PRIVACY FIRST

eigen keuzes in een vrije omgeving

JAARVERSLAG 2014

Stichting Privacy First
Amsterdam

30 juni 2015

© 2015 STICHTING PRIVACY FIRST

Inhoudsopgave

1. Voorwoord 1

2. Speerpunten 2

2.1 Paspoortproces ... 2

2.2 Zaak 'Burgers tegen Plasterk' ... 4

2.3 Kort geding tegen bewaarplicht telecomgegevens ... 4

2.4 Kentekenparkeren ... 5

2.5 Trajectcontroles ... 6

2.6 Automatische nummerplaatherkenning (ANPR) ... 7

2.7 Campagne SpecifiekeToestemming.nl ... 8

3. Privacy First Solutions 9

4. Politieke lobby 10

4.1 Lokaal ... 10

4.2 Nationaal ... 10

4.3 Internationaal en Europees ... 11

5. Communicatie 11

5.1 Massamedia ... 11

5.2 Individuele burgers ... 13

5.3 Internet ... 14

6. Evenementen 14

7. Organisatie 16

8. Financiën 16

1. Voorwoord

Het afgelopen jaar was een bewogen jaar voor Privacy First, met een aantal aandachtsgebieden waarbij de privacyschendingen steeds hetzelfde patroon kennen. Gedwongen gebruik van centraal ingerichte technologie, veelal buiten het parlement om of middels gebrekkige wetgeving zonder toetsing aan grondrechten, gevolgd door slechte organisatie en implementatie. Dit in plaats van te starten vanuit de uitgangspunten van onze democratische rechtsstaat, de implementatie hiervan goed te regelen en te onderzoeken hoe en welke technologische mogelijkheden op privacyvriendelijke wijze ingepast kunnen worden. Privacy First staat voor toepassing van technologie ten dienste van de burger i.p.v. andersom, waarbij de burger altijd de regie over zijn of haar eigen data blijft behouden.

Door privacyschendingen raken de basisprincipes van onze rechtsstaat steeds verder aangetast. Dit leidt in de toekomst tot ontwrichting van onze maatschappij vanuit een wantrouwende en niet-gelijkwaardige overheid die als controle-apparaat optreedt in plaats van als dienstverlener en waarborger van onze rechtsstaat. Democratische verworvenheden die hierbij in het geding raken zijn onder meer het recht op anonimiteit en bewegingsvrijheid in de openbare ruimte, de onschuldpresumptie, het verschoningsrecht van advocaten en journalisten, het medisch geheim en het gebruik van contant geld.

Sinds 2001 ziet Privacy First er geen vrijheden voor burgers bijkomen, maar slechts steeds meer beperkingen. Als een spionagenet dat langzaam maar zeker de burger in een totale houdgreep krijgt. De basis van onze vrije samenleving wordt hierdoor bedreigd. Opvallend is dat na de onthullingen van Edward Snowden de aandacht voor privacy bij het publiek groeiende is, maar dat dit zeker niet het geval is bij de overheid en enkele monopolistische ICT-bedrijven.

Privacy First heeft als belangrijkste focus dat Nederland Privacy Gidsland wordt in de wereld en zo een positief voorbeeld geeft ten opzichte van het *total surveillance* denken in de VS, China en andere staten die uitgaan van angst en wantrouwen naar de burger. Privacy First is ervan overtuigd dat we aan het begin staan van een informatierevolutie en we juist nu kunnen bouwen aan duurzame IT-infrastructuren die de rechtsstaat ondersteunen en versterken, met behoud van ieders privacy én veiligheid. Voor 2015 zie ik veel mogelijkheden om het privacybewustzijn op de volgende thema's verder te versterken:

- Het kenteken en de OV-chipkaart als elektronische enkelband;
- Het nieuwe EPD (LSP) en de afbraak van het medisch geheim;
- De criminalisering van contant geld en anonieme betalingsvormen;
- Cybercriminaliteit en *hacking* door de overheid;
- Big Bata en *profiling* van burgers door overheden en bedrijven;
- Social media en privacywaarborgen;
- Infiltratie in de persoonlijke woonomgeving met 'slimme meters' van nutsbedrijven.

In 2015 starten wij een nieuw platform op de website van Privacy First om op alle mogelijke thema's door te verwijzen naar privacyvriendelijke diensten en producten. Op deze wijze stimuleert Privacy First de groei van een privacyvriendelijke ICT-industrie met privacy-oplossingen als exportproduct!

Bas Filippini,
voorzitter Stichting Privacy First

2. Speerpunten

Vast beleid van Privacy First is om onze aandacht primair te richten op (dreigende) privacyschendingen die grote groepen mensen tegelijk (kunnen) treffen. In onze selectie van onderwerpen laten wij ons daarbij leiden door 1) de schaal, 2) de ernst en 3) de mogelijke impact en gevolgen van een bepaalde schending. Massale, ernstige privacyschendingen worden door Privacy First eerst onderzocht en publiekelijk benoemd. Vervolgens tracht Privacy First de betreffende schending op te heffen middels stille diplomatie en politieke lobby, gevolgd door een publiekscampagne, juridische actie of – als uiterste middel – een rechtszaak. In lijn met deze criteria richtte de aandacht van Privacy First zich sinds haar oprichting voornamelijk op biometrie: het kunnen herkennen van mensen aan unieke lichaamskenmerken, waaronder vingerafdrukken en gezichtsscans. Andere onderwerpen waar de aandacht van Privacy First zich de laatste jaren structureel op richt zijn cameratoezicht, de OV-chipkaart, medische privacy en *profiling*. In 2013 voegden wij hier het thema "privacy en geheime diensten" aan toe, in 2014 gevolgd door het thema "privacy en mobiliteit", waaronder kentekenparkeren, Automatische Nummerplaatherkenning (ANPR) en trajectcontroles. Hieronder zetten wij onze voornaamste speerpunten voor u op een rij.

2.1 Paspoortproces Privacy First c.s.

De afgelopen jaren voerde Privacy First samen met 19 mede-eisers (burgers) een grootschalige civiele rechtszaak tegen één van de zwaarste privacyschendingen uit de Nederlandse geschiedenis: de opslag van ieders vingerafdrukken onder de nieuwe Paspoortwet. Dergelijke opslag was met name bedoeld om kleinschalige identiteitsfraude met paspoorten (*look-alike* fraude) te bestrijden, maar zou ook worden gebruikt voor opsporing en vervolging, terrorismebestrijding, rampenbestrijding, inlichtingenwerk etc. Dit vormde een flagrante schending van ieders recht op privacy. In een zogeheten algemeen-belangactie (art. 3:305a BW) hebben Privacy First c.s. in mei 2010 de Nederlandse Staat civielrechtelijk gedagvaard teneinde de opslag van vingerafdrukken onder de Paspoortwet door de rechter onrechtmatig te laten verklaren wegens strijd met hoger (Europees) privacyrecht. In februari 2011 verklaarde de rechtbank Den Haag ons Paspoortproces echter (onterecht) niet-ontvankelijk. De rechtbank kwam daardoor niet aan een inhoudelijk oordeel over de Paspoortwet toe. Privacy First kondigde

meteen hoger beroep aan. Mede onder druk hiervan gingen vervolgens de Tweede Kamer en minister Donner (Binnenlandse Zaken, BZK) overstag en werd de opslag van vingerafdrukken in de zomer van 2011 grotendeels stopgezet. Drie jaar later (ons hoger beroep liep nog steeds) werden de gewraakte bepalingen uit de Paspoortwet deels ingetrokken. Bovendien werd in januari 2014 de verplichte afname van vingerafdrukken voor Nederlandse identiteitskaarten afgeschaft. Een maand later deed het Gerechtshof Den Haag eindelijk uitspraak in ons Paspoortproces: het Hof verklaarde Privacy First alsnog ontvankelijk en oordeelde dat de (eerdere) opslag van vingerafdrukken onrechtmatig was wegens strijd met het recht op privacy. Deze uitspraak van het Hof maakte tevens de weg vrij voor Privacy First (en andere maatschappelijke organisaties) om *in het algemeen belang* rechtszaken te kunnen blijven voeren ter behoud en bevordering van het recht op privacy (of andere mensenrechten). Enkele maanden later stelde minister Plasterk (BZK) echter cassatie tegen de uitspraak van het Hof in bij de Hoge Raad. Ondanks grondig verweer door Privacy First (daartoe bijgestaan door Alt Kam Boer Advocaten in Den Haag) werden zowel Privacy First als alle mede-eisers op 22 mei 2015 door de Hoge Raad alsnog niet-ontvankelijk verklaard. Dit nieuwe standaardarrest van de Hoge Raad heeft mogelijk grote negatieve gevolgen voor de Nederlandse rechtsbescherming tegen onrechtmatige (privacyschendende) wetgeving; klik HIER voor ons nader commentaar. De Hoge Raad verwijst de zaak als het ware door naar de Raad van State, waar de laatste jaren meerdere vergelijkbare, bestuursrechtelijke zaken van individuele burgers tegen de nieuwe Paspoortwet aanhangig waren. Naar aanleiding van de niet-ontvankelijkheid bij de Hoge Raad heeft Privacy First het gehele Paspoortproces-dossier dan ook integraal laten indienen bij de Raad van State, ter versterking van de lopende zaken daar. Privacy First c.s. wachten sindsdien met spanning het oordeel van de Raad van State af. Tevens bereiden Privacy First c.s. een klacht bij het Europees Hof voor de Rechten van de Mens voor wegens schending van het recht op privacy (art. 8 EVRM) alsmede het recht op toegang tot de rechter en een effectief rechtsmiddel (art. 6 en 13 EVRM). Ondanks de kafkaëske anticlimax bij de Hoge Raad ligt daarmee een Europese veroordeling van Nederland in het verschiet.

© Guus Schoonewille

Paspoortproces van Privacy First c.s., Paleis van Justitie, Den Haag

2.2 Zaak 'Burgers tegen Plasterk'

Uit de onthullingen van Edward Snowden is de laatste jaren gebleken dat de spionagepraktijken van inlichtingendiensten zoals de Amerikaanse NSA vrijwel geen grenzen kennen. In plaats van de Amerikanen tot de orde te roepen bleken geheime diensten in andere landen echter juist gretig gebruik te maken van de inlichtingen die door hun buitenlandse bondgenoten op illegale wijze verkregen zijn. Daardoor wordt de privacywetgeving die burgers tegen dergelijke praktijken behoort te beschermen dubbel geschonden: door buitenlandse geheime diensten zoals de NSA die op onrechtmatige wijze inlichtingen verzamelen én door geheime diensten in eigen land die deze inlichtingen vervolgens gebruiken. Om deze praktijken een halt toe te roepen besloot een nationale coalitie van Nederlandse burgers en organisaties (waaronder Privacy First) eind 2013 om de Nederlandse Staat voor de rechter te dagen en te eisen dat per direct een einde zou worden gemaakt aan de ontvangst en het gebruik van illegale buitenlandse inlichtingen over Nederlandse burgers. Bovendien dient iedere burger over wie dergelijke inlichtingen verzameld zijn daarvan op de hoogte te worden gesteld en dienen de betreffende gegevens te worden gewist. Naast Privacy First bestaat de coalitie van procespartijen onder meer uit de Nederlandse Vereniging van Journalisten (NVJ), de Nederlandse Vereniging van Strafrechtadvocaten (NVSA) en Internet Society Nederland (ISOC.nl). Privacy First voert deze rechtszaak primair in het algemeen belang, ter herstel van het recht op privacy van iedere burger in Nederland. De rechtszaak staat onder leiding van bureau Brandeis; de advocaten van dit jonge Amsterdamse kantoor vertegenwoordigden Privacy First eerder met succes in ons Paspoortproces. Op 23 juli 2014 deed de rechtbank Den Haag echter een teleurstellende uitspraak: hoewel alle procespartijen (burgers en organisaties) ontvankelijk werden geacht, wees de rechtbank alle vorderingen af. Hierbij sloeg de rechtbank de plank op tal van aspecten echter dusdanig mis, dat het vonnis in hoger beroep vrijwel onmogelijk stand zal kunnen houden. Privacy First ziet het hoger beroep bij het Hof Den Haag dan ook met vertrouwen tegemoet. Bovendien zal deze zaak ook buiten rechte (in de politieke arena) gewonnen kunnen worden middels kritische herziening van de Nederlandse Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2002).

2.3 Kort geding tegen bewaarplicht telecomgegevens

Meer succes had Privacy First in een cruciaal kort geding tegen de Wet bewaarplicht telecomgegevens (Wbt). Onder deze wet werden sinds 2009 de communicatiegegevens (telefonie- en internetverkeer) van iedereen in Nederland respectievelijk 12 en 6 maanden opgeslagen voor de opsporing en vervolging van strafbare feiten. Iedere burger werd hierdoor als het ware een potentiële

verdachte. In kort geding eiste een brede coalitie van organisaties en bedrijven eind 2014 dat deze wet buiten werking zou worden gesteld wegens strijd met het recht op privacy. De eisers waren Stichting Privacy First, de Nederlandse Vereniging van Strafrechtadvocaten (NVSA), de Nederlandse Vereniging van Journalisten (NVJ), het Nederlands Juristen Comité voor de Mensenrechten (NJCM), internetprovider BIT en telecomaanbieders VOYS en SpeakUp, e.e.a. onder leiding van Boekx Advocaten in Amsterdam. Volgens de eisende partijen was de Nederlandse bewaarplicht van telecommunicatie (dataretentie) in strijd met fundamentele grondrechten die privéleven, communicatie en persoonsgegevens beschermen. Dat was in april 2014 immers ook reeds het oordeel van het Europees Hof van Justitie over de vrijwel identieke Europese dataretentierichtlijn, gevolgd door negatieve oordelen over de Nederlandse Wbt door de Raad van State, het College Bescherming Persoonsgegevens en de Eerste Kamer. Voormalig minister Opstelten van Justitie weigerde niettemin de Wbt buiten werking te stellen. De wet zou door de minister gehandhaafd worden totdat een wetswijziging in werking getreden was, en dat kon nog jaren duren. In een uniek vonnis (wetten worden zelden door rechters buiten werking gesteld, laat staan in kort geding) maakte de rechter hier echter korte metten mee door de gehele Wbt per direct buiten werking te stellen wegens strijd met het recht op privacy. Vervolgens besloot de Staat niet in hoger beroep te gaan, waardoor het vonnis sindsdien definitief is. Privacy First beschouwt dit als een historische overwinning. Mocht in de toekomst opnieuw een algemene bewaarplicht van telecommunicatie worden ingevoerd, dan zullen Privacy First c.s. die opnieuw bij de rechter aanvechten.

© Lisa S. / Shutterstock.com

2.4 Kentekenparkeren

In steeds meer Nederlandse gemeenten wordt kentekenparkeren ingevoerd: bij parkeren wordt het kenteken geregistreerd middels invoering in een parkeerautomaat en is betaling vaak nog slechts mogelijk via een pinpas, creditcard of mobiele parkeer-*app*. Alle parkeerdata worden vervolgens opgeslagen in gemeentelijke databanken of centraal in de nationale databank van het zogeheten Servicehuis Parkeer- en Verblijfsrechten (SHPV). Als vrije burger heeft u echter het recht om anoniem te kunnen reizen in eigen land. En dus ook anoniem te kunnen parkeren, zonder opslag van uw kenteken. Daarnaast heeft u het recht om te kunnen betalen met een wettig betaalmiddel dat anonimiteit verschaft, bijvoorbeeld contant geld. Nadat Privacy First in 2013 een grootschalige protestactie had georganiseerd tegen kentekenparkeren in Amsterdam, besloot deze gemeente om alle parkeerdata te wissen en voortaan louter nog de gegevens van foutparkeerders tijdelijk op te slaan i.v.m. eventueel bezwaar en beroep. Voor Privacy First zijn deze concessies echter onvoldoende: zolang kentekenparkeren niet wordt vervangen door een privacyvriendelijk alternatief (bijvoorbeeld

invoering van parkeervaknummers), zal Privacy First zich ertegen blijven verzetten. In 2014 deed Privacy First dit middels een rechtszaak van onze voorzitter tegen de gemeente Amsterdam. Aanleiding voor deze zaak was een boete die de voorzitter ontving nadat hij principieel had geweigerd zijn kenteken in te voeren voor een (aantoonbaar betaalde) parkeerplek. In deze rechtszaak werden door onze advocaat Benito Boer (Alt Kam Boer Advocaten, Den Haag) talloze privacybezwaren tegen kentekenparkeren ingebracht. En met succes: op 30 januari 2015 verklaarde de rechtbank Amsterdam het beroep van onze voorzitter tegen de parkeerboete gegrond. Sindsdien is iedereen in Nederland niet langer verplicht om bij het parkeren een kenteken in te voeren, zolang men maar kan aantonen betaald te hebben voor de parkeerplek (bijvoorbeeld middels een kwitantie of parkeerkaartje). Burgers die ondanks dit vonnis alsnog met een parkeerboete geconfronteerd worden, kunnen daartegen eenvoudig bezwaar en beroep indienen middels het model-bezwaarschrift op de website van Privacy First (klik HIER). Voor Privacy First vormt deze overwinning bij de Amsterdamse rechtbank slechts een eerste stap op weg naar privacyvriendelijk parkeren: voor 2015 heeft Privacy First reeds nieuwe rechtszaken tegen kentekenparkeren in voorbereiding, waaronder tegen de verplichting om elektronisch (en dus traceerbaar) te betalen. Daarnaast ondersteunt Privacy First burgers in individuele bezwaar- en beroepsprocedures.

2.5 Trajectcontroles

Naast kentekenparkeren zijn ook trajectcontroles Privacy First al jaren een doorn in het oog: bij dergelijke controles worden alle automobilisten op een bepaald (snelweg)traject middels cameratoezicht gevolgd, waarna afhankelijk van ieders gemiddelde snelheid wel/geen snelheidsbekeuring volgt. Voor dit systeem bestaat tot op heden echter geen specifieke, met privacywaarborgen omklede rechtsbasis. Dit is in strijd met het Europese privacyrecht (art. 8 EVRM) en art. 10 van de Nederlandse Grondwet. Bovendien blijven alle trajectcontrole-data minstens drie dagen in politiedatabanken bewaard, óók van het gros van de automobilisten dat niet te hard rijdt. De politie heeft daardoor zicht op een groot deel van de bewegingen van alle automobilisten in Nederland. Deze gegevens kunnen ook worden gedeeld met andere overheidsinstanties, waaronder justitie, AIVD en Belastingdienst. Iedere automobilist wordt hierdoor een potentiële verdachte. Reeds in 2012 vormde dit

aanleiding voor de voorzitter van Privacy First om bezwaar en beroep in te dienen tegen een boete die hij via een trajectcontrole ontving. Pas in april 2015 diende vervolgens de rechtszaak van onze voorzitter tegen deze boete bij de rechtbank Utrecht. De Utrechtse politierechter bleek echter nauwelijks bereid om e.e.a. te toetsen aan hoger privacyrecht en wees de zaak af. De politierechter beschouwt trajectcontroles slechts als “geringe privacyinbreuk” en acht de algemene Politiewet en waarschuwingsborden langs de snelweg voldoende privacywaarborg. Privacy First vindt dit onbegrijpelijk en zal deze kwestie gaan voorleggen aan het Europees Hof voor de Rechten van de Mens in Straatsburg. Tevens bereidt Privacy First nadere juridische stappen tegen trajectcontroles op nationaal niveau voor. Evenals in de zaken tegen kentekenparkeren wordt Privacy First hiertoe bijgestaan door onze advocaat Benito Boer (Alt Kam Boer Advocaten, Den Haag).

2.6 Automatische nummerplaatherkenning (ANPR)

Vast beleid van Privacy First is om massale privacyschendingen bij de rechter aan te vechten en onrechtmatig te laten verklaren. Een actueel wetsvoorstel dat zich daar bij uitstek toe leent is het voorstel van minister Van der Steur (Veiligheid en Justitie) inzake *Automatic Number Plate Recognition* (ANPR). Onder dit ANPR-wetsvoorstel zullen de kentekens van alle auto's (oftewel ieders reisbewegingen) door middel van cameratoezicht vier weken in politiedatabanken worden opgeslagen voor opsporing en vervolging. Iedere automobilist wordt hierdoor een potentiële verdachte. Privacy First acht dit volstrekt disproportioneel. Het huidige ANPR-voorstel werd reeds in februari 2013 bij de Tweede Kamer ingediend door voormalig minister Opstelten. Voorheen was ook minister van Justitie Hirsch Ballin reeds in 2010 van plan om een vergelijkbaar voorstel in te dienen met een bewaartermijn van 10 dagen. Vervolgens verklaarde de Tweede Kamer dit onderwerp echter controversieel. Opstelten en Van der Steur doen er met hun huidige voorstel dus alsnog een paar scheppen bovenop. Volgens de huidige regels dienen de ANPR-gegevens van onschuldige burgers echter binnen 24 uur te worden gewist; in de optiek van het College Bescherming Persoonsgegevens (CBP) dienen alle kentekens die niet verdacht zijn (zogenaamde “no-hits”) zelfs direct uit de databases te worden verwijderd. Van der Steur gaat hier nu dus lijnrecht tegenin door ook de kentekens van niet-verdachte burgers vier weken te willen opslaan. Dit vormt een flagrante schending van het recht op privacy van iedere automobilist.

Indien de Tweede en Eerste Kamer het huidige ANPR-wetsvoorstel alsnog aannemen zal Privacy First (in coalitie met andere maatschappelijke organisaties) de Nederlandse Staat dagvaarden en de wet buiten werking laten stellen wegens strijd met het recht op privacy. Indien nodig zullen Privacy First en mede-eisers hiertoe doorprocederen tot aan het Europees Hof voor de Rechten van de Mens in Straatsburg.

Tevens werd in 2014 bekend dat de Belastingdienst via geheime convenanten met de politie continu en massaal alle ANPR-data over Nederlandse automobilisten ontvangt. Deze data kunnen vervolgens jarenlang bij de Belastingdienst opgeslagen blijven en daar alsnog worden opgevraagd door politie, justitie, AIVD etc. Privacy First acht deze buitenwettelijke uitwisseling en U-bochtconstructie volstrekt onrechtmatig. Zolang het CBP en de Tweede Kamer niet ingrijpen behoudt Privacy First zich het recht voor om deze kwestie eveneens aan de rechter voor te leggen.

Foto: Chris Zwolle, Flickr

ANPR en trajectcontrole op de A12 bij Utrecht

2.7 Campagne SpecifiekeToestemming.nl

Op initiatief van Privacy First en de Stichting Bescherming Burgerrechten is in april 2014 een grootschalige internetcampagne gelanceerd rondom het recht op medische privacy: www.SpecifiekeToestemming.nl . Deze campagne wordt sindsdien gesteund door tal van maatschappelijke organisaties, zorgverleners en academici. Kern van de campagne is dat specifieke toestemming (weer) het leidende principe moet worden bij de uitwisseling van medische gegevens. Dit in tegenstelling tot de generieke toestemming die geldt bij de private opvolger van het Elektronisch Patiëntendossier (EPD), het Landelijk Schakelpunt (LSP). Bij generieke toestemming is niet te voorzien door wie iemands medische gegevens kunnen worden ingezien, gebruikt, uitgewisseld etc. Generieke toestemming is daarmee per definitie in strijd met twee klassieke uitgangspunten in het privacyrecht: het beginsel van doelbinding en het recht op vrije, voorafgaande en volledig geïnformeerde toestemming bij de verwerking van persoonsgegevens. Het wetsvoorstel 'Cliëntenrechten bij elektronische verwerking van gegevens' van minister Schippers (Volksgezondheid) dreigde dergelijke generieke (brede, ongerichte) toestemming in 2014 echter wettelijk te verankeren ten koste van het bestaande recht op specifieke (gerichte, welbepaalde) toestemming. Bij specifieke

toestemming moeten cliënten voorafgaand aan het delen van hun medische gegevens kunnen bepalen of, en zo ja welke, gegevens mogen worden gedeeld met welke zorgverleners voor welke doeleinden. Dat beperkt de risico's en maakt het mogelijk voor cliënten om controle te houden over de uitwisseling van hun medische data. Mede onder druk van onze campagne is generieke toestemming in juli 2014 door de Tweede Kamer uit het wetsvoorstel geschrapt en blijft daarmee specifieke ("gespecificeerde") toestemming over; dit zal vervolgens geïmplementeerd moeten worden in alle bestaande en toekomstige systemen voor de uitwisseling van medische gegevens, waaronder het huidige LSP (voormalig EPD). De Eerste Kamer neigt inmiddels zelfs naar verwerping van het wetsvoorstel zolang het bestaande recht op specifieke toestemming daarin onvoldoende gewaarborgd is. Daarnaast zijn diverse marktontwikkelingen gaande die erop duiden dat bij nieuwe systemen specifieke toestemming de norm is en blijft, en dat 'privacy by design' de nieuwe standaard wordt. Daarmee kan deze campagne van Privacy First reeds een succes genoemd worden.

Campagne-banner SpecifiekeToestemming.nl

3. Privacy First Solutions

Naast rechtszaken en politieke lobby vindt Privacy First het inmiddels de hoogste tijd om ook bedrijven actief te betrekken bij een toekomstig privacyvriendelijk Nederland. Met ons nieuwe initiatief Privacy First Solutions wil Privacy First daartoe bestaande drempels verlagen om privacyvriendelijke oplossingen toe te passen. In interactie met partners vanuit diverse disciplines willen we het bedrijfsleven stimuleren om innovatieve privacy-oplossingen te ontwikkelen en te implementeren. Als stip op de horizon streven we naar Nederland als Privacy Gidsland. Om dit doel te bereiken, focussen we binnen Privacy First Solutions vooralsnog op drie doelstellingen:

1. Door middel van discussie en kennisoverdracht continu onderzoeken hoe het recht op privacy zich verhoudt tot moderne technologische ontwikkelingen.
2. Bedrijven stimuleren om *privacy by design* toe te passen en van privacy een *unique selling point* te maken.
3. Een platform bieden voor bedrijven die privacyvriendelijk opereren en innoveren, opdat zij nationaal en internationaal een voortrekkersrol kunnen gaan spelen.

Privacy First gelooft dat privacy voor bedrijven bij uitstek de kans biedt om maatschappelijk verantwoord te ondernemen en zich positief te profileren. Veel bedrijven willen reeds laten zien dat zij de privacy van hun klanten belangrijk vinden. Zorgvuldige omgang met persoonsgegevens door bedrijven is immers van groot belang voor het vertrouwen van consumenten. Privacy First is het initiatief Solutions gestart met het doel om bedrijven en organisaties te verenigen op het gebied van privacy. Door ervaringen te delen en samen na te denken over oplossingen, kunnen we via Privacy First Solutions een bijdrage leveren aan een toekomstig Nederland waarin privacyvriendelijk ondernemen de norm is.

Privacy First Solutions startte met een succesvol *pre-launch* evenement op 2 december 2014. Na een introductie over de noodzaak van het initiatief was er ruimte voor een aantal *best practices* en goede ideeën, zoals Greenhost, de privacyvriendelijke internetprovider, gevolgd door Hack-je-Hokje en de DataWijzer, twee initiatieven van de Nationale DenkTank om online profilering inzichtelijk te maken en privacyvoorwaarden eenvoudig samen te vatten in icoontjes. In 2015 werkt Privacy First onder meer aan het ontwikkelen van een platform waar organisaties samen kunnen komen om met elkaar te brainstormen over privacyvriendelijk ondernemen en innoveren. Daarnaast zijn er diverse evenementen en projecten gepland en zal Privacy First in toenemende mate overheden en bedrijven gaan adviseren bij de ontwikkeling van privacyvriendelijke wetgeving, beleid en techniek.

4. Politieke lobby

4.1 Lokaal

In 2014 werd Privacy First door gemeenteraadsleden uit diverse steden benaderd voor informatie en advies ter bepaling van lokale standpunten over (met name) kentekenparkeren, cameratoezicht en gemeentelijke Privacy Impact Assessments.

4.2 Nationaal

Naast diverse emails aan individuele Eerste en Tweede Kamerleden verzond Privacy First in 2014 de volgende brieven aan de Tweede Kamer, met afschrift aan relevante bewindspersonen:

- Brief d.d. 8 april 2014 aan Tweede Kamer (vaste commissie voor Veiligheid en Justitie) inzake wetsvoorstel ANPR;
- Brief d.d. 6 juni 2014 namens SpecifiekeToestemming.nl aan Tweede Kamer (vaste commissie voor Volksgezondheid, Welzijn en Sport) inzake het wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens;
- Email d.d. 15 oktober 2014 aan Tweede Kamer (vaste commissie voor Infrastructuur en Milieu) inzake de OV-chipkaart.

4.3 Internationaal en Europees

Naar aanleiding van eerdere kritische lobby van Privacy First bij het VN-Comité tegen Foltering rondom *Taser*-wapens (stroomstootwapens) werd Privacy First begin 2014 door het Zwitserse voorzitterschap van de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE) uitgenodigd voor enkele bijeenkomsten in Wenen (Oostenrijk) rond de thema's marteling, privacy en de bescherming van persoonsgegevens. Daarnaast werd Privacy First onder meer uitgenodigd voor het CPDP-privacycongres in Brussel en het ALB-dataprotectiecongres in Kuala Lumpur. Tevens onderhield Privacy First in 2014 contacten met diverse Europarlementariërs. Vanaf 2015 wil Privacy First actiever worden op Europees niveau.

5. Communicatie

5.1 Massamedia

In 2014 is het mediabereik van Privacy First opnieuw sterk gegroeid en inhoudelijk diverser geworden. Naast verzoeken om interviews wordt Privacy First ook vaak door journalisten benaderd om achtergrondinformatie en onderzoekstips. Daarnaast verschijnt Privacy First steeds vaker in buitenlandse media. Hieronder een selectie van onze mediamomenten in 2014:

- Security.nl, 7 jan. 2014: 'ID-kaart zonder vingerafdrukken over enkele weken beschikbaar'
- AD/Rotterdams Dagblad, 28 jan. 2014: 'Gegevens parkeerders blijven toch bewaard'
- Security.nl, 30 jan. 2014: 'Kohnstamm: Europese vuist tegen NSA-surveillance nodig'
- NU.nl, 11 feb. 2014: 'Commissie EU stemt voor verplicht alarmsysteem in auto's'
- Radio 1, 13 feb. 2014: interview met Privacy First over gebrek aan privacy in Nederland
- NRC.nl, 18 feb. 2014: 'Hof: centrale opslag vingerafdrukken in strijd met recht op privacy'
- NRC Next, 19 feb. 2014: 'Vingerafdrukken centraal opslaan is in strijd met de wet'
- ZDNet, 19 Feb. 2014: 'No, you can't store people's fingerprints in a central database, Dutch court rules'
- Ravage Webzine, 26 feb. 2014: 'Europese auto's krijgen spionagekastje'
- BNR Nieuwsradio, 10 maart 2014: interview met Privacy First over klantdata-proef ING
- Leeuwarder Courant, 12 maart 2014: 'Duizenden camera's en zeventien miljoen ogen'
- Netzpolitik.org (Duitsland), 12 maart 2014: 'Militärgeheimdienst der Niederlande der illegalen Datenweitergabe überführt'
- Volkskrant.nl, 2 april 2014: 'Cameradrones toegestaan - wat betekent dat voor u?'

- RTL.nl, 2 april 2014: 'Kentekens voortaan vier weken opgeslagen'
- NU.nl, 3 april 2014: 'Opslag camerabeelden kentekens door politie stap dichterbij'
- RTL Nieuws, 3 april 2014: televisie-interview met voorzitter Privacy First over opslag ANPR-gegevens
- Radio 1, 9 april 2014: interview met voorzitter Privacy First over wetsvoorstel 4 weken opslag ANPR
- NU.nl, 22 april 2014: 'Geef patiënt regie over medische gegevens'
- TROS Radar & VARA Kassa, 22 april 2014: 'Geef patiënt regie over medische gegevens'
- SmartHealth.nl, 24 april 2014: 'Kan iedere zorgverlener bij al je medische gegevens?'
- Zorgvisie, 25 april 2014: 'Landelijke campagne voor behoud medische privacy'
- NRC Handelsblad, 30 april 2014: 'Geef arts en patiënt eigen dossier terug'
- Radio 1 (NOS), 13 mei 2014: interview met Privacy First over rechtszaak 'Burgers tegen Plasterk'
- Trouw, 14 mei 2014: 'Wirwar van camera's langs de snelweg'
- Omroep Gelderland, 5 juni 2014: tv-interview met Privacy First over civiele drones
- Telegraaf, 8 juni 2014: 'Gevangen in 'datakluwen'; privacyvoorvechters pleiten op Big Brother Dag voor vrijheid'
- Lexology (Verenigd Koninkrijk), 15 juli 2014: 'Dutch government violated article 8 ECHR by requesting and saving personal data in central register'
- NU.nl, 23 juli 2014: 'Nederland mag gegevens blijven uitwisselen met NSA'
- NOS Teletekst, 23 juli 2014: 'AIVD mag gegevens krijgen van VS'
- Security.nl, 24 juli 2014: 'Hoger beroep tegen uitspraak over uitwisseling NSA-data'
- Radio 1 (NOS), 7 augustus 2014: interview met Privacy First over gebrek aan wetgeving rond drones
- Frankfurter Allgemeine Zeitung (Duitsland), 12 augustus 2014: 'Big Brother in Holland'
- AD/Rotterdams Dagblad, 20 aug. 2014: 'Stop met bewaren van gegevens parkeerders'
- Advocatenblad, augustus 2014: 'Typisch Opstelten'
- BNR Nieuwsradio, 11 sept. 2014: interview over "slimme camera's" op Schiphol
- Verkeer in Beeld, 20 oktober 2014: 'Kritiek op OV-chipkaart blijft aanhouden'
- Personal Computer Magazine, 22 oktober 2014: 'Belastingdienst kijkt op grote schaal mee met politiecamera's'
- EenVandaag, 28 oktober 2014: interview met Privacy First over gebruik van ANPR-camera's door Belastingdienst
- Metronieuws.nl, 7 november 2014: 'Amsterdam voor de rechter om kentekenparkeren'
- Trouw, 11 november 2014: 'Is kentekenparkeren een aantasting van de privacy?'
- Telegraaf, 11 november 2014: 'Privacykwestie voor rechtbank; weigeraar kentekenparkeren laat zaak voorkomen'
- Radio 1, 11 november 2014: 'Anoniem parkeren moet kunnen'

- RTL Nieuws, 11 november 2014: reportage over rechtszaak Privacy First tegen kentekenparkeren
- Volkskrant.nl, 19 november 2014: 'Privacybeschermers kritisch over 'koevoetcontrole' bouwmarkten'
- De Gelderlander, 21 november 2014: 'Wat als je lijkt op een crimineel?'
- Radio 2, 26 november 2014: interview met Privacy First over onduidelijke regelgeving rond drones
- AT5, 26 november 2014: discussie met Privacy First over DNA-databank voor opsporing
- NRC Handelsblad, 6 december 2014: 'Kort geding tegen staat om opslag van internet- en belgegevens'
- NU.nl, 6 december 2014: 'Kort geding tegen Nederlandse staat vanwege bewaarplicht'
- NOS Teletekst, 6 december 2014: 'Kort geding tegen bewaarplicht data'
- Trouw, 8 december 2014: 'Mag provider gegevens opslaan?'
- Leeuwarder Courant, 13 december 2014: 'Mag die duimafdruk van mijn paspoort af?'

Interview met Bas Filippini (Privacy First), 3 april 2014 © RTL Nieuws

5.2 Individuele burgers

Dagelijks ontvangt Privacy First vragen van burgers over de meest uiteenlopende privacykwesties. In 2014 voerden de volgende onderwerpen de boventoon:

- Kentekenparkeren;
- Verplichte afname van vingerafdrukken voor paspoorten;
- Trajectcontroles;
- Automatische Nummerplaatherkenning (ANPR) op snelwegen;
- Gemeentelijk cameratoezicht;
- Camerasysteem @MIGO-BORAS;
- Medische privacy en EPD/LSP;

- OV-chipkaart;
- Slimme energiemeters;
- Privacy bij werkgevers.

In vrijwel alle gevallen kon Privacy First deze vragen naar tevredenheid beantwoorden, soms na raadpleging van relevante experts in ons netwerk. Bij gebrek aan kennis of ervaring terzake verwijst Privacy First mensen door naar andere maatschappelijke organisaties of naar gespecialiseerde overheidsinstanties.

5.3 Internet

De websites van Privacy First vormen onze primaire nieuws- en opiniekanalen. Naast onze Nederlandstalige website www.privacyfirst.nl is er ook het Engelstalige www.privacyfirst.eu. Sinds eind 2013 worden beide sites gesponsord door de privacyvriendelijke provider Greenhost. Sinds begin 2014 is het aantal bezoekers op onze websites ruim verdubbeld; inmiddels bedraagt dit zo'n 25.000 bezoekers per maand. Ook is Privacy First met name actief op Twitter en heeft Privacy First sinds eind 2014 een eigen LinkedIn-groep voor iedereen die zich graag met privacykwesties bezighoudt. Daarnaast is Privacy First actief op Facebook en blijven wij graag ruimte bieden voor (eventueel anonieme) gastcolumns en ingezonden artikelen op onze website(s). Privacy First zal medio 2015 onze Nederlandstalige website geheel vernieuwen met betere mogelijkheden voor donaties, anonieme communicatie, social media en burgerparticipatie. Wilt u graag op de hoogte blijven van alle ontwikkelingen rondom Privacy First? Meldt u dan aan voor onze digitale nieuwsbrief via info@privacyfirst.nl !

6. Evenementen

In januari 2014 was Privacy First wederom *event supporter* van de internationale conferentie *Computers, Privacy & Data Protection* (CPDP) in Brussel. Dit megacongres brengt jaarlijks honderden Europese en Noord-Amerikaanse privacy-experts uit de wetenschap, overheid, bedrijfsleven en *civil society* bij elkaar. Daarnaast gaf Privacy First in 2014 onder meer gastcolleges en presentaties bij het Amsterdam Platform for Privacy Research (APPR), de Hogeschool Rotterdam en de Rietveld Academie. Symposia en bijeenkomsten waar Privacy First in 2014 actief aan deelnam vonden onder meer plaats bij het Platform Bescherming Burgerrechten, Breed Mensenrechten Overleg Nederland, DDMA, Nederlands Juristen Comité voor de Mensenrechten (NJCM), URIOS, ECP-EPN, Platform Identity Management Nederland, Vereniging voor Media- en Communicatierecht (VMC), Vereniging voor OverheidsManagement (VOM), Koninklijke Nederlandse Akademie van Wetenschappen (KNAW), Ad de Jonge Centrum en De Balie. Tevens werd Privacy First in 2014 o.a. geconsulteerd door het College voor de Rechten van de Mens (privacy en bescherming van persoonsgegevens) en had Privacy First persoonlijke meetings met o.a. het CBP, AIVD, Tweede Kamerleden van D66, PvdA, VVD, ChristenUnie en SP, VNO-NCW, het nieuwe Public Interest Litigation Project

(PILP), Crowdsuing.nl, NL Confidential (voorheen Meld Misdaad Anoniem), Dime (Data is me) en IT's Privacy. Verder was Privacy First in 2014 betrokken bij meerdere scripties, waaronder als opdrachtgever voor een juridische scriptie over cameratoezicht op de werkvloer.

Vincent Böhre (Privacy First) bij het VOM-Reuring!Café met AIVD & NCTV, 19 januari 2015, Den Haag

Foto: Rein J., Shutterfly.com

Privacy First organiseerde de laatste jaren regelmatig thema-avonden annex borrels voor het grote publiek en onze achterban, waaronder onze vrijwilligers, donateurs en experts uit ons netwerk van journalisten, wetenschappers, ICT'ers en juristen. Sinds 2012 vonden deze avonden steevast plaats op de kantoorlocatie van Privacy First in het voormalige Volkskrantgebouw in Amsterdam. Wegens de recente verbouwing van het Volkskrantgebouw tot hotel (Volkshotel) heeft Privacy First echter besloten om deze bijeenkomsten in 2014 tijdelijk op te schorten totdat het nieuwe Volkshotel en het bijbehorende café-restaurant Canvas na de zomer van 2014 hun deuren geopend zouden hebben. Vervolgens organiseerde Privacy First eind 2014 in Canvas de succesvolle 'pre-launch' van ons nieuwe initiatief Privacy First Solutions, met inspirerende sprekers van Greenhost en de Nationale DenkTank. In 2015 is Privacy First van plan om meer van dergelijke evenementen te (co-)organiseren, zowel op onze eigen kantoorlocatie in het Volkshotel als op externe locaties in Nederland. Wilt u graag een uitnodiging voor ons eerstvolgende evenement ontvangen? Mail ons! Dan zetten wij u op de gastenlijst.

Martijn van der Veen (Privacy First) tijdens de pre-launch van Privacy First Solutions, 2 december 2014, Amsterdam Foto: Maarten Tromp

7. Organisatie

Privacy First is een onafhankelijke, ANBI-erkende stichting die grotendeels uit vrijwilligers bestaat. De kern van de organisatie van Privacy First bestond in 2014 uit de volgende personen:

- drs. Bas Filippini (oprichter en voorzitter)
- mr. Vincent Böhre (*director of operations*)
- drs. Martijn van der Veen (kwartiermaker Privacy First Solutions).

De groep vrijwilligers van Privacy First bleef in 2014 stabiel en bestaat grotendeels uit professionals die Privacy First structureel ondersteunen, zowel inhoudelijk (verschillende privacy-thema's en vertaalwerkzaamheden) als organisatorisch (ICT, fondsenwerving, PR en fotografie). Daarnaast beschikt Privacy First over een uitgebreid netwerk aan experts uit alle hoeken van de samenleving, variërend van wetenschappers, juristen en ICT'ers tot journalisten, politici en ambtenaren.

8. Financiën

Stichting Privacy First is voor haar werkzaamheden grotendeels afhankelijk van individuele donaties. Het donateursbestand van Privacy First is de laatste jaren snel gegroeid en in 2014 zijn de inkomsten van Privacy First meer dan verdubbeld. Bovendien wordt Privacy First sinds begin 2015 financieel gesteund door Stichting Democratie en Media t.b.v. ons meerjarige project Privacy First Solutions. Vast beleid van Privacy First is om alle inkomsten zoveel mogelijk te besteden aan

inhoudelijk relevante zaken en de operationele kosten zo laag mogelijk te houden. Reis- en lunchkosten zijn in principe voor ieders eigen rekening, communicatie verloopt (ook telefonisch) grotendeels via internet en dure borrels of andere luxe zaken zijn voor Privacy First taboe. Op deze manier komt iedere euro zo effectief mogelijk ten goede aan de privacy van iedere Nederlander.

Jaaroverzicht 2014 (euro)		**2013 (euro)**
Inkomsten:		
Donaties	73.933	32.938
Onderhuur	1.928	1.272
Overige inkomsten	3.379*	273

*: proceskostenvergoeding Hof Den Haag in Paspoortproces Privacy First c.s.

Uitgaven:		
Personeelskosten	42.901	27.956
Juridische kosten	33.389	348
Huisvesting	3.464	5.089
Campagnekosten	2.595	190
Evenementen	1.868	577
Websites	1.156	758
Bancaire en verzekeringskosten	783	548
Kantoorkosten	350	1.094
Reiskosten	256	129
Postbus en frankeringskosten	252	213
Communicatiekosten	137	165
Promotiemateriaal	61	258
Overige kosten	51	130

Wilt u Privacy First graag steunen? Maak dan een donatie over naar IBAN: NL95ABNA0495527521 (BIC: ABNANL2A) t.n.v. Stichting Privacy First te Amsterdam. Privacy First is erkend als Algemeen Nut Beogende Instelling (ANBI). Uw giften aan Privacy First zijn daarom belastingaftrekbaar.

Postbus 16799
1001 RG Amsterdam
Telefoon: 020-8100279
Email: info@privacyfirst.nl
Website: www.privacyfirst.nl

Privacy First is ingeschreven in het Stichtingenregister van de KvK Amsterdam onder nr. 34298157.
RSIN/fiscaal nummer: 819211710.