



Verslag Bits of Freedom
van
Informatiemiddag bewaarplicht 14 oktober 2009

**nog veel onduidelijkheid in bewaarplichtdossier
privacy in gevaar door plannen voor centrale opslag en bevraging**

15 oktober 2009

Inleiding en samenvatting

1. Op 14 oktober 2009 vond in Amersfoort de 'Informatiemiddag bewaren telecommunicatiegegevens' plaats. Hier is door verschillende overheidsinstanties toegelicht hoe zij de Wet bewaarplicht telecommunicatiegegevens (“**Dataretentiewet**”) technisch willen implementeren. De digitale burgerrechtenbeweging Bits of Freedom was hierbij aanwezig. Hieronder volgt een verslag van deze middag.
2. De hoofdconclusie is dat – hoewel er nog veel onduidelijkheid is in het bewaarplicht-dossier – de gepresenteerde plannen, in het bijzonder de gedachte om het Centraal Informatiepunt Onderzoek Telecommunicatie (“**CIOT**”) een centrale rol te geven bij de opslag en bevraging van verkeersgegevens, ernstige risico's voor de privacy met zich brengen:
 - De overheid voorziet een centrale rol van CIOT bij de opslag en bevraging van verkeersgegevens in de toekomst;
 - Het Ministerie van Binnenlandse Zaken wil, zo lijkt het, marktwerking introduceren bij het “assisteren” van aanbieders om te voldoen aan bevragingsverzoeken door opsporingsdiensten, en overweegt bedrijven dus een belangrijke overheidstaak te laten uitvoeren;
 - Het Agentschap Telecom heeft nog onvoldoende zicht op welke categorieën aanbieders onder de bewaarplicht vallen, en dit creëert onduidelijkheid voor betrokken partijen; en
 - Bij het ontwikkelen van technische standaarden voor de implementatie van de bewaarplicht door ETSI, wordt rekening gehouden met het opslaan van gegevens die niet onder de bewaarplicht zouden moeten vallen, zoals e-mailheaders en IPTV-gegevens.
3. Met name de mogelijke plannen om het CIOT een centrale rol te geven bij de bevraging en opslag van verkeersgegevens zouden zeer onwenselijk zijn, omdat uit het audit-rapport uit 2007 en 2008 van het CIOT blijkt dat reeds nu bij bevraging via het CIOT de bestaande juridische waarborgen onvoldoende worden nageleefd. Er is op dit moment geen enkele garantie dat het CIOT deze waarborgen wel zou naleven, als haar taken veel verder zouden worden uitgebreid.
4. Bits of Freedom zal tijdens de volgende consultatie over historische gebruiksgegevens op 22 oktober in Utrecht verder pleiten voor een systeem met voldoende technische waarborgen tegen onbevoegd gebruik.

Introductie (Van Dongen): overheidsbeleid nog onzeker

5. De informatiemiddag werd geopend met een kort welkomstwoord door dagvoorzitter Hellen van Dongen, plaatsvervangend directeur Telecommunicatie van het Ministerie van Economische Zaken.

6. Nadat zij de grote opkomst voor de middag had genoteerd en het publiek had medegedeeld dat dit dossier altijd al beheerst werd door “emotie”, gaf zij aan dat veel van wat de toeschouwers gingen horen nog onzeker is, dat er nog veel te bepalen is en dat toeschouwers nog gelegenheid krijgen om hun zienswijze naar voren te brengen. Zij gaf aan dat zij vandaag niet over nut en noodzaak van de wet wilde hebben. De presentaties zouden de contouren aangeven van nieuw overheidsbeleid.

Toelichting wetsgeschiedenis (Stap): verkeersgegevens niet noodzakelijk, wel nuttig

7. De eerste inhoudelijke spreker van de middag, Bob Stap van het Ministerie van Justitie, lichtte de parlementaire behandeling van de Wet bewaarplicht telecommunicatiegegevens toe.
8. Een opmerkelijke bijdrage, nu Stap openlijk toegaf dat telecommunicatiegegevens niet noodzakelijk zijn om het bewijs rond te krijgen: “zijn de gegevens noodzakelijk? Nee. Zijn ze nuttig? Ja. Met name in het kader van de opbouw en richting van het opsporingsonderzoek.” Dit is relevant, omdat volgens vaste jurisprudentie van het Europees Hof voor de Rechten van de Mens een inperking van de privacy pas toelaatbaar is, als deze noodzakelijk is: het is onvoldoende als deze slechts 'nuttig' is.
9. Stap bleek uit te gaan van een in de parlementaire behandeling geslopen misvatting over de strafvorderlijke bevoegdheden van opsporingsdiensten. Opsporingsdiensten zouden slechts toegang hebben tot verkeersgegevens, indien er sprake is van een verdenking van een strafbaar feit waarop een maximale gevangenisstraf van vier jaren of meer is gesteld. Dit is niet juist, omdat ook in het kader van minder zware delicten deze bevoegdheden gelden (bijvoorbeeld ook bij triviale delicten als “het gebruiken van een hond als trekkracht”, zie art. 67 lid 1 sub b en sub c Wetboek van Strafvordering).
10. Verrassend was ook de van opmerking van Stap, over de “beeldvorming door de hoogleraren, die politiek hebben bedreven” door in een tweetal opiniestukken in de krant hun zorgen over dataretentiewetgeving te uiten. Volgens Stap was hun bijdrage politiek getint, en “niet op argumenten gebaseerd”.
11. Tot slot stelde Stap dat het bewaren van en de toegang tot telecommunicatiegegevens is omgeven met strikte wettelijke waarborgen. “Wij doen ons best ons daaraan te houden, anders worden wij afgestraft door de rechter.” Dit wekt volgens Bits of Freedom de onterechte suggestie dat reprimandes achteraf voldoende zijn om naleving van juridische waarborgen te garanderen. Dat is onjuist: het is noodzakelijk om waarborgen in het systeem op te nemen die onrechtmatige bevraging vooraf onmogelijk maken. Zonder die waarborgen gaat het in de praktijk mis, zoals blijkt uit het onlangs openbaar geworden “Eindrapport Audit CIOT 2008” (zie onder, te vinden op: <https://rejo.zenger.nl/focus/1253127301.php>).

Vergoeding kosten (Bruinsma): overheid wil markt voor opvraging verkeersgegevens

12. In de tweede presentatie, verzorgd door Joost Bruinsma van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, stond de vergoeding van de door aanbieders gemaakte kosten centraal.

13. De presentatie van Bruinsma wekte de suggestie dat de overheid hoopt dat er een markt ontstaat voor het bemiddelen tussen bevragingen door opsporingsdiensten en verstrekking door aanbieders. De overheid weet echter nog niet precies wat ze gaat doen: het plan om voort te borduren op een reeds bestaand zogenoemd “dienstverlenermodel” (waarvan niet duidelijk werd wat dit inhoudt) werd gepresenteerd als een “denkrichting.” Een aantal vragen uit de zaal gaf wel iets meer duidelijkheid. Zo moet het begrip 'dienstverlener' begrepen worden als een intermediair tussen aanbieder en opsporingsdiensten, hoogstwaarschijnlijk een marktpartij, bij wie aanbieders zich kunnen aansluiten om hun kosten te beperken. Aanbieders zullen alleen de administratieve- en personeelskosten vergoed krijgen, en investerings- of opslagkosten zullen in principe niet vergoed worden. Het is duidelijk dat, mocht het voornemen om bedrijven zo een belangrijke overheidstaak te laten uitvoeren doorgaan, dit extra privacyrisico's met zich zou brengen.

Rol toezichthouder (Oosthoek): onduidelijk wie onder bewaarplicht valt

14. Aad Oosthoek van het Agentschap Telecom (“**Agentschap**”) ging dieper in op de rol van de toezichthouder bij de naleving van de wettelijke verplichtingen door aanbieders.
15. Het bleek onduidelijk welke categorieën aanbieders nu onder de wettelijke bewaarplicht vallen. Het Agentschap beraadt zich bijvoorbeeld nog over de vraag of webhosting service providers hieronder vallen (zij bieden vrijwel altijd e-maildiensten aan). Oosthoek kon over dergelijke technische aangelegenheden geen zekerheid bieden, waarop een aanbieder opmerkte dat hij zojuist een nieuwe broek had gekocht, “omdat ik uit de vorige ben gescheurd vanwege de spagaat waar jullie mij in dwingen. Moet ik wel of niet bewaren?” Het Agentschap beloofde binnenkort met een “definitielijst” te komen, en die zou aanbieders meer houvast moeten bieden.
16. Daarnaast was de aangekondigde coulance van het Agentschap in het eerste toezichtjaar opvallend. Daaruit blijkt dat aanbieders noch toezichthouders klaar zijn voor handhaving van de bewaarplicht in de praktijk.

Bevragen historische gegevens (Mook en Bladder): “business cases” richting centrale opslag

17. De lezingen van Jan Pieter Mook en Rene Bladder, respectievelijk werkzaam bij het Ministerie van Justitie en het CIOT, gingen in op het door opsporingsdiensten bevragen van historische verkeersgegevens (Mook) en historische gebruiksgegevens (Bladder). Beide lezingen waren ronduit verontrustend vanuit het perspectief van privacy.
18. Het Ministerie van Justitie en het CIOT pleitten voor een volledig geautomatiseerde bevraging van alle telecommunicatiegegevens via het “doorgeefluik” CIOT, zowel voor wat betreft historische gebruiksgegevens als verkeersgegevens. Dit zou geïmplementeerd worden door wijziging van het Besluit verstrekking gegevens telecommunicatie.
19. Dat zou ernstige risico's voor de privacy van telecomgebruikers met zich brengen. Er kan worden vastgesteld dat de nu al geldende waarborgen voor de bescherming van privacy, onvoldoende worden gerespecteerd. Dit bleek uit de analyse van Bits of Freedom van het audit rapport van het CIOT van 2008: zo vergaten opsporingsambtenaren een proces

verbaal op te maken, worden PIN-codes uitgewisseld en worden privacy-beschermende maatregelen gezien als “administratieve last” (zie de nieuwsbrief van Bits of Freedom van 13 oktober 2009, te vinden op: <http://www.bof.nl/nieuwsbrief131009.txt>).

20. Efficiëntie en effectiviteit lijken zwaar te wegen bij deze plannen, die steeds als “business cases” gekarakteriseerd werden. Het vergroten van de bevoegdheden van “gegevensmakelaars” als het CIOT bespaart volgens de sprekers geld en tijd.
21. Bladder maakte melding van een aanstaande consultatie over de “business case” inzake historische gebruiksgegevens op 22 oktober a.s in Utrecht, en nodigde allen, waaronder Bits of Freedom, expliciet uit om daarbij aanwezig te zijn. Hoewel werd aangegeven dat privacy steeds “een issue” was, lijken vertegenwoordigers van het privacybelang voorheen nooit actieve medespelers bij het voorbereiden van deze “business cases” geweest – bijvoorbeeld door deel te nemen aan de stuurgroepen die beslissen of de maatregelen wel of niet worden uitgevoerd. Sinds het “CBP zich heeft teruggetrokken uit dit domein”, is er evenmin sprake van advisering over privacyvraagstukken voorafgaand aan het nemen van beslissingen door zulke stuurgroepen. Bladder verwachtte bij een “Go” van de “business case” een implementatie bij “gegevensmakelaar” CIOT in december.
22. De presentatie van met name Bladder leidde tot veel reacties van het publiek. Bits of Freedom benadrukte in haar reactie dat het opsporingsbelang een legitiem belang is, maar zij vroeg tegelijkertijd aandacht voor de zorgwekkende bevindingen uit het audit rapport van het CIOT van 2008. Er blijkt een grote afstand tussen wettelijke voorschriften en de praktijk, terwijl de overheid niet geneigd is om transparant te zijn, bijvoorbeeld ten aanzien van (on)rechtmatigheid van de bevragingen of de effectiviteit daarvan. Bits of Freedom pleitte dan ook voor het inbouwen van technische maatregelen in het nieuwe systeem om deze inbreuken onmogelijk te maken.
23. Bladder reageerde op de inbreng van Bits of Freedom door te stellen dat er sprake was van een “éenzijdige belichting van het verhaal” en een “kennisachterstand” door Bits of Freedom. Volgens Bladder is “één onrechtmatige bevraging op de meer dan drie miljoen niet zoveel”. Deze laatste stelling is een mislezing van de bevindingen van de audit, aangezien er geen kwantitatieve analyse van onrechtmatige bevragingen gegeven wordt in het rapport. Daarentegen maakt de audit melding van het ontbreken van systematische- of periodieke controle op de bevragingen in zowel 2007 als 2008.
24. Toen Bits of Freedom vervolgens wilde reageren werd zij afgekappt door de dagvoorzitter met de mededeling: “dit is een bijeenkomst voor aanbieders. De uitnodiging van het CIOT is door Bits of Freedom geaccepteerd, we moeten nu verdere met de volgende vraag.” Hoewel Bits of Freedom bij de afsluitende borrel werd medegedeeld dat zij toch niet welkom was op de bijeenkomst op 22 oktober, gaat zij ervan uit dat dit op een misverstand berust. Zij heeft een open brief geschreven aan het CIOT waarin zij haar aanwezigheid voor de goede orde bevestigt.
25. De volgende vraag van een aanbieder haakte in op de door Bits of Freedom aan de kaak gestelde afstand tussen wet en praktijk: “shouldn't you fix your problems, before starting new ones?” Een andere aanbieder wees zijn collega's erop dat zij niet hoeven mee te werken om een uitbreiding van het CIOT: “let op, de wettelijke voorschriften daargelaten, zijn jullie niet

verplicht om aan dit soort uitbreidingen van het CIOT mee te werken. Het hoeft dus niet.” De vraag is wat voor met name kleine aanbieders zwaarder weegt: kostenreductie (uitbreiding CIOT) of het beschermen privacybelang van hun gebruikers (inperking CIOT).

Europese standaardisatie (Van der Arend): standaardisatie moet bevraging mogelijk maken

26. Volgend op deze meer bestuurlijke aspecten van de bewaarplicht, volgde een presentatie van Peter van der Arend, voorzitter Lawful Interceptions van het Europees Telecommunicatie en Standaardisatie Instituut (“ETSI”).
27. ETSI is belast met het ontwikkelen van specifieke protocollen voor deze automatische bevragingen van telecommunicatiegegevens, omdat het anders “een puinhoop” wordt. ETSI is een club waar deelnemers uit verschillende landen in zitting nemen. Nederlandse deelnemers zijn alle grote operators, alsmede de Ministeries van Economische Zaken, Binnenlandse Zaken en van Justitie.
28. Uit de presentatie bleek dat Van der Arend “alle mogelijkheden die leden willen zien” onderdeel laat uitmaken van de dataretentiestandaard. Uit de presentatie en de antwoorden bleek dat e-mail headers en IPTV (die niet onder de bewaarplicht zouden moeten vallen) ook binnen de standaard kunnen vallen. Van der Arend grapte: “als de Amerikanen dat willen.”

Einddiscussie en commentaar: centrale opslag wordt serieus overwogen, onduidelijkheid blijft

29. Tijdens de einddiscussie kwamen nog enkele belangrijke thema's aan het licht, zoals het eigenaarschap van de data en de aansprakelijkheid in verband daarmee.
30. Bits of Freedom vroeg “namens de aanbieders” (omdat haar eerder was verweten dat zij geen “aanbieder” was) of de geschetste ontwikkelingen zich richting centrale opslag van telecommunicatiegegevens zouden begeven. Bladder knikte, en antwoordde: “als Bits of Freedom dat namens de aanbieders wil, dan vind ik dat prima.” Maar het cryptische vervolgantwoord van de dagvoorzitter luidde, dat het antwoord op deze vraag al genoeg “uit de presentaties moest blijken”. Bits of Freedom constateert dat centrale opslag serieus wordt overwogen en zal dit zeer kritisch blijven volgen, vooral nu is gebleken dat er in de praktijk het nodige fout gaat bij de reeds in werking zijnde 'light'-versie van het CIOT.
31. Centrale opslag zou bijzonder onwenselijk zijn, omdat het een vergaande erosie van het grondrecht op privacy tot gevolg zou hebben. Nu bevinden telecommunicatie-gegevens zich nog in de meer dan 300 databases van de Nederlandse aanbieders, die verantwoordelijk en aansprakelijk zijn voor die data, en vanuit bedrijfsoverwegingen het privacybelang van hun klanten beschermen. Bij centrale opslag hoeft de overheid slechts één database te bevragen, terwijl bovendien alle gegevens eenvoudiger gekoppeld kunnen worden. De mogelijkheden van profilering worden daardoor verder uitgebreid. Bovendien leert de praktijk dat de overheid intransparant is, als het gaat om het aantal bevragingen van verkeersgegevens en de effectiviteit van die bevragingen (deze informatie wordt aangemerkt als staatsgeheim, en is daarom niet openbaar).
32. Na afloop vroegen meerdere mensen zich af wat men nu precies wijzer was geworden van

deze informatiebijeenkomst. Er zijn geen goede antwoorden gegeven op de vragen die zijn gesteld, terwijl de presentaties aanleiding gaven tot toenemende verwarring en zorg over mogelijke verrassingen die implementatie van de bewaarplicht nog in petto heeft. Termen als “business cases”, “gegevensmakelaars”, “denkrichtingen”, “koppelvlakken” en “automatiseringsprocessen” maakten het niet duidelijker.

33. Bits of Freedom onderschrijft dat het belang van opsporingsdiensten bij inzage in telecommunicatiegegevens een legitiem belang is. Maar de maatregelen waarmee dit belang wordt gewaarborgd, dienen steeds in overeenstemming te zijn met de fundamentele rechten en vrijheden van iedere burger, zoals neergelegd in internationale verdragen en de Nederlandse Grondwet. De betrokken organen lijken de juridische complexiteit van privacybescherming en de administratieve lasten die privacy met zich brengt, echter als grote drempel te ervaren. En als zulke belangrijke onderwerpen als kosten, definties, toezicht, bevraging en (de)centrale opslag niet in de wet geregeld worden, leidt dit tot verwarring en onzekerheid bij lagere overlegorganen (de informatiemiddag was hiervan een duidelijk voorbeeld). Juridische en technische waarborgen die privacy moeten beschermen worden daardoor genegeerd of onjuist geïmplementeerd.

Over Bits of Freedom

34. De Stichting Bits of Freedom verdedigt burgerrechten in de digitale wereld, waaronder het recht op privacy. De organisatie staat onder leiding van Ot van Daalen. Het bestuur van Bits of Freedom bestaat uit Doke Pelleboer (ex-directeur van XS4ALL), Joris van Hoboken (onderzoeker bij het Instituut voor Informatierecht van de Universiteit van Amsterdam) en Karianne Thomas (advocaat bij advocatenkantoor Van Doorne).

* * *