Stichting Bits of Freedom
Postbus 10746
1001 ES Amsterdam

M +31(0)654386680
E ot.vandaalen@bof.nl
W www.bof.nl

Bankrekening 55 47 06 512
Bits of Freedom, Amsterdam
KVK-nr. 34 12 12 86

Ministerie van Verkeer en Waterstaat
t.a.v. dhr. ir. C.M.P.S. Eurlings
Plesmanweg 1-6
2597 JG Den Haag
per email:
dbo-spzpostbus@minvenw.nl

Betreft:
Introductie kilometerheffing

Datum:
Amsterdam, 16 februari 2010

Geachte heer Eurlings,

1. Eind 2009 is door het kabinet een wetsvoorstel voor de kilometerheffing geïntroduceerd. De kilometerheffing is potentieel een zeer privacy-inbreukmakende ontwikkeling. Hiermee zal immers de locatie van iedere auto continu worden geregistreerd. De stichting Bits of Freedom ("**Bits of Freedom**") heeft dan ook met zorg hiervan kennis genomen, en nader onderzoek gedaan naar de privacy-implicaties. In dit advies wil zij haar conclusies met u delen:

    - Het getuigt van realiteitszin dat – anders dan bij eerdere grootschalige overheidsprojecten met een vergelijkbare privacy-impact – het kabinet dit keer op voorhand heeft geprobeerd om maatregelen te nemen die de persoonlijke levenssfeer moeten beschermen. Bij toepassing van het garantiespoor wordt de persoonlijke levenssfeer dan ook redelijk beschermd. In die situatie zullen immers slechts periodiek geaggregeerde gegevens worden doorgestuurd naar het inningsbureau. Bits of Freedom plaats wel haar vraagtekens bij de noodzaak om maandelijks 1% van de (onverdachte) houders aan een controle via de handhavingsportalen te onderwerpen. Ook moet het garantiespoor blijven bestaan.
    - Bits of Freedom moet echter constateren dat nog niet kan worden voorkomen dat het systeem in de toekomst gebruikt gaat worden om alle burgers continu te bespioneren. Gegevens die via het hoofdspoor worden verzameld, zijn minder goed beschermd, en Bits of Freedom vreest dat door systeemdwang vrijwel alle Nederlanders gebruik zullen gaan maken van een hoofdspoor-optie waarbij *real-time* gegevens zullen worden doorgestuurd naar de erkende dienstverlener. Bits of Freedom stelt bovendien vast dat in het huidige voorstel niet kan worden voorkomen dat ook het garantiespoor in de toekomst zal worden gebruikt om vrijwel *real-time* de informatie van gebruikers door te sturen naar het inningsbureau.

- Bits of Freedom adviseert daarom om nadere maatregelen te nemen die kunnen waarborgen dat ook in de toekomst de privacy wordt beschermd. Ten eerste moet de broncode van het kastje dat via het garantiespoor wordt aangeboden, voor iedere Nederlander beschikbaar zijn, en moet de houder door middel van een checksum kunnen verifiëren dat deze broncode ook in het kastje is opgenomen. Hiermee hangt samen dat de specificaties van de hardware openbaar moeten zijn. Ten tweede moet in de wet worden opgenomen dat de gegevens die worden verzameld in het kader van de kilometerheffing niet zullen worden gebruikt voor doeleinden anders dan het innen van de kilometerheffing. Tot slot moet het hoofdspoor niet worden ingevoerd.

2. Bits of Freedom licht dat hieronder toe.

Bij toepassing van het garantiespoor wordt de persoonlijke levenssfeer redelijk beschermd

3. In de huidige voorgestelde implementatie van de kilometerheffing zijn maatregelen genomen om de persoonlijke levenssfeer te beschermen. In het voorstel worden in het zogenoemde “garantiespoor” immers slechts periodiek de geaggregeerde gegevens doorgestuurd naar het inningsbureau. Dat is dus het “aantal geregistreerde kilometers dat tegen de verschillende tariefsoorten is afgelegd” (zie par. 3.3.1 van de Memorie van Toelichting). Het is voor het inningsbureau dus vrijwel niet mogelijk om aan de hand van deze gegevens te achterhalen waar een auto op welk moment is geweest.

4. Bits of Freedom plaatst wel haar vraagtekens bij de noodzaak om 1% van de onverdachte houders maandelijks aan een controle te onderwerpen. Dat zijn per maand immers ongeveer 100.000 automobilisten die aan een screening zullen worden onderworpen. Zij vraagt zich af hoe dit zich verhoudt met de grondwettelijke eisen van proportionaliteit en subsidiariteit, en adviseert dit percentage substantieel te verlagen.

5. Tevens is het Bits of Freedom onvoldoende duidelijk of het garantiespoor zou blijven bestaan. Zij begrijpt dat het garantiespoor mogelijk in de toekomst zou worden opgeheven. Mocht zij dat goed hebben begrepen, dan dringt Bits of Freedom erop aan dat dit aspect van de plannen wordt herzien. Zij zal hieronder namelijk ook aangeven dat wat haar betreft het hoofdspoor niet geïntroduceerd moet worden; daarmee hangt samen dat het garantiespoor dus moet blijven bestaan.

Bij gebruik van erkende dienstverleners is persoonlijke levenssfeer minder goed beschermd

6. De persoonsgegevens die worden doorgestuurd in het kader van het garantiespoor, staan in schril contrast met de gegevens die worden doorgestuurd als een houder gebruik zal maken van een erkende dienstverlener. Dan wordt immers aan een derde – namelijk de erkende dienstverlener – *real-time* doorgegeven waar de auto zich op welk moment bevindt. Deze gegevens worden weliswaar weer in geaggregeerde vorm doorgestuurd aan het inningsbureau, maar blijven tegelijkertijd wel opgeslagen bij de erkende dienstverlener.

> Het is in theorie mogelijk dat binnen het hoofdspoor juist kastjes worden ontwikkeld die de privacy even goed beschermen als binnen het garantiespoor het geval zou zijn. Dat is echter niet te verwachten, nu het hoofdspoor juist zou worden aangeboden om de doorgifte van *real-time* locatiegegevens voor andere doeleinden, zoals fileinformatie en routebeschrijving, te combineren met de doorgifte ten behoefte van de kilometerheffing.

7. De gegevens zijn bij een erkende dienstverlener in minder goede handen dan bij de houder. Ten eerste hebben opsporingsdiensten toegang tot die gegevens, bij verdenking van een misdrijf als omschreven in artikel 67 eerste lid Wetboek van Strafvordering ("**Sv**") (art. 126nd Sv). Bovendien is een databank waar alle gegevens van houders worden verzameld een interessant doelwit van criminelen, en het blijkt in de praktijk heel moeilijk om dit soort databanken te beschermen (het lukt zelfs commercïele creditcardmaatschappijen immers niet hun databanken afdoende te beschermen). Tot slot is de houder onvoldoende op de hoogte van hoe zijn gegevens precies gebruikt worden, als deze door een erkende dienstverlener worden beheerd. Het is goed mogelijk dat een erkende dienstverlener deze doorverkoopt in strijd met wet- en regelgeving: het Zwartboek Datalekken dat Bits of Freedom aanlegt toont aan dat dit niet denkbeeldig is.[1]

8. Toch is te verwachten dat houders juist vaker gebruik zullen maken van de erkende dienstverleners. Zelfs als dit geen kostenvoordelen zou hebben – zoals het Ministerie schrijft in par. 3.6.1 van de Memorie van Toelichting – dan zal dit over het algemeen ingegeven zijn door gebruiksgemak: het is bijvoorbeeld makkelijker om file-informatie en informatie ten behoeve van de kilometerheffing door middel van een kastje aan te bieden resp. te registreren, dan hiervoor twee verschillende kastjes te gebruiken. Bits of Freedom verwacht dat door systeemdwang houders doorgaans zullen kiezen voor de erkende dienstverlener, en dat daarmee de ingebouwde privacywaarborgen van het garantiespoor in werkelijkheid geen effect zullen hebben.

In de toekomst kan ook de bescherming van het garantiespoor worden uitgekleed

9. Nog zorgwekkender is, dat er vooralsnog geen maatregelen zijn genomen om *function creep* van het garantiespoor te voorkomen. Zelfs als het garantiespoor nu de privacy redelijk beschermt, kan niet worden verzekerd dat dit in de toekomst ook zo zal zijn. Er wordt immers in het voorstel de mogelijkheid geschapen om draadloos nieuwe software te installeren in het kastje. Dat betekent dat technisch gezien in de toekomst ook in het garantiespoor (bijna) *real-time* locatiegegevens kunnen worden doorgegeven. Bovendien zijn de juridische obstakels voor uitbreiding van het garantiespoor ook beperkt: de verdere concretisering en technische detaillering van de aan de registratievoorziening te stellen eisen zullen bij ministeriële regeling worden vastgesteld (zie artikel 4.5, zesde lid). Een ministeriële regeling behoeft geen goedkeuring van het parlement, en kan dus makkelijk worden aangepast.

> Zie de toelichting bij artikel 4.6: "Tenslotte moet de registratievoorziening op de juiste wijze gegevens, aanwijzingen en programmatuur die in het kader van de uitvoering van deze wet worden toegezonden, kunnen ontvangen, opslaan en toepassen. Het kan daarbij zowel gaan om technische updates (verbeterde programmatuur) als om wijzigingen van de tarieven, alsmede spitstrajecten en -tijden."

10. Het is bovendien naïef om te veronderstellen dat er geen politieke druk zal ontstaan om in de toekomst de functionaliteit van het garantiespoor uit te breiden. Nu al geven zowel de VVD als de PvdA toe, dat zij er niet op tegen zijn dat deze gegevens ook voor opsporing en vervolging gebruikt kunnen worden. Mochten die gegevens gebruikt kunnen worden om criminaliteit te voorkomen, dan zal de politiek op een gegeven moment onder druk gezet

1 Zie https://www.bof.nl/ons-werk/prive-gegevens/zwartboekdatalekken/.

worden om de functionaliteit van deze kastjes uit te breiden om *real-time* Nederlanders te volgen.

> Zie ook *Kamerstukken II* 2008/09, 30 517, nr. 16: de heer Heerts (PvdA) zei hierover: “[...] ook rond het gedoe met kastjes in auto’s […] ben ik er niet op voorhand tegen dat soortgelijke gegevens, via bepaalde barrièremodellen, ook voor opsporing en vervolging gebruikt kunnen worden. ” De heer Teeven (VVD) merkt in hetzelfde debat op: “Het is nieuw voor mij dat de PvdA-fractie vindt dat de kastjes ook criminaliteitsbestrijding als doelstelling hebben. Ik zal daarover niet flauw zijn. Kijk, als zo’n middel er is, als wij portalen hebben om de files te meten die gaan ontstaan en daar hangen camera’s, is de VVD-fractie met de PvdA-fractie van mening dat dit ook kan bijdragen aan de criminaliteitsbestrijding. Als we zware criminelen moeten volgen, moeten we dat vooral doen. Zo is het natuurlijk ook met die kastjes. Uiteindelijk zitten daar gegevens in die ook dienstbaar kunnen zijn aan criminaliteitsbestrijding.” De reactie van het kabinet naar aanleiding van de vaststelling van het CBP dat ANPR-gegevens in strijd met de wet werden opgeslaten (“dan passen wij de wet aan”), is veelzeggend.

Het wetsvoorstel moet ook *function creep* in de toekomst voorkomen

11. Gelet hierop, adviseert Bits of Freedom dat in het voorstel voor de kilometerheffing ook maatregelen worden genomen die *function creep* in de toekomst kunnen voorkomen:

- Ten eerste moet de broncode van het kastje dat via het garantiespoor wordt aangeboden, beschikbaar zijn, en de houder moet dit zelf kunnen compileren om de checksum te controleren. Ook de Raad van State merkte in haar advies op, dat “aan het draagvlak voor de kilometerprijs […] afbreuk wordt gedaan, indien de registratievoorziening voor de houder een 'zwarte doos' blijft die voor hem oncontroleerbaar en onaantastbaar gegevens registreert en aan het inningsbureau ter beschikking stelt, zeker indien hij tegen deze gegevens vervolgens in rechte niet kan opkomen”.[2] Dat is terecht: iedere Nederlander heeft er recht op, om te weten hoe de software die zijn gegevens verplicht registreert en verwerkt, in de praktijk functioneert. Alleen door de broncode beschikbaar te maken, zal aan dit bezwaar tegemoet kunnen worden gekomen. Voor de duidelijkheid: de beveiliging van het kastje neemt doorgaans juist *toe* als de broncode beschikbaar wordt gesteld, omdat zo sneller fouten in de algoritmes kunnen worden opgespoord. De mogelijkheid om draadloos de software van het kastje bij te werken, moet hiermee ook rekening houden, zodat altijd de broncode wordt meegestuurd. De houder moet kunnen weigeren om de software te installeren als de checksum van de gecompileerde broncode niet overeen komt met de checksum van de binary in het kastje. Hiermee hangt samen dat de de specificaties en de functionaliteit van de hardware openbaar moeten worden gemaakt.
- Ten tweede moet in de wet worden opgenomen dat de gegevens die worden verzameld via de kilometerheffing niet zullen worden gebruikt voor doeleinden anders dan het innen van de kilometerheffing. Wat dat betreft vindt Bits of Freedom het zorgwekkend dat in par. 3.6.5 van de Memorie van Toelichting is opgemerkt, dat de belangenafweging in het kader van de Wet bescherming persoonsgegevens buiten toepassing blijft als het gaat om bijvoorbeeld de voorkoming, opsporing en vervolging van strafbare feiten of om de veiligheid van de Staat. Als het kabinet serieus de privacy wil beschermen bij de invoering van de kilometerheffing, dan dient zij bij wet op te nemen dat deze gegevens niet voor andere doeleinden worden gebruikt. Mocht een nieuw kabinet deze gegevens in de toekomst toch willen gebruiken voor andere doeleinden, zoals de opsporing, dan zal het parlement hierop in ieder geval controle kunnen uitoefenen. Bovendien moet in

2 *Kamerstukken II* 2009/10, 32216, nr. 4.

het wetsvoorstel worden verhelderd, dat de houder niet gedwongen kan worden om gedetailleerde gegevens ter beschikking te stellen aan opsporingsdiensten, nu dit op gespannen voet staat met het *nemo tenetur*-beginsel (dit beginsel komt erop neer dat niemand gedwongen kan worden om mee te werken aan zijn eigen veroordeling).
- Tot slot moet het hoofdspoor niet worden ingevoerd. Daarmee zet de overheid de deur wijdopen naar vergaande *function creep*, en zal door systeemdwang iedere Nederlander uiteindelijk toch gedwongen worden zijn real-time locatiegegevens beschikbaar te stellen aan derden. De overheid moet in plaats daarvan slechts het garantiespoor invoeren.

Wij dringen er met klem op aan dat het kabinet deze adviezen meeneemt in een aangepaste versie van het wetsvoorstel en graag ontvangen wij een antwoord op deze brief. Uiteraard ben ik graag bereid om het bovenstaande nader toe te lichten, mocht daaraan behoefte bestaan.

Hoogachtend,

Ot van Daalen