Reactie Vodafone op internetconsultatie Wet op de Inlichtingen en Veiligheidsdiensten 20XX
1 september 2015

Deze reactie is openbaar en ingediend via: http://www.internetconsultatie.nl/wiv

Uw ministerie heeft belanghebbenden in de gelegenheid gesteld om een reactie in te dienen op de ter consultatie neergelegde concept-wetsvoorstel Wet op de Inlichtingen en Veiligheidsdiensten 20XX van 2 juli 2015 (zie http://www.internetconsultatie.nl/wiv). Vodafone Libertel B.V. ("Vodafone") dankt u voor deze gelegenheid.

Vodafone sluit zich aan bij de schriftelijke reactie die Nederland ICT op dit concept-wetsvoorstel heeft gegeven. In aanvulling hierop hebben wij de onderstaande opmerkingen.

De concept-wet moet veel duidelijker

De concept-wet en de memorie van toelichting zijn zeer onduidelijk over de reikwijdte van de bevoegdheden van de diensten, de verplichtingen van bedrijven om medewerking te verlenen, welke bedrijven hiermee te maken zullen krijgen, de te verwachten kosten en wie welk deel van die kosten dienen te dragen.

Transparantie, vertrouwen en toezicht

Vodafone is de afgelopen jaren in toenemende mate door consumenten en bedrijven verzocht meer openheid te geven over de mate waarin en de wijze waarop wij medewerking verlenen aan verzoeken van opsporings-, veiligheids- en inlichtingendiensten. Het ministerie van BZK geeft deze transparantie voor inlichtingen- en veiligheidsdiensten zelf niet en kwalificeert bovendien zelfs geaggregeerde tapstatistieken als staatsgeheim, zodat ook bedrijven niet transparanter kunnen zijn.

Het Ministerie van Justitie heeft ons laten weten dat het openbaren van dergelijke statistieken door telecombedrijven, voorzover het de opsporingsdiensten betreft, weliswaar niet verboden is, maar doet een klemmend beroep op telecombedrijven om deze gegevens niet te openbaren omdat het de opsporing zou kunnen schaden.

De zorgen van klanten over de veiligheid van gegevens worden door het gebrek aan publieke informatie over de activiteiten van de betreffende diensten niet geadresseerd. Dit tast het vertrouwen van zowel consumenten als bedrijven in telecomvoorzieningen onnodig aan. Daarnaast is onafhankelijk en effectief toezicht op de activiteiten zonder adequate informatie niet goed mogelijk en zijn er vanuit diverse hoeken grote vraagtekens gezet bij de grondwettelijke legitimiteit.

Wij zijn van mening dat transparantie ook sterk zou kunnen worden verbeterd zonder de effectiviteit van de diensten te schaden en menen dat het primair de verantwoordelijkheid van overheid is om die transparantie te bieden. Zie voor een uitgebreide beschouwing van de dilemma's en onze positie hierin het Vodafone Law Enforcement Disclosure Report 2015.

Doordat bevoegdheden en medewerkingsplichten met de concept WIV20xx vrijwel onbeperkt worden uitgebreid, zonder daarbij transparantie en toezicht te versterken, beweegt Nederland precies in omgekeerde richting van bijvoorbeeld de Verenigde Staten.

Wij verzoeken u in uw overwegingen de volgende zaken mee te nemen:

- De reikwijdte van de wet te verduidelijken en nader te onderbouwen waarom die reikwijdte passend is (of beperken als deze niet passend blijkt te zijn)
- Ter harte nemen van de Ten Standards for Oversight and Transparancy for National Intelligence Services, Institute for Information Law
- Lessen te trekken uit de ontwikkelingen in de VS, waar bevoegdheden juist weer worden beperkt en momenteel veel aandacht is voor toezicht op de diensten.
- In samenwerking met bedrijven, experts, ministeries van V&J en EZ verbeterde transparantie voor publiek en toezicht, ook betreffende verwante bevoegdheden uit de telecommunicatiewet en het Wetboek van Strafvordering, nader vorm te geven.
- Efficiënte en proportionele inzet van middelen te bevorderen door de betreffende diensten zelf de kosten te laten dragen van de inzet van hun bevoegdheden.

Uiteraard zijn wij graag bereid onze visie nader toe te lichten.

Tele2 Nederland B.V.
Postbus 22697
1100 DD Amsterdam
Phone +31(0)20 750 10 00
tele2.nl

Kvk Amsterdam 33303418
Tele2 is een handelsnaam
van Tele2 Nederland B.V.

Diemen, 27-8-2015

Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties en Ministerie van Defensie

Betreft: Internetconsultatie Wet op de inlichtingen- en veiligheidsdiensten 20XX

Geachte heer, mevrouw,

Tele2 Nederland B.V. dankt u voor de mogelijkheid om in dit vroege stadium commentaar te mogen geven op het voorstel voor de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten. Tele2 gaat ervan uit dat de betrokken ministeries de structurele juridische en praktische problemen die nu in het wetsvoorstel zitten (zoals in deze reactie nader toegelicht) zullen adresseren en een gewijzigde versie nogmaals ter consultatie zullen aanbieden.

De consequenties van de voorgenomen maatregelen zullen volgens Tele2 als volgt zijn:

- De Inlichtingen- en veiligheidsdiensten slachten "de kip met gouden eieren", namelijk de randvoorwaarden die maakten dat klant- en bedrijfsgegevens die voordien als veilig mochten worden verondersteld en waardoor Nederland een aantrekkelijke (digitale) vestigingsplaats is geworden.. Door zichzelf vrijwel onbeperkte toegang tot communicatie en databases zorgen veiligheidsdiensten ervoor dat het klimaat voor bedrijven om zich in Nederland te vestigen vanuit een financieel, privacy en beveilingsperspectief onhoudbaar wordt.
- Ieder bedrijf of maatschappelijke organisatie (ongeveer 360.000 volgens het CBS) welke in Nederland actief is zal, gegeven de definitie van "aanbieder van communicatiediensten" zijn of haar databases doorzoekbaar en het netwerk aftapbaar moeten maken en de kosten hiervoor zelf moeten dragen. De vraag dient zich aan in hoeverre Nederlandse en buitenlandse bedrijven, in de wetenschap dat ze onevenredig veel tijd, geld en energie zullen moeten spenderen om de gewenste doorzoekbaarheid en aftapbaarheid te realiseren, Nederland nog als aantrekkelijk vestigingsland zullen aanschouwen. Ditzelfde geldt uiteraard voor klanten van deze bedrijven die, indien zich een vergelijkbaar alternatief voordoet dat niet gebonden is aan fysieke grenzen (lees: internet) besluiten deze af te nemen indien deze onder een minder stringent wettelijk regime vallen.
- Er zal geen enkel onderdeel van de Nederlandse maatschappij zijn, dat niet onder de reikwijdte van de (bulk)interceptie Inlichtingen- en veiligheidsdiensten zal vallen. De wet ademt de sfeer uit dat het verkrijgen van bulkgegevens een doel op zich is, waarbij het beschikken over en het inzage hebben in volledig buiten de feitelijke eigenaar van de gegevens om plaats vindt. De effectiviteit en daarmee subsidiariteit en proportionaliteit zijn gemakshalve buiten beschouwing gelaten.
- Nederlandse Inlichtingen- en veiligheidsdiensten krijgen de mogelijkheid om bevriende Buitenlandse inlichtingendiensten vrijelijk te voorzien van informatie (waaronder verkeers- en verbruiksgegevens van individuele klanten) zonder enige vorm van toezicht.

Een aantal wijzigingen ten opzichte van de huidige WIV 2002 leiden tot deze consequenties:

- Organisaties zijn verplicht toegang te geven tot en/of kopieën te maken van gegevensbestanden, zelfs als deze zich in het buitenland bevinden. Voor Tele2 is het onmogelijk dat zij hier aan kan, mag en zal meewerken, aangezien een deel van onze infrastructuur en systemen in andere EU-landen staan.

Tele2 Nederland B.V.
Postbus 22697
1100 DD Amsterdam
Phone +31(0)20 750 10 00
tele2.nl

Kvk Amsterdam 33303418
Tele2 is een handelsnaam
van Tele2 Nederland B.V.

Diemen, 27-8-2015

- De organisaties die verplicht is mee te werken aan interceptie wordt uitgebreid van aanbieders van openbare elektronische communicatienetwerken en -diensten tot aanbieders van een communicatiedienst, zoals gedefinieerd in het Wetboek van Strafvordering. In de praktijk is dit een ieder, variërend van Twitter, Whatsapp, webhosting en clouddiensten tot nieuwssites, patiëntenverenigingen, sportclubs, vakbonden, kerkgenootschappen, universiteiten, hotels en bedrijven. Tot nu is er voor deze organisaties geen verplichting en werken zij hooguit in incidentele gevallen op basis van vrijwilligheid mee.
- Deze organisaties zijn met invoering van deze wet ook verplicht mee te werken aan bulkinterceptie, een verplichting die nu zelfs niet geldt voor telecommunicatiebedrijven.
- De investeringskosten voor gerichte en bulktaps en informatieverstrekking dienen deze organisaties zelf te dragen, in afwijking van de huidige praktijk welke nu geldt voor zowel opsporingsdiensten als inlichtingen en veiligheidsdiensten.
- De impact die de implementatie en realisatie van deze verplichte medewerking met zich mee zal brengen in kosten, mankracht en tijd is voor elke organisatie (groot of klein) aanzienlijk en niet te veronachtzamen.
- De diensten krijgen de mogelijkheid om te handelen met ongeëvalueerde bulkgegevensbestanden.

Het concept maakt vooral duidelijkheid dat (rechts)begrippen als proportionaliteit en doelmatigheid niet ten grondslag liggen aan de voorgenomen wijziging van de Wet op de inlichtingen-en veiligheidsdiensten. Het wordt duidelijk dat de diensten toegang willen tot alle communicatie, van iedereen, zonder dat zij de benodigde investeringen in tijd en geld willen dragen.

Tele2 Nederland B.V. is van mening dat er in specifieke situaties een belang kan zijn voor inlichtingen-en veiligheidsdiensten die voorziet in het hebben van toegang tot communicatie voor het vergaren van inlichtingen. Het huidige wetsvoorstel is echter onuitvoerbaar voor een aanbieder. Het zadelt onze klanten op met lasten en verplichtingen die zij niet kunnen dragen en waarbij de meesten uiteindelijk de hulp van Tele2 nodig zullen hebben om het uit te voeren. Hiernaast brengt de wet onze organisatie en individuele medewerkers mogelijk in conflict met wetgeving in andere landen. De wet is ook onduidelijk over de reikwijdte van de verplichtingen ten aanzien van wie onder de wet vallen en wat er redelijkerwijs door de diensten aan medewerking verwacht mag worden. De wet is onduidelijk over de hoogte van de lasten die het met zich mee breng. Om deze redenen is Tele2 van mening dat het huidige voorstel vooral averechts zal werken en de informatiepositie van de diensten op de lange termijn vooral kan schaden en daarmee de veiligheid van Nederland in gevaar zal brengen.

In de bijgesloten bijlage treft u een nadere reactie aan op specifieke onderdelen van het voorstel.

Hoogachtend,
Tele2 Nederland B.V.

Rudolf van der Berg
Regulatory Affairs

Mobile 0636356625
rudolf.vanderberg@tele2.com

Tele2 Nederland B.V.
Postbus 22697
1100 DD Amsterdam
Phone +31(0)20 750 10 00
tele2.nl

Kvk Amsterdam 33303418
Tele2 is een handelsnaam
van Tele2 Nederland B.V.

Diemen, 27-8-2015

Overzicht

De memorie van toelichting op het Voorstel van Wet op de inlichtingen- en veiligheidsdiensten 20XX (WIV20XX) stelt terecht dat de bijzondere bevoegdheden ten aanzien van het intercepteren, ontcijferen en opvragen het meest herzien worden. De wetgever legt echter niet uit hoe ingrijpend deze bevoegdheden herzien zijn, hoezeer deze nu afwijken van de praktijk die bij opsporingsdiensten geldt en waarom de voorgestelde aanpak wel effectief zal zijn / benodigd is. Voorbeelden zijn:

- De wetgever legt niet uit dat door het gebruik van het begrip 'communicatiedienst' de kring van partijen die onder de verplichting voor interceptie, ontcijferen en opvragen vallen uitgebreid wordt van ongeveer 1.000 aanbieders van telecommunicatienetwerken en diensten naar 360.000 organisaties met een website of netwerk (bron: CBS data over rechtspersonen niet zijnde eenmanszaken en andere vormen van klein bedrijf).
- Tot nu toe was de samenwerking met de diensten ten aanzien van het verstrekken en intercepteren van digitale gegevens voor het overgrote deel vrijwillig. Voor aanbieders van telecommunicatienetwerken en –diensten was het een plicht. Met de voorgestelde wetswijziging wordt dit echter een plicht voor ieder bedrijf in Nederland (mede ook omdat de gewenste inlichtingen bijna altijd digitaal beschikbaar zullen zijn). Daarbij kunnen zij verplicht worden om de diensten rechtstreeks toegang te geven tot hun databases.
- Bulkinterceptie dient voor iedere communicatiedienst mogelijk gemaakt te worden en betaald te worden als de diensten daar om verzoeken. Echter, de memorie van toelichting zegt nu al dat de diensten niet toegerust zijn om op deze opsporingsmethode op enige schaal toe te passen. Dit betekent dat de effecten discriminatoir zullen zijn, waarbij de ene partij zwaar moet investeren en een andere partij die dezelfde diensten aanbiedt geen of andere kosten heeft.
- De inlichtingendiensten willen ook dat de organisatie waar zij gegevens van opvragen zelf de investerings-, onderhouds- en exploitatiekosten draagt. De vrijwillige medewerking kent voor de opsporingsdiensten een vergoeding van de gemaakte kosten. Hier creëert de WIV20XX een discriminatoir regime, waarbij dezelfde handelingen bij de ene partij vergoedt worden, omdat ze door een opsporingsdienst verzocht zijn en een andere partij de kosten zelf moet vergoeden, omdat het een verzoek is van een IVD.
- Voor Tele2 betekent dit dat zij in haar eigen netwerken substantiële investeringen moeten doen om bulkinterceptie mogelijk te maken. Daarbij zullen we ongetwijfeld voor onze klanten allerlei eenmalige en langdurige oplossingen moeten verzinnen in onze dienstverlening aan hen (waar deze dienstverlening nu in het geheel niet in voorziet), om te kunnen voldoen aan lasten die zij van de diensten hebben ontvangen. Het is hoogst waarschijnlijk dat internationale klanten die een beperkte binding hebben met Nederland, hun dienstverlening naar andere Europese landen zullen verplaatsen.
- Voor Tele2 betekent dit mede dat zij tezamen met haar klanten naar oplossingen zal (moeten) zoeken. Veelal zal dit betekenen dat klanten de getroffen databases en communicatie in het buitenland zal plaatsen. Tele2 medewerkers zullen bij de keuze voor medewerking met deze wet geconfronteerd worden met de vraag of zij in Nederland strafbaar willen zijn voor het niet medewerken of in het buitenland strafbaar willen zijn voor het verstrekken van de gegevens.

Uitbreiding kring van aanbieders van communicatie

De WIV2002 bevat enige specifieke bijzondere bevoegdheden jegens aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten in de zin van de Telecommunicatiewet ten aanzien van gegevensverstrekking over een gebruiker en zijn communicatie. De Telecommunicatiewet bevat daarnaast nog bepalingen dat telecommunicatienetwerken en –diensten aftapbaar moeten zijn en de investerings-,

Tele2 Nederland B.V.
Postbus 22697
1100 DD Amsterdam
Phone +31(0)20 750 10 00
tele2.nl

Kvk Amsterdam 33303418
Tele2 is een handelsnaam
van Tele2 Nederland B.V.

Diemen, 27-8-2015

onderhouds- en exploitatiekosten zelf moeten dragen. Er zijn ongeveer 1000 telecommunicatiebedrijven actief in Nederland. Tele2 is niet gelukkig met deze verplichtingen en bijbehorende kostenverdeling, maar accepteert dat deze nu eenmaal zo is en zal dit debat dan ook niet heropenen in het kader van deze consultatie.

Dat gezegd hebbende, de wetgever had zijn redenen waarom deze verplichtingen en kostenverdeling specifiek geldt voor aanbieders van telecommunicatienetwerken en –diensten en niet voor andere communicatiediensten. De Telecommunicatiewet is primair een marktordeningswet en beperkt zich tot transmissiesystemen en het geheel of hoofdzakelijk overbrengen van signalen, met specifieke uitsluiting van diensten van de informatiemaatschappij die niet geheel of hoofdzakelijk bestaan uit het overbrengen van signalen via elektronische communicatienetwerken. (art 1.1e en f TW). De aftapbaarheidsverplichting zorgt ervoor dat dit soort netwerken aftapbaar dienen te zijn (Art. 13.1 TW), zodat zij onverwijld kunnen tappen. Door bij de Telecommunicatiewet aan te sluiten werd echter ook voorkomen dat een ieder, die een vorm van communicatie aanbood via een besloten netwerk, dan wel via een dienst van de informatiemaatschappij de verplichting had deze communicatie aftapbaar te maken. De Eerste Kamer heeft daarbij voorkomen dat hoofdstuk 13 middels lid 7 (dat niet in werking is getreden) ook van toepassing werd voor niet-openbare netwerken. Het opvallende (en voor de kostengerelateerde punten relevante) is echter dat dat artikel expliciet bepaalde dat deze netwerken wel recht hadden op vergoeding van de investerings-, exploitatie- en onderhoudskosten voor de noodzakelijke technische voorzieningen.

De WIV20XX stelt dat de kring van partijen waarop de verplichting rust te klein is en uitgebreid moet worden tot aanbieders van internetcommunicatie, webhostingbedrijven, e-mail aanbieders etc. Deze partijen zijn geen aanbieders die onder de Telecommunicatiewet vallen en dus kunnen de diensten deze partijen niet dezelfde verplichtingen opleggen als telecommunicatieaanbieders. Dit stoort de diensten blijkbaar. Zij stellen dan ook voor een ieder die een communicatiedienst, zoals gedefinieerd in het wetboek van Strafvordering, aanbiedt, te verplichten om mee te werken en de investeringskosten hiervoor zelf te dragen. De wetgever heeft in 2004-2005 bij de introductie van de wet Computer Criminaliteit II, ter implementatie van de Convention on Cybercrime (een verdrag van de Raad van Europa), "aanbieder van een communicatiedienst" als nieuwe term geïntroduceerd in art. 126la Sv. om duidelijk te maken dat de verplichtingen uit Strafvordering veel verder reiken dan de groep aanbieders van openbare telecommunicatienetwerken en –diensten;
"In deze afdeling wordt verstaan onder:

- *aanbieder van een communicatiedienst: de natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst;*
- *gebruiker van een communicatiedienst: de natuurlijke persoon of rechtspersoon die met de aanbieder van een communicatiedienst een overeenkomst is aangegaan met betrekking tot het gebruik van die dienst of die feitelijk gebruik maakt van een zodanige dienst."*

Het gebruik van het begrip communicatiedienst was nodig volgens de wetgever, omdat de Convention on Cybercrime een veel bredere reikwijdte had dan openbare telecommunicatie netwerken en -diensten. Bijvoorbeeld hostingactiviteiten (welke Tele2 aanbiedt onder de naam InterNLnet) vallen niet onder de Telecommunicatiewet. De memorie van toelichting zegt hierover:

Tele2 Nederland B.V.
Postbus 22697
1100 DD Amsterdam
Phone +31(0)20 750 10 00
tele2.nl

Kvk Amsterdam 33303418
Tele2 is een handelsnaam
van Tele2 Nederland B.V.

Diemen, 27-8-2015

> *"Het Verdrag definieert het begrip «service provider» om duidelijk te maken jegens welke entititeiten bepaalde strafvorderlijke bevoegdheden gehanteerd moeten kunnen worden. Het begrip wordt gedefinieerd als iedere publieke of private instelling die aan de gebruikers van haar diensten de mogelijkheid biedt te communiceren met behulp van een computersysteem en iedere andere instelling die computergegevens verwerkt of opslaat ten behoeve van (de gebruikers van) zo'n communicatiedienst. Bij dit laatste kan men bijv. denken aan de aanbieders van webhostingdiensten en beheerders van websites."*

Elders wordt ook duidelijk gemaakt dat het hier ook over private en besloten netwerken kan gaan.

Meer nog dan de wetgever zich ooit had kunnen voorstellen zijn de bepalingen die voortkomen uit het Convention on Cybercrime vandaag de dag toepasbaar op bijna ieder bedrijf of organisatie. Er is nauwelijks nog een bedrijf dat geen besloten bedrijfsnetwerk heeft, communicatie pleegt via Internet en een website heeft. Daarbij zijn er een veelheid van plekken waar privé, zakelijk, openbaar en besloten gecommuniceerd wordt. De definitie beperkt zich dan ook niet alleen tot 'over-the top' diensten Twitter, Gmail, Facebook, Instagram en Snapchat. Het gaat hier ook om datingsites, patiëntenforums, autosites, IT-sites, plaatjessites, bedrijfssites en overheidssites. De nu al in onbruik geraakte term Web2.0 stond voor het communicerende web. Alles en iedereen communiceert. Het is niet mogelijk om een dienst te leveren via het internet zonder een vorm van communicatie. Daarbij heeft de opkomst van het Internet der Dingen ervoor gezorgd dat burgers 24 uur per dag gemonitord worden door communicerende apparaten. Tel daarbij op dat de definitie zich ook uitstrekt tot besloten netwerken en het is duidelijk dat er nauwelijks een organisatie van enige omvang is die niet door de WIV20XX geraakt wordt. Een ruwe schatting op basis van gegevens van het CBS maakt duidelijk dat de kring van partijen die de lasten dragen van de nieuwe WIV20XX. uitgebreid wordt tot ongeveer 360.000 organisaties. Dit roept uiteraard de vraag op of de effectiviteit van voorliggende wetgeving evenredig toeneemt.

Het voorstel creëert daarbij een rare overlap tussen de verwerking van gegevens door de diensten (art. 22) en de bijzondere bevoegdheden. Op basis van het nieuwe lid 3 kunnen zij online toegang krijgen tot de gegevens in databases. Er is geen beperking op de soort gegevens dan wel diegene die hieronder valt. Daarmee hebben zij al een groot deel van de bijzondere bevoegdheden die in artikel 32 tot 40 gegeven worden ten aanzien van het opvragen van gegevens over communicatie. Het lijkt dat artikelen 38,39 en 40 voornamelijk redundant zijn en dienen ter bevestiging dat de diensten gratis toegang willen.

Van vrijwilligheid naar plicht

De huidige WIV2002 geeft de diensten al vergaande bevoegdheden tot het opvragen van de inhoud en metadata van communicatie van burgers. Artikel 17 geeft bijvoorbeeld de mogelijkheid aan de diensten om zich te wenden tot de verantwoordelijke voor een gegevensverwerking. Artikel 24 geeft hen de mogelijkheid om een geautomatiseerd werk te hacken. Artikel 25 geeft hen de bevoegdheid tot het met een technisch hulpmiddel gericht aftappen, ontvangen, opnemen en afluisteren van elke vorm van gesprek, telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk, ongeacht waar een en ander plaats vindt. In principe kunnen zij deze bevoegdheden wenden tot iedere persoon en organisatie. In de digitale wereld van vandaag zijn er derhalve weinig gegevens waar de diensten geen toegang toe kunnen krijgen, mits zij toestemming hebben van de betrokken Minister en in sommige gevallen er medewerking is van de houder van de gegevens.

Blijkbaar is deze vrijwilligheid niet voldoende en is een medewerkingsplicht nodig. Het is extra opvallend dat dezelfde bevoegdheden wanneer deze uitgeoefend worden door

Tele2 Nederland B.V.
Postbus 22697
1100 DD Amsterdam
Phone +31(0)20 750 10 00
tele2.nl

Kvk Amsterdam 33303418
Tele2 is een handelsnaam
van Tele2 Nederland B.V.

Diemen, 27-8-2015

opsporingsdiensten bij het onderzoeken van misdrijven wel op basis van vrijwilligheid toegepast kunnen worden. Zij kunnen dit doen door bijzondere opsporingsbevoegdheden toe te passen welke in Art 126 van het wetboek van Strafvordering beschreven staan. Zo geeft Art. 126m de mogelijkheid tot interceptie ook voor communicatie die niet afgewikkeld wordt over openbare telecommunicatienetwerken- en diensten. Zeker gezien het minder acute karakter en langere duur van de onderzoeken van de diensten, versus het acuut en korte termijn oplossen of voorkomen van misdrijven door de opsporingsdiensten is dit een vreemde keuze. Dezelfde gegevens die onder de nieuwe WIV20XX verplicht moeten worden geleverd en de basis kunnen vormen voor een ambtsbericht en daarop volgend justitieel onderzoek, mogen de opsporingsdiensten daarna alleen op basis van vrijwilligheid opvragen. Het lijkt dan ook onwaarschijnlijk dat deze medewerkingsplicht echt zo noodzakelijk is als dat de wetgever doet voorkomen.

Van gericht naar bulk

Een nieuwe bevoegdheid is die van de ongerichte bulktap. Het is nog zeer onduidelijk hoe de wetgever denkt deze bevoegdheid in te vullen. Zowel de onderbouwing van de redenen waarom de verplichting nodig is, als de invulling, roepen grote vragen op. Duidelijk is wel dat deze verplichting zal leiden tot grote rechtsongelijkheid voor een ieder die door de wetgever gezien wordt als aanbieder van een communicatiedienst en gezien dient te worden als een grote inbreuk in de privacy van Nederlanders en afnemers van diensten in Nederland in het algemeen.

De bevoegdheid wordt uit een gezet in artikel 33 tot en met 37 voor respectievelijk verwerving, voorbewerking, selectie en metadata-analyse, informatieplicht en medewerkingsplicht. De artikelen zijn echter in grote mate overlappend en uitwisselbaar, zodat het niet duidelijk wordt waarom er verschillende artikelen nodig zijn. De aanbieder is verplicht om elke vorm van bulkinterceptie die door de Minister goedgekeurd is toe te staan in zijn netwerk. De aanbieder kan verplicht worden de verwerving, voorbewerking, selectie en meta-data analyse voor de diensten realtime en online uit te voeren in zijn eigen netwerk, maar het kan ook offline bij de diensten gebeuren. De complexiteit van de benodigde deep packet inspectie apparatuur voor real-time en online analyse van anomalieën en malware is echter van een geheel andere orde dan een passieve splitter op een glasvezel. Waar de diensten de ene maand genoegen nemen met een splitter, kunnen ze de volgende maand de meest complexe oplossing eisen. Aanbieders hebben geen enkele grond een dergelijke last te weigeren. Het gevolg is dat de diensten een blanco cheque gekregen hebben te experimenteren met nieuwe apparatuur voor deze bevoegdheid. Dat de diensten zelf ook geen idee hebben hoe ze deze bevoegdheid in moeten vullen blijkt wel uit de MvT:

> *Mede om ervaring op te doen op grond waarvan gerichte vervolgstappen kunnen worden genomen, zal de interceptie na inwerkingtreding van de wet in de aanvangsjaren tot enkele fysieke toegangspunten beperkt blijven.*

Naar de mening van Tele2 is deze verregaande bevoegdheid strijdig met het beginsel van proportionaliteit. Op geen enkele wijze kan een aanbieder van communicatie een financiële en technische planning uitvoeren laat staan dat zij mag uitgaan van een normale bedrijfsvoering waarbij geld, tijd en mankracht wordt ingezet ten behoeve van reguliere dienstverlening. Immers, de algehele planning van werkzaamheden van enig een aanbieder kan terzijde worden geschoven indien de diensten besluiten dat er andere prioriteiten zijn. Daarbij kan voor een vergelijkbaar verzoek een concurrent een heel andere technische oplossing opgelegd worden, omdat de diensten het ook niet precies weten.

De aanbieder wordt ook nog eens verplicht om de installaties in stand te houden gedurende 12 maanden na afloop van een last. NB: dit is apparatuur die een aanbieder zelf niet kent, wil hebben of waarvan deze enige kennis bezit. Dit betekent dat alle contracten met leveranciers voor de extreem kostbare apparatuur ook nog 12 maanden moeten worden betaald en dat

Tele2 Nederland B.V.
Postbus 22697
1100 DD Amsterdam
Phone +31(0)20 750 10 00
tele2.nl

Kvk Amsterdam 33303418
Tele2 is een handelsnaam
van Tele2 Nederland B.V.

Diemen, 27-8-2015

elke wijziging aan het netwerk beoordeeld moet worden op zijn effect voor de bestaande bulktap oplossing. Dit betekend effectief een bevriezing van de huidige situatie in het netwerk en daarmee van de diensterverlening. Gemakshalve wordt hier de continuïteit van de dienstverlening, waarvoor aanbieder ook voor zorg dient te dragen even buiten beschouwing gelaten. Dit alles omdat de diensten misschien van gedachten of prioriteiten veranderen en dus een tap opnieuw in willen zetten. Naar de mening van Tele2 mag de aanbieder niet verplicht worden om op basis van ogenschijnlijke willekeur zaken dienen te implementeren en ook nog eens in stand te houden nadat de diensten gestopt zijn.

De belangrijkste reden die gegeven wordt voor het veranderen van deze bevoegdheid, is dat de MIVD deze bevoegdheid al had voor het intercepteren van buitenlands radioverkeer. De redenatie is dat nu veel meer dataverkeer over glasvezelverbindingen gaat, de bevoegdheid hier naar uitgebreid moet worden. Hierbij wordt vergeten dat de hoeveelheid radioverkeer in die tijd ook gestegen is, zelfs al is het minder snel gestegen dan die van draadgebonden communicatie. Het valt te verwachten dat er nu meer inlichtingen verkregen worden uit het radioverkeer dan jaren geleden. Daarbij wordt ook niet uitgelegd waarom de bestaande bevoegdheden om gericht te tappen in netwerken niet ingezet kunnen worden. Zeker omdat de traditionele tegenstanders van de MIVD de strijdkrachten van andere landen zijn en deze veelal vanaf bekende netwerken zich met het Internet verbinden.

Een andere reden die niet veel aandacht krijgt in de MvT is de internationale handel tussen inlichtingendiensten in bulkdata. Artikel 77 lid 2 geeft de diensten de mogelijkheid om ongeëvalueerde data te verhandelen met buitenlandse diensten. Dit betekend dat Nederlandse diensten grootschalige verkeer van Nederlandse burgers (en buitenlandse) in Nederland kunnen intercepteren en dit ongezien en zonder enige waarborgen overhandigen aan buitenlandse diensten. Dit kan niet de bedoeling zijn in een democratische rechtsstaat.

Voor aanbieders als Tele2 kan verplichte samenwerken met de diensten bij de uitvoering van deze plichten alleen maar leiden tot imagoschade, ontevreden klanten en afbreuk van het gevoel van integriteit. De Snowden onthullingen zijn een goed voorbeeld van hoe de maatschappij negatief reageert op de samenwerking tussen inlichtingendiensten en bedrijfsleven

Dragen van de kosten

Het wetsvoorstel kent klaarblijkelijk vier verschillende kostenregimes. Voor een ieder die vrijwillig mee werkt, lijkt het mogelijk dat alle noodzakelijke kosten vergoed worden. De tekst is hierover niet expliciet, maar impliciet lijkt dat wel de werkwijze van de dienst. Voor postbedrijven bestaat er een vergoeding van de directe kosten. Hoe de directe kosten berekend mogen worden zegt de toelichting niets. Voor de aanbieders van communicatie bestaat alleen de vergoeding van de personeels- en administratiekosten. Voor de ontsleuteling van gegevens zal de aangesproken partij echter de volle last zelf moeten dragen. Een dergelijk groot verschil leidt tot een grote mate van ongelijkheid. Het berichtenverkeer over een pakketje en het bijbehorende pakketje kunnen onder alle vier de kostenregimes vallen. Een verzoek aan een bedrijf over wie iets besteld heeft, zal onder het vrijwillige regime vallen, het raadplegen van de online track en trace gevens en bijbehorende IP-adressen van de verzender en ontvanger vallen onder het communicatievergoedingsregime, de ontsleuteling van de communicatie over een beveiligde verbinding zal voor last van de postvervoerder komen en de uitlevering van het pakketje wordt weer vergoed. Er is geen enkele vorm van rechtsgelijkheid tussen de verschillende partijen die allen voor hetzelfde onderzoek vergelijkbare handelingen moeten uitvoeren. Hun positie in de keten en de gebruikte technologieën bepalen of zij in aanmerking komen voor vergoeding. Hier lijkt de dienst vooral gebruikers van complexere moderne technologieën niet te willen vergoeden.

Tele2 Nederland B.V.
Postbus 22697
1100 DD Amsterdam
Phone +31(0)20 750 10 00
tele2.nl

Kvk Amsterdam 33303418
Tele2 is een handelsnaam
van Tele2 Nederland B.V.

Diemen, 27-8-2015

Dit is een grote afwijking voor zij die door de diensten nu als communicatiedienst aanbieder gezien worden. Onder de WIV2012 vielen zij nog onder het regime van vrijwilligheid. De vrijwilligheid bracht met zich mee dat een bedrijf om een bijdrage in de kosten kon vragen. In de WIV20XX willen de diensten dit beperken tot de administratie- en personeelskosten, direct gerelateerd aan het uitvoeren van de interceptie. De investerings-, onderhouds- en exploitatiekosten komen niet meer voor vergoeding in aanmerking. Deze regeling bestond al voor de 1000 telecommunicatieaanbieders in Nederland, zoals Tele2, maar wordt nu ook doorgezet naar de 359.000 anderen die onder de nieuwe regeling vallen.

De wetgever doet voorkomen dat de vergoedingsregeling een logische stap is omdat het ook hier om communicatie gaat. Echter voor de opsporingsdiensten die bij dezelfde bedrijven onderzoek doen naar misdrijven geldt de regeling van artikel 592 lid 2 Strafvordering, dat zegt:

- *De kosten van het nakomen van een vordering tot het verstrekken van gegevens of tot het medewerking verlenen aan het ontsleutelen van gegevens krachtens de artikelen 126m, 126n, 126nc tot en met 126ni, 126t,126u, 126uc tot en met 126ui en 126zja tot en met 126zp kunnen de betrokkene uit 's Rijks kas worden vergoed. Hierbij kan een lager bedrag worden vergoed voor zover degene tot wie het bevel zich richt, niet de administratie heeft gevoerd en de daartoe behorende boeken, bescheiden en andere gegevensdragers heeft bewaard als voorgeschreven in artikel 10 van Boek 2 en artikel 15i van Boek 3 van het Burgerlijk Wetboek.*

Dit betekent dat een bedrijf als Tele2 voor een deel van haar dienstverlening (bijv. hosting) wel recht heeft op de vergoeding uit 's Rijks kas van de werkzaamheden en investeringen en voor een ander deel de kosten zelf moet dragen. In beider gevallen gaat het om dezelfde werkzaamheden met een zelfde vermeende dringende maatschappelijke reden die haar medewerking vereist.

Ook voor onze klanten zal dit een grote wijziging zijn, omdat zij veelal met Tele2 moeten samenwerken om aan een last voor (bulk) interceptie of gegevensverstrekking te voldoen. Dergelijke capaciteit zal niet altijd eenvoudig voor handen binnen het bedrijf van die klant. Zij zullen dus hun telecommunicatieaanbieders, maar naar alle waarschijnlijkheid ook expertise van derden moeten inhuren. Discussies uit het verleden leren dat de diensten dergelijke kosten zien als investeringskosten die niet voor vergoeding in aanmerking komen onder het regime van de Telecommunicatiewet.

Voor beginnende bedrijven, vooral innovatie Internet (of Things) start-ups, zal een vestiging in Nederland geen reële optie zijn. Er is nauwelijks een ambitieuze start-up die geen communicatie element in haar propositie heeft en derhalve niet onder deze regeling valt. Niet alleen vanwege de kostenvergoeding, maar ook omdat de tijd en kennis van ontwikkelaars gaat zitten in het faciliteren van de inlichtingen- en veiligheidsdiensten in plaats van in het ontwikkelen van innovatieve diensten. In ons omringende landen gaan de verplichtingen minder ver en kunnen zij veelal wel aanspraak maken op vergoeding. In plaats van af te wachten zullen zij besluiten in het geheel niet in Nederland te beginnen, maar bijvoorbeeld in Zweden of het Verenigd Koninkrijk.

Voor bulkintercepties welke tot nu toe niet door aanbieders van communicatie uitgevoerd zal het vergoedingsregime leiden tot grote ongelijkheid. Volgens de memorie van toelichting:

> *Deze kosten zullen de komende periode in nauw overleg met relevante aanbieders in de telecomsector in kaart worden gebracht. Het overleg met relevante aanbieders in de telecomsector is tevens vereist om te achterhalen hoe deze bevoegdheid in een technisch complexe omgeving op de meest doeltreffende en doelmatige manier kan worden toegepast, met zo min mogelijk inbreuken op de persoonlijke levenssfeer van burgers. Bij de implementatie van de interceptie van telecommunicatie op*

Tele2 Nederland B.V.
Postbus 22697
1100 DD Amsterdam
Phone +31(0)20 750 10 00
tele2.nl

Kvk Amsterdam 33303418
Tele2 is een handelsnaam
van Tele2 Nederland B.V.

Diemen, 27-8-2015

> *kabelgebonden netwerken in het kader van de nieuwe wet is voorts sprake van schaalbaarheid in omvang en tijd. De keuzes die hierbij worden gemaakt hebben vanzelfsprekend gevolgen voor het financiële beslag. Mede om ervaring op te doen op grond waarvan gerichte vervolgstappen kunnen worden genomen, zal de interceptie na inwerkingtreding van de wet in de aanvangsjaren tot enkele fysieke toegangspunten beperkt blijven.*

Hiermee wordt feitelijk van Tele2 en de rest van de sector verwacht dat zij de bulkinterceptie oplossingen van de inlichtingendiensten gaan ontwerpen en inrichten. Tele2 zal hier niet vrijwillig aan meewerken aan een dergelijk overleg om elke schijn van belangenverstrengeling en onwenselijkheid van de voorgestelde wetgeving te onderstrepen.

Het vergoedingsregime voor bulkintercepties is hoogst discriminatoir, door de wijze waarop bulkintercepties in de komende jaren beperkt zullen zijn tot fysieke toegangspunten en de verschillende implementatiemogelijkheden, zoals bv de verschillen tussen real-time en online vs. analyse achteraf en offline. Real-time en online analyse vereist dat de aanbieder dure en complexe Deep Packet Inspection apparatuur installeert die wellicht dergelijke analyses kunnen doen. Hiernaast schaalt, voor zover Tele2 bekend, de beschikbare apparatuur niet tot het niveau van moderne verkeersstromen en dus zal het verkeer in kleinere delen opgedeeld moeten worden wat de impact voor een aanbieder alleen maar groter maakt. Dit zou een volledige reorganisatie van de core netwerken van een aanbieder vereisen wat jaren kan duren en aanzienlijke impact kent in de continuïteit van de dienstverlening. Maar ook een passieve tap waarbij het volledige core netwerk verkeer doorgezet wordt naar de diensten is geen optie, want de diensten zijn niet in staat om de honderden gigabits per seconde verkeer die zelfs een relatief kleine partij als Tele2 heeft te verwerken. Daarom zullen zij Tele2 toch verplichten om apparatuur te kopen die aanzienlijk duurder is.

De verplichting om de voorziening nog 12 maanden in stand te houden na afloop van een last zorgt voor een verdere verhoging van die kosten. Het is feitelijk een kostenverdubbelaar, doordat veel software, hardware en 24/7 support benodigd bij bulkinterceptie gekocht wordt in een dienstenmodel op basis van geactiveerde capaciteit voor een bepaalde periode (veelal een jaar). Dus als na een half jaar een bulkinterceptie stopt, dan zal de aanbieder van een communicatiedienst toch een additioneel jaar aan dienstverlening moeten afnemen, voor apparatuur waar de IVDs waarschijnlijk niet eens gebruik van maken.

Effecten voor Tele2

Voor Tele2 Nederland B.V. zou de WIV20XX leiden tot grote onzekerheid over wat er van onze klanten, onze medewerkers en van ons bedrijf verwacht kan worden door de diensten. Onze klanten zullen geconfronteerd worden met een kwalificatie als communicatiedienst en daardoor van ons als netwerk- en dienstenleverancier allerlei ondersteuning nodig hebben. Veelal zal die ondersteuning er toe leiden dat de betreffende gegevens en communicatie niet meer in Nederland zullen plaatsvinden. Dat lijkt ons de eenvoudigste oplossing.

Tele2 medewerkers zullen bij de keuze voor medewerking met deze wet geconfronteerd worden met de vraag of zij in Nederland strafbaar willen zijn voor het niet medewerken of in het buitenland strafbaar willen zijn voor het verstrekken van de gegevens. Een significant deel van de infrastructuur van Tele2 Group wordt gedeeld door de landen waar wij operationeel zijn. Veelal bevindt die apparatuur zich in Estland en Zweden. Estland heeft de Convention on Cybercrime ook geratificeerd en heeft daarmee (net als Nederland) het onbevoegd toegang geven tot communicatiegegevens strafbaar gesteld. Vanuit Ests perspectief zal het geven tot en overhandigen van gegevens uit deze databases aan de Nederlandse inlichtingendiensten zonder de toestemming van de Estse overheid een overtreding van deze wet zijn. Onze medewerkers en management zal dan ook een Kafka-eske afweging moeten maken;

Tele2 Nederland B.V.
Postbus 22697
1100 DD Amsterdam
Phone +31(0)20 750 10 00
tele2.nl

Kvk Amsterdam 33303418
Tele2 is een handelsnaam
van Tele2 Nederland B.V.

Diemen, 27-8-2015

Strafbaar zjjn in Nederland of buiten Nederland. Binnen de wet van twee landen werken kan blijkbaar niet.

Waar tot nu toe de hostingwerkzaamheden en andere dienstverlening buiten de reikwijdte van de Telecommunicatiewet vielen, vallen zij wel onder de reikwijdte van de WIV20XX. Echter de kosten hoeven pas genomen te worden als er een daadwerkelijke last komt. Dit is een financiële roulette, waar het bedrijf alleen maar nadelige gevolgen van ondervind.

De bulkinterceptie mogelijkheid is zo ambigue opgeschreven, dat het een blanco cheque aan de inlichtingendiensten geeft om te eisen wat zij willen, zonder dat ze de kosten daarvoor hoeven te dragen. Tele2 kan dus geen lange termijnplanning meer maken voor haar netwerken en diensten. Elk moment kan er een verplichting tot bulkinterceptie uit de inlichtingendiensten komen die een volledige wijziging van die netwerken en diensten vereist.

Additionele punten

Er zijn nog een aantal additionele punten waar Tele2 kort aan wil refereren, maar niet heel diep op wil ingaan:

- Wij vinden het zorgwekkend dat het gebruik van de IMSI-catcher uitgebreid wordt tot (bulk)interceptie van verkeer. Het huidige gebruik van de IMSI-catcher breekt al in op de licenties van Tele2 en daarmee de dienstverlening aan haar klanten. Interceptie van verkeer betekent feitelijk dat de diensten een zogenaamde "man in the middle aanval" uitoefenen over onze netwerken op onze klanten.
- De tekst is nu zodanig technologieneutraal, dat de diensten vrijelijk elk netwerk draadloos (bv Wifi) en bedraad kunnen intercepteren zonder medewerking van de eigenaren. Een dergelijke vrijheid gaat veel te ver.

SURF

Datum	31 augustus 2015
Ons kenmerk	20150831-003-EVJE-FRJA
Onderwerp	reactie internetconsultatie Wet op de inlichtingen- en veiligheidsdiensten

SURF erkent dat er in specifieke situaties een belang kan zijn voor inlichtingen- en veiligheidsdiensten in het hebben van toegang tot communicatiediensten. Het voorliggende wetsvoorstel stuit echter op principiële bezwaren en beperkt SURF in het uitvoeren van haar doelstellingen. Het voorstel strekt zich uit tot het dienstenaanbod van SURF en heeft daarmee direct consequenties voor haar gebruikers.

SURF maakt graag van de gelegenheid gebruik om haar zorgen met betrekking tot het voorstel kenbaar te maken.

SURF als samenwerkingsorganisatie van het Nederlandse hoger onderwijs en onderzoek biedt haar gebruikers ICT diensten waaronder communicatiediensten zoals SURFinternet. SURF heeft als doelstelling het leveren van een geavanceerd dienstenaanbod met veel aandacht voor privacy voor de gebruiker en beveiliging van gegevens en infrastructuur. Juist voor de onderzoekscommunity die SURF bedient is het van belang om veilig en vertrouwelijk te kunnen communiceren. Bijvoorbeeld als het gaat om de uitwisseling van patiëntgegevens bij medisch onderzoek.

Voorop staat dat SURF als samenwerkingsorganisatie en als aanbieder van diensten een zorgplicht heeft jegens haar gebruikers. Een zorgplicht met betrekking tot de veiligheid en betrouwbaarheid van onze diensten maar ook voor wat betreft grondrechten van onze gebruikers. We vinden dat het voorstel te eenzijdig het opsporing- en beveiligingsbelang dient en daarmee onvoldoende recht doet aan de bescherming van de grondrechten.

Wat daarbij steekt is dat een uiteindelijke beslissing over de toepassing van bevoegdheden niet bij een onafhankelijke rechter terecht komt. We sluiten ons daarbij volledig aan bij de reactie van de Internet Society Nederland op het wetsvoorstel en onderschrijven de vragen die zij hebben bij specifieke elementen uit te voorstel zoals met betrekking tot de toestemming, hack bevoegdheid en bewaartermijnen.

Een ander belangrijk punt van zorg heeft betrekking op de medewerking aan verzoeken waar aanbieders van communicatiediensten toe verplicht kunnen worden en de mogelijk investeringen die dat van aanbieders vraagt. SURF stelt zich ten doel haar doelgroep te voorzien van een veilig en innovatief netwerk. Om dit te bewerkstelligen is het noodzakelijk dat SURF in vrijheid beslissingen kan

Bezoekadres
Kantoren Hoog Overborch
Hoog Catharijne
Moreelsepark 48
3511 EP Utrecht

Postadres
Postbus 19035
3501 DA Utrecht

Contact
T +31 88 787 30 00
E info@surf.nl
W www.surf.nl

Bedrijfsgegevens
K.v.K nr.: 41182408

nemen over de inrichting van haar netwerk en diensten, niet gehinderd door beperkingen die met de uitvoering van dit wetsvoorstel gepaard gaan.

Juist door te investeren in innovatie, en een architectuur en beveiliging te kiezen die optimaal presteert beschikt de Nederlandse onderwijs- en onderzoekscommunity over een wereldwijd toonaangevend netwerk. Een positie waarvan de Nederlandse overheid en de SURF-gebruikers hebben aangegeven dat ze willen dat die behouden blijft en die bovendien aansluit bij de ambitie van de overheid met betrekking tot Nederland als digitale toegangspoort voor Europa.

In meer algemene zin spant SURF zich in voor een open, veilig en betrouwbaar internet. Het voorstel biedt te weinig waarborgen met betrekking tot deze principes, met name wat betreft proportionaliteit, en zet een rem op de verdere ontwikkeling van het internet waarbij deze principes leidend zijn. We verwijzen hierbij naar het WRR rapport 'De publieke kern van het internet' en naar het essay 'De anarchistische trekjes van Internet' van SURFnet's CTO Erik Huizer, dat is gepubliceerd in het boek 'Omstreden vrijheid' (Van Gennep, Amsterdam februari 2015) en tevens is te vinden op https://www.surf.nl/binaries/content/assets/surf/nl/2015/artikel_omstreden_vrijheid_erik_huizer_nl.pdf.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

Reactie Microsoft op vervanging Wet op de Inlichtingen- en Veiligheidsdiensten 2002

Microsoft verwelkomt de mogelijkheid via een internetconsultatie commentaar te geven op het voorstel voor vervanging van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002).

Microsoft begrijpt de cruciale rol die wetshandhaving speelt in het waarborgen van veiligheid in onze samenleving. Daarbij is het echter wel van groot belang dat wetgeving waarmee inlichtingen- en veiligheidsdiensten een mandaat krijgen om bepaalde activiteiten te onderzoeken, in adequate waarborgen voorziet om fundamentele rechten van mensen te beschermen, waaronder het recht op privacy van gebruikers van technologie. Microsoft is een wereldwijd opererend technologiebedrijf en aanbieder van een breed scala aan online diensten. Daarom zijn we ons er goed van bewust dat het een uitdaging is een balans te vinden tussen de rechten, waaronder het recht op privacy, van burgers en instituties enerzijds en de belangen van overheidsinstanties anderzijds. In de praktijk zien we dat afwijkende nationale methodes voor het verzamelen van informatie door inlichtingen- en veiligheidsdiensten voor conflicten zorgen voor bedrijven die zich moeten houden aan wetgeving in verschillende jurisdicties. Balans en harmonisatie moeten daarom twee belangrijke uitgangspunten zijn bij de hervorming van wetgeving die van toepassing is op de inlichtingen- en veiligheidsdiensten.

Om dat te bereiken moedigde Microsoft, samen met een aantal andere technologiebedrijven, overheden overal ter wereld eerder al aan vijf kernprincipes te hanteren in de hervorming van dergelijke wetgeving. We zijn ervan overtuigd dat deze principes, te vinden op www.reformgovernmentsurveillance.com, een leidraad kunnen zijn voor de door de Nederlandse regering voorgestelde vervanging van de Wiv 2002. Met het omarmen van deze principes kan de Nederlandse overheid niet alleen de nationale veiligheid van Nederland beschermen, maar ook de fundamentele rechten van technologiegebruikers versterken, innovatie ondersteunen en het vertrouwen van gebruikers in technologie herstellen.

In aanvulling op deze principes moedigen we de Nederlandse regering aan de volgende elementen aan te passen in het voorliggende wetsvoorstel:

Definities van diensten waar de wet op van toepassing is

Wanneer geïmplementeerd in haar huidige vorm zijn bepalingen in de nieuwe wet van toepassing op '*elke aanbieder van een communicatiedienst*', die '*de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of die gegevens opslaat ten behoeve van een zodanige dienst, of de gebruikers van die dienst.*' Waar de Wiv 2002 zich nog richtte tot de *aanbieder van een openbaar telecommunicatienetwerk* en/of *openbare telecommunicatiedienst* in de zin van de Telecommunicatiewet, richt de nieuwe wet zich op het bredere begrip *aanbieder van een communicatiedienst.* Op basis van de Memorie van Toelichting bij het wetsvoorstel wordt duidelijk dat met dit begrip een veel bredere groep van

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

diensten, en dus ook aanbieders, wordt bestreken. Volgens de Memorie van Toelichting vallen onder het begrip *aanbieder van een communicatiedienst* ook aanbieders van besloten netwerken en –diensten, aanbieders van webhostingdiensten, website-beheerders en aanbieders van online opslag, email of spraakdiensten.

Deze aanpassing betekent een significante verruiming van de bestaande wet. Door de in het voorstel opgenomen verplichtingen op te leggen aan een bredere groep aanbieders en diensten heeft het wetsvoorstel de potentie om het vertrouwen van gebruikers in technologie ernstig te schaden, en innovatie te ontmoedigen. Met een dergelijke wet kan een aanzienlijke hoeveelheid informatie, die door gebruikers via technologiebedrijven wordt opgeslagen of verstuurd, worden ingezien door de Nederlandse inlichtingen- en veiligheidsdiensten, met wantrouwen van die gebruikers in deze bedrijven tot gevolg. Dat wantrouwen kan op haar beurt weer leiden tot terughoudendheid bij gebruikers om nieuwe technologie te gaan gebruiken, net als de bereidheid van technologiebedrijven – met in het bijzonder start-ups en MKB-bedrijven – om te innoveren doordat de potentiële markt voor producten en diensten krimpt. Daarnaast zouden de verplichtingen waar *aanbieders van communicatiediensten* onder het wetsvoorstel aan moeten voldoen niet overeenkomen met hun verplichtingen in andere jurisdicties – in Europa en daarbuiten – waarmee de Nederlandse ICT-markt ernstig kan worden verstoord.

<u>Geografische reikwijdte</u>
Hoewel wij aannemen dat de voorgestelde wet en de daarin opgenomen verplichtingen geen extraterritoriale werking hebben, bevat het wetsvoorstel dubbelzinnigheden over de daadwerkelijke territoriale reikwijdte. Als voorbeeld van deze dubbelzinnigheid kan worden gewezen op de volgende vermelding in het wetsvoorstel: "(...) de diensten zijn bevoegd tot het met een technisch hulpmiddel gericht aftappen, ontvangen, opnemen en afluisteren van elke vorm van gesprek, telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk, ongeacht waar een en ander plaatsvindt."

Het is bovendien onduidelijk onder welke omstandigheden de verplichtingen uit deze wet van toepassing zullen zijn op *aanbieders van communicatiediensten* die internationaal opereren. Enkele factoren die hierbij een rol zouden kunnen spelen zijn:

- de locatie waar de aanbieder is gevestigd:
- de locatie waar de gegevens zich bevinden of de communicatie plaatsvindt;
- de omstandigheid dat de dienst wel of niet wordt aangeboden aan gebruikers in Nederland;
- de omstandigheid dat de gegevens of communicatie afkomstig is van en/of bestemd is voor gebruikers die zich niet in Nederland bevinden;
- combinaties van de vier hierboven genoemde factoren.

Helaas wordt in het wetsvoorstel en de daarbij behorende Memorie van Toelichting geen enkele duidelijkheid gegeven onder welke omstandigheden *aanbieders van*

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

communicatiediensten gehouden zijn om aan de verplichtingen uit deze wet te voldoen. Zo is bijvoorbeeld onduidelijk of de verplichtingen uit deze wet ook van toepassing zullen zijn op aanbieders die hun diensten (mede) in Nederland aanbieden maar in het buitenland gevestigd zijn en waarbij de gegevens zich eveneens in het buitenland bevinden. De onduidelijkheid over de territoriale reikwijdte van de wet is voor buitenlandse partijen die internationaal opereren problematisch en zorgt bovendien voor grote rechtsonzekerheid. De Nederlandse regering dient op dit punt meer duidelijkheid te verschaffen. Daarbij zou het marktpartijen helpen als de Nederlandse regering aan de hand van de hierboven vermelde factoren de verschillende scenario's afloopt waarin de wet en de daarin vermelde verplichtingen wel of niet van toepassing zijn op aanbieders die internationaal opereren.

Wij roepen de Nederlandse regering op in het wetsvoorstel duidelijk te maken dat het mandaat geboden aan de inlichtingen- en veiligheidsdiensten zich strikt beperkt tot de inhoud en gegevens die ten minste zijn opgeslagen in Nederland, en dat verplichtingen tot onderschepping van gegevens *alleen* van toepassing zijn op *bedrijven* met ten minste een infrastructuur in Nederland. De reden daarvoor is simpel: dergelijke verplichtingen opleggen aan aanbieders van diensten wiens infrastructuur *buiten* Nederland is gevestigd zal tot conflicten kunnen leiden met de wettelijke verplichtingen die deze bedrijven moeten nakomen in die andere landen waar hun infrastructuur is gevestigd. Gezien het feit dat ook andere landen vergelijkbare wetgeving aan het doorvoeren zijn zal de resulterende lappendeken aan conflicterende wetgeving niemands belang dienen.

Zoals ook opgenomen in het evaluatierapport van de Commissie Dessens uit 2013 (p. 41), weerhouden principes van soevereiniteit en non-interventie in het internationaal recht staten ervan activiteiten te ondernemen op het grondgebied van andere staten zonder expliciete toestemming van die staat. Wij zijn van mening dat de Nederlandse inlichtingen- en veiligheidsdiensten die *aanbieders van communicatiediensten* die *buiten* Nederland zijn gevestigd, om medewerking verzoeken dit enkel en alleen zouden mogen doen door samenwerking met de relevante autoriteiten in de desbetreffende jurisdictie waar de aanbieder is gevestigd. Deze samenwerking moet plaatsvinden met respect voor de nationale regelgeving waar deze buiten Nederland gevestigde aanbieders aan moeten voldoen, net als aan relevante verdragsrechtelijke raamwerken of bestaande samenwerkingsovereenkomsten tussen de diensten.

In plaats van eenzijdig te opereren, moeten overheden volgens gevestigde internationale raamwerken en andere samenwerkingsovereenkomsten werken om zo te garanderen dat het aftappen van communicatie of het vergaren van gegevens consistent is met de wetgeving van het land waar de gegevens zijn opgeslagen en de aanbieder is gevestigd. Als bestaande mechanismen niet adequaat blijken te werken moeten deze niet worden omzeild, maar moet er juist een op principes gebaseerde, transparant, efficiënt en duurzaam raamwerk worden ontwikkeld om rechtmatige verzoeken om gegevens tussen verschillende jurisdicties in goede banen te leiden. Daarmee worden zowel de rechten beschermd van gebruikers wiens gegevens worden onderschept, als de soevereiniteit gewaarborgd van andere landen.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

Harmonisatie met andere jurisdicties

Microsoft dringt er bij de Nederlandse regering ook op aan om de wetgeving op dit gebied goed te coördineren met andere jurisdicties, in het bijzonder andere EU-lidstaten, om ervoor te zorgen dat wetgeving een harmoniserende aanpak voorstaat ten aanzien van de regulering van *aanbieders van communicatiediensten*. Dat is nodig omdat bedrijven over grenzen heen opereren – hun klanten zijn vaak ingezetenen van verschillende landen – waarbij heldere, werkbare en technisch haalbare regels nodig zijn om hun verplichtingen in die verschillende landen na te kunnen komen.

Zoals nu opgesteld, zou het wetsvoorstel het huidige wereldwijde stelsel van nationale wet- en regelgeving op dit gebied – dat nu al inconsistent en gefragmenteerd is – nodeloos verder compliceren. Deze tegengestelde standaarden vormen een uitdaging voor bedrijven die diensten aanbieden in meer dan één land. Als een EU-lidstaat bijvoorbeeld communicatie wil aftappen en dit alleen mogelijk zou zijn door fysiek handelen in een andere EU-lidstaat, dan zou de wetgeving van de jurisdictie waarin gehandeld moet worden in strijd kunnen zijn met de wetgeving in de jurisdictie van waaruit het aftappen gewenst is.

Om duidelijkheid voor *aanbieders van communicatiediensten* te vergroten en de kosten van compliance te verlagen zou de Nederlandse regering het proces van aftappen van communicatie en het opvragen van gegevens zoveel mogelijk in lijn moeten brengen met dat van andere jurisdicties. Als een potentiële onderschepping van communicatie of verstrekking van gegevens impact heeft op meerdere jurisdicties, dan moeten de overheden van deze jurisdicties samenwerken om de rechtmatigheid van dat verzoek te bepalen, in plaats van aanbieders tegenstrijdige verplichtingen op te leggen. Coördinatie door EU-lidstaten op basis van de *Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie (EU-rechtshulpverdrag)* van 2005 , is slechts één voorbeeld van hoe staten hebben samengewerkt om een pan-Europees raamwerk te creëren dat soortgelijke problemen aanpakt in de sfeer van strafvorderlijke bevoegdheden van opsporingsinstanties. Een soortgelijk raamwerk zou ook moeten worden ontwikkeld voor de grensoverschrijdende activiteiten van de inlichtingen- en veiligheidsdiensten. Op basisniveau zou de Nederlandse regering ook moeten garanderen dat het type gegevens dat kan worden onderschept of worden opgevraagd en het format daarvan onder de nieuwe wet geharmoniseerd worden met het type en het format van de gegevens die kunnen worden onderschept of opgevraagd op grond van verplichtingen die andere landen opleggen. Zonder een geharmoniseerde implementatie van deze principes bestaat er een significant risico op economische lasten voor de Nederlandse maatschappij.

Voor meer informatie ben ik uiteraard beschikbaar. Ik ga graag verder in gesprek over de details van onze reactie, mogelijke aanvullende vragen, of mogelijkheden voor aanvullende samenwerking. Zoals aan het begin van dit commentaar aangegeven, vinden we de hervorming van deze wetgeving van het grootste belang en werken we graag samen met alle

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

belanghebbenden om ervoor te zorgen dat de uiteindelijk aangenomen wet voor zowel wetshandhaving als bescherming van de rechten van burgers en marktpartijen voldoende handvaten biedt.

Hoogachtend,

Jochem de Groot

Government Affairs, Microsoft Nederland

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en
Ministerie van Defensie

Betreft: Internetconsultatie Wet op de inlichtingen- en veiligheidsdiensten 20XX

31 augustus 2015, Den Haag, Helsinki, Olpe

Geachte mevrouw, heer,

Wij danken u voor de gelegenheid een reactie te geven op het wetsvoorstel ter vervanging van de huidige Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002). Deze reactie is geschreven namens PowerDNS.COM BV, Dovecot Oy en Open-Xchange AG. PowerDNS is een Nederlandse leverancier van producten ten behoeve van aanbieders van telecommunicatiediensten, en is de software achter ongeveer 30% van alle domeinnamen op Internet. Dovecot levert naar schatting de technologie achter 50% van alle mailbox servers. Afsluitend, Open-Xchange onze (aanstaande) moedermaatschappij levert software die de email en overige communicatie ondersteunt van meer dan 120 miljoen gebruikers. Onze respectievelijke softwareproducten zijn in gebruik bij de grootste aanbieders van telecommunicatiediensten ter wereld.

De hoofdauteur van dit document heeft vanuit zijn vorige carriere twaalf jaar ervaring met 'Lawful Interception' (LI) in het brede & internationale spectrum van het implementeren van tap-installaties, het ontwikkelen, leveren en gebruiken van LI software tot het meeschrijven aan relevante Nederlandse wet- en regelgeving. Deze inzending is zorgvuldig opgesteld om geen blijk te geven van het kennisniveau en modus operandi van de Nederlandse inlichtingen- en veiligheidsdiensten (verder: de Diensten).

Wij vrezen dat in de huidig voorgestelde vorm de nieuwe Wet op de inlichtingen- en veiligheidsdiensten eerder een gevaar is voor "het voortbestaan van de democratische rechtsorde en de veiligheid" (artikel 8) dan dat deze daaraan bijdraagt.

Wij delen de zeer grote zorgen over de privacyschendingen en de doel- en rechtmatigheid van dit nieuwe wetsvoorstel zoals geuit door andere respondenten van deze consultatie. Onze zorg hierover kon niet groter zijn. In deze inzending echter willen wij ons concentreren op specifieke tekortkomingen en grove fouten in het voorliggend voorstel, met name aangaande de artikelen met betrekking tot de afluisterbevoegdheden.

In dit document delen wij eerst kort de problemen die wij waarnemen, gevolgd door onze aanbevelingen. Mogelijk ietwat ongebruikelijk vervolgen wij daarna met een uiteenzetting van hoe de communicatiegerelateerde artikelen van het voorstel onderling samenhangen (met diagram). Na behandeling van enige praktische punten sluiten wij ter illustratie af met een scenario hoe een nieuwe 'WIV 20XX' gevolgen zou kunnen hebben voor de Dienst Automatisering van de Tweede Kamer.

Voor wij aanvangen willen wij de vele partijen die mee hebben geholpen[1], direct of indirect, bij de totstandkoming van dit document bedanken.

In het kort zien wij in het voorliggende voorstel de volgende problemen:

- Het voorstel handhaaft het curieuze stelsel dat ambtenaren zelf toestemming mogen geven tot het grootschalig bulk afluisteren en opslaan van communicatie, maar dat de betrokken dienst daarmee nog

[1] https://twitter.com/PowerDNS_Bert/status/637904099699224576

POWERDNS Stay Open. OX® DOVECOT

geen 'kennis neemt' van deze communicatie. Deze 'kopen maar niet kijken' constructie bindt de kat op het spek.

- De nieuwe "medewerkingsplicht" voor tappen is in het geheel niet uitgewerkt, waardoor een hoge mate van onzekerheid (zowel in kosten als verplichtingen) voor het bedrijfsleven wordt gecreëerd. Deze onzekerheid zal voor veel bedrijven en zeker voor de onze, leiden tot het besluit servers en communicatiediensten snel buiten Nederland te plaatsen, en zeker geen nieuwe investeringen te doen die onder de reikwijdte van deze wet vallen.
    - De medewerkingsplicht kan bijvoorbeeld **ongelimiteerde** investeringen vergen die volgens het huidige voorstel niet vergoed zullen worden.
        - Er is geen enkel kader voor proportionaliteit van de inzet en ingrepen die bij aanbieders verplicht worden gesteld.
    - Het is onduidelijk wie er aansprakelijk is bij storing van de onder deze plicht geplaatste apparatuur en wie de schade bij onderbreking van de communicatiedienstverlening zou vergoeden. **Iedere toevoeging van interceptieapparatuur verlaagt per definitie de betrouwbaarheid en veiligheid van een netwerk.**
    - Er zijn geen technische standaarden vastgelegd waarmee invulling gegeven kan worden aan medewerkingslasten aangaande bulk tappen, waardoor benodigde programmatuur en apparatuur niet voorbereid of aangeschaft kan worden. Dit leidt tot hele dure 'after sales' gesprekken met leveranciers van netwerkapparatuur.
- De rechtspositie van aanbieders van communicatiediensten bij niet willen of kunnen voldoen aan een medewerkingslast lijkt te bestaan uit 'strafrechtelijk vervolgd worden voor een misdrijf met een gevangenisstraf van twee jaar'[2]. Er is geen mogelijkheid tot beroep.
    - Het voorstel vordert vrijheidsstraf of een boete bij gebrek aan medewerking door aanbieders van communicatiediensten, of zelfs 'onopzettelijk gebrek aan medewerking'. Wij vrezen dat met het dreigement van vrijheidsstraf lager technisch personeel en kleinere aanbieders zich gedwongen zullen voelen sowieso mee te werken, en niet de kans of toegang krijgen tot een adequaat verweer
    - Ook voor bedrijfsmatige aanbieders is het denkbaar dat de gevangenisstraffen en boetes op medewerkers verhaald zullen worden[3]
- Artikel 22 lid 3 maakt de levering van communicatie mogelijk die eigenlijk valt onder artikelen 30 tot en met 40, met dien verstande dat onder het regime van artikel 22 de Diensten direct zonder verdere toestemmingen of lastgevingen geheel kennis mogen nemen van de informatie.
- De sterke dwang voor ongeclausuleerde medewerking zou, bij onwil of onmacht tot medewerking, uitgeruild kunnen worden tegen het 'vrijwillig' leveren van andere gegevens, bijvoorbeeld klantenbestanden, overige communicatiestromen, betalingsgegevens of locatiegegevens onder artikel 22 lid 3. Er is dan sprake van *détournement de pouvoir*. Het artikel 22 regime is voor de Diensten sowieso aantrekkelijker dan de medewerkingsplicht, indien de leverancier van de informatie vrijwillig meewerkt.
- Het voorliggende voorstel definieert een klasse ambtenaren ('supertappers') die zelf zonder nadere toestemming volledig *kennis mogen nemen* van alle bulk getapte communicatie. Dit is ongehoord en schendt ieder principe van behoorlijk overheidshandelen. Dit is een staat in een staat.
    - Mede hierom is het verlenen van toestemming voor de bestaande en nieuwe bevoegdheden door ambtenaren en betrokken ministers zelf zeer problematisch
- Deze 'supertapper' ambtenaren zijn in een buitengewoon penibele positie. Bij uitsluiting van hun collega's[4] kunnen zij kijken naar de 'ruwe' afgeluisterde informatie, ook uit die bronnen waar in bulk (ongericht) afgeluisterd wordt. Indien de minister (nog) geen toestemming heeft verleend om middels artikel 35 *kennis te nemen* van getapte informatie staan deze medewerkers onder grote collegiale druk van teams om een tip van de sluier op te lichten of eventueel een voorschot te nemen op te verwachten ministeriele toestemming. Wij wensen niemand deze rol toe.
- De Diensten mogen zelf, zonder toestemming van de betrokken minister[5], 'selectiecriteria' bepalen waarmee via artikel 35 kennis mag worden genomen van bulk afgeluisterde informatie. Specifiek bepaalde

---

[2] Uit artikel 132: "Overtreding van de in het eerste lid strafbaar gestelde feiten wordt gestraft a. in geval van een misdrijf, met gevangenisstraf van ten hoogste twee jaar of geldboete van de vierde categorie; b. in geval van een overtreding, met hechtenis van ten hoogste zes maanden of geldboete van de vierde categorie"

[3] https://nl.wikipedia.org/wiki/Strafrecht_(Nederland)#Daderschap_van_de_privaatrechtelijke_rechtspersoon

[4] Uit artikel 33: "welke ter uitvoering van het bepaalde in dit artikel bij uitsluiting van anderen kennis mogen nemen van de ingevolge artikel 33 verworven gegevens ten behoeve van de in het eerste lid, tweede volzin, bedoelde activiteiten"

[5] Uit artikel 35 "Het vaststellen van de selectiecriteria geschiedt (...) namens deze het hoofd van de dienst.".

selectiecriteria ('Jansen' of 'twitter.com') zijn mogelijk direct gerelateerd aan een door de Minister goedgekeurde selectielast, maar kunnen ook vrijwel alle ongerelateerde communicatie selecteren.

- De definitie van aanbieder van communicatiediensten[6] omvat, voor zover wij kunnen zien, vrijwel ieder bedrijf met een telefoon, fax, mailserver of webforum, naar schatting 360000 organisaties in Nederland. De definitie omvat niet alleen daadwerkelijke aanbieders van communicatiediensten maar ook allen die **namens** een dergelijke aanbieder data opslaan of verwerken.
    - Dit maakt een eindeloze keten van leveranciers mogelijk die zo allen 'aanbieder van een communicatiedienst' worden!
- De diensten mogen hun bijzondere bevoegdheden inzetten voor een aantal waardige doelen zoals het voortbestaan van de democratische rechtsorde en 'de veiligheid'. In aanvulling hierop handhaaft het huidige voorstel de mistige grondslag 'gewichtige belangen van de staat' (artikel 8). Dit is een gigantische 'loophole' waarmee allerhande (nieuwe, zware) bevoegdheden gelegitimeerd kunnen worden. Indien een bevoegdheid geen nood vindt in voortbestaan van de democratische rechtsorde of de veiligheid, wat kan het dan nog zijn?

Aanbevelingen

- Verhuis het door ambtenaren en minister verlenen van toestemming voor afluisteren naar de rechterlijke macht, gelijk artikel 29 nu voor het briefgeheim
- Werk de medewerkingsplicht veel verder uit, en regel daarbij minimaal:
    - Welke medewerkers binnen een organisatie aangesproken mogen worden, en dat dit een directiemedewerker met beslissingsbevoegdheid zal moeten zijn waarvan verwacht kan worden dat deze zich juridisch kan laten bijstaan in de beoordeling van het verzoek
    - Een beroepsmogelijkheid voor aanbieders van communicatiediensten anders dan afwachten van een dagvaarding voor vervolging voor een misdrijf met een gevangenisstraf van 2 jaar
        - Faciliteer tevens dat er voldoende juristen met de juiste screening beschikbaar zijn om deze aanbieders bij te staan
        - Bij deze beroepsmogelijkheid zou ook de proportionaliteit van de medewerkingslast bekeken moeten worden. Is het bijvoorbeeld legitiem om een kleine opleidingsinstelling te dwingen een gehele tapinstallatie aan te schaffen voor 1 mogelijke tap?
    - Dat de diensten ongelimiteerd aansprakelijk zijn voor schade als gevolg van storingen veroorzaakt door implementatie van het medewerkingsverzoek, met omgekeerde bewijslast
    - In welke mate communicatieaanbieders verplicht kunnen worden tot investeringen die geen ander doel dienen dan 'meewerken' en vanaf welk bedrag de overheid ook de investeringskosten zal dragen
    - Dat de vergoeding voor operationele kosten van hooggekwalificeerd technisch personeel meer bedraagt dan 50 euro per uur (het uit de Telecommunicatiewet overgenomen bedrag).
    - Dat verduidelijkt is of de medewerkingsplicht ook vervuld mag worden door buitenlands (ongescreened) personeel
- Aanbevelingen op technisch vlak voor de medewerkingsplicht:
    - Verplicht de Diensten zich te committeren aan het exclusieve gebruik van gepubliceerde protocollen en technieken
    - Stimuleer de ontwikkeling van een open source platform dat voor veel gebruikte communicatieplatformen 'medewerking' voor artikelen 32 en 38 implementeert; daarmee kan aan de bulk van de 360000 kleine aanbieders van communicatiediensten tegemoet worden gekomen,
        - Stel een testplatform beschikbaar waarop organisaties hun tapvoorziening kunnen testen
- Sluit de open deur van "andere gewichtige belangen van de staat" (artikel 8) uit als grondslag voor het inzetten van (minimaal) artikelen 30, 32, 33, 37 en 38.
- Beperk de definitie van aanbieders van communicatiediensten tot daadwerkelijke aanbieders van deze diensten, en verwijder de clausule dat eenieder die diensten levert AAN een aanbieder van communicatiediensten ook een dergelijke aanbieder is.

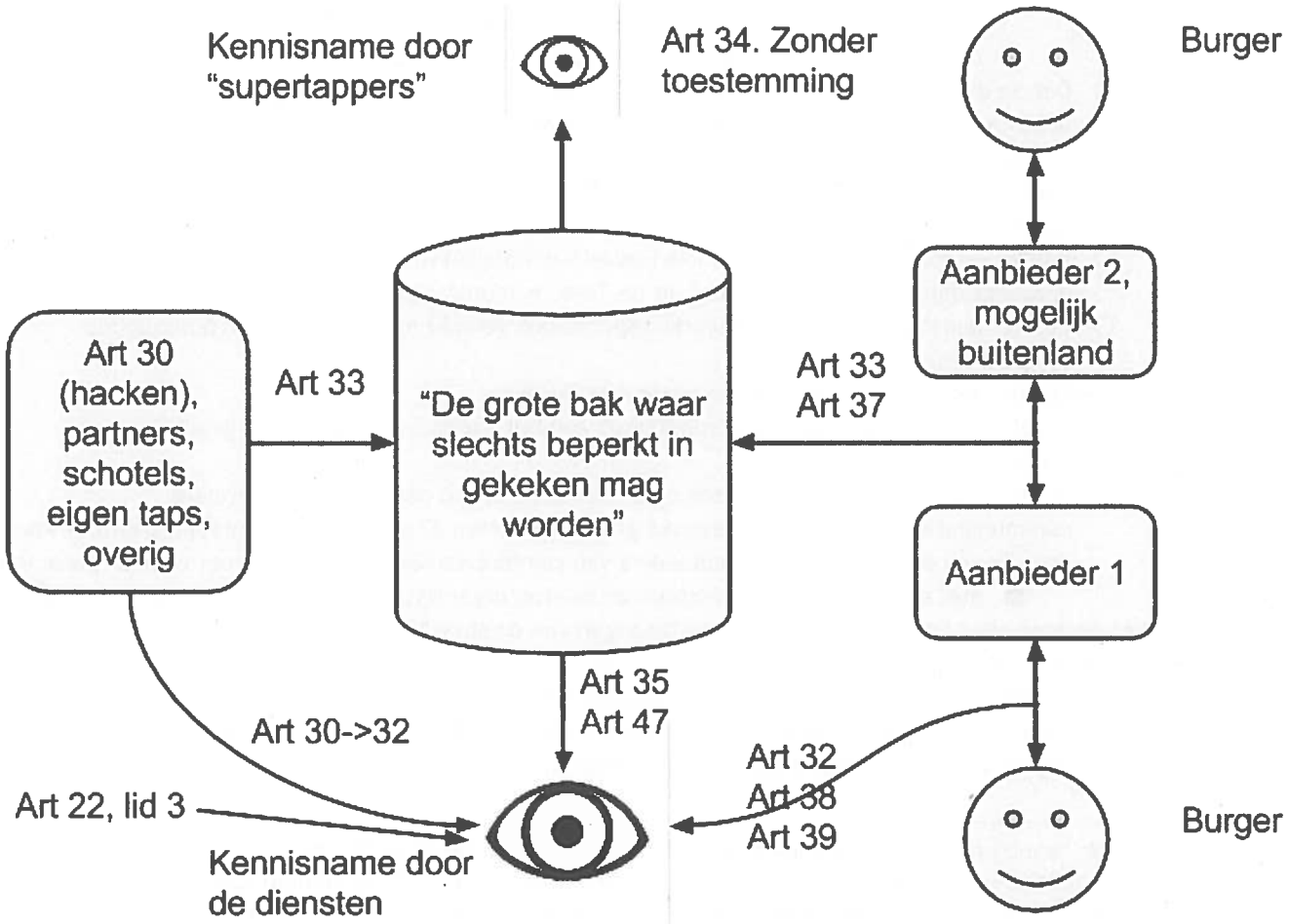
---

[6] Uit artikel 31: "aanbieder van een communicatiedienst: de natuurlijke of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, **of die gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst"**

- Voeg een lid toe aan artikel 22 waarbij expliciet wordt gemaakt dat gegevens die ingewonnen zouden kunnen worden via artikelen 30 tot en met 40 ook daadwerkelijk onder het regime van die artikelen verkregen moeten worden.
- Voeg een lid toe aan artikel 22 waarbij leverancier van gegevens aan AIVD verklaart dat deze gegevens daadwerkelijk vrijwillig overhandigd zijn, en niet ter compensatie voor onmacht of onwil te voldoen aan de medewerkingsplicht communicatiegegevens.
- Aangaande de 'supertappers' uit artikel 35:
    - Verschaf deze aangewezen ambtenaren een zeer heldere rechtspositie, waardoor zij nooit onder druk gezet kunnen worden door hun meerderen om de kennis die zij 'bij uitsluiting' mogen nemen binnen de dienst te delen, ook niet 'heel even'.
        - Overweeg deze ambtenaren in dienst te laten zijn van een ander ministerie
    - Als onderdeel van deze rechtspositie dient deze ambtenaren de mogelijkheid geboden te worden de vice-president van de Raad van State of de president van de Hoge Raad direct te benaderen indien zij in gewetensnood komen. Deze gesprekken dienen geprivilegieerde informatie te zijn en behandeld te worden als geheimhouderscommunicatie.
- Leg verslag van de hoeveelheid 'hits' op basis van door ambtenaren bepaalde selectiecriteria uit artikel 35, en inschatting welk percentage hits gerelateerd was aan door de minister goedgekeurde selectielasten. Dit voorkomt selectie op termen die (veel) te breed matchen.

Samenvatting relevante artikelen en hun samenhang

Het voorliggende wetsvoorstel handhaaft de internationaal gezien curieuze constructie dat de Diensten communicatie mogen afluisteren en verzamelen, zonder dat er toestemming is ook "kennis te nemen" van deze communicatie. Met andere woorden, er mag een 'bak' gevuld worden met gegevens, en die gegevens mogen drie jaar lang in de bak blijven zitten, maar men mag er niet alles mee doen. De diensten mogen volledig kennisnemen van communicatie die na toestemming (artikel 35) uit de bak 'geselecteerd' is.



In de huidige WIV mag de bak gevuld worden met 'niet-kabelgebonden communicatie met oorsprong in het buitenland'. Daarnaast kunnen specifieke individuen en organisaties afgeluisterd worden. Nieuw in het voorliggend voorstel is dat alle kabels nu ook 'ongericht' (bulk) getapt mogen worden om de bak te vullen.

In aanvulling op de huidige WIV mogen er ook automatische analyses op de gesloten bak uitgevoerd worden, waarbij slechts voor sommige analyses specifiek toestemming vereist is. Tevens creëert het voorstel een bijzondere nieuwe klasse ambtenaren ('supertappers') die ook zonder specifieke toestemming in de bak mogen kijken, met als bedoeling dat zij daarmee hun analyses vorm kunnen geven en kunnen helpen bij het bepalen van selectiecriteria waarvoor vervolgens toestemming gevraagd kan worden.

Dit wordt verantwoord met het idee dat de gegevens die in de 'verzamelen maar niet kijken'-bak zitten geen echte privacy-schending opleveren (maar zie onder).

Ook bijzonder in deze context is dat de nieuwe WIV een medewerkingsplicht voor bulk afluisteren oplegt aan aanbieders van communicatiediensten **en zelfs aanbieders van diensten aan communicatiediensten**. Tevens definieert men deze aanbieders als 'zij die onder de Telecommunicatiewet aanbieders zijn, aangevuld met zij die dat volgens deze wet niet zijn'. Met andere woorden, vrijwel iedereen.

Onderlinge samenhang artikelen

Middels **artikel 32** (stromend) en **artikel 38** (opgeslagen) moeten aanbieders als gedefinieerd in **artikel 31** communicatie van specifieke organisaties, individuen geïdentificeerd door telefoonnummers, emailadressen, facebook logins, etc, overdragen aan de diensten. Een dergelijke 'gerichte tap' kan ook gerealiseerd worden door een computer/telefoon/geautomatiseerd werk te hacken via **artikel 30**, waarbij sowieso kennis wordt genomen van alle informatie op dit geautomatiseerd werk.

Via **artikel 33** mogen de diensten bulk communicatie vergaren uit diverse bronnen om deze 3 jaar te bewaren **zonder er kennis van te nemen**. Alleen de 'supertappers' mogen de gegevens in de bulk 'bak' zonder nadere toestemming bestuderen. Via **artikel 37** worden alle aanbieders van communicatie (en ook hun onderliggende leveranciers) verplicht mee te werken aan bulk afluisteren van hun netwerken ten behoeve van **artikel 33**.

Middels **artikel 34** mogen de 'supertappers' de inhoud van de bulk bak bestuderen en analyseren (**artikel 47**), onder andere om selectiecriteria te maken die dan via **artikel 35** de rest van de diensten in staat stellen 'kennis te nemen' van geselecteerde data.

Informatie over netwerken (topologie, configuratie, geen communicatie-inhoud of metadata) kan opgevraagd worden via **artikel 36.** Informatie over gebruikers moet geleverd worden via **artikel 40**. Metadata van communicatie uit heden, verleden en toekomst kan opvraagd worden via **artikel 39**.

Tenslotte kunnen de Diensten zich middels **artikel 22** tot eenieder (overheidsonderdeel of niet) wenden om, ondanks wat overige wet- en regelgeving daarover zegt, eenmalig of permanent (online) toegang te krijgen tot "gegevens".

Enkele praktische punten

Voor gericht tappen zijn over de afgelopen jaren goede procedures uitgewerkt. Alle (grote) Nederlandse aanbieders zijn aftapbaar, en de kleinere hebben zich verenigd in een organisatie die onderling tapapparatuur uitwisselt[7]. Nederland is hiermee een voorbeeld voor de hele wereld. Via open onderhandelde standaarden worden getapte gegevens overgedragen en er is een rijk scala aan leveranciers van benodigde hard- en software.

Voor de nieuwe (bulk)tapbevoegdheden is echter in het nieuwe wetsvoorstel niets geregeld, behalve dat aanbieders 'mee moeten werken'.

Dit zou bijvoorbeeld in kunnen houden dat de provider toe moet staan dat een 'zwarte doos' in het netwerk geplaatst wordt waar aangewezen fibers doorheen moeten lopen. Deze doos zou dan met een extra verbinding

[7] Nederlandse Beheersorganisatie Internetproviders: http://www.nbip.nl/diensten/tapdiensten/

aangesloten kunnen worden op de Diensten. Tevens zal de goede werking van deze 'zwarte doos' moeten worden gewaarborgd, bijvoorbeeld dat deze op juiste wijze van voedingsspanning zal moeten worden voorzien.

In andere gevallen kan het er ook neerkomen dat de medewerking bestaat uit het extensief herconfigureren van apparatuur en het aanschaffen en installeren van nieuwe hardware- en softwaremodules om door de overheid gewenst verkeer op te sturen.

Ook ten aanzien van geheimhouding zijn er vragen te stellen. Een traditionele gerichte taplast kan zeer beperkt bekend zijn binnen een aanbieder van telecommunicatiediensten. Hoewel iedereen kan weten dat krachtens de wet de provider aftapbaar moet zijn voor specifieke gebruikers kan de identiteit van de afgeluisterde gebruikers eenvoudig afgeschermd worden.

Bij bulk afluisteren in gevolg van artikel 37 is het veel lastiger om geheim te houden welke verbindingen afgeluisterd worden, daar er apparatuur in het netwerk geplaatst wordt die gekoppeld is met specifieke netwerkelementen die niet alle klanten bedienen.

Het ligt voor de hand dat als onderdeel van de medewerkingsplicht de diensten het gebruik van Nederlands, gescreened, personeel zullen verplichten. Gegeven de grote internationalisering en vrijwel universele outsourcing zal dit een disproportionele belasting leggen op aanbieders van communicatiediensten.

Wegens het gebrek aan verdere definitie van 'medewerking' blijven wij over dit alles in onzekerheid.

Aansprakelijkheid

Uit ervaring blijkt dat interceptieapparatuur de betrouwbaarheid van netwerken verlaagt, alleen al doordat simpelweg meer handelingen verricht moeten worden en er "meer kapot kan".

Tevens kan de apparatuur zelf bijvoorbeeld kortsluiting veroorzaken, defect raken (want, wie is bevoegd hierop onderhoud op te plegen?) of het netwerk (onbedoeld) zwaarder te belasten door (te) veel gegevens naar de overheid te sturen.

De Nederlandse overheid zou voldoende vertrouwen in haar handelen moeten hebben om aanbieders middels een omgekeerde bewijslast een ruime vergoeding te garanderen voor eventuele schade naar aanleiding van onder 'verplicht meewerken' geleverde diensten.

Een mogelijk scenario

Onder het voorliggende wetsvoorstel (in tegenstelling tot de huidige WIV) kunnen de diensten de Dienst Automatisering (DA) van de Tweede Kamer verplichten om:

- Netwerkdiagrammen op te leveren, hoe de diverse fracties op het parlementaire netwerk zijn aangesloten, gegevens over hoe de draadloze (wifi) infrastructuur gekoppeld is (Art 36)
- Te vertellen wat het wachtwoord is voor het access point van de VVD fractie (indien bekend bij de DA) (Art 30)
    - En anders graag een kopie van al het netwerkverkeer naar deze fractie (Art 33/37)
- Een tap op alle telefoongesprekken van de SP fractie (over zowel de interne als de externe lijnen) (33/37)
- Een tap op alle telefoongesprekken naar Israël vanuit de Kamer (33/37)
- **Apparatuur aan te schaffen om deze telefoontaps mogelijk te maken**
- Een kopie te leveren van de data opgeslagen ten behoeve van de PvdA fractie ('de netwerkschijf') (Art 38)
- De doorgaande overdracht te verlangen van alle opgeslagen en toekomstige email en al het Microsoft Lync verkeer van de gehele D66 fractie (Art 38)
- De installatie van een "zwarte doos" op de wifiverbinding die aan journalisten beschikbaar gesteld wordt (Art 33/37)
- Een permanente kopie van al het netwerkverkeer van het gehele parlement (Art 33/37)

De vergoeding voor bovenstaande handelingen zal het salaris zijn van de betrokken medewerkers, vermeerderd met direct gerelateerde kosten (administratief, bureau, ondersteuning). Investeringen voor hardware of software gemoeid met de overdracht zal niet vergoed worden. Voordat de taps 'live' gaan zal er overleg plaatsvinden.

Indien de DA niet mee zou werken aan bovenstaande verzoeken kan men dit weigeren, waardoor de strafmaat direct overgaat van 'overtreding' naar 'misdrijf' en daarmee een boete uit de 4e categorie of een gevangenisstraf van 2 jaar, wegens 'opzettelijk niet meewerken'. Als het de DA ondanks haar beste bedoelingen niet lukt om te voldoen aan de eisen blijft de celstraf beperkt tot zes maanden (of de equivalente boete).

Onbekend is wie er precies de cel in zou moeten als de boete niet betaald wordt:

- Het hoofd van de Dienst Automatisering
- De voorzitter van het presidium, de kamervoorzitter
- De direct benaderde systeembeheerder
- De minister van Binnenlandse Zaken als budgethouder

Ook onduidelijk is of de betrokken verdachte een fatsoenlijk verweer zou kunnen voeren, daar de medewerker van de AIVD/MIVD ongetwijfeld een geheimhoudingsovereenkomst heeft afgesloten met betrokkenen, en alle details staatsgeheim zijn

Indien de 'zwarte doos' een storing in het netwerk veroorzaakt, de stoppen door laat staan, of uitbrandt, is onduidelijk of deze schade vergoed zou worden. Ook zal er geheimhouding betracht moeten worden over het incident.

Afsluitend

Het voorliggende voorstel baart ons grote zorgen. We hopen dat de bovenstaand geconstateerde problemen en de gesuggereerde oplossingen voor u stof tot nadenken zijn.

Indien het voorgaande tot vragen leidt zijn wij gaarne bereid tot een nadere toelichting. Gelieve in dat geval contact op te nemen met Bert Hubert via bert.hubert@powerdns.com of 015-7850372.

Met vriendelijke groet,

Bert Hubert
Namens PowerDNS.COM BV, Open-Xchange AG en Dovecot Oy

POWERDNS Stay Open. OX® DOVECOT

GREENPEACE

greenpeace international
Ottho Heldringstraat 5, 1066 AZ, Amsterdam, Netherlands
t +31 20 718 2000 f +31 20 514 8151
k.v.k. reg. 41200415 stichting greenpeace council
www.greenpeace.org

De Minister-President, Minister van Algemene Zaken
De Minister van Binnenlandse Zaken en Koninkrijksrelaties
De Minister van Defensie
De Minister van Veiligheid en Justitie

Amsterdam, 1 september 2015

Betreft: Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX

Excellenties,

Greenpeace International (GPI) heeft kennis genomen van bovengenoemd wetsvoorstel en maakt hierbij gebruik van de mogelijkheid via de internetconsultatie haar zienswijze naar voren te brengen.

Het onderzoeken van en publiceren over milieumisstanden vormt een belangrijk onderdeel van de activiteiten van Greenpeace (zowel GPI als de nationale en regionale Greenpeace-kantoren). In sommige gevallen worden wij daarbij geholpen door bronnen die graag anoniem willen blijven. Tot de misstanden die Greenpeace-kantoren de laatste jaren met hulp van vertrouwelijke bronnen bloot hebben kunnen leggen behoren bijvoorbeeld de illegale uitvoer van elektronica-afval,[1] hoge bijvangstniveaus in de tonijnvisserij[2] en verduistering van publieke middelen in de Japanse walvisvaart.[3]

Twijfel of hun identiteit wel echt geheim blijft kan voor mensen die weet hebben van een misstand reden zijn om niet naar de pers of een niet-gouvernementele organisatie (NGO) te stappen. De maatschappelijke gevolgen van een dergelijk 'chilling effect' kunnen aanzienlijk zijn; te denken valt aan informatie over de gebrekkige beveiliging van een kerncentrale of chemische verontreiniging van voedsel die niet of te laat naar buiten komt.

Het is daarom van belang dat het recht op bronbescherming wettelijk gewaarborgd wordt en dat de overheidsdiensten die zich met onderzoek en opsporing bezighouden slechts bij uitzondering en na zorgvuldige rechterlijke toetsing inbreuk op dit recht kunnen maken.

Wij hebben de bijdrage van de Studiecommissie Journalistieke Bronbescherming van de Vereniging voor Media- en Communicatierecht aan deze consultatie met instemming gelezen, en sluiten ons aan bij de daarin gedane aanbevelingen.

In aanvulling op die bijdrage vestigen wij uw aandacht graag op het belang dat bronbescherming niet alleen toekomt aan journalisten in enge, traditionele zin, maar ook aan andere maatschappelijke waakhonden, bijvoorbeeld NGO's, die met behulp van vertrouwelijke bronnen informatie over misstanden openbaren.

Regelmatig blijkt dat Greenpeace-kantoren de aandacht van inlichtingen- en veiligheidsdiensten in verschillende landen genieten; het afgelopen jaar bijvoorbeeld in India en Zuid-Korea.[4] In hoeverre dat op dit

---

[1] Zie http://www.greenpeace.org/international/en/news/features/e-waste-nigeria180209/
[2] Zie http://www.greenpeace.org.uk/blog/oceans/video-global-tuna-industry-doesnt-want-you-see-20111117
[3] Zie http://www.greenpeace.org/international/en/publications/reports/whaling-on-trial/
[4] Zie http://www.ndtv.com/cheat-sheet/greenpeace-targeted-by-intelligence-bureau-again-10-developments-579397 en http://www.theguardian.com/environment/2015/feb/24/spy-cables-greenpeace-kumi-naidoo-targeted-security-threat-g20-seoul

GREENPEACE

greenpeace international
Ottho Heldringstraat 5, 1066 AZ, Amsterdam, Netherlands
t +31 20 718 2000 f +31 20 514 8151
k.v.k. reg. 41200415 stichting greenpeace council
www.greenpeace.org

moment in Nederland speelt is niet duidelijk, maar ook van deze onduidelijkheid kan een 'chilling effect' ten aanzien van bronnen uitgaan.

De Studiecommissie Journalistieke Bronbescherming verwijst (zie aanbeveling 3 van 22 oktober 2014) naar *Recommendation No. R (2000) 7 to Member States on the Right of Journalists not to Disclose their Sources of Information* van het Comité van Ministers van de Raad van Europa. Hoewel bronbescherming in deze aanbeveling als een recht van journalisten omschreven wordt, wordt de term 'journalist' zodanig breed en open geformuleerd dat daaronder ook medewerkers van een NGO zouden kunnen vallen:

> *"the term "journalist" means any natural or legal person who is regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication".*

Daarnaast heeft het Europees Hof voor de Rechten van de Mens in inmiddels een groot aantal zaken benadrukt dat NGOs, net als de media, aan te merken zijn als 'maatschappelijke waakhonden', en uit dien hoofde aanspraak op dezelfde rechtsbescherming onder het Europees Verdrag voor de Rechten van de Mens kunnen maken:

> *"The Court has ... accepted that non-governmental organisations, like the press, may be characterised as social "watchdogs". In that connection their activities warrant similar Convention protection to that afforded to the press."*
>
> *- Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung v. Austria,* 28/11/2013, § 34.[5]

Naar onze mening betekent dit ook dat nationale wetgeving die invulling geeft aan het recht op bronbescherming zoals dat voortvloeit uit artikel 10 EVRM op gelijke voet van toepassing dient te zijn op NGO's en hun medewerkers.

Wij geven u daarom graag in overweging om onder artikel 24, lid 4, niet te spreken over een 'journalist', maar meer in algemene zin over personen of instellingen die in het kader van regelmatige of beroepsmatige nieuwsgaring beschikken over gegevens afkomstig van een bron. Een alternatief zou zijn om in de Memorie van Toelichting expliciet te verwijzen naar het brede journalistenbegrip onder de aanbeveling van de Raad van Europa, alsmede de jurisprudentie van het EHRM die de rechten van NGO's gelijkschakelt met die van de pers.

Hoogachtend,

Daniel Simons

Daniel Simons
Legal Counsel Campaigns & Actions
Greenpeace International

---

[5] Van gelijke strekking zijn bijvoorbeeld ook *Vides Aizsardzības Klubs v. Latvia,* 27/05/2004, § 42; *Társaság a Szabadságjogokért v. Hungary,* 14/04/2009, § 27; *Animal Defenders International v. the United Kingdom,* 22/04/2013, § 103; *Youth Initiative for Human Rights v. Serbia,* 25/06/2013, § 20.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en
Ministerie van Defensie

Betreft: Internetconsultatie Wet op de inlichtingen- en veiligheidsdiensten 2015

31 augustus 2015, Groningen, Antwerpen, Kaapstad

Beste volksvertegenwoordiger,

Je hebt door middel van de internetconsultatie belanghebbende gevraagd mee te denken over de wet op de inlichtingen- en veiligheidsdiensten. Dit stuk is geschreven namens zakelijke telecomprovider Voys gevestigd in Nederland, België en Zuid-Afrika, wholesale telecomprovider VoIPGRID en iedere Nederlandse ondernemer en burger die iets doen op het internet, want allen worden geraakt door dit voorstel.

Ik kijk een tijdje naar de man die iedere tien seconden in zijn handen klapt. Na een minuut of vijf spreek ik hem aan: "Waarom klapt u in uw handen?". "Dat is om de olifanten weg te jagen," zegt de man. "Olifanten, maar er zijn hier toch helemaal geen olifanten?" is mijn reactie, waarop hij zegt: "Nou, zie je wel dat het werkt!".

Er zijn drie redenen waarom het wetsvoorstel een radicale make-over verdient.

1. Het wetsvoorstel druist in tegen de Grondwet

- Artikel 7 van de Nederlandse Grondwet geeft de Nederlandse burger het recht op vrijheid van meningsuiting.
- Artikel 10 van de Nederlandse Grondwet geeft de Nederlandse burger het recht op privacy.

Dit wetsvoorstel ondermijnt beide rechten, omdat vrije meningsuiting moet bestaan bij de weet dat er niemand meeluistert.

2. Gebrek aan trias politica

Het wetsvoorstel ondermijnt de scheiding van de wetgevende, uitvoerende en rechterlijke macht, omdat er geen juridische toetsing nodig is bij het toepassen van de voorgestelde wet.

3. Mass surveillance werkt niet

De NSA heeft een begroting van $10,8 miljard en twee[1] onafhankelijke onderzoeken hebben het volgende aangewezen: *"We have not identified a single instance involving a threat to the United States in which the NSA program made a concrete difference in the outcome of a counterterrorism investigation".*

---

[1] https://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program-2.pdf
https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

Mass surveillance is exorbitant duur en werkt simpelweg niet, maar eigenlijk zou dat niet moeten uitmaken als het wetsvoorstel tegen de grondwet in druist.

Op 3 november 1848 werd de Grondwet afgekondigd die de basis vormt van onze parlementaire democratie. Mijn voorstel is om samen met jou als volksvertegenwoordiger, de internet/telecomsector en privacyorganisaties op **3 november 2015** aan tafel te gaan zitten. Zo kunnen we gezamenlijk een privacy- en veiligheidsvriendelijk wetsvoorstel schrijven welke tevens de basis kan vormen voor een nieuwe wet omtrent de bewaarplicht.

Namens Voys, VoIPGRID en de Nederlandse burger,

Mark Vletter

PRIVACY FIRST

Postbus 16799
1001 RG Amsterdam
Tel. 020 - 8100279

Aan:
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie Constitutionele Zaken en Wetgeving
Via www.internetconsultatie.nl

Uw ref.	:	
Onze ref.	:	SPF-20150831
Datum	:	31 augustus 2015
Betreft	:	Commentaar Privacy First op concept-wetsvoorstel ter invoering van een nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv)

Geachte heer/mevrouw,

Hierbij geeft Stichting Privacy First graag een eerste reactie op het huidige concept-wetsvoorstel ter herziening van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) 2002. Daarbij herinnert Privacy First allereerst graag aan de inhoud van de openbare toespraak die het hoofd van de AIVD (de heer Rob Bertholee) in september 2012 ten kantore van Privacy First in Amsterdam hield. Het door Privacy First gepubliceerde verslag van deze toespraak[1] is destijds door de AIVD zelf geaccordeerd. Enkele relevante passages uit dit verslag luiden als volgt:

> "[Bertholee] kan zich voorstellen dat correlatie (koppeling) en internationale uitwisseling van gegevens door de burger ervaren wordt als "Big Brother" en dat men zich daar zorgen om maakt. Als burger maakt Bertholee zich daar zelf ook zorgen over.
> (...)
> Bij het vragen om informatie door de AIVD aan burgers mag overigens geen sprake zijn van enige vorm van druk. Hetzelfde geldt voor het vragen van informatie aan journalisten: journalisten zijn geheel vrij om daar wel of niet aan mee te werken. "Als een journalist er niet aan wil meewerken, dan is dat jammer voor de AIVD, maar daar houdt het mee op," aldus Bertholee.
> (...)
> Wat eventuele herziening van de Wiv2002 betreft merkt Bertholee op dat de huidige wettelijke ruimte voor de AIVD voldoende is en dat hij niet meer bevoegdheden nodig heeft.
> (...)
> Bertholee eindigt zijn lezing door nog eens te benadrukken dat de AIVD geen dossiers van iedereen bijhoudt, niet iedereen onder de tap houdt, (...) niet elke

[1] Zie *Hoofd AIVD: "Ik ben geen voorstander van Big Brother"* (20 september 2012), https://www.privacyfirst.nl/aandachtsvelden/metaprivacy/item/576-hoofd-aivd-geen-voorstander-van-big-brother.html. Zie tevens https://www.security.nl/posting/38120/Hoofd+AIVD+geen+voorstander+van+Big+Brother.

> computer hackt, geen handhavende bevoegdheden heeft [en] geen druk op mensen uitoefent (...)."

De belangrijkste boodschap van Bertholee aan het publiek destijds was dat "hij geen voorstander was van Big Brother." Begin 2015 herhaalde hij deze boodschap ter gelegenheid van het semi-openbare ReuringCafé bij de Vereniging voor OverheidsManagement: "Het recht op privacy is voor mij net zo heilig als voor Privacy First", aldus Bertholee tegenover een zaal vol topambtenaren.

Als het hoofd van de AIVD zélf al vindt dat hij voldoende bevoegdheden heeft en waarschuwt voor Big Brother, dan heeft de Nederlandse regering bij iedere uitbreiding van deze bevoegdheden bij voorbaat de schijn tegen zich. In het licht hiervan kunnen met name de volgende aspecten uit het huidige concept-wetsvoorstel in de optiek van Privacy First niet door de beugel:

Strafbare feiten

Allereerst opvallend is dat de huidige bevoegdheid van agenten om strafbare feiten te plegen vrijwel ongemoeid wordt gelaten en niet nader juridisch wordt ingekaderd. Dit ondanks de reeds bestaande (maar nooit uitgevoerde) opdracht in de huidige Wiv om deze bevoegdheid alsnog van juridische waarborgen te voorzien middels een algemene maatregel van bestuur (AMvB).[2] Ook de commissie Dessens achtte dergelijke nadere normering – terecht – wenselijk. Desondanks wenst het kabinet de grondslag voor de betreffende AMvB af te schaffen.[3] Het plegen van strafbare feiten door agenten blijft daarmee grotendeels plaatsvinden in een juridisch vacuüm. Privacy First acht dit onwenselijk, riskant en ronduit gevaarlijk.

Hack-bevoegdheid en decryptiebevel

Een tweede verwerpelijk onderdeel van het wetsvoorstel is de bevoegdheid om ieders computer te kunnen hacken en mensen te kunnen verplichten om versleutelde bestanden voor de diensten te ontsleutelen, dit laatste op straffe van 2 jaar hechtenis.[4] Privacy First acht dit volstrekt in strijd met het recht op privacy, want niet noodzakelijk en disproportioneel. Daarnaast is het voorstel in strijd met het verbod van zelfincriminatie (*nemo tenetur*). Het voorstel legt de basis voor toekomstig machtsmisbruik en vormt in de optiek van Privacy First een typische bouwsteen voor een politiestaat i.p.v. een democratische rechtsstaat. Dit geldt eveneens vóór het onderdeel in het wetsvoorstel met betrekking tot de invoering van een massale internettap; deze bevoegdheid is ronduit totalitair. De door het kabinet veronderstelde noodzaak hiervan wordt in het voorstel slechts gesteld en nauwelijks onderbouwd, laat staan aangetoond.[5] In een democratische samenleving is de maatschappelijke noodzaak van een dergelijke bevoegdheid echter überhaupt ondenkbaar. Dit voorstel is daarmee bij voorbaat onrechtmatig.

---

[2] Zie Wiv 2002, art. 21 lid 7.

[3] Zie concept-Memorie van Toelichting (MvT), pp. 42-43.

[4] Zie concept-artt. 30 & 132 Wiv; zie tevens concept-MvT, pp. 51-55.

[5] Zie concept-MvT, pp. 62-63.

Datamining & profiling

De bevoegdheden tot het opvragen en gebruiken van gegevens zijn in het huidige wetsvoorstel vrijwel onbegrensd. Het voorstel maakt daartoe zelfs directe toegang tot de databanken van derde partijen (overheid én bedrijfsleven) mogelijk. Bij al deze partijen zullen bovendien complete databanken opgevraagd kunnen worden. Dit alles ten behoeve van koppeling, *datamining* en *profiling*, waarmee een uiterst gedetailleerd (zelfs voorspellend) beeld van groepen en individuen kan worden gecreëerd.[1] Deze bevoegdheden zijn volstrekt disproportioneel en zouden in dit wetsvoorstel juist ingeperkt moeten worden, in elk geval waar het gevoelige (bijvoorbeeld medische of biometrische) data betreft.

Notificatieplicht

Een lichtpuntje in het wetsvoorstel is de handhaving van de notificatieplicht. Deze geldt echter slechts jegens individuen en niet jegens organisaties die (als zodanig) evengoed *targets* kunnen zijn geweest.[2] Privacy First adviseert dan ook om deze bepaling te amenderen in de zin dat de notificatieplicht tevens voor organisaties zal gaan gelden.

Informanten

Privacy First adviseert om de huidige Wiv alsnog te voorzien van een verbod om journalisten als informanten in te zetten. Dit in het belang van een vrije pers en de journalistieke bronbescherming. In het belang van een gezond maatschappelijk middenveld zou een dergelijk verbod eveneens kunnen worden ingevoerd met betrekking tot de inzet van agenten en informanten bij maatschappelijke (non-gouvernementele) organisaties.

Actieve openbaarheid

Privacy First adviseert om de huidige Wiv alsnog te voorzien van bepalingen ter actieve openbaarmaking van (historische) documenten van de diensten. De praktijk van "declassification and transparency" in andere landen (waaronder voorheen de Verenigde Staten) kan in dit opzicht een bron van inspiratie vormen.

Internationale uitwisseling

De rechtsbasis voor internationale uitwisseling van inlichtingen werd de laatste jaren gevormd door het obscure artikel 59 Wiv. Dit artikel voldoet bij lange na niet aan de moderne eisen die art. 8 EVRM aan een dergelijke bepaling stelt. In wezen vindt de huidige praktijk van uitwisseling tussen AIVD/MIVD en buitenlandse geheime diensten daardoor al jaren plaats in een juridisch zwart gat. Het verheugt Privacy First dan ook dat art. 59 Wiv grotendeels wordt herzien en mensenrechtelijk wordt versterkt in de nieuwe artikelen 76-78. Deze herziening vormt *grosso modo* een positieve stap vooruit. Probleem blijft echter de internationale uitwisseling van

---

[1] Zie concept-artt. 22 & 47 Wiv; zie tevens concept-MvT, pp. 24-27, 77-78, 102-103.

[2] Zie concept-MvT, p. 99.

ongeëvalueerde bulk-data; dergelijke uitwisseling wordt door het concept-wetsvoorstel en de bijbehorende Memorie van Toelichting (MvT) ten onrechte gelegitimeerd.[8] Deze thematiek speelt sinds eind 2013 een cruciale rol in de rechtszaak *Burgers tegen Plasterk* van Privacy First c.s. tegen de Staat.[9] De voortzetting van deze zaak in hoger beroep blijft door het huidige wetsvoorstel onverminderd actueel en urgent.

Internationale rechtsorde

Nederland heeft de algemene mensenrechtelijke plicht om het recht op privacy in eigen land voortdurend te *bevorderen* i.p.v. te beperken. Door dit wetsvoorstel schendt Nederland deze algemene plicht; het recht op privacy wordt hierdoor immers massaal ingeperkt. Dit zet de vertrouwensrelatie tussen de Nederlandse overheid en de Nederlandse bevolking op scherp, wat zal leiden tot een maatschappelijk *chilling effect*. Dit is funest voor de vrije dynamiek in onze democratische rechtsstaat. Het wetsvoorstel en bijbehorende technologie zullen bovendien worden gekopieerd en misbruikt door minder democratische regimes in het buitenland. Het wetsvoorstel vormt daarmee een internationaal precedent voor een wereldwijde *Rule of the Jungle* i.p.v. de *Rule of Law*. Dit is in strijd met de grondwettelijke plicht van de Nederlandse regering om de ontwikkeling van de internationale rechtsorde te bevorderen.[10] In het licht van het Nederlandse buitenlands beleid dient dit wetsvoorstel derhalve verworpen te worden.

Toezicht

In het huidige wetsvoorstel is het toezicht op de diensten te vrijblijvend en te politiek van aard. In de optiek van Privacy First dient dit toezicht te worden versterkt en onafhankelijker te worden gemaakt, hetzij middels bindend rechtmatigheidstoezicht vooraf door de CTIVD, hetzij middels bindend toezicht vooraf door de rechter. Dergelijk toezicht dient te gelden bij de uitoefening van álle bijzondere bevoegdheden van de diensten. Pas dan zal een rechtsstatelijke uitoefening van deze bevoegdheden optimaal gewaarborgd en voldoende toekomstbestendig zijn.

Vingerafdrukken

Saillant detail is tenslotte nog dat op p. 44 van de MvT wordt opgemerkt dat "[v]an een afzonderlijke regeling voor het onderzoek naar vingerafdrukken wordt afgezien, omdat de resultaten van een dergelijk onderzoek in de praktijk niet altijd bruikbaar zijn en als gevolg daarvan de inzet van deze mogelijkheid uitermate beperkt is." Dit sluit aan bij de eerdere bekentenissen van voormalig minister Donner en staatssecretaris Teeven dat bij biometrische verificatie van de vingerafdrukken die de

[8] Zie concept-MvT, pp. 20, 107, 141-142.

[9] Zie https://www.privacyfirst.nl/acties/rechtszaken/item/691-rechtszaak-tegen-staat-wegens-illegale-dataspionage.html.

[10] Art. 90 Grondwet.

laatste jaren zijn afgenomen t.b.v. Nederlandse paspoorten sprake bleek te zijn van een foutenpercentage van maar liefst 21-30%.[11] Privacy First doet hierbij dan ook nogmaals de oproep om de afname van vingerafdrukken voor paspoorten per direct af te schaffen.

Conclusie

Het huidige concept-wetsvoorstel komt, in de woorden van het Europees Hof voor de Rechten van de Mens, neer op "destroying democracy on the ground of defending it".[12] Dit wetsvoorstel dient dan ook grondig verbeterd danwel verworpen te worden. Bij gebreke hiervan behoudt Privacy First zich het recht voor om dit wetsvoorstel, zodra van kracht, door de rechter te laten toetsen en onrechtmatig te laten verklaren.

Privacy First hoopt u met dit advies van dienst te zijn. Desgevraagd zijn wij graag tot een nadere toelichting op bovenstaande punten bereid.

Hoogachtend,

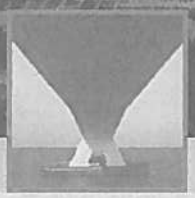
Stichting Privacy First

Vincent A. Böhre
director of operations

[11] Zie *Kamerstukken II* 2010/2011, 25764, nr. 47, p. 19 en *Kamerstukken II* 2012/2013, nr. 32317, nr. 163, p. 15.

[12] EHRM, *Klass and others v. Germany* (Appl. no. 5029/71), 6 september 1978, par. 49.





BIT BV
Galileilaan 19 - 6716 BP Ede
Postbus 536 - 6710 BM Ede
T: +31 318 648688
F: +31 318 643334
E: info@bit.nl - http://www.bit.nl
KvK-nr : 09090351

bit
internet technology

Betreft	Internetconsultatie WIV

Ede, 31 augustus 2015

Geachte excellenties,

BIT, aanbieder van internet service provider en datacenter diensten, is verheugd dat de betrokken ministers de mogelijkheid geven tot reactie op het wetsvoorstel. Gezien onze eigen reactie en die van vele andere inzake betrokken bedrijven en organisaties en verontruste burgers gaan we ervan uit dat er diverse wijzigingen op het huidige voorstel doorgevoerd zullen worden. Wij zijn graag bereid om onze zienswijze nader toe te lichten en inhoudelijk te reageren op een gewijzigd voorstel.

BIT is teleurgesteld dat de borging van inzet van bijzondere bevoegdheden inzake digitale communicatie niet net als die voor poststukken ook bij een rechter getoetst wordt. Het verschil in behandeling tussen beide vormen van communicatie is achterhaald. Digitale communicatie dient een zelfde bescherming te genieten als reguliere post, zoals dit ook al eerder door de Nederlandse, Europese en internationale organisaties beargumenteerd is.

Inzake de bulk interceptie van digitale communicatie merken wij op dat er, ook internationaal, geen overtuigende argumenten worden gegeven dat dit type van onderzoek effectief is. Daarnaast is gebleken dat dergelijk onderzoek grote impact heeft op het ondernemersklimaat voor IT ondernemingen. Dergelijke gevolgen gaan recht in tegen overheidsbeleid inzake IT en start-ups. Niet alleen IT bedrijven zullen bedenkingen hebben bij vestiging in Nederland, een negatieve impact op de groei van cliëntele voor Nederlandse IT ondernemingen wordt tevens verwacht. Het zonder beperkingen kunnen delen van gegevens met buitenlandse informatiediensten versterkt de negatieve gevolgen op de aantrekkelijkheid van Nederlandse IT bedrijven voor hun (potentiële) cliëntele. Omdat ondernemers in het voorstel opgezadeld worden met kosten voor (bulk-)interceptie, zal hun concurrentiepositie ten opzichte van internationale concurrenten verslechteren.

BIT vindt het ongewenst dat de borging van de bijzondere bevoegheid hacking beperkt is tot de minister. Omdat op voorhand niet duidelijk kan zijn op wat voor en wie zijn systeem ingebroken wordt en er zelfs wijzigingen op doorgevoerd kunnen worden, dienen deze bevoegdheden uiterst omzichtig ingezet te worden. Een rechterlijke toetsing van deze bevoegdheden is daarom op zijn plaats. Het is verder ongewenst dat de informatiediensten hiertoe onveilige systemen van derden kan gebruiken en deze systemen bewust onveilig kan laten. Het bewust kwetsbaar laten of maken voor inbraak en/of misbruik van systemen van derden gaat in tegen overheidsbeleid om systemen juist veiliger te maken.

Het wetsvoorstel in zijn huidige vorm kent volgens BIT diverse maatregelen met ongewenste negatieve gevolgen waarvan de effectiviteit bovendien niet aangetoond is en de borging onvoldoende is.

Met vriendelijke groet,

Wido Potters

Response to draft bill Intelligence and Security Services (WiV)

This response is in reaction to the call for contributions for the consultation of the draft proposal of law from the Ministry of Security and Justice (the so called 'Wet op de Inlichtingen- en Veiligheidsdiensten). We welcome the opportunity to react to the draft legislation. Google will address three elements:

1. General concerns
2. Specific measures regarding encryption and entering communication services
3. Concerns on oversight and transparency

For the purposes of this consultation we will focus on these elements. We shall follow developments closely and reserve the right to raise other issues should these come to the fore.

1. General concerns

The draft bill Intelligence and Security Services (WiV) raises concerns as regards to precedent and international consequences. In part these echo the concerns stated for the draft bill versterkingen bestrijding Computercriminaliteit III.

While we understand the intention of the Dutch Government to ensure an adequate remit for the national security services this bill raises serious issues. The measures proposed are extremely intrusive and detrimental to the fundamental rights of civilians and companies worldwide (privacy, confidentiality of correspondence, freedom of expression, freedom of information, freedom to conduct a business, integrity of property). Clear boundaries, procedural safeguards and strong, independent oversight are essential.

- **Bad global precedent:** First of all the broad range of the draft proposal for example the opening of the possibility to enter communication services and to force de-encryption undermine the trust and safety of the same services. These services, often global by nature, would be compromised and user trust lost. On principle this is setting a bad precedent.

- **Divergence within Dutch Government policy** Secondly undermining the security and trust of these - more often than not - internet based services is in direct contradiction with the intent of the Dutch Government in other area's. For example establishing the Netherlands as 'digital gateway' to Europe.[1] In other areas too it appears to be at odds with international policy ambitions. It contradicts the Dutch leadership on freedom of expression online, and is clearly not an example that one

[1] https://www.rijksoverheid.nl/documenten/rapporten/2013/07/02/strategisch-aanvalsplan-the-netherlands-digital-gateway-to-europe

would want to set for the world.[2] Finally, how would this fit with the chair's statement of the Dutch hosted GCCS 2015?[3]

- **Risk for investment climate:** In 2013 the Netherlands Foreign Investment Agency reported a landmark year for investment. With technology companies leading with a growing investment in for example datacentre investments from 1 to 6 centers and upwards for 500 million euro's.[4] The wider scope of the draft bill would appear to endanger the investment climate in the Netherlands, especially where it concerns these kind of (future infrastructure) investments. The issue of investment climate was also rightly pointed out by Nederland ICT in their consultation on the earlier draft proposal Computercriminaliteit III.[5]

2.Specific measures

This section focusses on two specific measures. The measures are particularly intrusive and detrimental to both user and company trust.

- Paragraph 3.2.2.6 **"Verkennen van en binnendringen in geautomatiseerde werken"**

  This paragraph raises serious concerns. In the paragraph measures mentioned include "entering communication services" and "undoing encryption". The first measure would require a specific request based on a court order. This safeguard is not present as regards to this specific element of the proposal. Also the scope of the article is very broad and opens the possibility to gather metadata (art. 30.9). Also the mention of 'authority to (..) breach any security" (art 30.1) would be very damaging for user and company trust and seriously endanger the safety of worldwide cloud-based systems.

  The article on "undoing encryption (art. 30.5) runs counter long standing efforts on encryption. The vast majority of users benefit from having their data and devices encrypted given the risk of everyday threats like losing a phone or having a computer stolen, account hacking, phishing etc, and governments still have access to user data via valid legal processes.

  Google uses the latest technology to help users stay safe. Encryption is simply the 21st

[2] The Minister of Foreign Affairs published a policy letter focussing on the importance of human rights and freedoms. In the letter internet is specifically addressed as one of the pillars of the human rights policy. In Chapter 2, 'Mensenrechten anno 2013: innovatieve aanpak', the sub-chapter 'Innovatie via internet' states "De wijde verspreiding van internet en mobiele telefoons biedt iedereen de kans om mensenrechten schendingen direct onder de aandacht te brengen. (...) Het potentieel van het internet moet verder worden benut voor mensenrechten.".

[3] https://www.gccs2015.com/news/outcome-conference

[4]https://www.rijksoverheid.nl/actueel/nieuws/2014/03/16/recordaantal-extra-banen-dankzij-buitenlandse-investeringen

[5] Nederland ICT, "Reactie op consultatie Wetsvoorstel Computercriminaliteit III', 1 juli 2013, page 5.

century method of protecting personal documents and communication, just as safes and combination locks were in the past. These new steps protect everyday law-abiding citizens, who may lose their phones, or have them stolen, and therefore be put at risk of identity theft, financial fraud, or worse. Numerous government agencies have encouraged/supported technology companies using encryption.

We have encrypted the private links between our datacenters, some of which are in Europe, and we also encrypt user data in rest. In the most recent versions of Android, encrypting data on the device is the default. In 2015, Google announced that the newest release of the Android mobile operating system will allow for device manufacturers to automatically encrypt data on the device. We're doing this to give consumers more protection; for example, this helps protect the sensitive data that users store on their phones in the event of theft or loss. We have also introduced a Chrome plugin, End-to-End, that enables users to encrypt data before it leaves their browser in such a way that only the intended recipient is able to decrypt it. Most laptop and desktop computers have been protected by encryption for a long time. We believe mobile users should have the same protections.

It's important to note that encryption does not prevent law enforcement from obtaining user data from Google through the legitimate legal channels. In valid emergency situations, we can respond promptly. In other situations, requests for content go through MLAT processes. Furthermore, there are serious doubts surrounding the effectiveness to de-encryption in law enforcement. According to a July 2014 report by the U.S. courts, encryption only foiled investigators in 0.25% of wiretap cases (or 9 out of 3500 cases) in 2013, showing that there are often multiple avenues to the same information if government needs it for a case. Only 41 out of 3500 cases involved any encryption at all, and police were able to circumvent encryption in 32 of those cases.[6]

- Paragraph 3.2.2.7 **"Onderzoek van communicatie"**

As also mentioned in our contribution to the consultation on the proposal "Wet versterking bestrijding computercriminaliteit III" extraterritoriality is an especially sensitive issue. The entering, breaching or de-encryption of global and/or cloud-based services undermines the security of users and companies worldwide also doing significant damage to the integrity of the systems. So the in article 32.1 (and article 33.1) mentioned option "to tap, receive, record and listen to any form of conversation, telecommunication or information transfer by means of an automated operation, *regardless of where such takes place*" is very worrying.

[6] http://www.uscourts.gov/statistics-reports/wiretap-report-2013#sa9

3. Oversight and transparency

When considering legislation on surveillance we feel strong checks and balances need to be built in. Any oversight needs to be strong, independent and accessible for citizens. In this proposal all these points seems to be lacking. Google supports, with other leading Internet companies, clear principles for global government surveillance reform efforts.[7] Also we would urge the Dutch Government to consider taking into account the standards mentioned in the recent IVIR report 'Ten standards for oversight and transparency of national intelligence services'.

Our users and their trust is a key concern for us. We feel strongly that users need to be informed about what happens to their data when under our care. Our goal is to empower users by providing data to inform discussions about the free flow of information online. That is why we have been publishing a Transparency Report since 2010 and have been continuously working since to broaden the scope of information we publish. Since we issued our first Transparency Report in 2010, government demands for user data have increased by 250% in the U.S. It is simply not the case that US law enforcement agencies using legitimate legal means are either "going dark" or being stymied by Internet companies and their efforts to protect user data using encryption. The current proposal lacks information on how requests and actions by Government would be published for the general public. For our part we will follow our practice in the United States of America to take any requests and actions by the Government into account when publishing our Transparency Report on the Netherlands, also for the security services. We understand that governments have a duty to protect their citizens; it's why we work hard to comply with legitimate legal requests from law enforcement. Between January and June 2014, we provided some or all user data 84% of the time in response to search warrants issued by U.S. law enforcement agencies. Nevertheless, we strongly believe that government surveillance programs should operate under a legal framework that is rule-bound, narrowly tailored, transparent, and subject to complete and independent oversight.

Without transparency and oversight in intelligence and security services, Google can't keep doing what we do best: creating technology that improves people's everyday lives.

Rogier Klimbie, Head of Public Policy Benelux, Google

Email: rklimbie@google.com

[7] http://www.reformgovernmentsurveillance.com/ and http://googlepublicpolicy.blogspot.nl/2015/03/congress-must-reform-our-surveillance.html

Consultatie WIV

SpeakUp BV
Postbus 1330
7500 BH Enschede
t: +31 88 77 32 587
f: +31 88 77 32 588
e: info@speakup.nl
Kvk: 08141739
BTWnr: NL8153.86.837.B01
Bank: 53.60.41.032
IBAN: NL30ABNA0536041032
BIC: ABNANL2A

Document info

Titel:	Consultatie WIV
Onderwerp:	Internetconsultatie Wet op de inlichtingen- en veiligheidsdiensten 20XX
Eigenaar:	Florian Overkamp
Classificatie:	Publiek

Document historie

Versie	Status	Toelichting	Auteur	Datum
1.0	Definitief		FO	31-08-15

Distributielijst

Alle medewerkers van SpeakUp

Inhoudsopgave

1 Inleiding

SpeakUp heeft kennis genomen van het wetsvoorstel voor een 'Wet op de inlichtingen en veiligheidsdiensten 20xx'. In onze reactie op dit wetsvoorstel zullen wij ons toespitsen op de aspecten die ons als aanbieder van elektronische communicatiediensten raakt. Daarnaast plaatsen we enkele opmerkingen vanuit algemeen maatschappelijk perspectief. Overigens gaan wij in op de meest primaire bezwaren, op grond waarvan wij van mening zijn dat dit voorstel eigenlijk al geheel onhoudbaar is: ***there is no easy fix***. Wij hopen dat op basis van de reacties op de consultatie (waaronder deze) een nadere dialoog geopend kan worden om wel tot werkbare voorstellen te komen. De secundaire zaken laten we dan ook voor wat het is.

In zijn algemeenheid is onze conclusie het volgende: Het wetsvoorstel in haar huidige vorm voorziet in een verregaande uitbreiding van bevoegdheden en medewerkingsplichten waarbij, naar onze mening, onvoldoende invulling wordt geven aan de randvoorwaarden die daar vanuit nationale en europese (grond)wetten en verdragen bij horen. Daarnaast leidt het wetsvoorstel tot een big-brother samenleving die in de beedste zin des woords niet wenselijk is:

- Zeer grote impact op privacy van burgers, en geen zicht op effectiviteit: proportionaliteit is onvoldoende;
- Toezicht verloopt via CTIVD achteraf: toetsing door rechterlijke macht of onafhankelijke autoriteit vooraf ontbreekt;
- Doordat wordt aangehaakt op de bredere definitie uit de Convention on Cybercrime voldoet nagenoeg ieder netwerk, iedere communicatiedienst (en daarmee nagenoeg ieder bedrijf in Nederland) tot het informatiedoel van de inlichtendiensten. Door de enorme hoeveelheid en het gebrek aan standaardisatie werkt dit kostenopdrijvend voor het bedrijfsleven en in het verlengde daarvan burgers

2 De Wet Inlichtingen- en Veiligheidsdiensten 20xx

2.1 Ongerichte informatievergaring

- De huidige wet- en regelgeving voorziet al afdoende in mogelijkheden om gericht informatievergaring (metadata en aftappen) toe te passen. Het wetsvoorstel voorziet echter ook in mogelijkheden om ongerichte informatievergaring toe te passen. Daarnaast worden veel meer organisaties onderworpen aan medewerkingsplicht ten behoeve van deze informatievergaring. ***Vervolgens is in het wetsvoorstel en het memorie van toelichting nauwelijks onderbouwing waarom deze zeer ingrijpende maatregel noodzakelijk is terwijl het zeer goed mogelijk is dat er minder ingrijpende alternatieven voorhanden zijn.***
- Het wetsvoorstel voorziet in ruime bevoegdheden om data van communicatiedienst-aanbieders te vergaren. Sterker nog, het wetsvoorstel gebruikt een definitie die veel meer bedrijven kan aanspreken dan voorheen het geval was. In het memorie van toelichting wordt al opgemerkt dat de diensten momenteel niet in staat zijn om deze informatie te verwerken. ***Dit betekent dat men zoekt naar een speld in een hooiberg – de doelmatigheid is twijfelachtig.***
- Desalniettemin worden de kosten voor inrichting geheel op de bedrijven afgewenteld. ***Dit zal leiden tot een situatie waar deze kosten de concurrentiekracht van bedrijven ten opzichte van andere landen aantast.***
- Het wetsvoorstel biedt bedrijven onzekerheid ten aanzien van deze te maken kosten: De toelichting stelt dat medewerking een beperkt aantal aanbieders zal raken. Het is dus onzeker of de diensten ooit gebruik zullen maken van de mogelijkheid om informatie te vergaren bij een netwerk, maar het netwerk dient daartoe wel ingericht te zijn of te kunnen zijn op enige korte termijn. ***Bedrijven investeren dus mogelijk 'verplicht' in inrichting die niet gebruikt wordt.***
- De toelichting geeft weer dat men nog ervaring moet opdoen op grond waarvan vervolgstappen door de diensten genomen kunnen worden. Hieruit valt af te leiden dat men zelf ook nog niet precies weet hoe dit alles effectief moet worden ingezet, en bedrijven moeten maar gewoon meedoen. ***Dit betekent een carte blanche waardoor bedrijven niet eens weten waar en wanneer zij voor financiele verassingen komen te staan.***
- De bewaartermijnen van vastgelegde communicatie is zeer ruim. Voor ongericht vergaarde informatie is sprake van een termijn van 3 jaar, en onder voorwaarden nog langer. ***Deze termijn van bewaring van ongerichte informatie is bijzonder lang.***

2.2 Toezicht

- Het wetsvoorstel voorziet in ruime bevoegdheden om data van communicatiedienst-aanbieders te vergaren. Zoals we al (onder andere) gezien hebben in de casus rondom de WBT (ECLI:NL:RBDHA:2015:2498) meent ook onze rechterlijke macht dat toetsing door een rechterlijke instantie of onafhankelijke administratieve instantie vooraf noodzakelijk is. Dit is in het wetsvoorstel niet geregeld. ***Deze aanpak is niet in lijn met de begrippen proportionaliteit en doelmatigheid.***

2.3 Maatschappelijke impact

- Het wetsvoorstel ziet toe op een zeer brede toegang van de inlichtendiensten tot algemene (ongerichte) gegevens, gecombineerd met een zeer lange bewaartermijn. In het licht van art. 8 van het EVRM werd al overwogen dat slechts het opslaan van gegevens al een inbreuk vormt. Het is nadrukkelijk niet zo dat pas het gebruik van de gegevens een inbreuk kan vormen. ***Het opslaan op zichzelf al vormt een zeer ingrijpende inbreuk op de privacy van burgers.***
- Naast deze inbreuk op zich leidt deze aanpak ook tot een maatschappelijk effect dat iedere burger zich 'in de gaten gehouden' voelt. Het ondermijnt rechtstreeks alle communicatieplatformen die juist steunen op de vertrouwelijkheid, zoals klokkenluidersplatformen. ***Het voorstel ondermijnt de vertrouwelijkheid van burgers bij geheimhouders (journalisten, advocaten etc.).***
- Toezicht vooraf versus achteraf: CTIVD kan achteraf besluiten dat een bevraging of tap-actie niet proportioneel was. Echter, in dat geval is het kwaad al geschied. Het is in het verleden al meermaals aan de orde geweest dat diensten te ver zijn gegaan bij bijvoorbeeld het aftappen van journalisten. Ondanks uitspraken van onder meer het EHRM tegen dit soort inbreuken is ook in het onderhavige wetsvoorstel geen sprake van toetsing vooraf. ***Dit leidt tot een chilling effect.***
- De brede vergaring lijkt ook te worden aangewend als ruilhandel van gegevens met andere (buitenlandse) inlichtingendiensten. Toezicht op wat er daarna met die gegevens gebeurt is practisch onmogelijk. ***Deze vorm van koehandel met de privacy van burgers is volstrekt onacceptabel.***

3 Tot slot

Zoals in de inleiding al aangegeven is er in onze optiek geen easy fix om dit wetsvoorstel in acceptabele vorm te krijgen. Onze volksvertegenwoordiging moet zich serieus afvragen hoe het kan dat zij enerzijds ageert op schendingen van mensenrechten in andere landen en anderszijds zelf wetsvoorstellen indienen die net zo hard hiermee de handen licht. En als wij buitenlandse diensten aanspreken op hun activiteiten jegens onze burgers, dan ligt het zeker niet voor de hand om in ruil daarvoor zelf die inlichten maar te vergaren.