



PRIVACY FIRST

eigen keuzes in een vrije omgeving

JAARVERSLAG 2018

Stichting Privacy First
Amsterdam

9 december 2019

Inhoudsopgave

1.	Voorwoord	1
2.	Visie en beleid	2
3.	Projecten en evenementen	3
3.1	Nederlandse Privacy Awards & Nationale Privacy Conferentie	3
3.2	Publieksdebat over kinderen en privacy	5
3.3	Sleepwet-referendumdebat	6
3.4	Privacy First Solutions.....	7
3.5	Privacy First als dagelijkse vraagbaak.....	7
3.6	Stagiairs	7
3.7	Overige activiteiten	7
4.	Politieke lobby	8
4.1	Sleepwet referendum campagne	8
4.2	Nieuwe wet op orgaandonatie.....	9
4.3	EU Passenger Name Records (PNR).....	9
4.4	Wetsvoorstel Computercriminaliteit III ('politie-hackwet')	10
4.5	Afschaffing raadgevend referendum	10
4.6	Invoering van Taser-wapens (stroomstootwapens) bij politie.....	11
4.7	Verplichte vingerafdrukken in identiteitskaarten	12
5.	Rechtszaken	14
5.1	Nieuwe Wet op de inlichtingen- en veiligheidsdiensten ('Sleepwet')	14
5.2	Zaak Burgers tegen Plasterk	15
5.3	Systeem Risico Indicatie (SyRI)	16
5.4	ANPR (Automatische Nummerplaat Herkenning).....	17
5.5	Kentekenparkeren & recht op contante/anonieme betaling.....	17
5.6	Trajectcontrole	18
5.7	Landelijk Schakelpunt (LSP).....	19
5.8	Individuele rechtszaken Michiel Jonker	19
6.	Communicatie	20

6.1	Massamedia	20
6.2	Internet.....	20
7.	Organisatie	21
8.	Financiën	22

1. Voorwoord

Het afgelopen jaar hebben er veel ontwikkelingen binnen de rechtsstaat plaatsgevonden en is de privacy van de burger verder afgenomen. Ontwikkelingen in de financiële wereld met betrekking tot de *war on cash*, PSD2 en UBO brengen de burger steeds verder in het nauw met betrekking tot zijn soevereiniteit inzake bestedingen. In de medische wereld komt centralisatie en het landelijk EPD steeds weer tevoorschijn, terwijl goede decentrale alternatieven steeds meer voorhanden zijn. In het algemeen is de Sleepwet-filosofie leidend binnen de overheid en diensten waardoor het complete leven van de burger continu en permanent gemonitord gaat worden. Vrijheid wordt ingeruild voor dwang en uniformiteit om binnen “de norm” te bewegen, te denken en te handelen, vanuit een grote dosis zelfcensuur. In de openbare ruimte, binnen scholen, bibliotheken en winkels, overal is dezelfde, vaak door de overheid en bedrijfsleven gestimuleerde trend waarneembaar. Dit met omkering van klassieke rechtsprincipes tot gevolg. Uitzonderingen worden de regel, in plaats van bevestiging van de regel. Privacy First staat voor eigen keuzes in een vrije ruimte en ziet ondanks de genoemde ontwikkelingen grote kansen voor Nederland als privacy gidsland. Hoogtepunt is de uitreiking van onze jaarlijkse Nederlandse Privacy Awards, waarin bedrijven en organisaties duurzame privacy-oplossingen introduceren en daarmee een lichtend alternatief zijn voor de huidige trend. Ook komend jaar zullen wij weer veel van onze acties, rechtszaken en lobby voortzetten. Wij hopen daarbij op uw steun als donateur!

Voor een vrij 2020!

Bas Filippini,
voorzitter Privacy First

2. Visie en beleid

Privacy First is in 2008 opgericht als onafhankelijke stichting ter behoud en bevordering van ieders recht op privacy. Privacy is een universeel mensenrecht en de basis van onze democratische rechtsstaat. Naast de persoonlijke levenssfeer omvat het recht op privacy ook de bescherming van persoonsgegevens, vertrouwelijke communicatie en lichamelijke integriteit. Van alle mensenrechten staat het recht op privacy in deze tijd het meest onder druk. Privacy First maakt zich daarom sterk om dit recht zoveel mogelijk te beschermen en te bevorderen. Als Algemeen Nut Beogende Instelling (ANBI) doet Privacy First dit in het algemeen belang, hetzij voor de gehele bevolking, hetzij voor kwetsbare bevolkingsgroepen. Privacy First hanteert daarbij een brede, principiële oriëntatie op privacy, zowel in relatie tot onze vrije, open samenleving alsook met betrekking tot andere relevante mensenrechten. Ons blikveld en onze activiteiten strekken zich daarbij uit tot zowel het digitale als het analoge domein. Deze werelden raken echter in toenemende mate geïntegreerd en maken de klassieke 'analoge ruimte' steeds kleiner. De impact die technologie op iemands persoonlijke levenssfeer heeft lijkt in een steeds hogere versnelling te komen. In 2017 waren termen als 'Big Data' en 'Cloud' nog buzzwords, nu bevat vrijwel ieder initiatief van de overheid en bedrijfsleven termen als 'smart' en 'artificial intelligence'. Door een gebrek aan normenkader en ethische discussie ontstaat een groot risico dat Nederland één groot 'Living Lab' wordt, oftewel in een voortdurende experimentele staat verkeert zonder passende waarborgen. Om deze ontwikkelingen te keren en in goede banen te leiden pleit Privacy First naast goede wetgeving al jaren voor *privacy by design*: vanaf het allereerste ontwerp privacy inbouwen in diensten en technologie. De komst van de nieuwe Europese privacywet AVG geeft ons daarbij meer wind in de rug. Tegelijkertijd opereert Privacy First in een krachtenveld waardoor de privacy voortdurend bedreigd wordt. Het werk van Privacy First wordt daardoor steeds urgenter en relevanter.

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 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 de laatste jaren voornamelijk op biometrie, cameratoezicht, de OV-chipkaart, medische privacy, mobiliteit en anonimiteit in de openbare ruimte. Daarnaast is Privacy First steeds actiever op het thema privacy & geheime diensten, Big Data, *profiling* en financiële privacy.

Onze kernmissie is om de bevolking te behoeden voor massa surveillance en Nederland te ontwikkelen tot internationaal Privacy Gidsland. Hieronder lichten wij onze voornaamste activiteiten uit 2018 graag toe.

3. Projecten en evenementen

3.1 Nederlandse Privacy Awards & Nationale Privacy Conferentie

Op 28 januari 2019 organiseerden ECP en Privacy First opnieuw gezamenlijk onze jaarlijkse Nationale Privacy Conferentie. Dit is inmiddels hét jaarlijkse Nederlandse privacy-evenement rond de Europese Dag van de Privacy. Ons doel van dit evenement is om met het bedrijfsleven, overheid, wetenschap en maatschappelijk middenveld gezamenlijk te bouwen aan een privacyvriendelijke informatiemaatschappij en Nederland te helpen ontwikkelen tot internationaal Privacy Gidsland. De congreslocatie was ditmaal Nieuwspoort in Den Haag en de belangstelling bleek opnieuw enorm: meer dan 200 professionals hadden zich gratis aangemeld, met een zaalcapaciteit van 160 personen. Iedere congresdeelnemer ontving het [‘Blauwe Boekje’](#) van dr. Jaap-Henk Hoepman (Radboud Universiteit Nijmegen) over *privacy by design*. Keynote speakers tijdens het congres waren Aleid Wolfsen (Autoriteit Persoonsgegevens), Sophie in 't Veld (Europees Parlement), Brenno de Winter, Jeroen Terstegge (Privacy Management Partners) en Tijmen Schep (Setup). Dagvoorzitter was presentator Tom Jessen (RTL, BNR).



Aleid Wolfsen (voorzitter Autoriteit Persoonsgegevens) tijdens de Nationale Privacy Conferentie, 28 januari 2019. Foto: Tamara Heck.

Als afsluitend onderdeel van de conferentie werden door Privacy First onze jaarlijkse Nederlandse Privacy Awards uitgereikt. In de zomer van 2018 heeft Privacy First zelf (op eigen kosten en met eigen personeel) een speciale website voor de Awards

ontwikkeld: www.privacyawards.nl. Vervolgens ontving Privacy First bijna 20 inzendingen voor de Awards, waarvan de meesten zeer hoogwaardig. Beoordeling van alle inzendingen en bedrijfsbezoeken door onze onafhankelijke Awards-jury vond vervolgens plaats gedurende de herfst en winter van 2018. Genomineerd in de categorie



Nederlandse PRIVACY AWARDS

Consumentenoplossingen werden *Private Search 2.0* (Startpage.com), *VraagApp* en *Schluss*, in de categorie Bedrijfsoplossingen *Privacy op Schooltas* en *Privacy*

Designer (Privacy Company & SURF) en in de categorie Overheidsdiensten *Passantentellingen* (gemeente Nijmegen) en het project *Privacy by Design* van de Belastingdienst. Tijdens de conferentie hebben alle genomineerden hun projecten middels Award-pitches aan het publiek gepresenteerd. *Private Search 2.0* en *Privacy Designer* werden vervolgens door de jury tot winnaars uitgeroepen. Daarnaast ging de Aanmoedigingsprijs naar het initiatief *PublicSpaces*.



Winnaars Nederlandse Privacy Awards 2019.

De jury van de Nederlandse Privacy Awards bestond in 2018 uit de volgende personen:

- Bart van der Sloot (senior researcher, Universiteit Tilburg; juryvoorzitter)
- Bas Filippini (oprichter en voorzitter Privacy First)
- Paul Korremans (partner Comfort-IA; functionaris gegevensbescherming; docent VNG, OSR en UvA; tevens bestuurslid Privacy First)
- Marie-José Bonthuis (eigenaar IT's Privacy)
- Esther Janssen (advocaat Informatierecht en grondrechten, bureau Brandeis)

- Esther Keymolen (techniekfilosoof, TILT, Universiteit Tilburg)
- Matthijs Koot (senior security specialist, Secura BV)
- Marc van Lieshout (senior onderzoeker TNO en zakelijk directeur PI.lab)
- Wendeline Sjouwerman (privacy specialist lokale overheden en zorg).

Een uitgebreid verslag van het congres en de Awards vindt u op [onze website](#).



De Nationale Privacy Conferentie en de Nederlandse Privacy Awards werden in 2018 mede mogelijk gemaakt door Stichting Democratie & Media. Begin 2020 zullen Privacy First en ECP dit inspirerende evenement opnieuw organiseren. Zou uw organisatie graag partner of sponsor willen worden? Neem dan contact op met Privacy First!

3.2 Publieksdebat over kinderen en privacy

Begin 2018 organiseerde Privacy First op onze kantoorlocatie in het Volkshotel (Amsterdam) een drukbezochte Nieuwjaarsborrel en succesvol publieksdebat over het thema kinderen & privacy. Sprekers waren Bas Filippini (Privacy First), Huib Gardeniers (Net2Legal), Simone van Dijk (Privacy First), Arda Gerkens (Eerste Kamer) en Iris Hoen (Wille Donker Advocaten). Zie voor een uitgebreid verslag <https://www.privacyfirst.nl/solutions/evenementen/item/1103-verslag-van-publieksdebat-over-kinderen-privacy.html>. Privacy First heeft in toenemende mate zorgen op dit terrein en zet zich sinds 2018 steeds actiever in om de privacy van kinderen en leerlingen (met name in het basisonderwijs) te bevorderen, allereerst middels kritische gesprekken met verantwoordelijke organisaties in de private en publieke sector.



Nieuwjaarsspeech Bas Filippini (voorzitter Privacy First), 17 januari 2018. Foto: Bertus Gerssen.

3.3 Sleepwet-referendumdebat

In het kader van het referendum over de nieuwe Wet op de inlichtingen- en veiligheidsdiensten organiseerde Privacy First op 15 maart 2018 in het Parool Theater (Amsterdam) een kritisch publieksdebat over de privacy-aspecten rond de nieuwe ‘Sleepwet’. De volledige debatavond werd live uitgezonden op internet en in de aanloop naar het referendum tevens meerdere malen integraal herhaald door NPO Politiek. Sprekers tijdens deze avond waren achtereenvolgens Dick Schoof (Nationaal Coördinator Terrorismebestrijding en Veiligheid), Nine de Vries (Amnesty International Nederland) en Otto Volgenant (Boekx Advocaten). Onze moderator was Bart de Koning (onderzoeksjournalist op het gebied van privacy en veiligheid). Tijdens het debat was er veel ruimte voor discussie tussen de sprekers onderling en met het publiek, gevolgd door een borrel waar wij samen konden proosten op een succesvol referendum!



Sleepwet referendum debat, 15 maart 2018. V.l.n.r.: Bart de Koning, Nine de Vries, Dick Schoof en Otto Volgenant. Beeld: Engage TV.

3.4 Privacy First Solutions

Privacy First wordt in toenemende mate door bedrijven en overheden gevraagd om advies. In uitzonderlijke gevallen, wanneer de intenties van de betreffende organisatie in lijn liggen met de missie van Privacy First, willen we graag een bijdrage leveren. Privacy First doet dit sinds enkele jaren onder de vlag van ons overkoepelende project Privacy First Solutions. Voorbeelden van Privacy First Solutions projecten in 2018 waren de ontwikkeling van een mogelijk keurmerk rond de nieuwe Europese betaalrichtlijn PSD2 i.s.m. de Volksbank en de Nederlandse Betaalvereniging. Tevens heeft Privacy First eind 2018 in dit verband het initiatief genomen voor de ontwikkeling van een PSD2-me-niet-register, zie onze nieuwe campagnewebsite www.psd2meniet.nl. Daarnaast was Privacy First (op initiatief van de Belastingdienst) sinds oktober 2018 kritisch betrokken bij een High Pressure Privacy Impact Assessment (DPIA) binnen de Belastingdienst, extern uitgevoerd door Privacy Management Partners (PMP). Op deze wijze tracht Privacy First – in het algemeen belang – bepaalde maatschappelijke ontwikkelingen positief te beïnvloeden en de privacy niet alleen “van buitenaf” maar ook “van binnenuit” zoveel mogelijk te laten waarborgen. Privacy First verwacht in 2019 diverse andere Solutions-projecten met nieuwe partners te kunnen initiëren.

3.5 Privacy First als dagelijkse vraagbaak

Privacy First wordt dagelijks telefonisch en per email benaderd door burgers, journalisten, studenten en scholieren met de meest uiteenlopende vragen en verzoeken op privacysterrein. Privacy First tracht de betreffende vragen altijd zo goed



en zo snel mogelijk te beantwoorden, maar dit vergt (soms te)veel van onze kleine stichting. Om deze reden verwijst Privacy First mensen soms door naar andere relevante organisaties, instanties, juristen en advocaten.

3.6 Stagiairs

In 2018 schreef een HBO-rechtenstudente bij Privacy First met succes haar scriptie over het wetsvoorstel ANPR. Nieuwe stagiairs en scriptiestudenten zijn bij Privacy First altijd welkom, mits actueel relevant voor ons werkkerrein.

3.7 Overige activiteiten

Privacy First was in 2018 actief bij diverse relevante congressen, seminars en meetings, waaronder bij de Universiteit Leiden, Platform Bescherming Burgerrechten, Woonbond, ECP, Instituut voor Informatierecht (UVA), Amnesty

International, Volksbank, Koninklijke Bibliotheek, NJCM, Universiteit van Amsterdam (spreker), Nieuwspoor, KPMG, Comité van Waakzaamheid, Pro Bono Connect, Vereniging Privacy Recht, Piratenpartij, CTIVD, V@School, Humanistisch Verbond, Vitens, WODC, Universiteit Tilburg, VVD (spreker), Staatscommissie Parlementair Stelsel, Hague Internet Summit (VN, Vredespaleis), Facebook, Belastingdienst, ministerie van Justitie en Veiligheid (spreker), Fox IT, Kaspersky, PILP, DNB (spreker), Good Pitch Europe, Lions (spreker), gemeente Haarlem, College voor de Rechten van de Mens, Nationale Referendumcommissie, Privacy Management Partners, One Conference, Autoriteit Persoonsgegevens, Vereniging van Ethici, Nederlandse Betaalvereniging, IIR (spreker), Nationale Ombudsman, Vereniging voor Biometrie & Identiteit (spreker) en Waag Society.

De medewerkers van Privacy First worden regelmatig als spreker uitgenodigd bij publieksevenementen van overheid, bedrijfsleven en wetenschap. In dat kader werkt Privacy First sinds enkele jaren samen met sprekersbureau Athenas. Verder voert Privacy First continu stille diplomatie op ons brede werkterrein; in dit verband had Privacy First in 2018 talloze meetings met overheden, bedrijven en andere organisaties.

4. Politieke lobby

4.1 Sleepwet referendum campagne

De belangrijkste en meest invloedrijke activiteit van Privacy First in 2018 was onze campagne in de aanloop naar het referendum over de nieuwe wet op inlichtingen- en veiligheidsdiensten, de zogeheten Sleepwet. Als één van de eerste organisaties in Nederland kreeg Privacy First hiervoor een relatief hoge subsidie van de Nationale Referendumcommissie. Privacy First heeft deze middelen vervolgens besteed aan diverse Sleepwet-campagne activiteiten in de periode januari – maart 2018, bestaande uit 1) een kritisch publieksdebat, 2) campagne op de website van Privacy First, 3) activering van media en beïnvloeding van de publieke opinie, 4) nieuwsmonitoring en campagne op social media, 5) persadvertenties en 6) politieke lobby en stille diplomatie.



Een groot deel van de bevolking is door deze activiteiten bereikt, en met succes: op 21 maart 2018 stemde een nipte meerderheid TEGEN de Sleepwet. Naast dit succes

heeft onze campagne waarschijnlijk ook geleid tot een hoger nationaal privacybewustzijn in algemene zin. Naar aanleiding van het referendum kwam van overheidswege tevens een belofte van beperktere inzet van de nieuwe sleepnet-bevoegdheid in het binnenlands domein. Bovendien heeft het referendum politieke druk gegenereerd om de Sleepwet kritisch te gaan herzien. Desondanks trad de Sleepwet op 1 mei 2018 vrijwel ongewijzigd in werking en zijn de beloofde wetswijzigingen nog altijd niet ingediend.

4.2 Nieuwe wet op orgaandonatie

In februari 2018 heeft de Eerste Kamer bij nipte meerderheid een controversiële nieuwe Wet op orgaandonatie aangenomen. Tenzij men actief bezwaar maakt (of reeds heeft gemaakt) zal iedere Nederlander hierdoor als orgaandonor geregistreerd worden. Privacy First had de Eerste Kamer vooraf met klem geadviseerd om tegen deze wet te stemmen, aangezien deze in onze optiek in strijd is met het recht op privacy en lichamelijke integriteit. Het recht op lichamelijke integriteit is onderdeel van het recht op privacy en als zodanig beschermd onder zowel art. 8 EVRM als art. 11 Grondwet. Art. 11 Grondwet geldt ook na de dood. In tegenstelling tot sommige andere privacyrechten heeft het recht op lichamelijke integriteit en fysieke zelfbeschikking bovendien een relatief absoluut karakter; in beginsel heeft iedereen voorafgaande expliciete zeggenschap over zijn/haar eigen lichaam en organen. Slechts met expliciete en specifieke (per orgaan gedifferentieerde) individuele toestemming vooraf kan iemand als orgaandonor geregistreerd worden. Een donor-systeem waarbij iedereen bij voorbaat door de overheid tot donor wordt verklaard is hiermee per definitie in strijd. Privacy First betreurt het dan ook dat zo'n ingrijpende wet als deze Donorwet, waarover zoveel verdeeldheid en gebrek aan breed maatschappelijk draagvlak heerst, door de Eerste Kamer is aangenomen.

4.3 EU Passenger Name Records (PNR)

Na jarenlange vertraging (wegens privacybezwaren) werd in 2018 de Nederlandse implementatie van de Europese richtlijn inzake Passenger Name Records (PNR) parlementair behandeld. Ondanks structurele kritiek van Privacy First werd de PNR-wet vervolgens door zowel de Tweede als de Eerste Kamer aangenomen. Door deze nieuwe PNR-wet zullen talloze gegevens van alle vliegtuigpassagiers met vertrek of aankomst in Nederland 5 jaar lang in een centrale overheidsdatabank worden bewaard en gebruikt ter voorkoming, opsporing, onderzoek en vervolging van misdrijven en terrorisme. Gevoelige persoonsgegevens (waaronder naam- en adresgegevens, telefoonnummers, emailadressen, geboortedata, reisdata, ID-documentnummers, bestemmingen, medepassagiers en betaalgegevens) van vele miljoenen passagiers zullen daardoor jarenlang beschikbaar zijn voor *datamining* en *profiling*. Dit komt neer op massa-surveillance van grotendeels onschuldige burgers. Tot op heden is de juridisch vereiste maatschappelijke noodzaak en proportionaliteit van dit systeem niet aangetoond. PNR vormt daarmee een flagrante schending van

het recht op privacy en de vrijheid van beweging. Bovendien is de effectiviteit van PNR tot op heden nooit aangetoond: “statistische onderbouwing is niet voorhanden”, aldus zelfs de verantwoordelijke minister Grapperhaus (Justitie en Veiligheid). Privacy First verwacht dan ook dat de bovenliggende Europese PNR-richtlijn spoedig door het Europees Hof van Justitie zal worden getoetst en onrechtmatig zal worden verklaard. Daarna zal dezelfde situatie ontstaan als enkele jaren geleden bij de Europese telecom-bewaarplicht: zodra deze Europese richtlijn ongeldig is verklaard, zal de Nederlandse implementatiewetgeving door Privacy First in kort geding buiten werking worden gesteld.

4.4 Wetsvoorstel Computercriminaliteit III (‘politie-hackwet’)

In juni 2018 nam de Eerste Kamer het controversiële wetsvoorstel Computercriminaliteit III aan. Deze wet geeft de politie de bevoegdheid om vrijwel ieder apparaat te kunnen hacken. Bij deze wet is echter nooit sprake geweest van een grondige en onafhankelijke Privacy Impact Assessment. De vereiste maatschappelijke noodzaak en proportionaliteit van deze wet zijn tot op heden evenmin aangetoond. In de optiek van Privacy First wordt dit type wetgeving vooral gedreven door technologisch determinisme: alles wat technisch kan, wordt wettelijk



mogelijk gemaakt. Van enige wettelijke inperking in technologische zin is bewust geen sprake: de werking van het wetsvoorstel zal zich uitstrekken tot vrijwel alles wat met het internet in verbinding staat. In de toekomst dus vrijwel de gehele maatschappij, waaronder het

Internet of Things. In politiekringen wil men zelfs rijdende auto's kunnen hacken en stilzetten, met alle gevaren van dien voor de verkeersveiligheid. De misdrijven waarbij dit wetsvoorstel kan worden ingezet, kunnen bovendien simpelweg door de Minister worden uitgebreid bij Algemene Maatregel van Bestuur. Privacy First heeft het parlement dan ook meerdere malen verzocht om deze wet te verwerpen, danwel er tenminste paal en perk aan te stellen. Mede naar aanleiding van onze kritiek zal de inzet van de nieuwe bevoegdheden vooraf door een rechter-commissaris worden getoetst en zal er geen hacking van onschuldige derden plaatsvinden.

4.5 Afschaffing raadgevend referendum

Ondanks het succesvolle referendum over de nieuwe Wet op de inlichtingen- en veiligheidsdiensten heeft de Eerste Kamer in juni 2018 het raadgevend referendum afgeschaft. Privacy First betreurt dit en verwacht dat dit de bestaande kloof tussen burger en bestuur verder zal vergroten. Ook zal het leiden tot verder verlies van vertrouwen in de nationale politiek. Dit verzwakt onze democratie en, zonder de

corrigerende werking van het referendum, ook onze rechtsstaat.

Internationaalrechtelijk is een nationaal referendum een vorm van intern zelfbeschikkingsrecht: het collectieve recht van een nationale bevolking om haar eigen democratische toekomst te bepalen. Zoals alle mensenrechten dient dit recht voortdurend te worden beschermd en bevorderd. Een referendum is bovendien een democratische verworvenheid die niet zomaar, zonder legitieme aanleiding en objectieve rechtvaardiging, kan worden afgeschaft. Dit is mogelijk in strijd met het mensenrechtelijke regressieverbod: het verbod om democratisch verworven rechten van burgers zomaar terug te draaien. Begin 2018 heeft Privacy First de Eerste en Tweede Kamer hier tevergeefs op geattendeerd. Naar aanleiding hiervan werd Privacy First door de Eerste Kamer in maart 2018 uitgenodigd voor een expertmeeting over de internationaalrechtelijke aspecten van het raadgevend referendum. Nadien heeft Privacy First de Nederlandse afschaffing van het referendum tevens aangekaart bij de Verenigde Naties en de Nederlandse regering hierover ter verantwoording laten roepen bij het VN Mensenrechtencomité in Genève.

Op de vroegere DDR na is Nederland nu het enige land ter wereld dat het referendum na invoering weer heeft afgeschaft. Na Athene (democratie 1.0) en onze huidige 19e-eeuwse parlementaire democratie (2.0) is het in de optiek van Privacy First daarom hoog tijd voor meer burgerparticipatie en democratische vernieuwing: *Shared Democracy*, democratie 3.0. Evenals de Staatscommissie Parlementair Stelsel pleit Privacy First daarbij voor de invoering van een bindend correctief referendum (en een Constitutioneel Hof) ter versterking van onze democratische rechtsstaat. Privacy First zal zich hiervoor blijven inzetten.

4.6 Invoering van Taser-wapens (stroomstootwapens) bij politie

Van oudsher hanteert Privacy First een breed, mensenrechtelijk begrip van het recht op privacy. Hieronder valt ook het recht op lichamelijke integriteit. Dit recht staat de laatste jaren in toenemende mate onder druk: denk bijvoorbeeld aan preventief fouilleren op straat, bodyscans op luchthavens, vingerafdrukken in paspoorten, DNA-databanken, de nieuwe wet op orgaandonatie, discussies over verplicht vaccineren, etc. Naast art. 8 EVRM wordt het recht op lichamelijke integriteit in Nederland apart beschermd door art. 11 van de Grondwet. Op internationaal niveau behoort het recht op lichamelijke integriteit tot de categorie mensenrechten die de sterkste bescherming genieten, waaronder het absolute verbod op marteling of foltering.

In 2018 stuurde het Nederlands Juristen Comité voor de Mensenrechten (NJCM) namens een brede coalitie van maatschappelijke organisaties een zogeheten ‘schaduwrapportage’ over Nederland naar het VN Comité tegen Foltering. Op initiatief van Privacy First is daarbij, evenals in 2013, de kwestie van Taser-wapens (stroomstootwapens) nadrukkelijk aan de orde gesteld. De Nederlandse regering is namelijk al jaren van plan om iedere Nederlandse politieagent een eigen Taser-wapen te geven. Tot op heden zijn alleen de arrestatieteams van de Nederlandse politie met Taser-wapens uitgerust. Dat bredere, algemene inzet van Taser-wapens zal leiden tot structurele excessen ligt in de lijn der verwachting. In dit verband spreken met name alle Amerikaanse schandalen met Taser-wapens boekdelen. In de optiek van Privacy First kan het gebruik van Taser-wapens gemakkelijk leiden tot schending van het internationale verbod op foltering, wrede of onmenselijke behandeling en het daaraan verwante recht op lichamelijke integriteit. Taser-wapens verlagen immers de geweldsdrempel en laten nauwelijks uiterlijke sporen achter. Tegelijkertijd kunnen Taser-wapens ernstige fysieke en mentale schade veroorzaken. Dit levert ernstige risico’s op voor de Nederlandse bevolking, met name ook voor bepaalde kwetsbare groepen.



Mede naar aanleiding van de kritische input van Privacy First heeft het VN Comité tegen Foltering in december 2018 een aantal richtlijnen (*Concluding Observations*) aan de Nederlandse regering uitgevaardigd, waaronder het dringende verzoek om geen Taser-wapens in te voeren voor het gehele Nederlandse politiekorps en dit te beperken tot die gevallen waarin het gebruik van een Taser-wapen strikt noodzakelijk en proportioneel kan worden geacht. Tevens waarschuwt het Comité nadrukkelijk om geen Taser-wapens te gebruiken bij kwetsbare personen. Het Comité toont zich bovendien zeer bezorgd over de manier waarop Taser-wapens tot nu toe door de Nederlandse politie zijn gebruikt. Privacy First waardeert dit kritische oordeel en de principiële stellingname van het Comité. Dit creëert bovendien een sterk precedent voor andere landen wereldwijd. Privacy First zal erop blijven toezien dat de Nederlandse overheid de richtlijnen van het Comité naleeft.

4.7 Verplichte vingerafdrukken in identiteitskaarten

Sinds 2009 geldt in Nederland de controversiële Europese verplichting om vingerafdrukken in paspoorten op te nemen. Tot nu toe zijn identiteitskaarten van deze Europese verplichting uitgezonderd. Desondanks werden sinds 2009 ook in Nederlandse identiteitskaarten vingerafdrukken opgenomen. Wegens privacybezwaren werd deze Nederlandse verplichting per januari 2014 afgeschaft en in 2016 door de Raad van State met terugwerkende kracht onrechtmatig verklaard.

Sindsdien heeft de Europese Commissie echter aan nieuwe Europese wetgeving gewerkt om de opname van vingerafdrukken in alle Europese identiteitskaarten alsnog weer te verplichten. Privacy First heeft de Nederlandse regering diverse malen opgeroepen om zich hiertegen te verzetten. Immers:

1. In mei 2016 heeft de Raad van State reeds geoordeeld dat de verplichte opname van vingerafdrukken in Nederlandse identiteitskaarten in strijd is met het recht op privacy wegens gebrek aan noodzaak en proportionaliteit.

2. Uit diverse Wob-verzoeken van Privacy First is de laatste jaren gebleken dat het te bestrijden fenomeen (*look-alike* fraude met ID-documenten) dusdanig kleinschalig is, dat verplichte afgifte van vingerafdrukken ter bestrijding hiervan volstrekt disproportioneel en dus onrechtmatig is.

3. Bij de vingerafdrukken in paspoorten en ID-kaarten gold de laatste jaren een biometrisch foutenpercentage van maar liefst 30%, zo erkende staatssecretaris Teeven in de Tweede Kamer. Eerder gaf minister Donner in de Tweede Kamer een foutenpercentage van 21-25% toe.

4. Mede vanwege deze hoge foutenpercentages worden de vingerafdrukken in paspoorten en identiteitskaarten in het binnenland tot op heden vrijwel niet gebruikt. Aan de landsgrenzen, bij de douane en op luchthavens worden de vingerafdrukken zelfs totaal niet gebruikt.



5. Vanwege de hoge foutenpercentages instrueerde staatssecretaris Bijleveld (Binnenlandse Zaken) reeds in september 2009 alle Nederlandse gemeenten om (in principe) geen vingerafdruk-verificaties uit te voeren bij de uitgifte van paspoorten en identiteitskaarten. Bij een biometrische “mismatch” dient het betreffende ID-document immers retour aan de paspoortfabrikant gezonden te worden, wat bij hoge aantallen tot snelle maatschappelijke ontwrichting zou leiden. Het ministerie van Binnenlandse Zaken maakte zich in dit verband zorgen om sociale onrust en mogelijk geweld bij gemeentebalies. De betreffende zorgen en instructies vanuit het ministerie van Binnenlandse Zaken gelden tot op heden nog steeds.

6. Momenteel lopen bij het Europees Hof voor de Rechten van de Mens nog diverse individuele Nederlandse rechtszaken waarin de verplichte afgifte van vingerafdrukken voor paspoorten en ID-kaarten aangevochten wordt wegens strijd met art. 8 EVRM (recht op privacy).

7. Voor mensen die om welke reden dan ook geen vingerafdrukken wensen af te geven (biometrisch gewetensbezwaarden, art. 9 EVRM) zou in elk geval een uitzondering moeten worden bedongen.

5. Rechtszaken

Als maatschappelijke organisatie gaat het Privacy First erom zo effectief mogelijk te opereren met de beperkte middelen die wij hebben. Als stille diplomatie, politieke lobby en campagnes vruchteloos blijken, voert Privacy First daarom principiële rechtszaken tegen wetgeving en beleid die tot grootschalige privacyschendingen leiden. De afgelopen jaren deed Privacy First dit met succes tegen de centrale opslag van ieders vingerafdrukken onder de Paspoortwet en de opslag van ieders telecommunicatiedata onder de Wet bewaarplicht telecommunicatiegegevens. Privacy First voert dergelijke zaken bij voorkeur in coalitieverband en middels pro bono ondersteuning door geschikte advocatenkantoren.

5.1 Nieuwe Wet op de inlichtingen- en veiligheidsdiensten ('Sleepwet')

In juli 2017 nam de Eerste Kamer de controversiële nieuwe Wet op de inlichtingen- en veiligheidsdiensten aan. Door deze wet dreigt massa-surveillance in Nederland sindsdien een *fait accompli* te worden: nieuwe bevoegdheden onder deze wet zijn o.a. een massale internet-tap waardoor grote groepen mensen tegelijk afgeluisterd kunnen worden. Ter voorkoming hiervan vond op initiatief van een vijftal Amsterdamse studenten op 21 maart 2018 een nationaal referendum over deze zogeheten 'Sleepwet' plaats. Tijdens dit referendum heeft een meerderheid van de Nederlandse bevolking zich duidelijk TEGEN deze wet uitgesproken. In reactie hierop heeft het Nederlandse kabinet echter slechts enkele summiere, oppervlakkige beleidswijzigingen en enkele niet-fundamentele wetswijzigingen in het vooruitzicht gesteld. Op 1 mei 2018 trad de 'Sleepwet' vervolgens vrijwel ongewijzigd in werking.



Referendum

Kort geding tegen Sleepwet

Vast beleid van Privacy First is om massale privacyschendingen te voorkomen. De inwerkingtreding van de huidige Sleepwet vormt onmiskenbaar een massale privacyschending: het internet-verkeer van onschuldige burgers kan hierdoor op grote schaal worden afgetapt. Bovendien zullen deze data van onschuldige burgers massaal en ongeëvalueerd worden uitgewisseld met buitenlandse geheime diensten. Dit vormt een flagrante schending van het recht op privacy. Mogelijke wetswijzigingen om dit achteraf te 'repareren' konden dan ook niet worden afgewacht; de privacyschendingen zouden dan immers al zijn geschied. Een brede coalitie van o.a. Bits of Freedom en Privacy First heeft het kabinet daarom in april 2018 verzocht om de invoering van (de meest privacyschendende onderdelen van)

de Sleepwet uit te stellen totdat alle gewenste wetswijzigingen in het parlement behandeld zouden zijn. Nadat het kabinet dit verzoek had geweigerd was onze coalitie vervolgens genoodzaakt om een civielrechtelijk kort geding te voeren om de meest privacyschendende onderdelen van de Sleepwet buiten werking te laten stellen wegens strijd met hoger (Europees) privacyrecht. Naast Privacy First bestond de coalitie voor dit kort geding uit Bits of Freedom, het Nederlands Juristen Comité voor de Mensenrechten (NJCM), Nederlandse Vereniging van Strafrechtadvocaten (NVSA), Platform Bescherming Burgerrechten, Free Press Unlimited, BIT, Voys, Speakup, Greenpeace International, Waag Society en Mijndomein Hosting. De zaak werd behandeld door Boekx Advocaten en gecoördineerd door het Public Interest Litigation Project (PILP) van het NJCM. Op 7 juni 2018 vond het kort geding plaats bij de rechtbank Den Haag. Op 26 juni 2018 heeft de rechtbank de zaak helaas afgewezen. Dit vonnis is uiterst teleurstellend. Weliswaar lag de juridische lat in deze zaak hoog: om dit kort geding te kunnen winnen diende de rechter de Sleepwet "onmiskenbaar onverbindend" te verklaren wegens overduidelijke (onmiskenbare) strijdigheid met internationaal of Europees recht. Het vonnis van de rechter leest echter vooral als een doelredeneratie in het voordeel van de Staat, waarbij diverse bezwaren van onze coalitie in het vonnis onbenoemd zijn gebleven. Tevens dient te worden benadrukt (zoals de rechtbank zelf ook doet) dat dit vonnis slechts een voorlopig oordeel inhoudt en dat in deze zaak geen sprake was van een grondige, "volle" toetsing.

De coalitie vindt dat de regering, mede gezien de uitslag van het referendum, had moeten wachten met het invoeren van de aangevochten onderdelen uit de Sleepwet totdat het parlementaire wetgevingsproces naar aanleiding van het referendum zou zijn afgerond. Ongewijzigde invoering van de Sleepwet per 1 mei 2018 en pas later (op immer onbekende datum in de toekomst) een wetswijziging voorleggen is en blijft dan ook onjuist.

De coalitie heeft diverse mogelijke juridische vervolgstappen besproken. Mede afhankelijk van het verdere parlementaire traject ligt nu een grootschalige bodemprocedure tegen de Sleepwet in het verschiet.

5.2 Zaak Burgers tegen Plasterk

Sinds eind 2013 voert Privacy First samen met andere organisaties en burgers de rechtszaak 'Burgers tegen (Minister) Plasterk'. Aanleiding voor deze civielrechtelijke zaak tegen de Nederlandse Staat vormden de onthullingen van Edward Snowden over de praktijken van (buitenlandse) inlichtingendiensten, waaronder de Amerikaanse NSA en Britse GCHQ. Onze coalitie eist dat de Staat stopt met het gebruiken van buitenlandse inlichtingen die niet in overeenstemming met de Nederlandse wet zijn verkregen. Onze advocaten van bureau Brandeis voeren deze zaak op basis van hun eigen pro bono fonds voor maatschappelijke rechtszaken. De aangesloten organisaties zijn: Stichting Privacy First, de Nederlandse Vereniging van

Strafrechtadvocaten (NVSA), de Nederlandse Vereniging van Journalisten (NVJ) en Internet Society Nederland. Na negatieve vonnissen van zowel de rechtbank als het Hof Den Haag heeft ook de Hoge Raad op 7 september 2018 onze cassatie in deze zaak echter verworpen. Daarmee biedt de Hoge Raad sindsdien een vrijbrief voor Nederlandse geheime diensten om zonder rechtsbescherming grote hoeveelheden gegevens van Nederlandse burgers te blijven verzamelen via buitenlandse inlichtingendiensten. Onze advocaten hebben deze zaak begin 2019 voortgezet bij het Europees Hof voor de Rechten van de Mens (EHRM) in Straatsburg. Parallel hieraan loopt bij het EHRM o.a. een vergelijkbare Britse zaak van Big Brother Watch tegen de Britse regering. Privacy First hoopt dat het Hof in beide zaken spoedig tot een kritisch oordeel zal komen.

5.3 Systeem Risico Indicatie (SyRI)

Eind maart 2018 heeft een brede coalitie van maatschappelijke organisaties de Nederlandse Staat gedagvaard ter buitenwerkingstelling van het Systeem Risico Indicatie. Het Systeem Risico Indicatie (SyRI) licht met geheime algoritmen grote groepen mensen (en zelfs complete woonwijken) door om burgers heimelijk te profileren op het risico dat ze frauderen met sociale voorzieningen. Naast massale schending van het recht op privacy is dit systeem tevens in strijd met het recht op een eerlijk proces en heeft het een discriminerende en stigmatiserende werking. Volgens de coalitie van eisers vormt SyRI daarom een bedreiging voor de rechtsstaat en dient de wetgeving waarop SyRI gebaseerd is onrechtmatig te worden verklaard.

De groep eisers bestaat uit de Stichting Platform Bescherming Burgerrechten, het Nederlands Juristen Comité voor de Mensenrechten (NJCM), Stichting Privacy First, Stichting KDVP, de Landelijke Cliëntenraad en FNV. Auteurs Tommy Wieringa en Maxim Februari, die zich eerder zeer kritisch uitspraken over SyRI, hebben zich op persoonlijke titel bij de procedure aangesloten. De coalitie wordt vertegenwoordigd

door Anton Ekker (Ekker Advocatuur) en Douwe Linders (SOLV Advocaten). Ook deze zaak wordt gecoördineerd door het Public Interest Litigation Project (PILP) van het NJCM.



Bij voorbaat verdacht

De partijen bij deze procedure zijn niet tegen het bestrijden van fraude door de overheid. Zij vinden alleen dat dit op grond

van een concrete verdenking dient te gebeuren. Er mag niet middels sleepnetacties in het privéleven van niet-verdachte Nederlandse burgers worden gezocht naar mogelijke risico's op fraude. Deze disproportionele methode doet volgens de eisende partijen meer kwaad dan goed. Er bestaan betere en minder ingrijpende vormen van fraudebestrijding dan SyRI.

Onder druk van deze rechtszaak zijn meerdere gemeenten (waaronder Rotterdam) reeds gestopt met de inzet van SyRI. Op 29 oktober 2019 vond bij de rechtbank Den Haag de rechtszitting in de zaak plaats. De uitspraak van de rechtbank staat vooralsnog gepland op 5 februari 2020.

Voor meer informatie en updates verwijst Privacy First u graag naar de speciale campagnewebsite van het Platform Bescherming Burgerrechten: Bijvoorbaatverdacht.nl.

5.4 ANPR (Automatische Nummerplaat Herkenning)

Na jarenlange vertraging (wegens privacybezwaren) nam de Eerste Kamer eind 2018 een draconische wet aan waardoor de reisbewegingen van miljoenen automobilisten in Nederland continu 4 weken in een centrale politiedatabank zullen belanden, ongeacht of men ergens van verdacht wordt. Dit is de wet inzake Automatische Nummerplaat Herkenning (*Automatic Number Plate Recognition*, ANPR) die per 1 januari 2019 in werking trad.



Mede dankzij de financiële steun van talloze donateurs bereidt Privacy First sindsdien een cruciale rechtszaak (kort geding en eventuele bodemprocedure) ter buitenwerkingstelling van deze wet voor. De ANPR-wet vormt immers een massale privacyschending en hoort simpelweg niet thuis in een vrije democratische rechtsstaat. Via Pro Bono Connect heeft Privacy First het advocatenkantoor CMS ingeschakeld om deze zaak voor ons te voeren. Door omstandigheden is de lancering van deze rechtszaak helaas vertraagd, maar de voorbereidingen bevinden zich inmiddels in een vergevorderd stadium en de verwachting is dat onze ANPR-zaak spoedig zal plaatsvinden bij de rechtbank Den Haag. In dit verband is door Privacy First inmiddels tevens een grootschalig Wob-verzoek ingediend bij twee verantwoordelijke ministeries.

5.5 Kentekenparkeren & recht op contante/anonieme betaling

Sinds 2014 voert Privacy First o.a. rechtszaken tegen (verplicht) kentekenparkeren. Begin 2015 won Privacy First voorzitter Bas Filippini in dit verband een bestuursrechtelijke zaak tegen de gemeente Amsterdam: sindsdien zijn automobilisten in heel Nederland niet langer verplicht om bij het parkeren hun kenteken in te voeren. Begin 2016 werd dit oordeel bevestigd door de Hoge Raad. Een nieuwe fiscaalrechtelijke zaak van de voorzitter van Privacy First ter algehele afschaffing van kentekenparkeren en ter behoud van het recht op contante (anonieme) betaling werd begin 2019 helaas afgewezen door het Hof Amsterdam. In deze zaak staat een aantal nieuwe principiële rechtsvragen rond kentekenparkeren en het recht op contante betaling centraal. Privacy First verwacht dat de Hoge Raad

medio 2020 uitspraak zal doen in deze zaak. Tevens hoopt Privacy First dat deze zaak zal leiden tot zogeheten prejudiciële vragen over het recht op contante betaling bij het Europees Hof van Justitie in Luxemburg.

Door de uitspraak van het Hof Amsterdam blijven de eerdere (door de Hoge Raad bevestigde) uitspraken dat invoering van het kenteken bij parkeren niet verplicht is overigens onaangetast.

Kentekenparkeren is en blijft daarmee dus vrijwillig: een eventuele parkeerboete bij niet-invoering van een kenteken dient in bezwaar en beroep te worden vernietigd, mits de parkeerder kan aantonen dat voor het parkeren betaald is.



Privacy First voert deze rechtszaken ter behoud en versterking van het recht op anonimiteit in de openbare ruimte. Dit recht staat de laatste jaren in toenemende mate onder druk en dreigt inmiddels illusoir te worden. Indien nodig zal Privacy First deze zaak daarom voortzetten tot aan het Europees Hof voor de Rechten van de Mens in Straatsburg.

Deze zaak wordt tegen sterk gereduceerd tarief gevoerd door Alt Kam Boer Advocaten in Den Haag.

5.6 Trajectcontrole

Een vergelijkbare nieuwe zaak van de voorzitter van Privacy First heeft betrekking op trajectcontroles bij snelwegen: zonder specifieke wettelijke basis en privacy-waarborgen vormt trajectcontrole een massale, continue privacyschending. Begin 2018 wees de rechtbank Haarlem deze strafrechtelijke zaak



echter af, gevolgd door het Hof Leeuwarden in juli 2019. Het Hof Leeuwarden weigerde het systeem van trajectcontrole als zodanig te toetsen aan het recht op privacy. Wel bleek in deze zaak dat alle trajectcontrole-data (van onschuldige automobilisten) minstens 72 uur bewaard blijven en voor andere doelen dan verkeershandhaving kunnen worden gebruikt. Desondanks heeft de Autoriteit Persoonsgegevens tot op heden niet ingegrepen en is Privacy First genoodzaakt om deze zaak voort te zetten bij het Europees Hof voor de Rechten van de Mens in Straatsburg.

Ook deze zaak wordt tegen sterk gereduceerd tarief gevoerd door Alt Kam Boer Advocaten in Den Haag.

5.7 Landelijk Schakelpunt (LSP)

De afgelopen jaren voerde de Vereniging Praktijkhoudende Huisartsen (VP Huisartsen) een grootschalige civiele rechtszaak tegen de private opvolger van het Elektronisch Patiëntendossier: het Landelijk Schakelpunt (LSP). Eind 2017 werd deze zaak helaas afgewezen door de Hoge Raad, met als belangrijk lichtpunt dat in de uitspraak door de Hoge Raad duidelijk wordt aangestuurd op *privacy by design* voor medische systemen. Positief was bovendien dat in het advies (“conclusie”) van de Advocaat-generaal bij de Hoge Raad uitgebreid werd gerefereerd aan de *amicus curiae* brief die Privacy First en het Platform Bescherming Burgerrechten in cassatie hadden ingebracht. Deze brief was ingediend in het kader van onze gezamenlijke langlopende campagne SpecifiekeToestemming.nl ter behoud en bevordering van het recht op medische privacy. De zaak kreeg in cassatie (mede op advies van Privacy First) via het Public Interest Litigation Project (PILP) pro bono ondersteuning door advocatenkantoor Houthoff Buruma. Op initiatief van Privacy First heeft Houthoff vervolgens pro bono namens enkele individuele mede-eisers (huisartsen) de zaak voortgezet bij het Europees Hof voor de Rechten van de Mens. In september 2018 werd deze zaak door het EHRM echter vrijwel onbeargumenteerd niet-ontvankelijk verklaard.



5.8 Individuele rechtszaken Michiel Jonker

Bij hoge uitzondering (gezien onze beperkte personeelscapaciteit) steunt Privacy First rechtszaken van individuele burgers, mits dergelijke zaken van dusdanige aard zijn dat onze steun daarbij onontbeerlijk is, dit in het belang van positieve precedentvorming, maatschappelijke impact, bewustwording en beïnvloeding van wetgeving en beleid. Een goed voorbeeld hiervan zijn de rechtszaken van de Arnhemse privacy-activist Michiel Jonker ter behoud en bevordering van anoniem reizen met het openbaar vervoer, het recht op contante betaling in het openbaar vervoer en in openbare gelegenheden, en ter invoering van een gemeentelijke anonieme afvalpas c.q. *privacy by design*. Sinds enkele jaren voert Jonker over deze kwesties diverse handhavingszaken bij de Autoriteit Persoonsgegevens, de rechtbank Arnhem en de Raad van State. En met succes: onder druk van de zaken van Jonker werd de Autoriteit Persoonsgegevens door de rechter gedwongen om onderzoek te doen naar de “anonieme” OV-chipkaart en werd de persoonsgebonden afvalpas onrechtmatig verklaard. De rechtszaken van Jonker leiden daarnaast vaak

tot inspirerende mediapublicaties en kritische vragen op gemeentelijk en nationaal niveau. Jonker voert deze zaken overigens grotendeels op eigen kracht, zonder advocaat. Nieuwe zaken van Jonker zijn in voorbereiding en zullen opnieuw door Privacy First worden gesteund.

6. Communicatie

6.1 Massamedia

In 2018 is het mediabereik van Privacy First opnieuw gegroeid en inhoudelijk diverser geworden: gemiddeld was er in 2018 elke dag een mediapublicatie waarin Privacy First werd genoemd of geciteerd, vaak in de pers of op internet en soms ook op radio of televisie. Naast verzoeken om interviews wordt Privacy First ook vaak door journalisten benaderd om achtergrondinformatie en onderzoekstips, soms ook door buitenlandse media.



Vincent Böhre (Privacy First) bij EenVandaag, 7 maart 2018. © EenVandaag

6.2 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. Beide sites worden deels gesponsord door de privacyvriendelijke provider Greenhost. Het aantal bezoekers op onze websites is in 2018 opnieuw gegroeid en bedroeg in totaal gemiddeld 60.000 per maand. Ook is Privacy First met name actief op Twitter en heeft een eigen LinkedIn-groep voor privacy-professionals. Zowel onze Twitter- als onze LinkedIn-aanhang groeien al jaren gestaag. Daarnaast is Privacy First actief op Facebook en blijft graag ruimte bieden voor (eventueel anonieme) gastcolumnns en ingezonden artikelen op onze website(s). Wilt u graag op de hoogte blijven van alle ontwikkelingen rondom Privacy First? Meldt u dan aan via info@privacyfirst.nl !

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 2018 uit de volgende personen:

- Bas Filippini (oprichter en voorzitter)
- Vincent Böhre (directeur en jurist)
- Martijn van der Veen (projectleider Privacy First Solutions)
- Robbie van Herwerden (juridisch onderzoeksmedewerkster)
- Simone van Dijk (themaspecialist kinderen & privacy)
- Esther Gruppen (politiek adviseur Privacy First).

Het bestuur van Privacy First is in de zomer van 2018 uitgebreid en bestaat sindsdien uit de volgende personen:

- Bas Filippini (voorzitter)
- Paul Korremans (penningmeester)
- Marc Smits (secretaris)
- Ancilla van de Leest (algemeen bestuurslid).

De Raad van Advies van Privacy First is in de zomer van 2018 opgericht en bestaat sindsdien uit de volgende personen, op persoonlijke titel:

- prof. Hans Franken (emeritus hoogleraar Informatierecht, Universiteit Leiden)
- Quirine Eijkman (ondervoorzitter College voor de Rechten van de Mens & Lector toegang tot het Recht, Hogeschool Utrecht)
- Wilmar Hendriks (privacy professional & executive coach, Control Privacy)
- Eva de Leede (senior-beleidsmedewerker Energie, Ministerie van Economische Zaken en Klimaat)
- Joris Sprakel (advocaat sociaal-economische mensenrechten, Fischer Groep; Lecturer Human Rights Law, Haagse Hogeschool).

De groep vrijwilligers van Privacy First groeide in 2018 opnieuw en bestaat grotendeels uit professionals die Privacy First structureel ondersteunen, zowel inhoudelijk (verschillende privacy-thema's en vertaalwerkzaamheden) als organisatorisch (ICT, fondsenwerving, PR, fotografie) en juridisch (research). Daarnaast beschikt Privacy First over een uitgebreid netwerk van experts uit alle hoeken van de samenleving, variërend van wetenschappers, juristen en ICT'ers tot journalisten, politici en ambtenaren.

Begin 2019 zijn de statuten van Privacy First vrijwel volledig herzien en geactualiseerd. Tevens heeft Privacy First een nieuw reglement voor onze Raad van Advies opgesteld. Dit gebeurde met pro bono ondersteuning door het advocatenkantoor Nauta Dutilh, via Pro Bono Connect.

Privacy First is in augustus 2018 verhuisd naar een nieuwe (relatief voordelige en uitstekend toegeruste) kantoorlocatie op de Keizersgracht in Amsterdam. Dit aangezien ons huurcontract in het Amsterdamse Volkshotel die zomer afliep en het Volkshotel helaas alleen nog huurders uit de creatieve sector wilde huisvesten.

Privacy First is eind 2018 voor haar telefonie overgestapt naar het privacyvriendelijke Voys Telecom (tevens bedrijfssponsor van Privacy First en mede-eiser in onze rechtszaken tegen de Sleepwet).



Vincent Böhre (Privacy First) voor de nieuwe kantoorlocatie van Privacy First.

8. Financiën

Stichting Privacy First is voor haar werkzaamheden grotendeels afhankelijk van individuele donaties en sponsoring door fondsen en advocatenkantoren. Het donateursbestand van Privacy First is de laatste jaren snel gegroeid en in 2018 zijn de inkomsten van Privacy First opnieuw gestegen (30% t.o.v. 2017). Sinds 2015 wordt Privacy First gesteund door Stichting Democratie en Media; sinds 2017 betreft dit meerjarige institutionele steun. Privacy First hoopt diverse andere binnen- en buitenlandse fondsen aan zich te kunnen verbinden ter versterking en

verduurzaming van onze organisatie in Nederland en (op termijn) ter operationalisering van Privacy First in het buitenland.

Naast financiële steun door individuele donateurs en fondsen staat Privacy First ook open voor sponsoring door bedrijven, mits Privacy First volledig vrij en onafhankelijk kan blijven functioneren. Zo wordt Privacy First sinds 2016 materieel gesteund door ICT-bedrijf Detron middels verstrekking van benodigde computers en printers voor onze kantoorlocatie. Zowel onze salarisadministratie als onze financiële administratie worden door een extern administratiekantoor gevoerd; het betreffende kantoor biedt haar diensten aan als bedrijfssponsoring. De websites van Privacy First worden deels gesponsord door provider Greenhost en via TechSoup Nederland kan Privacy First goedkoop software aanschaffen. Kaspersky sponsort sinds 2017 onze antivirussoftware. Sinds eind 2017 wordt Privacy First tevens gesteund door Voys Telecom. Verder is sinds eind 2018 Secura BV als sponsor betrokken bij de Nederlandse Privacy Awards. Zou u graag ook met uw organisatie Privacy First willen sponsoren? Neem dan contact met ons op!

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. Onze communicatie verloopt daartoe (ook telefonisch) grotendeels via internet. Dure borrels of andere luxe zaken zijn voor Privacy First taboe. Onze campagnes en ondersteunende werkzaamheden worden deels uitgevoerd door professionele vrijwilligers. Evenementen van Privacy First worden bij voorkeur georganiseerd op onze eigen kantoorlocatie of op externe gesponsorde locaties. De processtukken in onze rechtszaken worden deels door Privacy First zelf geschreven of ondersteund middels eigen feitelijk en juridisch onderzoek. Vast beleid van Privacy First is bovendien om grootschalige rechtszaken in principe louter in coalitieverband te voeren via het Public Interest Litigation Project (PILP) en Pro Bono Connect van het Nederlands Juristen Comité voor de Mensenrechten (NJCM). Dit om de kosten en financiële risico's te spreiden en de kans op juridische winst te verhogen. Op deze manier komt iedere gedoneerde euro zo effectief mogelijk ten goede aan de privacy van iedere Nederlander.

Hieronder treft u ons financiële jaaroverzicht 2018 aan. Sponsoring van rechtszaken door advocatenkantoren is hierin niet inbegrepen.

Jaaroverzicht	2018	2017
Inkomsten:		
Donaties en subsidies	€ 118.741	€ 91.455
Onderhuur	-	€ 400

Uitgaven:

Personeelskosten	€ 90.021	€ 63.137
Juridische kosten	-	€ 14.006
Campagnekosten	€ 22.696	-
Evenementen	€ 7.874	€ 2.340
Huisvesting	€ 5.675	€ 4.980
Bancaire en verzekeringskosten	€ 2.068	€ 825
Reiskosten	€ 1.813	€ 1.610
Websites	€ 1.182	€ 1.667
Communicatiekosten	€ 601	€ 767
Postbus en frankeringskosten	€ 472	€ 431
Kantoorkosten	€ 440	€ 232
Representatiekosten	€ 440	€ 758
Werkkostenregeling	€ 397	€ 454
Abonnementen	€ 266	€ 253
Overige kosten	€ 294	€ 868

Wilt u Privacy First graag steunen? Maak dan een donatie over naar IBAN: NL95ABNA0495527521 (BIC: ABNANL2A) t.n.v. Stichting Privacy First te Amsterdam, of steun ons anoniem via de [donatiepagina](#) op onze website. 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.