PRIVACY FIRST

Postbus 16799
1001 RG Amsterdam
Tel. 020 - 8100279

Aan:
Tweede Kamer der Staten-Generaal
Vaste commissie voor Binnenlandse Zaken
Per email: cie.biza@tweedekamer.nl

Afschrift aan:
Minister van Binnenlandse Zaken en Koninkrijksrelaties
Minister van Defensie

Uw ref.	:	
Onze ref.	:	SPF20170131
Datum	:	31 januari 2017
Betreft	:	Commentaar Privacy First op wetsvoorstel 34588 (wet op de inlichtingen- en veiligheidsdiensten)

Geachte Kamerleden,

Volgende week zult u met de Minister van Binnenlandse Zaken in debat gaan over een – in onze ogen – uiterst totalitair wetsvoorstel: de nieuwe wet op de inlichtingen- en veiligheidsdiensten (Wiv). Zonder acute urgentie wordt dit wetsvoorstel momenteel onder hoge druk door het parlement behandeld.

Talloze bezwaren van gezaghebbende adviesorganen zoals de Raad van State, de Autoriteit Persoonsgegevens, de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), het College voor de Rechten van de Mens, de Raad voor de Rechtspraak en zelfs de continentale Raad van Europa zijn daarbij tot nu toe in de wind geslagen. Waarschuwingen vanuit wetenschap en bedrijfsleven worden structureel genegeerd. Onlangs organiseerde uw Kamer weliswaar een ‘hoorzitting’ rond het wetsvoorstel, maar tegenstanders van het wetsvoorstel waren daarbij niet welkom. Privacy First acht de parlementaire behandeling van dit wetsvoorstel tot op heden dan ook onvoldoende kritisch van opzet.

Wij zullen hieronder onze meest fundamentele bezwaren tegen dit wetsvoorstel daarom opnieuw voor u uiteenzetten en cruciale aanbevelingen doen.

Sleepnetbevoegdheid en bewaartermijn

Onder het huidige wetsvoorstel krijgen AIVD en MIVD de bevoegdheid om het internet grootschalig af te tappen, massaal te monitoren en de vergaarde data jarenlang op te slaan voor eventueel later gebruik of internationale uitwisseling, oftewel een digitaal sleepnet met onvoorzienbare afmetingen, doelen, gevolgen en neveneffecten. In ambtenarenjargon heet deze bevoegdheid “OnderzoeksOpdrachtGerichte interceptie” (OOG). Terecht noemde de Autoriteit Persoonsgegevens dit “het eufemisme van het jaar”. Deze bevoegdheid zal immers het ‘alziende oog’ van de

Nederlandse rijksoverheid gaan vormen. Dit past niet in een democratische rechtsstaat.

De internationaalrechtelijk vereiste maatschappelijke noodzaak (art. 8 EVRM) van deze bevoegdheid is tot op heden onaangetoond. Reeds hierom acht Privacy First de invoering ervan onrechtmatig. Naar alle maatstaven is deze bevoegdheid bovendien volstrekt disproportioneel en niet in lijn met het vereiste van subsidiariteit (d.w.z. het verplicht gebruikmaken van het lichtste, meest privacyvriendelijke middel om een legitiem doel te bereiken).

Daarnaast is een dergelijke bevoegdheid tot op heden niet aantoonbaar effectief (laat staan efficiënt) en wellicht juist contra-productief wegens de enorme overload aan irrelevante data. Volstaan zou dan ook kunnen en moeten worden met *targeted* en *tijdelijke* surveillance van relevante individuen en groepen, waarbij de rest van de maatschappij met rust gelaten wordt. Dergelijke surveillance dient altijd *zo gericht mogelijk* te zijn en gepaard te gaan met strikte, *bij wet voorziene*, concrete waarborgen tegen misbruik. Dergelijke waarborgen ontbreken vrijwel volledig in het huidige wetsvoorstel. Dit wetsvoorstel dient daarom verworpen te worden.

Illegale bewaartermijn

Onlangs oordeelde het Europees Hof van Justitie dat overheden nimmer gerechtigd zijn om data van onschuldige burgers massaal te (laten) verzamelen en op te slaan voor eventueel later gebruik in het veiligheidsdomein.[1] Het Hof baseerde zich hierbij mede op art. 8 EVRM (het recht op privacy). De opslagtermijn van 3 jaar in het huidige wetsvoorstel is hierdoor juridisch onhoudbaar en dient per direct uit het wetsvoorstel te worden geschrapt. Bij gebreke hiervan verwacht Privacy First dat deze bewaartermijn (evenals de massale tapbevoegdheid zelf) door het Europees Hof voor de Rechten van de Mens onrechtmatig verklaard zal worden.

Internationale uitwisseling van bulk-data

Privacy First herhaalt hierbij haar fundamentele bezwaar tegen internationale uitwisseling van ongeëvalueerde bulk-data. Dergelijke uitwisseling overschrijdt alle juridische, ethische en morele grenzen, in elk geval waar het de data van een onschuldige burgerbevolking betreft. Privacy First verwacht dan ook dat deze bevoegdheid geen stand zal houden bij een internationale of Europese rechter en dringt er hierbij op aan om deze bevoegdheid te schrappen of grondig in te perken en van extra waarborgen te voorzien, waaronder een bindende rechtmatigheidstoets vooraf per geval.

Binnenkort zal het Hof Den Haag uitspraak doen over de kwestie van internationale uitwisseling tussen geheime diensten in de rechtszaak *Burgers tegen Plasterk* van Privacy First c.s. tegen de Nederlandse Staat. Tevens hebben Privacy First c.s. als derde partijen geïntervenieerd in de vergelijkbare Britse zaak van Big Brother Watch tegen het Verenigd Koninkrijk bij het Europees Hof voor de Rechten van de Mens. Privacy First ziet de uitspraken van beide hoven met vertrouwen tegemoet.

---

[1] Zie HvJ 21 december 2016, gevoegde zaken C-203/15 & C-698/15 (Tele2 Sverige *et al.*), ECLI:EU:C:2016:970.

Databanken van derde partijen

De bevoegdheden tot het opvragen en gebruiken van gegevens zijn in het huidige wetsvoorstel vrijwel onbegrensd. Het voorstel maakt daartoe zelfs directe, automatische toegang tot de databanken van de gehele publieke en private sector (overheid én bedrijfsleven) mogelijk. Bij al deze derde partijen zullen bovendien ook complete databanken opgevraagd kunnen worden. Dit alles ten behoeve van heimelijke koppeling, *datamining* en *profiling*, waarmee *real-time* een uiterst gedetailleerd (zelfs voorspellend) beeld van groepen en individuen kan worden gecreëerd. Privacy First verzoekt uw Kamer hierbij met klem om deze bevoegdheden te schrappen of grondig in te perken en van wettelijke waarborgen tegen misbruik te voorzien, waaronder bindend rechtmatigheidstoezicht vooraf.

Hack-bevoegdheid en decryptiebevel

"De diensten dienen zo gericht mogelijk te werken en niet door middel van decryptie de digitale veiligheid van grote groepen gebruikers te ondermijnen", zo schrijft de Minister terecht in de nota bij het wetsvoorstel.[2] De bevoegdheid om systemen van onschuldige derden (burgers en bedrijven) te kunnen hacken om zo een *target* te kunnen bereiken acht Privacy First echter te verregaand. Om deze reden is een dergelijke bevoegdheid in het domein van politie en justitie reeds uit het wetsvoorstel Computercriminaliteit III geschrapt. Niet valt in te zien waarom deze bevoegdheid desondanks wel aan AIVD en MIVD zou moeten toekomen. De huidige (reeds bestaande) bevoegdheid om systemen en communicatie van individuele *targets* te kunnen hacken acht Privacy First afdoende.

Bedrijven hebben het recht om hun systemen zo in te richten dat aan een decryptiebevel niet kan worden voldaan wegens de technische onmogelijkheid daarvan, bijvoorbeeld door gebrek aan sleutels. In minder democratische tijden en contreien kan dit recht voor bedrijven tevens omslaan in een maatschappelijke plicht, bijvoorbeeld om als bedrijf niet medeplichtig te worden aan onrechtmatige opsporing en vervolging. In de optiek van Privacy First dienen systemen bovendien zodanig te worden ontwikkeld dat *hacking* vrijwel onmogelijk is en de schade van een eventuele hack altijd zo beperkt mogelijk zal blijven. *Privacy by design* vergt immers niet louter de beste *encryptie* maar ook de beste *compartimentering*. Bovenstaande geldt mede ter verduidelijking van recente ongenuanceerde berichtgeving over het standpunt van Privacy First door de Telegraaf.[3]

Strafbare feiten

Privacy First herhaalt hierbij haar zorg over het feit dat de ongenormeerde bevoegdheid voor agenten om strafbare feiten te mogen plegen ongemoeid wordt gelaten. In de huidige Wiv uit 2002 bestaat de mogelijkheid tot nadere normering middels een Algemene Maatregel van Bestuur (AMvB). De Commissie Dessens adviseerde die AMvB alsnog in te voeren, maar het kabinet maakt dit onmogelijk door de grondslag voor de betreffende AMvB uit de wet te verwijderen. Met een

[2] Nota naar aanleiding van het verslag, *Kamerstukken II* 2016-2017, 34588, nr. 18, p. 66.

[3] Zie http://www.telegraaf.nl/binnenland/27260664/__Privacywaakhond_vindt_dat_kraken_WhatsApp_mag__.html (18 december 2016).

ongewisse politieke toekomst in het verschiet is dit voor de Nederlandse bevolking uiterst onwenselijk en gevaarlijk.

Notificatieplicht

In het huidige wetsvoorstel blijft de notificatieplicht slechts gelden voor individuele burgers en niet (ook) voor organisaties die evengoed *targets* kunnen zijn geweest. Naar aanleiding van eerdere kritiek hierop van Privacy First stelt de Minister in de memorie van toelichting bij het wetsvoorstel hierover het volgende: "De notificatieplicht vervult een rol in het kader van het bieden van rechtsbescherming aan de burgers tegen inbreuken op enkele specifiek aan hen toekomende grondrechten. De invoering van de notificatieplicht die ook geldt voor organisaties wordt (...) dan ook niet overwogen."[4] Dit is aperte onzin. Het recht op privacy en (met name) het recht op vertrouwelijke communicatie gelden immers ook voor rechtspersonen en organisaties als zodanig (waaronder stichtingen, verenigingen en bedrijven), zeker in de context van dit wetsvoorstel.

Verschoningsgerechtigden

In het huidige wetsvoorstel krijgen advocaten en journalisten (terecht) extra bescherming middels voorafgaande toetsing door de rechtbank Den Haag bij de inzet van bijzondere bevoegdheden jegens hen. Privacy First adviseert om deze rechterlijke bescherming uit te breiden naar alle groepen verschoningsgerechtigden, waaronder artsen, notarissen en geestelijken. Tevens dient te worden voorzien in aanvullende waarborgen voor journalistieke bronbescherming.

Toezicht

Conform ons eerdere advies is Privacy First in principe positief over het nieuwe bindende rechtmatigheidstoezicht vooraf bij de uitoefening van bevoegdheden door AIVD en MIVD. Privacy First herhaalt hierbij echter dat dergelijke toetsing vooraf dient te gelden bij de uitoefening van álle bijzondere bevoegdheden door de diensten. Al het toezicht vooraf, tijdens en achteraf dient bovendien grondig en volledig te zijn; in geen geval mag sprake blijken van oppervlakkige *rubber-stamping* of toezichtshiaten. Daarnaast is Privacy First positief over de invoering van bindend klachtrecht voor burgers en organisaties, hetzij bij de nationale Ombudsman, hetzij bij de CTIVD, waarbij Privacy First een voorkeur heeft voor staatsrechtelijke positionering van het klachtinstituut als Hoog College van Staat aangezien dit de onafhankelijkheid ervan versterkt en bestendigt. In navolging van de CTIVD zou Privacy First overigens graag bevestigd zien dat dit klachtrecht ook door relevante maatschappelijke organisaties zal kunnen worden uitgeoefend in het algemeen belang (algemeen-belangactie) en/of namens een specifieke groep personen (groepsactie), ook indien voor die personen een individueel klachtrecht openstaat.[5] Dit is reeds staande praktijk bij de nationale Ombudsman en bevordert de effectiviteit en

[4] Memorie van toelichting bij wet op de inlichtingen- en veiligheidsdiensten, *Kamerstukken II* 2016-2017, 34588, nr. 3, pp. 241-242.

[5] Zie CTIVD, Zienswijze op het wetsvoorstel voor een nieuwe wet op de inlichtingen- en veiligheidsdiensten d.d. 9 november 2016, Bijlage II (Kwaliteitsverbeteringen), p. 6.

efficiëntie van de klachtenprocedure. Tevens zou Privacy First graag expliciet bevestigd zien dat deze nieuwe, quasi-rechterlijke procedure niet zal leiden tot niet-ontvankelijkheid van personen en organisaties met betrekking tot vergelijkbare rechtsvragen in relevante procedures bij de rechterlijke macht.

Actieve openbaarheid

Privacy First adviseert opnieuw om het wetsvoorstel alsnog te voorzien van een bepaling 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.

Peaceful use of cyberspace

In de recente nota van de Minister bij het wetsvoorstel schrijft deze dat "voor Defensie cyberspace het vijfde domein voor militair optreden geworden is (naast land, zee, lucht en de ruimte)."[6] Privacy First herinnert u hierbij graag aan het feit dat de ruimte in juridische zin geen militair domein is; hier geldt immers het internationaal recht van *peaceful use of outer space*. In onze optiek zou in *cyberspace* een vergelijkbaar internationaal regime van *peaceful use* dienen te gelden. Als *'international legal capital'* zou Den Haag zich hier bij uitstek sterk voor kunnen maken.

Wetsvoorstel dient controversieel verklaard te worden

Een wetsvoorstel met een dusdanige (potentiële) impact op onze samenleving dient weldoordacht te zijn en de best mogelijke waarborgen te bevatten tegen onvoorzien gebruik en toekomstig misbruik. Bij het huidige wetsvoorstel is dit niet het geval. Privacy First adviseert u daarom om dit wetsvoorstel te verbeteren of te verwerpen, danwel het gehele wetsvoorstel controversieel te verklaren en het desgewenst alsnog grondig en kritisch te behandelen tijdens een volgende kabinetsperiode. Bij gebreke hiervan behoudt Privacy First zich het recht voor om het huidige wetsvoorstel, zodra van kracht, door de rechter te laten toetsen en onrechtmatig te laten verklaren.

Voor nadere informatie of vragen met betrekking tot bovenstaande is Privacy First te allen tijde bereikbaar op telefoonnummer 020-8100279 of per email: info@privacyfirst.nl.

Hoogachtend,

Stichting Privacy First

mr. Vincent A. Böhre
director of operations

[6] Nota naar aanleiding van het verslag, *Kamerstukken II* 2016-2017, 34588, nr. 18, p. 11.