

Aan:

Tweede Kamer der Staten-Generaal

Vaste commissie voor Volksgezondheid, Welzijn en Sport

Per email: cie.vws@tweedekamer.nl

Uw ref. :
Onze ref. : SPF20200420
Datum : 20 april 2020
Betreft : Position paper t.b.v. rondetafelbijeenkomst Corona-app 22 april 2020

Geachte Kamerleden,

Dank voor uw uitnodiging om deel te nemen aan de rondetafelbijeenkomst inzake de zogeheten Corona-app. In de optiek van Stichting Privacy First vormt een dergelijke app een bedreiging voor ieders privacy. Hieronder zullen wij dit kort toelichten.

Gebrek aan noodzaak en effectiviteit

Met grote zorg heeft Privacy First kennisgenomen van het voornemen van de Nederlandse overheid om een contact-traceerapp te gaan inzetten ter bestrijding van het Corona-virus. De maatschappelijke noodzaak van een dergelijke app is tot op heden niet aangetoond. Ervaringen vanuit het buitenland laten bovendien zien dat aan het nut en de effectiviteit ervan ernstig kan worden getwijfeld. Mogelijk werken deze apps zelfs contra-productief, aangezien de inzet ervan tot schijnveiligheid leidt. Daarnaast wordt de meest kwetsbare doelgroep (ouderen) met dit middel nauwelijks bereikt. Alleen al om deze redenen zou van de inzet van “Corona apps” moeten worden afgezien.

Surveillance maatschappij

Privacy First ziet het gebruik van dergelijke apps als een gevaarlijke ontwikkeling, aangezien dit kan leiden tot talloze onterechte verdenkingen, stigmatisering, onnodige onrust en paniek. Zelfs “geanonimiseerd” kunnen de gegevens uit dergelijke apps via koppeling alsnog tot individuele personen herleid worden. Bij grootschalig gebruik leidt dit tot een surveillance maatschappij waarin iedereen geobserveerd en geregistreerd wordt en men zich voortdurend gemonitord waant, met een maatschappelijk *chilling effect* tot gevolg.

Risico's op misbruik

Groot risico is dat de verzamelde data voor meerdere doelen zullen worden gebruikt en misbruikt door bedrijven en overheden. Het risico van heimelijke toegang, hacking, datalekken en misbruik is met name groot bij centrale i.p.v. decentrale (persoonlijke) opslag en bij gebrek aan open source software. Tegelijkertijd biedt ook louter persoonlijke opslag geen enkele garantie tegen misbruik, afhankelijk van technische kwetsbaarheden of aanwezige malware en spyware. In handen van criminele

organisaties vormen de verzamelde data bovendien een goudmijn voor criminele activiteiten.

Voor Privacy First wegen deze risico's van "Corona apps" niet op tegen de veronderstelde voordelen. Dus adviseert Privacy First uw Kamer om er bij het kabinet op aan te dringen niet tot de inzet van dergelijke apps over te gaan.

Testen i.p.v. appen

Vanuit de beginselen van proportionaliteit en subsidiariteit in de strijd tegen het Corona-virus bestaat volgens Privacy First een betere en effectievere oplossing, namelijk het grootschalig testen van de bevolking op het virus en op immuniteit. De benodigde testcapaciteit dient daartoe zo spoedig mogelijk beschikbaar te zijn.

Haastige spoed, zelden goed

Mocht ondanks bovenstaande bezwaren alsnog besloten worden tot de inzet van "Corona apps", dan kan dit pas gebeuren na een zorgvuldig maatschappelijk en democratisch proces met voldoende kritische, objectieve en onafhankelijke toetsing. Tot op heden is hier geen sprake van geweest, getuige de ontwikkelingen de afgelopen dagen. Privacy First adviseert uw Kamer in dit verband om het kabinet een pas op de plaats te laten maken en een moratorium op de inzet van "Corona apps" in te stellen.

Privacy by design

Het recht op anonimiteit in de openbare ruimte is een klassiek grondrecht en cruciaal voor het functioneren van onze democratische rechtsstaat. Een democratisch besluit tot opheffing hiervan is onacceptabel. Mocht alsnog besloten worden tot grootschalige inzet van "Corona apps", dan dient dit dus strikt anoniem, tijdelijk en op zuiver vrijwillige basis te gebeuren. Met individuele toestemming vooraf zonder enige vorm van druk, volledig geïnformeerd en voor een legitiem, specifiek doel. *Privacy by design* (het inbouwen van privacybescherming in de techniek) dient daarbij leidend te zijn. Voor Privacy First zijn dit harde juridische voorwaarden die niet onderhandelbaar zijn. Mocht hier niet aan voldaan worden, dan zal Privacy First dit bij de rechter aanvechten.

Voor nadere informatie of vragen met betrekking tot bovenstaande is Privacy First te allen tijde bereikbaar op telefoonnummer 020-8100279 of per email:

info@privacyfirst.nl.

Hoogachtend,

Stichting Privacy First

mr. Vincent A. Böhre, CIPP/E
directeur