen sector en overheid

De betrokken Ministeries (Justitie en Economische Zaken) hebben, ondanks toezeggingen daartoe, nog steeds niet overlegd met marktpartijen over de uitvoering en gevolgen van een bewaarplicht. Verder zijn marktpartijen in het geheel niet betrokken bij het onderzoek van de Erasmus Universiteit naar nut en noodzaak van de bewaarplicht. Dit maakt de toegevoegde waarde van het onderzoek op zijn minst twijfelachtig. Alvorens verdere besluitvorming over de bewaarplicht plaatsvindt, moet constructief worden overlegd met betrokken partijen over nut, noodzaak en proportionaliteit van de bewaarplicht.

Aanbieders vragen u om bovengenoemde bezwaren aan de orde te stellen tijdens het mondeling overleg met de Minister op 28 juni. Het is cruciaal de genoemde bezwaren worden opgelost voordat nadere besluitvorming over de bewaarplicht plaatsvindt. Wij maken ons grote zorgen over de intransparante besluitvorming met betrekking tot dit onderwerp in Europees verband en in Nederland.

¹ Zie bijvoorbeeld de persverklaring van Eurocop (bijlage 2), de Europese organisatie voor politie medewerkers. Hierin wordt gesteld dat: 'Experts have raised serious doubts in relation to the technological ability to deal with the vast amount of data that will have to be stored if the directive is applied. Using current technology a simple search request is likely to take several years.'

De belangen van de sector en van consumenten dreigen ondergeschikt te worden aan een bewaarplicht voor verkeersgegevens waarvan nut en noodzaak niet zijn aangetoond.

De aanbieders zijn vanzelfsprekend graag bereid hun argumentatie persoonlijk toe te lichten. U kunt hiervoor contact opnemen met Bart Heinink (0628908201, bart.heinink@nl.wanadoo.com). Een afschrift van deze brief wordt verzonden aan vaste commissies van Economische Zaken en Justitie van de Tweede Kamer.

Mede namens,

BIT B.V.
BT Nederland N.V.
N.V. Casema
CAIW
COLT Telecom B.V.
Enertel N.V.
Essent Kabelcom B.V.
KPN Internet
Luna.nl B.V.
MCI Nederland B.V.
Priority Telecom Netherlands B.V.
THUS plc. (handelsnaam Demon)
Tiscali B.V.
UPC Nederland B.V.
Versatel Nederland B.V.
XS4ALL Internet B.V.

Met vriendelijke groet,



Bart Heinink
Regulatory Counsel

Wanadoo Nederland B.V.

Bijlage(n): open brief ISP's d.d. 13 december 2004
Persbericht Eurocop: 'Europe wide retention of telecommunications data unlikely to help law enforcement agencies in the fight against terrorism'

De ondergetekende internetaanbieders van Nederland maken zich grote zorgen over het Europese plan om alle gegevens over het telefoon- en internetverkeer van alle klanten minstens een jaar te bewaren. De Eerste Kamer overlegt hierover op 30 november met minister Donner van Justitie, de Tweede Kamer op 1 december. Dat plan heeft tenminste drie grote nadelen: het belemmert innovatie, schendt de privacy en brengt hoge kosten met zich mee. Het moet daarom alleen worden overwogen als er glasheldere bewijzen zijn dat het absoluut noodzakelijk is. Maar dat bewijs ontbreekt volledig. Minister Donner heeft onlangs toegegeven dat er geen serieus onderzoek is dat aantoont dat een bewaarplicht zou helpen bij de opsporing van strafbare feiten. Hij weigert bovendien om dergelijk onderzoek te laten uitvoeren, ondanks eerdere toezeggingen aan de Tweede Kamer. Daarom dringen de providers er bij de leden van de vaste kamercommissie Justitie op aan om de regering te verbieden akkoord te gaan zolang de noodzaak niet is aangetoond.

WAAROM ZIJN INTERNETAANBIEDERS TEGEN DE BEWAARPLICHT?

innovatie

Het voorgestelde besluit legt een hele zware hypotheek op de toekomst van de telecomindustrie. Innovatieve nieuwe communicatiediensten kunnen alleen uitgeprobeerd worden als ze op voorhand voldoen aan strenge opsporingseisen ten aanzien van aftapbaarheid en straks aan de bewaarplicht verkeersgegevens. Dat is in volstrekte tegenspraak met het belang dat de overheid zegt te hechten aan innovatieve nieuwe breedbanddiensten voor de ontwikkeling van Nederland als kenniseconomie. Bovendien blijkt uit de praktijkervaring met de aftapverplichting dat de overheid haar eisen voortdurend bijstelt, waardoor providers telkens nieuwe investeringen moeten doen. Providers staan hierdoor voor een onmogelijke bedrijfseconomische opgave.

privacy

Iedereen maakt zich zorgen over terrorisme en criminaliteit. Daders moeten niet met een beroep op privacy aan opsporing kunnen ontkomen. Er zijn echter al heel veel opsporingsbevoegdheden, ook op internet. Verkeersgegevens zeggen heel veel over wie wij zijn en wat wij doen en denken. De nu voorgestelde bewaarplicht richt zich niet alleen op daders of verdachten, maar op iedere internetter, verdacht of niet. Er wordt een enorme vergaarbak aan privacygevoelige gegevens gecreëerd. 99% daarvan is afkomstig van onschuldige burgers. De voorgestelde bewaarplicht is zo onbegrensd en breed, dat het niet verbaast dat tal van juridisch deskundigen aangeven dat hiermee de grenzen van grondwet en internationale mensenrechtenverdragen worden overschreden. De bewaarplicht verkeersgegevens lijkt het sluitstuk van de overheidswens om providers in te zetten als hulpofficieren van justitie. Providers moeten al volledig aftapbaar zijn, en sinds 1 september 2004 elke opsporingsambtenaar desgevraagd allerlei informatie over klanten geven. De minister van Justitie verwacht dat er in totaal 900.000 keer per jaar naam, adres- en rekeninggegevens worden opgevraagd over bellers en internetters. Binnenkort komt er nog een nieuwe verplichting bij; om gegevens over specifieke verdachten 3 maanden lang te bevriezen en te bewaren. Het feit dat providers straks het gedrag van alle internetters systematisch moeten gaan afluisteren en in de gaten houden leidt ertoe dat internet een onveilig communicatiemiddel wordt, waarbij het grote publiek onnodig bang wordt gemaakt dat elke muisklik tot een verdenking kan leiden.

kosten hoog en onbegrensd

Het invoeren van een bewaarplicht verkeersgegevens vergt grote investeringen in mensen en middelen, in totaal naar verwachting vele miljoenen euros. De precieze kosten zijn nog onbekend omdat de verplichting nog niet precies is gedefinieerd. Er is ook geen enkel onderzoek gedaan naar de mogelijke kosten. Dat maakt een goede kosten-baten analyse uiteraard onmogelijk. Wel is duidelijk dat de consument uiteindelijk de rekening betaalt voor de ongewenste opslag van zijn eigen verkeersgegevens. Het gaat namelijk om zeer grote hoeveelheden informatie. Een doorsnee breedbandprovider met 100.000 klanten vervoert snel 5,5 Terabyte per dag, dat wil zeggen, 8.500 CD's per dag. Uit deze

verkeersstroom moeten de verkeersgegevens gedestilleerd worden, en opgeslagen in hele dure, zeer streng beveiligde, dubbel uitgevoerde databases om per klant te kunnen terugzoeken hoe lang iemand online is geweest, wat voor e-mail iemand heeft verstuurd en/of ontvangen en welke websites iemand heeft bekeken. In 2002 hebben internetaanbieders al enorme investeringen moeten doen om hun netwerken en diensten aftapbaar te maken. Hiervan heeft de overheid niets vergoed, ondanks massaal protest. De concurrentiepositie van Nederland en Europa staat hoog op de politieke agenda. Het is daarom een raadsel waarom het bedrijfsleven nu in alle haast en zonder gedegen onderzoek wordt opgezadeld met zeer hoge administratieve lasten.

uitvoerbaarheid

Over de uitvoerbaarheid van de bewaarplicht in de internetwereld lijkt nauwelijks nagedacht. In tegenstelling tot telecomaandieners houden internetproviders nauwelijks gegevens bij. Klanten betalen niet per e-mail of per bezochte website. Er is dus geen enkel bedrijfsbelang om dat soort gegevens te bewaren. Over het individuele surfgedrag is bij de meeste providers al helemaal niets bekend; omdat het om zeer privacy-gevoelige informatie gaat, die alleen met behulp van ingewikkelde filtersystemen kan worden vastgelegd. Dergelijke filters brengen bovendien de snelheid van het verkeer in gevaar. De overheid lijkt blind voor de werkelijkheid op internet; meer dan de helft van het e-mail verkeer bestaat uit spam en virussen. Ook al die rommel zouden providers moeten gaan bewaren, terwijl het opsporingsnut miniem is.

WAAROM IS DE NOODZAAK VOOR EEN BEWAARPLICHT NIET AANGETOOND?

Politie en justitie beschikken al over een groot arsenaal opsporingsmiddelen. Er is geen bewijs dat de beschikbare middelen onvoldoende zijn, of dat er strafbare feiten onopgelost zijn gebleven door het ontbreken van een bewaarplicht. In tegendeel, het enige beschikbare onderzoek (door de politie Rotterdam) wijst op het tegendeel. Ondanks toezeggingen aan de Tweede Kamer weigert minister Donner om nieuw onderzoek uit te laten voeren om de noodzakelijkheid te onderbouwen.

WAT MOET HET PARLEMENT DOEN?

Kennelijk is de regering er op uit om het voorstel nog voor het einde van het voorzitterschap van Europa door te drukken. Op 2 en 3 december vergadert de Europese raad van ministers van Justitie en Binnenlandse Zaken over het voorstel. Omdat het hier gaat om een bindend Kaderbesluit zijn de besprekingen op 30 november en 1 december in feite de laatste kans voor het Nederlandse parlement om invloed uit te oefenen. De internetproviders zijn van mening dat met de verdere bespreking van het voorstel moet worden gewacht tot dat er gedegen onderzoek is gedaan naar de noodzaak van een bewaarplicht en de kosten die ermee gemoeid zijn. Alleen als die gegevens op tafel liggen, kan de politiek een goede afweging maken.

PRESS STATEMENT European Confederation of Police

Responsible: Jan Velleman ☎ +352/43 49 61-22 ☎ +352/43 49 61-33 jv@eurocop-police.org EURO COP – 617, rue de Neudorf – L-2220 Luxembourg mobile: +49 174 20 29 033

Luxembourg, 2 June 2005

Europe wide retention of telecommunications data unlikely to help law enforcement agencies in the fight against terrorism

EuroCOP President Heinz KIEFER concerned over unsolved technical questions

In a first reaction towards the draft of a new EU framework directive on the retention of telecommunications data to boost the EU wide fight against crime and terrorism, Heinz KIEFER, President of the European Confederation of Police, EuroCOP, says he is sceptical as to whether this will actually help criminal investigations.

Experts have raised serious doubts in relation to the technological ability to deal with the vast amount of data that will have to be stored if the directive is applied. Using current technology a simple search request is likely to take several years. This significantly reduces the possible benefits to investigators who simply cannot afford to wait this length of time for the results of a phone number search.

Even if huge investments were made to speed up the researching process it remains easy for criminals to avoid detection through fairly simple means, for example mobile phone cards can be purchased from foreign providers and frequently switched. 'The result would be that a vast effort is made with little more effect on criminals and terrorists than to slightly irritate them', says Mr. KIEFER. 'Activities like these are unlikely to boost citizens' confidence in the EU's ability to deliver solutions to their demand for protection against serious crime and terrorism.'

While the new possibilities offered by IT technology require law enforcement services to rethink the way they investigate, it is necessary to clearly assess whether these technologies have reached a stage of development where they are able to offer actual benefits. Mr KIEFER: 'The EU has committed itself to a programme of 'better governance' when the new Commission took office. I am afraid that the draft framework directive on the retention of telecommunications data is not an example of this new approach.'

The European Confederation of Police, EuroCOP, is the umbrella organisation of 27 national Police Unions and Staff Organisations from 19 European States. It represents the interests of over 600.000 police officers in Europe. www.eurocop-police.org.