PRIVACY FIRST

Postbus 16799
1001 RG Amsterdam
Tel. 020 - 8100279

Aan:
Tweede Kamer der Staten-Generaal
Vaste commissie voor Veiligheid en Justitie
Per email: cie.vj@tweedekamer.nl

Uw ref.	:	
Onze ref.	:	SPF20171005-2
Datum	:	5 oktober 2017
Betreft	:	Bijlage position paper t.b.v. rondetafelgesprek inzake horizontale privacy

Geachte Kamerleden,

In deze bijlage geeft Privacy First graag een nadere toelichting op haar ingediende position paper over horizontale privacy.

1. Wat is horizontale privacy?
Onder horizontale privacy verstaan wij de relatie tussen burgers onderling waarbij zij binnentreden in elkaars persoonlijke levenssfeer en hierbij informatie registeren of instrumenten gebruiken die dit doen. Onze speciale aandacht hebben privacyschendingen die hieruit voort kunnen komen. Vooral in het digitale tijdperk waarin wij nu leven, liggen bewuste en onbewuste privacyschendingen op de loer.

2. Plaatsen van horizontale privacy
Horizontale privacy kent vele plaatsen. Hieronder hebben wij ze ingedeeld onder: (a) onderweg/openbare ruimte; (b) online en; (c) home/thuismarkt.

2.a Onderweg/openbare ruimte
Dashcam
Op maandag 2 oktober, kwam naar buiten dat een rechter in Duitsland een vrouw een boete heeft gegeven van €150,- voor het filmen met een *dashcam*, omdat zij hiermee de privacy van een andere burger had geschonden.[1] In vier Europese landen is de *dashcam* verboden, dat is in: Duitsland, Portugal, Oostenrijk en Luxemburg. Cameratoezicht behoort in principe toe aan de politie, daarnaast moet het cameratoezicht aan de burger kenbaar worden gemaakt.

Bij het filmen met een *dashcam* is er in zekere mate sprake van heimelijk toezicht. Het is voor een burger onmogelijk om zich daaraan te onttrekken, tenzij hij zich niet meer op de openbare weg begeeft. Daarnaast worden *dashcam*-beelden veelvuldig gepubliceerd, een korte zoekactie op *Youtube* op de woorden: 'Dashcam Nederland'

[1] RTL Nieuws, 2 oktober 2017, 'Duitse vrouw filmt verkeersovertreding maar krijgt zelf boete voor dashcam.

levert al zo'n 14.500 zoekresultaten op. Voor het plaatsen van de beelden, zal vaak geen toestemming zijn gegeven door de betrokkene.

Drones
Drones worden steeds populairder, gezien ze goedkoop (met camera en wifi-verbinding) te verkrijgen zijn. Daarmee zijn drones voor een groeiend publiek beschikbaar geworden. Het gebruik van een drone met camera schendt het recht op privacy. In dit kader is dan ook de *handleiding voor een gebruik van drones dat voldoet aan de waarborgen voor bescherming van de privacy* opgesteld.[2] Het grootste probleem ligt volgens Privacy First in de onherleidbaarheid van drones. Momenteel is het moeilijk om de bestuurder van een drone te achterhalen, de bestuurder kan zich namelijk op een grote afstand van de drone bevinden. Het achterhalen van de bestuurder kan noodzakelijk zijn in het kader van privacyschending, maar ook in het kader van aansprakelijkheid in het geval van een (ernstig) ongeluk met of door een drone. Het idee van Privacy First is het verplichten van een transponder in elke drone met een register van alle (publieke en private) drones in Nederland, vergelijkbaar met de gangbare praktijk in de (burger)luchtvaart.

Fotograferen en filmen in de openbare ruimte
In de openbare ruimte wordt nog veel meer gefilmd en gefotografeerd. Al dan niet met een camera, mobiele telefoon, Google Glass of andere device. Vaak zonder dat de betrokkene hier überhaupt van op de hoogte is. Deze beelden worden vaak verspreid zonder toestemming van de betrokkene, dit kan door middel van het delen van de beelden in besloten kring of door het te publiceren online. In Zweden is reeds besloten dat het niet meer is toegestaan om te fotograferen zonder toestemming van de betrokkene.[3]

Bedacht moeten we zijn op: wie de beelden opneemt, bij wie ligt het eigendom van de beelden. En hoe zit het met de verspreiding, verwijderen en combineren van de beelden en gegevens?

2.b Online
Sociale media
Tegenwoordig staan (video)beelden al direct op het internet, doordat deze gestreamd of geplaatst worden op diensten zoals *Youtube, Instagram, Facebook* of *Snapchat*. Daarnaast kies je vaak niet zelf het publiek, waaraan een bepaald beeld wordt gedeeld, doordat iemand anders het openbaar deelt, terwijl jijzelf je profiel hebt afgeschermd. Tevens is er vaak geen vrije keuze, welk beeld met je volgers/vrienden wordt gedeeld, doordat je wordt *getagd* op social media. Verder worden gegevens en foto's steeds vaker online opgeslagen in een *cloud* en zijn onze apparaten in huis aangesloten online.

[2] Zie Drones en privacy. Handleiding voor een gebruik van drones dat voldoet aan de waarborgen voor bescherming van de privacy d.d. 3 december 2015, *Kamerstukken II*, 2015-2016, 30806, nr. 34.
[3] NU.nl, 30 mei 2013, 'Zweden verbiedt fotografie zonder toestemming'.

2.c Home/Thuismarkt

Beveiligingsmaatregelen

In de thuismarkt zijn veel ontwikkelingen, steeds meer apparaten worden met het internet verbonden. De verantwoordelijkheid voor beveiligingsmaatregelen van deze apparaten ligt momenteel nog grotendeels bij de burger. Indien er geen goede beveiligingsmaatregelen worden getroffen, kan het gehele huishouden gevolgd kan worden door kwaadwillenden. Om het beveiligingsniveau van deze apparaten te vergroten kan er worden gedacht om het minimumbeveiligingsniveau als 'open norm' vast te leggen in wetgeving.

Geïntegreerde systemen

In opmars zijn ze zogenoemde geïntegreerde of embedded systemen, dit zijn elektrische systemen die zijn geïntegreerd in apparaten, die intelligent gedrag vertonen. Deze systemen vinden steeds meer hun plek in woningen. Zo heeft *Amazon* de *Echo* op de markt gebracht en *Google* de *Google Assistant*. Welke je tv, thermostaat, lampen, muziek kan bedienen, zelfs de boodschappen kan bestellen en je informatie kan geven over allerhande zaken. Door de input die je geeft aan het systeem, hoe meer het systeem over je leert.

Controlesystemen

Daarnaast zijn er nog de 'controlesystemen', zoals: camerabewaking, een deurbel met een camera, een app op de mobiel van de kinderen om deze te volgen, een GPS-systeem in de auto et cetera.

Smart-tv

In bijna de helft van de Nederlandse woonkamers is een *smart-tv* te vinden.[4] Fabrikanten van een *smart-tv* kunnen onder meer gegevens verzamelen over het kijkgedrag en de zoekopdrachten van de gebruikers. Sommige kunnen ook het internetverkeer en het klikgedrag in tv-apps registreren. Via *WikiLeaks* onthullingen is naar buitengekomen dat de CIA *smart-tv's* kan afluisteren, zelfs wanneer deze waren uitgeschakeld.[5]

2.d Nieuwe technologie en toekomstige technologie/ontwikkeling

De technologie is continue in ontwikkeling, hierdoor zullen steeds nieuwe apparaten en diensten bijkomen. Verder zullen deze apparaten en diensten vaker met het internet worden aangesloten. Hierdoor zal het *internet of things* alsmaar groeien en de *big data* berg zal toenemen. Als gevolg van de miniaturisering worden toepassingen voor een breder publiek beschikbaar.

Blockchain

De toepassingen van *blockchain* technologie worden steeds verder onderzocht. Aan de blockchain kleven ook meerdere privacy nadelen, zoals dat er grote hoeveelheden, vaak gevoelige, persoonsgegevens tussen partijen worden uitgewisseld. Verder kunnen er alleen gegevens worden toegevoegd en niet worden gewist, wat in strijd is met het recht om vergeten te worden. En als laatste kunnen er onduidelijkheden zijn wie precies de verantwoordelijke en de bewerker van deze gegevens zijn in de zin van

[4] Telecompaper, 10 maart 2017, 'Bijna helft Nederlandse huishoudens heeft smart tv, groei neemt af'.
[5] NOS, 7 maart 2017, 'WikiLeaks: CIA gebruikt smartphone en slimme tv voor afluisteren'.

de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming.

4. Misbruik van informatie/crimineel gedrag

Al voornoemde zijn voorbeelden van bewuste of onbewuste handelingen, of gebruik van diensten, die binnentreden in de persoonlijke levenssfeer. Angstvalliger wordt het wanneer de informatie die, via deze diensten, beschikbaar is geworden, wordt misbruikt voor bijvoorbeeld crimineel of ongewenst gedrag. Hierbij wordt dan ook goed duidelijk waarom privacy ook zo belangrijk is en waarom privacy beschermt dient te worden.

Cyberpesten

Bijna acht procent van de jongeren wordt gepest via het internet.[6] Dit is een toename ten aanzien van voorgaande jaren. Meisjes worden vaker online gepest dan jongens. Een op de acht meisjes wordt online gepest.[7] Onder jongeren is laster de meest voorkomende vorm van cyberpesten, waarbij kwetsende teksten, foto's, filmpjes of roddels worden verspreid op het internet.

Gevolgen van sexting (door minderjarigen)

In toenemende mate sturen jongeren naaktfoto's van zichzelf naar iemand anders. Uit een recente peiling blijkt dat 1 op de 15 jongeren eens een naaktfoto heeft verstuurd.[8] Hierbij zijn zij zich minder bewust van eventuele gevolgen. Steeds vaker horen wij helaas dat deze beelden op internet worden geplaatst of worden gedeeld met schoolgenoten. Vaak met grote (privacy)gevolgen voor het slachtoffer waarbij het vaak niet mogelijk is om het beeld in zijn heelheid van het internet te verwijderen. De strafbaarstelling voor dit feit ligt in de eerste plaats bij het in bezit hebben en het verspreiden van kinderporno. Als een jongere hiervoor wordt veroordeeld, heeft dit mogelijk grote gevolgen in de toekomst, omdat er altijd een aantekening zal blijven op het strafblad, wat gevolgen heeft voor een Verklaring Omtrent Gedrag. Daarnaast wordt als strafbaarstelling voor dit feit de grond belediging aangevoerd. De strafmaat hiervoor ligt rond de 20 uur taakstraf of 100 euro boete.[9]

Afpersing

Helaas is er ook een stijgende lijn te zien in afpersing met naaktfoto's onder volwassenen en onder jongeren.[10] Daarnaast is online afpersing door middel van ransomware steeds vaker in het nieuws.

Identiteitsfraude

Identiteitsfraude komt in verscheidende vormen. Op het internet is het makkelijk om de identiteit van een ander over te nemen, bijvoorbeeld door het maken van een

---

[6] CBS, 17 augustus 2015, 'Bijna 8 procent van de jongeren gepest op het internet'.

[7] CBS, 18 september 2017, 'Een op de acht meisjes wordt online gepest'.

[8] NOS, 6 februari 2017, '1 op de 15 jongeren online uit de kleren'.

[9] Richtlijn en kader voor strafvordering jeugd en adolescenten, inclusief strafmaten Halt (2016R008), Bijlage II Strafmaattabel jeugdzaken

[10] NOS, 25 januari 2017, 'Forse toename van afpersing met naaktfoto's via internet'.

sociale media profiel en privégegevens en foto's van het slachtoffer te kopiëren. Daarnaast horen we steeds vaker dat er via Marktplaats kopieën van een paspoort of

Identiteitskaart wordt gevraagd en vervolgens wordt misbruikt om anderen mee op te lichten.

Profiling
Doormiddel van het verzamelen en combineren van gegevens kan er een profiel van iemand ontstaan en gedefinieerd worden in een specifieke (risico)groep. De meest zichtbare vorm hiervan is het aanbieden van specifieke advertenties aan een persoon, op basis van een profiel.

5. Conclusies
Geconcludeerd kan worden dat de privacy van een ander, regelmatig wordt ingeperkt door burgers onderling. De vormen en plaatsen zijn zeer divers, zowel thuis, onderweg en online. Deze inperkingen gebeuren zowel bewust als onbewust.

6. Oplossingsrichtingen
Wij hebben een aantal open vragen, die wij hierbij willen stellen. Hoe creëer je een vrije omgeving? En hoe krijg je de verantwoordelijkheid terug over je eigen gegevens en data? Moet er niet veel meer worden gedaan om *privacy by design* en *privacy by default* te stimuleren? Hoe kunnen we de handhaving versterken?

Voor nadere informatie of vragen met betrekking tot bovenstaande is Privacy First bereikbaar op telefoonnummer 020-8100279 of per e-mail: info@privacyfirst.nl.

Hoogachtend,

Stichting Privacy First

Drs. L.T.C. (Bas) Filippini
voorzitter