BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Post Bits of Freedom
Prinseneiland 97
1013 LN Amsterdam

Bank NL73 TRIO 0391 1073 80
KvK 34121286

M +31 6 39 64 27 38
E rejo.zenger@bof.nl
W https://www.bof.nl

Minister van Economische Zaken
Minister van Veiligheid en Justitie

Betreft
Standpunt Bits of Freedom na eerste analyse van voorstel ePrivacy Verordening

Amsterdam
18 januari 2017

Geachte ministers Kamp en Van der Steur,

Eerder deze maand publiceerde de Europese Commissie (hierna: Commissie) haar voorstel voor een verordening[1] die de ePrivacy richtlijn[2] moet gaan vervangen. U zult op korte termijn over dit voorstel een standpunt innemen. Bits of Freedom wil u daarvoor graag het volgende onder de aandacht brengen.

Bits of Freedom ziet net als de Commissie het belang van aanvullende regels om het vertrouwen in en de veiligheid van digitale communicatie te waarborgen. De Commissie heeft daartoe een robuust voorstel gedaan, dat op enkele punten aanscherping behoeft. Bits of Freedom hoopt dat het Nederlandse kabinet deze conclusie deelt en zich in Europees verband inzet op instandhouding van het voorstel en de verbetering van enkele onvolkomenheden.

Bits of Freedom ligt haar standpunt, op basis van een eerste analyse van het voorstel, hieronder toe.

Voorgestelde wetgeving noodzakelijk voor vertrouwen van burgers

1. Bits of Freedom onderstreept de noodzaak van de voorgestelde regelgeving. In de eerste plaats is het van groot belang dat internetgebruikers kunnen rekenen op de vertrouwelijkheid van hun communicatie en (integriteit van)

1 Proposal for a regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

2 Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) van 12 juli 2002.

hun apparatuur. Die communicatie verdient bescherming om het recht op de bescherming van de persoonlijke levenssfeer en het recht op vrijheid van meningsuiting te waarborgen. De noodzaak om dit belang te beschermen zal in de nabije toekomst alleen maar groeien omdat steeds meer apparaten permanent met het internet zijn verbonden en doorlopend met systemen op het internet communiceren.

In de tweede plaats acht Bits of Freedom de voorgestelde regelgeving goed voor innovatie en economische groei. Zonder vertrouwen in de bescherming van digitale communicatie zullen internetgebruikers terughoudend zijn in het gebruik van online diensten.

Uitbreiding reikwijdte van regelgeving is zeer welkom

2. De uitbreiding van de reikwijdte naar de zogenaamde *over the top*-diensten is niet meer dan logisch. Vanuit het oogpunt van de gebruiker is er geen functioneel verschil in de verzending van een bericht via SMS en de verzending van een bericht via een dienst als WhatsApp, Telegram of Signal. Gebruikers verwachten dan ook dat regels over vertrouwelijkheid, die van toepassing zijn op "oude" telecommunicatiediensten, ook van toepassing zijn op functioneel gelijksoortige diensten zoals Instant Messaging en Voice over IP.

   Deze uitbreiding moet er overigens niet toe leiden dat opsporings- en inlichtingendiensten bij de uitvoering en implementatie van het voorstel, en de daaraan gerelateerde voorstellen, bij zulke *over the top*-diensten de effectiviteit van zogenaamde end-to-end encryptie ondermijnen.

3. De wenselijkheid van uitbreiding geldt ook voor de communicatie tussen computersystemen onderling, de zogenaamde *machine to machine*-communicatie. Het is aannemelijk dat in de komende jaren het aantal apparaten in en om huis dat voortdurend met andere computers op het internet is verbonden en communiceert, sterk zal toenemen. Ook voor de diensten die via deze apparaten worden geleverd geldt dat het vertrouwen van gebruikers valt of staat met de vertrouwelijkheid van de communicatie en integriteit van deze systemen.

Europese burgers willen dat privacy de standaardinstelling wordt

4. Het is teleurstellend dat de Europese Commissie er niet voor gekozen heeft om een hoog beschermingsniveau als standaard af te dwingen. In het voorstel is geregeld dat de gebruiker in de gelegenheid moet zijn om te bepalen of zogenaamde third parties informatie op zijn of haar apparatuur mag plaatsen of uitlezen.[3] Wat echter ontbreekt is de opdracht om

3 Artikel 10, lid 1

standaardinstellingen te implementeren die gebruikers beschermen tegen het ongevraagd plaatsen of uitlezen van informatie op hun apparatuur. Dit voorkomt onder andere dat het doen en laten van gebruikers niet zomaar door derden in kaart kan worden gebracht.

Overigens was dit in een eerdere (en gelekte) versie van het voorstel wél geregeld. Het lijkt er dus op dat de Europese Commissie *privacy by design* bewust uit het voorstel geschrapt heeft, zonder enige vorm van motivering. Dat steekt des te meer nu uit onderzoek van de Commissie blijkt dat bijna 90 procent van de gebruikers in de EU juist graag zulke standaardinstellingen wenst.[4]

5. In het voorstel is ook bepaald dat de gebruiker bij het in gebruik nemen van de software op de mogelijkheid tot configuratie van relevante instellingen gewezen moet worden.[5] De Commissie heeft echter nagelaten duidelijk te maken aan welke eisen die informatieverplichting moet voldoen. De gebruiker dient in alle vrijheid en goed geïnformeerd een beslissing te kunnen nemen. Daar wordt aan voorbij gegaan als de gebruiker bijvoorbeeld aan de hand van een onleesbare tekst wordt gewezen op de consequenties van elk van de instellingen. Dat geldt ook als de gebruiker door een gekoppelde inperking van functionaliteit gedwongen wordt tot het kiezen van een configuratie die in zijn nadeel werkt.

6. Tenslotte zou het goed zijn als de gebruiker niet alleen gewezen wordt op de mogelijke instellingen bij een installatie, maar ook op andere momenten waarop de gebruiker fundamentele wijzigingen in het systeem aanbrengt. Te denken valt bijvoorbeeld aan het moment dat de gebruiker ervoor kiest de fabrieksinstellingen terug te zetten.

Cookiewalls staan vrije keuze gebruiker in de weg

7. Bits of Freedom juicht het toe dat de Commissie op grote lijnen het beleid van Nederland op het gebied van cookies en soortgelijke technologieën volgt. Zo is de flexibilisering van het toestemmingsvereiste ten aanzien van zogenaamde *first party* analytische cookies een stap die Nederland al eerder heeft gezet. Het is echter teleurstellend dat de lijn die door Nederland is ingezet om zogenaamde cookiewalls voor overheidsdiensten aan banden te leggen niet door de Commissie wordt gevolgd. Het is immers onverteerbaar als gebruikers alleen nog maar van internetdiensten gebruik kunnen maken als zij moeten accepteren dat hun doen en laten door derden wordt bijgehouden.

8. Bits of Freedom maakt daarom enkele kanttekeningen bij het voorstel van

4 Flash Eurobarometer 443, onderzoek uitgevoerd in opdracht van de Europese Commissie, DG Connect, gepubliceerd in december 2016
5 Artikel 10, lid 2

de Commissie:

a. Het is belangrijk dat de gebruiker in staat is om diensten, waarvan het essentieel is dat de gebruiker die dienst kan gebruiken, ook echt kan gebruiken zonder toe te moeten staan dat zijn handelen (door derden) wordt bijgehouden en in kaart gebracht. Een zogenaamde cookiewall zou dus niet toegestaan mogen zijn, zeker niet als het gaat om diensten van de overheid, diensten die met publieke middelen zijn bekostigd of medische diensten.

> Mede op grond van het bepaalde in de Algemene Verordening Gegevensbescherming is het goed mogelijk te beargumenteren dat zulke cookiewalls in het geheel niet zijn toegestaan omdat op deze wijze geen 'vrijelijk' gegeven toestemming wordt gegeven.[6] Het is evenwel, om onduidelijkheid te voorkomen en in rechtszekerheid te voorzien, belangrijk dat dit expliciet wordt gemaakt in het onderhavige voorstel.

b. Het toestaan van het opslaan van informatie op de apparatuur van de gebruiker en het uitlezen van informatie op de apparatuur van de gebruiker ten behoeve van statistische doeleinden[7] acht Bits of Freedom onder voorwaarden acceptabel. Deze voorwaarden zijn in ieder geval dat de verkregen gegevens geen gedetailleerd beeld van individuele gebruikers oplevert en dat de verkregen gegevens voor geen ander doel worden gebruikt dan voor het verkrijgen van inzicht in het functioneren en gebruik van de dienst in algemene zin.

9. Niet goed is in te zien waarom de technische middelen waarmee de gebruiker toestemming kan geven, beperkt worden. Het voorstel regelt nu dat het verlenen van toestemming gedaan kan worden "by using the appropriate technical settings of a software application enabling access to the internet".[8] In de toelichting wordt gesproken over "a browser or other application". Door deze limitering worden mogelijke toekomstige alternatieven uitgesloten, terwijl de voorgestelde beperking geen doel heeft.

Uitzondering voor offline tracking van gebruikers ongewenst

10. Bits of Freedom maakt zich ernstig zorgen om de uitzondering voor het volgen van gebruikers van communicatieapparatuur in de fysieke wereld (hierna: *device tracking*).[9] Dit soort technologie wordt reeds nu al op grote

6 Zie artikel 7, lid 4 en overweging 43 van de Algemene Verordening Gegevensbescherming.
7 Artikel 8, lid 1, onder d
8 Artikel 9, lid 2
9 Het gaat om technologie die gebruikers van apparatuur kan volgen op basis van de signalen die die apparatuur voortdurend uitzend. Zo zal een mobiele telefoon voortdurend zoeken naar haar bekende *access points* voor draadloos internet in de omgeving. De signalen die daarbij worden

schaal toegepast en is niet alleen beperkt tot drukke winkelstraten maar wordt ook ingezet om, bijvoorbeeld, verkeersstromen op doorgaande wegen in kaart te brengen. De verzamelde gegevens geven bovendien niet alleen zicht op het doen en laten van passanten, maar hebben ook betrekking op omwonenden.[10] Bovendien zijn in sommige contexten, bijvoorbeeld in de omgeving van een geloofshuis, kliniek of seksshop, dit soort gegevens uiterst gevoelig. Het voorstel van de Commissie staat *device tracking* toe op voorwaarde dat gebruikers hierover worden gewaarschuwd.[11] In de praktijk zal dit veelal via een bordje gebeuren. Een dergelijke meldingsplicht is problematisch om meerdere redenen.

a. In de eerste plaats draagt de melding aan de gebruiker niet bij aan de wezenlijke bescherming van de rechten en vrijheden van de gebruiker. Het bordje zal alleen zichtbaar zijn voor diegene die daar specifiek op let. Een argeloze gebruiker zal het bordje niet opmerken in de overvloed van borden in een druk gebied. De bordjes waarmee gewaarschuwd wordt dat in een gebied met camera's toezicht wordt gehouden vallen immers ook al niet meer op. Daar komt bij dat bij grootschalige toepassing van dergelijke technologie waarschijnlijk enkel en alleen aan de buitenranden van zo'n gebied melding wordt gemaakt van *device tracking*. Bovendien zijn de camera's zelf nog in enige mate zichtbaar, een antenne is dat niet.

b. In de tweede plaats is het voor de gebruiker niet mogelijk om zich aan deze vorm van *tracking* te onttrekken, anders dan door basale functionaliteit van de eigen apparatuur uit te schakelen. Het is in redelijkheid niet te verwachten dat een gebruiker draadloos internet uitschakelt, zeker niet als de gebruiker ook gebruik wil maken van internettoegang die door winkeliers of horeca wordt aangeboden.[12] Dat geldt ook voor functionaliteit op basis van Bluetooth, zoals draadloze koppeling van een telefoon aan een headset of het gebruik van zogenaamde *beacons* in een winkel.

c. Anders dan de bedrijven die zulke diensten aanbieden vaak doen laten geloven is het bijzonder lastig, zo niet onmogelijk, om zo'n dienst in te richten op een manier waarbij de bescherming van de persoonlijke levenssfeer van de betrokkene wordt gerespecteerd. Zelfs indien de

uitgezonden kunnen met een antenne worden opgevangen. Omdat de signalen toestel-specifiek zijn kunnen gebruikers geïndividualiseerd en gevolgd worden. Dit werkt onder meer met de signalen die voor WiFi worden gebruikt, maar ook met Bluetooth.

10 Zie bijvoorbeeld https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-legt-wifi-tracker-bluetrace-last-onder-dwangsom-op

11 Artikel 8, lid 2 onder b

12 Zie ook overweging 18 waarin gesproken wordt over vrijelijk toestemming geven: "Basic broadband internet access [...] [is] to be considered as essential services for individuals to be able to communicate and participate to the benefits of the digital economy. Consent for processing data [...] will not be valid if the subject has no genuine and free choice, or is unable to refuse or withdraw consent without detriment."

verzamelde gegevens onomkeerbaar wordt versleuteld is betrekkelijk eenvoudig te achterhalen of een bepaalde gebruiker op een bepaald moment op een bepaalde locatie is geweest.[13]

d. Tenslotte is niet goed in te zien waarom deze vorm van gebruik van locatiegegevens een afwijkende behandeling verdient. Elders in het voorstel regelt de Commissie dat aanbieders van communicatiediensten zonder expliciete toestemming van de gebruiker geen gegevens over de locatie van die gebruiker mag verwerken.[14] Het is niet zo dat deze gegevens in geval van *device tracking* ineens minder gevoelig zijn.

Veranderingen in handhaving vereisen versteviging positie AP

11. Bits of Freedom merkt ook op dat de Commissie voorstelt de handhaving van deze regels onder te brengen bij de toezichthouder die verantwoordelijk is voor de handhaving van de Algemene Verordening Gegevensbescherming. Voor Nederland betekent dat dat de handhaving verschuift van de Autoriteit Consument en Markt naar de Autoriteit Persoonsgegevens. Bits of Freedom vindt dit een logische verschuiving, nu de voorgestelde regels complementair zijn aan de Algemene Verordening Gegevensbescherming.

12. Wat Bits of Freedom betreft betekent dit wel dat de positie van de Autoriteit Persoonsgegevens bij het in werking treden van de nieuwe regels moet worden versterkt. Het is immers niet realistisch te verwachten dat de toezichthouder haar werk goed kan blijven doen als het takenpakket zou worden uitgebreid zonder dat ook de capaciteit van de toezichthouder meegroeit.

Transparantie over tapstatistieken en gegevensverstrekkingen

13. In artikel 11 van het voorstel is bepaald dat aanbieders informatie over de vorderingen van opsporings- en inlichtingendiensten van gegevens van gebruikers aan de toezichthouder verstrekt als die daarom vraagt. Bits of Freedom pleit er voor dat aanbieders verplicht worden deze informatie geaggregeerd openbaar te maken. Transparantie van aanbieders over de mate en wijze waarop zij persoonlijke gegevens van gebruikers met overheden delen, draagt bij aan het vertrouwen van gebruikers. Veel aanbieders publiceren reeds nu al zogenaamde transparantierapporten. Sommige aanbieders beperken zich tot de ontvangen verzoeken, anderen

13 https://rejo.zenger.nl/focus/welk-digitaal-spoor-heeft-citytraffic-van-mij/ bevat een uitgebreide uitleg over de werking van zulke systemen en de wijze waarop het doen en laten van een persoon achteraf alsnog kan worden achterhaald.
14 Overweging 17

behandelen ook de juridische kaders waarin zij zulke verzoek beoordelen.[15] Het voorstel van de Commissie biedt de mogelijkheid om eindelijk de transparantie over tapstatistieken en gegevensverstrekkingen door aanbieders op uniforme wijze te regelen. Bits of Freedom roept Nederland op om te pleiten voor een dergelijke transparantiebepaling.

Kortom, Bits of Freedom is te spreken over het voorstel, maar hoopt evenwel dat het voorstel op punten wordt versterkt. Vanzelfsprekend is Bits of Freedom graag bereid dit standpunt nader toe te lichten, mocht daartoe behoefte bestaan.

Met vriendelijke groet,

Rejo Zenger

15 https://www.vodafone.com/content/dam/sustainability/2014/pdf/vodafone_full_report_2014.pdf