BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Stichting Bits of Freedom
Postbus 10746
1001 ES Amsterdam

T +31(0)6 24 53 4440
E axel.arnbak@bof.nl
W www.bof.nl

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

Ministerie van Justitie
Projectgroep Dataretentie
t.a.v. Ing. R.W. Bladder

Betreft:
Inbreng "Voorstel definitie HNAW"

Datum:
Amsterdam, 30 november 2009

Geachte heer Bladder,

1. De stichting Bits of Freedom ("**Bits of Freedom**") maakt hierbij graag gebruik van de mogelijkheid om inbreng te leveren op het "Voorstel definitie HNAW" (het "**Voorstel**"), en dankt de "Projectgroep dataretentie" voor het bieden van de gelegenheid hiertoe.

2. Bits of Freedom komt tot de volgende conclusies met betrekking tot het Voorstel:

   - De uitbreiding van het geautomatiseerd bevragen van NAW-gegevens naar het geautomatiseerd bevragen van Historische NAW-gegevens ("**HNAW**") intensiveert de inbreuk op de persoonlijke levenssfeer.
   - De huidige praktijk omtrent de bevraging van NAW-gegevens baart Bits of Freedom al grote zorgen, nu de wettelijke plichten door de verantwoordelijke ambtenaren onvoldoende worden nageleefd. Bovendien zijn effectief toezicht en transparantie ten aanzien van deze praktijk onder de maat.
   - Het is dan ook te betreuren dat het waarborgen van de privacy geen integraal onderdeel vormde van het totstandkomingsproces van het Voorstel, en dat Bits of Freedom pas nu, nu het Voorstel zich in een vergevorderd stadium bevindt, is gevraagd om input.

3. Bits of Freedom verwacht dat de volgende 'eisen' worden toegevoegd aan Voorstel:

   - Het opstellen van een zogenoemde "Privacy Impact Assessment" door een onafhankelijke instantie voorafgaand aan de goedkeuring van een mogelijke HNAW oplossing.[1] Daarbij moet nauwkeurig in kaart worden gebracht welke negatieve

1 De 'Privacy Impact Assessment' wordt ook wel Privacy Effect Rapportage of Risicoanalyse genoemd. Zie voor

gevolgen voor de privacy de implementatie van het Voorstel zou hebben. Daarbij zou ook onderzoek moeten worden gedaan naar de cumulatieve effecten tussen deze en andere reeds bestaande privacy-inbreukmakende maatregelen. Het College Bescherming Persoonsgegevens is de aangewezen instantie hiervoor.

- Het treffen van technische maatregelen om de rechtmatigheid van automatische bevragingen te garanderen ("Privacy by Design"). Dat betekent dat het Voorstel pas mag worden geimplementeerd als (1) bevraging slechts worden gedaan op grond van een elektronische lastgeving van de Officier van Justitie, zodat een bevraging alleen beantwoord wordt als deze *matcht* met de lastgeving; (2) de authorisatiemechanismen waarmee een opsporingsambtenaar toegang krijgt tot de bevragingsmodule, naast de nu gebruikte PIN-code worden aangevuld met andere hoogwaardige authorisatiemechanismen, die mogelijk gebruik maken van moeilijk namaakbare biometrische gegevens, zoals de irisscan; en (3) in de bevragingsmodule vragen worden gesteld aan de opsporingsambtenaar ter controle van de beoordeling van de rechtmatigheid (het wetsartikel, motivering, corresponderende elektronische lastgeving etc.).
- Tevens moet de broncode van de bevragingsmodule openbaar worden gemaakt. Op die manier kan iedere burger de rechtmatige werking van het systeem ook verifieren.Het is een misverstand om te denken dat door het geheimhouden van broncode, de veiligheid beter wordt gewaarborgd: in de security-gemeenschap is het "security-through-obscurity" principe al lang achterhaald. Ook moet het besturingssysteem voor de bevragingsmodule aan de hoogst geldende beveiligingseisen voldoen. Dit betekent dat het besturingssysteem naar alle waarschijnlijkheid een Linux-achtige variant moet zijn.
- Een meldplicht datalekken, voor alle betrokken partijen, als persoonsgegevens uit de HNAW-oplossing onverhoopt in handen van derden terecht komen.
- Het tot in detail monitoren van alle bevragingen via de HNAW-oplossing, om uitgebreide onafhankelijke controle in de audits mogelijk te maken.
- Structurele, openbare en onafhankelijk rapportage over de werking, rechtmatigheid en de veiligheid van de automatische bevraging.

4. Bits of Freedom verwacht daarnaast dat de volgende 'wensen' worden toegevoegd aan het Voorstel:

   - Als door een onafhankelijke toezichthouder wordt geconstateerd dat een ambtenaar zich herhaaldelijk heeft schuldig gemaakt aan onrechtmatige bevragingen, moet deze ambtenaar de toegang via de bevragingsmodule worden ontzegd. Tevens moeten afschrikwekkende disciplinaire maatregelen worden getroffen in zo een geval.
   - Het moet mogelijk zijn en blijven voor aanbieders om niet mee te werken aan de HNAW-oplossing, als blijkt dat deze de privacy van klanten of de veiligheid van data onvoldoende waarborgt.

Intensivering inbreuk persoonlijke levenssfeer door geautomatiseerde bevraging HNAW

5. De uitbreiding naar het geautomatiseerd bevragen van HNAW is een ***kwalitatieve*** verandering ten opzichte van de huidige bevragingsmogelijkheden van NAW-gegevens,

meer informatie "Aanbevelingen Bits of Freedom t.a..v. evaluatie Wet bescherming persoonsgegevens", par. 15-19, http://www.bof.nl/briefminjus070909.html

geregeld via het Centraal Informatiepunt Onderzoek Telecommunicatie (”**CIOT**”). Dit gebeurt onder dezelfde lage toegangsdrempels als voorheen, en kan in strijd zijn met artikel 8 EVRM.

6. Aan alle door het EHRM gestelde deelcriteria voor het beoordelen van de ernst van een inbreuk op het recht op privacy is voldaan.[2]Een enkele bevraging geeft nu een completer beeld van het gebruik van telecommunicatiediensten door een gebruiker, nu aan de identificerende gebruikersgegevens een datum geplakt wordt (1). De reikwijdte van de maatregel (2) is enorm: van alle gebruikers, ongeacht hun status (3), worden gebruiksgegevens bewaard die onder lage voorwaarden automatisch opgevraagd (4) zouden kunnen worden. Betrokkenheid bij de verdachte van een misdrijf is voldoende. De ernst van de potentiële inbreuk is weliswaar gering qua soort gegevens, maar groot qua bereik – met name gezien het karakter van de bevoegdheid als eerste stap in het opsporingsonderzoek, waardoor vele onschuldige burgers in het beeld van de opsporing komen.

7. De beoogde uitbreiding voor HNAW zal ook een ***kwantitatieve*** verandering met zich meebrengen, te weten een sterke toename van het aantal bevragingen van HNAW. Dit getal is voor NAW-gegevens inmiddels gestegen naar circa 2.8 miljoen bevragingen per jaar (in 2008), terwijl er 'slechts' 2.3 miljoen bevragingen waren begroot.[3] Zo neemt het aantal bevragingen jaarlijkse toe met gemiddels circa 25%. Mutatis mutandis geldt dit ook voor HNAW, een uitermate zorgwekkende ontwikkeling uit het oogpunt van privacy van burgers.

Terwijl de huidige praktijk rondom bevragingen van het CIOT al aanleiding geeft tot zorgen

8. Bovendien heeft Bits of Freedom in een recente analyse al vastgesteld, dat opsporingsdiensten de wettelijke waarborgen tegen onrechtmatige bevraging negeren en onvoldoende op de hoogte zijn van geldende wet- en regelgeving:[4]

    - In 2008 is in cruciale gevallen ten onrechte geen proces verbaal opgesteld. Bovendien is er geen controle van de bevragingen van het CIOT;
    - Persoonsgebonden PIN-codes voor het CIOT werden of worden ten onrechte onderling uitgewisseld;
    - Corrigerende maatregelen bij onrechtmatige bevraging blijven daardoor uit, bevragingen zijn immers niet meer tot een natuurlijke persoon herleidbaar;
    - De kennis van wet- en regelgeving van een deel van de betrokkenen is onvoldoende;
    - De opsporingsdiensten ervaren de privacybeschermende maatregelen als administratieve last, zodat de voorgeschreven procedures niet gevolgd worden.

9. Deze analyse illustreert dat het toezicht op opsporingsdiensten gebrekkig is. Daarnaast is de analyse gebaseerd op een WOB-verzoek. Uit de documenten die eerder niet openbaar werden gemaakt, waren bovendien een aantal belangrijke passages verwijderd. Niet alleen het toezicht op de opsporingsdiensten, maar ook de transparantie is dus onder de maat.

2 EHRM *Vogt v. Germany,* par. 48; Daarnaast EHRM *Silver a.o. v. The United Kingdom*, par. 88.

3 Zie: https://rejo.zenger.nl/focus/wob-20090703-jaarverslag-2008.pdf

4 Zie: http://www.bof.nl/persbericht131009.txt

En burgerrechten vormden geen integraal onderdeel van “Voorstel definitie HNAW”

10. Des te verrassender is het, dat privacy geen integraal onderdeel vormde vanaf het begin van van het totstandkomingsproces van het “Voorstel definitie HNAW”. Alhoewel de aanbieders en overige toezichthouders ook deels het privacy-belang hebben gewaarborgd, was er geen stap in het besluitvormingsproces waarin dit onderdeel centraal stond.

Over Bits of Freedom

11. Bits of Freedom verdedigt burgerrechten in de digitale wereld, waaronder het recht op privacy. De organisatie staat onder leiding van Ot van Daalen. Het bestuur van Bits of Freedom bestaat uit Doke Pelleboer (ex-directeur van XS4ALL), Joris van Hoboken (onderzoeker bij het Instituut voor Informatierecht van de Universiteit van Amsterdam) en Karianne Thomas (advocaat bij advocatenkantoor Van Doorne).

12. Bits of Freedom is graag bereid om haar inbreng nader toe te lichten als daaraan behoefte bestaat. Zij is daartoe bereikbaar via bovenvermelde contactgegevens.

Met vriendelijke groet,

Axel Arnbak
Bits of Freedom