PRIVACY FIRST

Postbus 16799
1001 RG Amsterdam
Tel. 020 - 8100279

Aan:
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Ministerie van Algemene Zaken
Ministerie van Defensie
Ministerie van Justitie en Veiligheid
Via: www.internetconsultatie.nl

Uw ref.	:	
Onze ref.	:	SPF20180817
Datum	:	17 augustus 2018
Betreft	:	reactie Privacy First op consultatie wijziging van de Wet op de inlichtingen- en veiligheidsdiensten 2017

Geachte heer/mevrouw,

Dank voor de consultatiemogelijkheid bij de *wijziging van de Wiv 2017*. De wijziging codificeert twee van de zes beloften van het kabinet omtrent de Wet op de inlichtingen- en veiligheidsdiensten, die eerder in beleidsregels zijn gevat. Graag maakt Stichting Privacy First van de gelegenheid gebruik om de volgende standpunten te communiceren.

Met de Wet op de inlichtingen- en veiligheidsdiensten 2017 is veel mis. Voor het referendum over deze wet heeft Privacy First een lange lijst opgesteld met punten tegen de Wiv die onverlet nog steeds overeind staan.[1] In de aanloop naar het referendum was te zien hoe de kiezers zich steeds beter informeerden en kritische kanttekeningen plaatsten bij de wet. Dit heeft er in geresulteerd dat de meerderheid van de kiezers *tegen* de Wiv 2017 heeft gestemd. Vervolgens is de Wiv 2017 echter ongewijzigd in werking getreden. Dit laat zien dat de kiezer niet serieus genomen wordt en dit tornt aan de beginselen van de democratische rechtsstaat.

Zoals door de ministeries zelf aangegeven heeft het wetsvoorstel geen gevolgen voor burgers, bedrijven en overheid. Dit komt doordat er geen aanpassingen in het wetsvoorstel worden gedaan die de positie van de burgers versterken. De wetswijziging is een wassen neus. Slechts twee van de ingestelde beleidsregels worden in de wijziging van de Wiv 2017 opgenomen. Ten eerste de zo gericht mogelijke inzet van (bijzondere) bevoegdheden en ten tweede de versnelde weging van samenwerking met buitenlandse diensten. De overige beleidsregels worden niet gecodificeerd en kunnen worden gewijzigd zonder invloed van het parlement.

[1] Zie https://www.privacyfirst.nl/aandachtsvelden/sleepwet/item/1108-abc-tegen-de-sleepwet.html en de bijlage.

Aan de zo gericht mogelijke inzet van de onderzoeksopdrachtgerichte (OOG) interceptie worden geen harde eisen verbonden. Dit biedt geen enkele waarborg tegen grootschalige interceptie. Het beruchte ‘sleepnet’ blijft zo onverlet van kracht.

Daarnaast heeft de kiezer zich duidelijk uitgesproken tegen het ongeëvalueerd verstrekken van gegevens van Nederlandse burgers aan buitenlandse diensten. Het ongeëvalueerd verstrekken aan buitenlandse diensten wordt in de beoogde wetswijziging niet aangepast. Integendeel: tegen de wens van de kiezer in werd recentelijk juist de samenwerking met onder andere de VS versterkt, door het toewerken naar de *“Six Eyes”*.

De tweede wijziging is de verkorting van de termijn voor het opstellen van wegingsnotities voor de beoordeling van buitenlandse diensten van twee jaar naar uiterlijk 1 januari 2019. Privacy First hoopt dat dit de zorgvuldigheid van het beoordelen van de buitenlandse diensten niet aantast.

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

Bijlage: ABC tegen de Sleepwet

Bijlage: **ABC tegen de Sleepwet**
18-03-2018

A. Aftappen
Door de bevoegdheid van 'onderzoeksopdrachtgerichte interceptie' - in de volksmond ook wel sleepnet genoemd - wordt het mogelijk voor de inlichtingen- en veiligheidsdiensten (geheime diensten) om het internetverkeer van grote groepen mensen tegelijk af te tappen. Zo kan er een tap worden geplaatst op een bepaalde gemeente, een wijk, buurt of straat, indien daar een ‘target’ van de geheime dienst woont. Daarbij wordt de communicatie van onschuldige burgers verzameld door middel van een digitaal sleepnet. Privacy First is van mening dat de gegevens van onschuldige burgers niet thuis horen bij de inlichtingendiensten. Bovendien neemt de effectiviteit van de inlichtingendiensten af door de te grote hoeveelheid aan vergaarde data.

B. Buitenland
Gegevens die vergaard zijn met het sleepnet mogen onder de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Sleepwet) ongeëvalueerd met het buitenland gedeeld worden. Dit betekent dat de Nederlandse inlichtingendiensten ongeziene en ongeselecteerde gegevens (van onschuldige burgers) met buitenlandse geheime diensten kunnen delen. Op het gebruik van deze gegevens is vervolgens geen toezicht meer te houden door de Nederlandse diensten.

Bewaartermijnen
Ongeëvalueerde gegevens die door middel van het sleepnet zijn verzameld, mogen drie jaar worden bewaard. Deze ongeëvalueerde gegevens mogen ook ongezien met het buitenland worden gedeeld. Gegevens die de inlichtingen- en veiligheidsdiensten relevant hebben bevonden, mogen bewaard worden zolang deze nog relevant zijn.

C. CTIVD
Het oordeel van de onafhankelijke toezichthouder CTIVD (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten) die achteraf toetst of de bevoegdheden rechtmatig zijn ingezet, is niet bindend. De minister kan de bevindingen en aanbevelingen naast zich neer leggen en eventueel doorgaan met het onrechtmatig inzetten van bevoegdheden.

Chilling effect
De nieuwe wet kan er voor zorgen dat mensen zich (onbewust) anders gaan gedragen dan ze zich zouden gedragen in een vrije omgeving. Dit kan een negatief effect hebben op de uitoefening van andere grondrechten dan het recht op privacy, zoals de vrijheid van meningsuiting of de vrijheid van vereniging, vergadering en demonstratie.

D. Databanken
De nieuwe wet maakt directe, automatische toegang tot databanken in de gehele

private én publieke sector mogelijk. Hiermee kunnen de inlichtingendiensten rechtstreeks toegang krijgen tot allerlei gevoelige databanken bij bedrijven, overheidsinstanties en andere organisaties, hetzij middels informanten of agenten (infiltranten) bij die organisaties, hetzij middels geheime overeenkomsten.

Decryptiebevel
Door de nieuwe wet dienen versleutelde data bij bedrijven, overheden of particulieren (bijvoorbeeld communicatiedata) op verzoek van de geheime dienst ontsleuteld te worden. Weigering om aan een decryptiebevel te voldoen wordt bestraft met 2 jaar hechtenis.

DNA-databank
Met de invoering van de wet krijgen de inlichtingen- en veiligheidsdiensten een eigen DNA-databank. Ze mogen het DNA verzamelen van zogenoemde 'targets' (doelwitten) en 'non-targets' (onschuldige burgers). Om dit DNA te verzamelen mag de inlichtingen- en veiligheidsdienst zich o.a. toegang verschaffen tot een besloten plaats, bijvoorbeeld een kantoor of woning. De Groene Amsterdammer heeft een zeer uitgebreid stuk geschreven over de "DNA Verzameldienst", dit is hier te lezen.

E. Europees Verdrag voor de Rechten van de Mens (EVRM)
Het recht op privacy is een mensenrecht: dit recht wordt beschermd door artikel 8 van het EVRM. Privacy First is van mening dat de nieuwe Sleepwet het recht op privacy schendt. Privacy First heeft dan ook een (concept)dagvaarding klaarliggen om de Staat voor de rechter te slepen zodra de Sleepwet in werking treedt. De rechter kan de Sleepwet dan toetsen en (deels) buiten werking stellen wegens schending van art. 8 EVRM.

F. Fake news door Nederlandse overheid
Volgens onze minister van Binnenlandse Zaken Ollongren is het niet noodzakelijk dat de overheid op haar website rijksoverheid.nl neutrale informatie plaatst over het Sleepwet-referendum. Hierdoor wordt er door de overheid geen objectieve informatie verstrekt aan de kiezers.

G. Geautomatiseerde werken
Zoals onder 'hackbevoegdheid' en "Internet of Things' uitgelegd, zullen door de Sleepwet alle apparaten gehackt mogen worden door de geheime diensten.

H. Hackbevoegdheid
Onder de nieuwe wet krijgen de inlichtingendiensten de mogelijkheid om een *target* te hacken via onschuldige derden. Dit houdt in dat de inlichtingendienst door het hacken van een derde (tante, zus, vriend, vriendin, echtgenoot, opa, collega, buurman, werk, overheid, bedrijf etc.) toegang krijgt tot informatie over het doelwit van de dienst. Dit betekent dat de apparaten van onschuldige burgers gehackt kunnen worden door de diensten. Deze burgers zullen hiervan nooit op de hoogte raken (er geldt hiervoor geen notificatieplicht).

I. Ik heb niks te verbergen
Iedereen heeft recht op een privéleven. De gegevens van onschuldige burgers horen daarom niet thuis bij de inlichtingen- en veiligheidsdiensten. Deze gegevens met onder andere medische informatie, persoonlijke gesprekken, privé emails, zakelijke emails, nieuwsberichten, hobbies, interesses en internet-zoekresultaten dienen daarom goed te worden beschermd. Daarnaast heeft u misschien 'niets' te verbergen, maar andere burgers zoals medische professionals, advocaten, activisten, klokkenluiders en journalisten wel.

Internet of Things
Steeds meer apparaten zijn op het internet aangesloten. Al deze apparaten kunnen onder de Sleepwet afgeluisterd of gehackt worden. Te denken valt aan een auto, camera, microfoon, printer maar eventueel ook zelfs een pacemaker. De Sleepwet sluit deze mogelijkheid immers niet uit.

J. Journalisten
De communicatie van journalisten kan met de nieuwe wet worden onderschept, door onder andere de inzet van het sleepnet. De geheime diensten kunnen dan van deze informatie kennis nemen. Dit vormt een bedreiging voor de persvrijheid en het journalistieke brongeheim. Pas achteraf zullen de diensten de informatie die niet noodzakelijk is voor het onderzoek zo snel mogelijk verwijderen.

K. Kabelgebonden interceptie
Onterecht wordt er gespeculeerd dat de inlichtingen- en veiligheidsdiensten momenteel niet op de kabel mogen aftappen en enkel via de ether. De inlichtingen- en veiligheidsdiensten mogen onder de huidige wet een tap plaatsen op de kabel, wanneer dit gericht is op bijvoorbeeld één individu. Met de nieuwe wet krijgen de inlichtingen- en veiligheidsdiensten de bevoegdheid om ongericht en grootschalig de kabel af te tappen (sleepnet).

L. Lubach
Arjen Lubach heeft in zijn uitzendingen van *Zondag met Lubach* drie items gemaakt over de Sleepwet en waarom het goed is om hier kritisch op te zijn. De filmpjes zijn hier te bekijken: Sleepwet 1, Sleepwet 2 en Sleepwet 3.

M. Mensenrechten
Privacy is een mensenrecht. Dit recht op bescherming van de persoonlijke levenssfeer geldt voor iedereen en wordt door talloze internationale en Europese verdragen gewaarborgd. Door de Sleepwet wordt dit recht massaal geschonden, aangezien de data van grote groepen onschuldige burgers door deze wet zullen worden verzameld, opgeslagen en internationaal uitgewisseld.

Medisch beroepsgeheim
Door de nieuwe wet kan de medische privacy van patiënten en het medisch beroepsgeheim van artsen niet gegarandeerd worden: de geheime diensten mogen bij iedereen, ook bij artsen en ziekenhuizen, relevante gegevens opvragen en toegang tot

hun data-systeem (Elektronisch Patiëntendossier) vragen of dergelijke systemen hacken. Dit kan bovendien leiden tot zorgmijdend gedrag bij patiënten en daarmee tot een bedreiging van de volksgezondheid.

N. Notificatieplicht
De notificatieplicht in de nieuwe wet schiet tekort. Vijf jaar na de inzet van een bevoegdheid onder de Sleepwet dient de betreffende persoon hierover in principe te worden geïnformeerd. Dit geldt echter slechts voor enkele van de nieuwe bevoegdheden. Privacy First is van mening dat de notificatieplicht moet gelden voor de inzet van álle bevoegdheden.

O. Onschuldpresumptie
Met de invoering van de nieuwe wet wordt het onschuldbeginsel omgedraaid. Door het sleepnet wordt potentieel elke burger 'verdacht', zonder concrete aanleiding om die burger te volgen. Daarnaast wordt de kans op *false positives* (onterechte verdenkingen) bij massale datavergaring erg groot.

P. Privacy
De privacy van onschuldige burgers wordt door de inzet van de Sleepwet geschonden. Zie hiervoor alle andere argumenten.

Q. Queeste naar data
Bij de overheid is een hongerlust naar data ontstaan. Waar landen om ons heen teruggaan naar een gerichte aanpak, gaat Nederland voor Big Data. Hierdoor wordt er steeds meer hooi verzameld en zal de speld steeds moeilijker te vinden zijn. Meer data zorgt niet meteen voor meer veiligheid.

R. Rechter
Een gerechtelijke toets vooraf aan de inzet van de bevoegdheden ontbreekt veelal. Zoals onder “TIB’ uitgelegd, mist de nieuwe toetsingscommissie de onderzoeksbevoegdheden voor effectief en onafhankelijk toezicht.

S. Sleepnet
Zie ‘Aftappen’

Strafbare feiten
Geheime agenten zijn zowel onder de huidige als de nieuwe wet bevoegd om strafbare feiten te plegen. De precieze reikwijdte van deze bevoegdheid is tot op heden echter onbekend. Onder de huidige wet kon deze bevoegdheid nader worden gereguleerd middels een (nooit ingevoerde) Algemene Maatregel van Bestuur (AMvB). De Commissie Dessens adviseerde enkele jaren geleden om die AMvB alsnog in te voeren. In de nieuwe Sleepwet is de grondslag voor deze AMvB echter geschrapt, waardoor sprake blijft van een juridisch vacuüm.

T. TIB
Onafhankelijk toezicht op alle fasen van de inzet van bevoegdheden door de diensten (voor, tijdens en achteraf) is onvoldoende gewaarborgd. Aangezien de

inlichtingendiensten heimelijk opereren, kunnen burgers waartegen de bevoegdheden worden ingezet niet zelf bezwaar maken. Hiervoor dient de inzet van bevoegdheden onafhankelijk te worden getoetst. De nieuwe Toetsingscommissie Inzet Bevoegdheden (TIB) toetst vooraf slechts of de minister terecht toestemming heeft gegeven voor de inzet van een relatief zware ('bijzondere') bevoegdheid onder de nieuwe wet. Deze toetsing is met minder waarborgen omkleed dan toetsing door de rechter. Daarnaast heeft de TIB geen eigen onderzoeksbevoegdheden en is compleet afhankelijk van de informatie die hen wordt gegeven. Verscheidene instanties, zoals de Autoriteit Persoonsgegevens, hebben gewaarschuwd dat moet worden voorkomen dat de TIB een ‘stempelmachine’ zal zijn.

T. Terreurschwalbe
Door voorstanders van de Sleepwet zal vaak het argument aangehaald worden dat deze wet aanslagen zal voorkomen, *Zondag met Lubach* liet dat zien. In andere landen is echter al gebleken dat gericht werken veel effectiever is. De tegenstanders van de Sleepwet zijn het er over eens dat de huidige wet aan vernieuwing toe is, maar eisen ook dat de wet op cruciale punten wordt aangepast en verbeterd.

U. Uitwisseling van gegevens
Zoals onder ‘Buitenland’ omschreven, kunnen de gegevens van onschuldige burgers en journalisten die worden verzameld door de inzet van het sleepnet, ongezien gedeeld worden met buitenlandse geheime diensten.

V. Veiligheid
Onterecht worden privacy en veiligheid tegenover elkaar gezet. In een vrije democratische samenleving gaan privacy en veiligheid hand in hand. Er kan een goede Wet op de inlichtingen- en veiligheidsdiensten worden opgesteld met goede privacywaarborgen, waarbij de informatie van onschuldige burgers niet bij de inlichtingendiensten terecht komt.

W. Waarborgen
De wet geeft te grote bevoegdheden aan de inlichtingen- en veiligheidsdiensten en te weinig privacywaarborgen voor burgers. Na het referendum dient de wet terug naar de tekentafel te gaan, van fatsoenlijke waarborgen te worden voorzien en op de inzet van bevoegdheden te worden herzien.

Z. Zero-days
De inlichtingen- en veiligheidsdiensten hebben de bevoegdheid om gebruik te maken van onbekende zwakke plekken (zogenaamde *zero-days*) in software. Voor de inlichtingen- en veiligheidsdiensten zijn deze kwetsbaarheden dan bekend, maar voor de makers of fabrikanten van de software niet. De inlichtingen- en veiligheidsdiensten hoeven deze kwetsbaarheid niet te melden aan de fabrikant van de software. Hierdoor kunnen eventuele kwaadwillenden (langdurig) misbruik maken van deze kwetsbaarheden. Ook ontstaat hierdoor een zwarte markt voor handel in dergelijke kwetsbaarheden en datalekken.