

Aan:
Tweede Kamer der Staten-Generaal
Vaste commissie voor Veiligheid en Justitie
Postbus 20018
2500 EA Den Haag

Uw ref. :
Onze ref. : SPF-20140408
Datum : 8 april 2014
Betreft : Open brief van voorzitter Stichting Privacy First inzake wetsvoorstel ANPR

Geachte leden van de Tweede Kamer,

U wordt gevraagd een wetsvoorstel te accorderen om de overheid het recht te geven alle kentekengegevens (oftewel reisgegevens) van automobilisten voor een periode van 4 weken op te slaan voor opsporing en vervolging. Iedere burger wordt hierdoor een potentiële verdachte. Let wel, de reisgegevens van 16 miljoen mensen over een periode van 4 weken om voornamelijk openstaande boetes te kunnen innen. Dit zal gebeuren middels uitbreiding van automatische kentekenregistratie (ANPR). In de huidige ANPR-praktijk worden alleen met rede verdachte kentekens (zogenoeten “hits”) bewaard en nagetrokken, overigens zonder dat hier reeds een specifieke, met privacywaarborgen omklede rechtsbasis voor bestaat. In plaats van de huidige praktijk alsnog van een degelijke rechtsbasis te voorzien, gaat minister Opstelten in zijn wetsvoorstel echter meteen 10 stappen verder door voortaan ieders kenteken in een politiedatabank op te slaan. Dit is zijn zoveelste centrale database ICT-project, startend met EUR 4 mln aan kosten, in werkelijkheid gaat dit richting EUR 50-100 mln. Privacy First herkent hierin het volgende patroon:

- Technologie gedreven “oplossingen” voor een zogenaamd maatschappelijk probleem, gelobbyd door ICT-leveranciers;
- Vervolgens lokaal de uitvoering testen en tijdelijk buiten de wet om proefdraaien (Rotterdam);
- Wetgeving aanpassen zonder naar de principes van de rechtsstaat te kijken;
- Tweede Kamer als stemvee gebruiken om wetsvoorstel er versneld doorheen te jagen;
- Indien Eerste Kamer niet akkoord, dan voorstel voor afschaffen “lastige” Eerste Kamer.

Privacy First verzoekt u met klem deze draconische wet, die lijnrecht ingaat tegen alle basisprincipes van onze rechtstaat NIET te accorderen en wel om de volgende redenen:

- Wat is de *noodzaak* om alle 16 miljoen burgers te controleren voor een kleine “bijvangst” naast de reeds bestaande database voor “hits”?
- Deze wet is volledig disproportioneel en leidt tot een maatschappelijk “chilling effect” en zelfcensuur bij burgers vanwege het feit dat de overheid continu over de schouder van de onschuldige burgers meekijkt.
- Deze wet zal leiden tot *function creep* (doelverschuiving) met nieuwe doelstellingen zoals extra belastingheffing, uitbreiding van trajectcontroles, kilometerheffing, milieubelasting en ongeoorloofde en ongebreidelde analyses van het reisgedrag van individuele burgers en groepen (*profiling*).
- De AIVD kan alle ANPR-gegevens opvragen. Navraag van Privacy First bij de AIVD leidt echter tot de conclusie dat de huidige wetgeving hen reeds voldoende ruimte geeft om hun werk te doen.
- Als de NSA-affaire en Snowden ons iets geleerd hebben is het wel dat ANPR-gegevens direct gebruikt zullen worden door inlichtingendiensten, uitgewisseld worden en dus volledig oncontroleerbaar worden.
- Indien deze wet wordt geaccordeerd is het hek van de dam, dan is met net zoveel reden een nieuw wetsvoorstel te maken waarin alle privébewegingen van alle 16 miljoen burgers in de openbare ruimte worden gemonitord en opgeslagen, eerst voor 4 weken en later onbepikt, om wellicht ergens een “verdenking” te kunnen vinden.
- Gezien de ervaringen in het verleden bieden dergelijke databases geen enkele garantie dat deze niet gehackt worden, dat de toegang en protocollen hierin gewaarborgd worden, dat er geen maandelijkse kopie door inlichtingendiensten wordt gemaakt, etc.
- De uitvoering en borging van deze wet is in geen enkel opzicht geregeld, zie ook de onderstaande vragen van Privacy First aan de minister. Aan de Kamer wordt zelfs gevraagd om de wet te accorderen zonder dat reeds sprake is van de bijbehorende Algemene Maatregel van Bestuur.
- Nu staan er al zo’n 500 ANPR-camera’s, dit aantal zal snel verder groeien en leiden tot een wettelijk geregeld elektronisch concentratiekamp waarin iedere automobilist vanaf de voordeur tot en met alle bestemmingen de gehele dag gevolgd kan worden.
- Zelfs in de huidige praktijk bestaan nog hiaten in het recht voor de burger om te weten of hij in een database met “hits” geregistreerd staat, en zo ja, hoe hier weer uit te komen en met welke waarborgen. In de praktijk blijkt vaak één intern telefoontje al voldoende om, zonder enig opsporingsbevel, een “nummertje” even te volgen op de snelweg...

Geachte leden van de Tweede Kamer, dit wetsvoorstel hoort slechts op twee plekken thuis: in een dictatuur of, in onze open democratische samenleving, in de prullenbak. Een minister die eerder in Rotterdam bewees het niet zo nauw met onze wetgeving te nemen en willens en wetens alle ANPR-gegevens 4 maanden op te laten slaan is in

mijn ogen niet te vertrouwen. Zoals de waard is vertrouwt hij zijn gasten, logisch toch? Mijn advies aan de minister is zijn functie vacant te stellen en te solliciteren bij de NSA waar nog een mooie functie is vrijgekomen na het vertrek van Snowden. Bij aanneming van dit wetsvoorstel zal Privacy First direct juridische actie nemen om de hoeksteen van ons rechtssysteem te waarborgen en onschuldige burgers uit de klauwen van de tot controlewaan zin verworpen overheid te behoeden.

Hieronder vindt u een aantal vragen welke wij eerder aan de minister hebben gesteld en waarop naar onze mening geen (afdoende) antwoord is gegeven. Na één gesprek met enkele privacy organisaties pretendeert de minister dat er een consultatie op dit wetsvoorstel is geweest en dat er een “Privacy Impact Analyse” (PIA) is uitgevoerd. Niets is echter minder waar. Tevens heeft een niet-onafhankelijke PIA geen enkel nut voor een wetsvoorstel dat sowieso niet voldoet aan de basisprincipes van onze rechtsstaat. Dit hebben wij ook aangegeven. En over deze principes valt niet te onderhandelen, tenzij wordt afgestapt van een democratische rechtsstaat.

Vragenlijst van Privacy First aan de minister:

- 1) In hoeverre is 4 weken opslag van ANPR-gegevens strikt *noodzakelijk* (i.t.t. “misschien nuttig” of “wellicht handig”) in een democratische, op vrijheid en vertrouwen gebaseerde samenleving (art. 8 EVRM)?
- 2) Op welke wijze voldoet dit wetsvoorstel aan de algemene mensenrechtelijke plicht van de Nederlandse Staat om het recht op privacy voortdurend te *bevorderen* i.p.v. dit recht uit te hollen?
- 3) Hoe versterkt dit wetsvoorstel de vertrouwensrelatie tussen de Nederlandse bevolking en de Nederlandse overheid?
- 4) Door wie is de Privacy Impact Assessment bij het wetsvoorstel opgesteld? Waarom is dit niet door een externe, onafhankelijke partij gedaan?
- 5) Hoe waarborgt dit wetsvoorstel het beginsel van dataminimalisatie?
- 6) Hoe waarborgt dit wetsvoorstel het beginsel van *privacy by design*?
- 7) Hoe worden de onschuldpresumptie en het verbod van zelfincriminatie (*nemo tenetur*) gewaarborgd in dit wetsvoorstel?
- 8) Hoe waarborgt dit wetsvoorstel het recht om in eigen land vrij en anoniem te kunnen reizen?
- 9) Hoe waarborgt dit wetsvoorstel de persvrijheid en journalistieke bronbescherming?
- 10) Hoe waarborgt dit wetsvoorstel de vrijheid van vereniging en de vrijheid van demonstratie?
- 11) Op welke wijze reguleert dit wetsvoorstel internationale uitwisseling van ANPR-data met buitenlandse overheden en (verdere) uitwisseling met derden?
- 12) Op welke wijze worden in dit wetsvoorstel *function creep* en misbruik van ANPR-data op korte, middellange en lange termijn ingedamd? Op welke wijze zijn bijvoorbeeld ANPR-*datamining* en *profiling* uitgesloten?
- 13) Hoe garandeert dit wetsvoorstel dat de opgeslagen ANPR-data niet zullen worden misbruikt door ambtenaren, *hackers*, criminele organisaties, buitenlandse overheden etc.?

- 14) Voor welke doeleinden, op welke wijze en met welke bewaartermijnen beoogt de AIVD de opgeslagen ANPR-data te gebruiken?
- 15) Wanneer zal de beloofde Algemene Maatregel van Bestuur bij dit wetsvoorstel gereed zijn? Waarom wordt de Tweede Kamer bij de opstelling hiervan gepasseerd?
- 16) Welke stijging in valse nummerplaten en bijbehorende identiteitsfraude zal dit wetsvoorstel naar verwachting veroorzaken? Welke tegenmaatregelen zijn hierbij voorzien?
- 17) De Europese Commissie was eerder kritisch over het Nederlandse camerasysteem @MIGO-BORAS. Is de Europese Commissie reeds op de hoogte gesteld van de uitbreiding van @MIGO-BORAS met 4 weken ANPR-opslag? Zo ja, wat was de reactie van de Commissie?
- 18) Hoe draagt dit wetsvoorstel bij aan de herovering van de vroegere internationale positie van Nederland als mensenrechtelijk gidsland? Hoe waarborgt de Nederlandse overheid dat dit wetsvoorstel en bijbehorende technologie niet zullen worden overgenomen en misbruikt door minder democratische regimes in het buitenland? Heeft hierover afstemming plaatsgevonden met het ministerie van Buitenlandse Zaken?
- 19) Wat zijn de financiële kosten en baten van dit wetsvoorstel (inclusief bijbehorende neveneffecten) op korte en lange termijn?
- 20) Bestaan de ANPR-referentielijsten uit zwarte en witte lijsten? Zo ja, welke criteria gelden voor plaatsing op de witte lijsten?

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

Hoogachtend,

drs. L.T.C. (Bas) Filippini,
voorzitter Stichting Privacy First