To: 5.1.2e [5.1.2e @rivm.nl]
From: 5.1.2e
Sent: Thur 4/9/2020 7:51:06 AM
Subject: Antw: dagstart
Received: Thur 4/9/2020 7:51:07 AM

Ja, maar pas later want ik zit in een deskundigenberaad

Van: 5.1.2e <5.1.2e @rivm.nl>
Datum: 9 april 2020 om 09:41:08 CEST
Aan: 5.1.2e <5.1.2e @rivm.nl>
Onderwerp: FW: dagstart

Hoi 5.1.2e
VWS vraagt of we vast 5.1.2e kunnen polsen als 5.1.2e van de implementatiecommissie, zodat voor het einde van de dag duidelijk is of 5.1.2e wel/niet zou kunnen/willen.
Zou dat lukken?
Groet,
5.1.2e

From: 5.1.2e) <5.1.2e @minvws.nl>
Sent: donderdag 9 april 2020 08:53
To: 5.1.2e) <5.1.2e @minvws.nl>; 5.1.2e <5.1.2e @rivm.nl>
Subject: dagstart

Morgen heren,
Ter info hieronder reacties van experts gisteren. Mogelijk nog interessante aanknopingspunten. Punten voor vandaag van mijn kant:

- Actuele stand aanbiedingen en eerste schifting door deloitte (indicatie voor 1300/ 5.1.2e belt parallel met 5.1.2e
- Samenstelling commissie, beschikbaarheid voorzitter (onafhankelijk alternatief beschikbaar)
- Opdracht, PvE en werkwijze rond T&T
- Update D3TP
- Informatiebeveiliging: aanbod parallel spoor naast commissie
- Svz afstemmingsoverleg BWL

5.1.2e

Uitgebreide reacties van experts

Autoriteit Persoonsgegevens:

- Als het kabinet slimme apps gaat inzetten bij de bestrijding van het coronavirus, wil de Autoriteit Persoonsgegevens daarover oordelen. "Zulke apps kunnen alleen als de privacy geborgd is. Anonimiteit is bij zo'n app het kernwoord", aldus de privacywaakhond. "Wij zijn daarbij zeer scherp, want mensen moeten erop kunnen vertrouwen dat de overheid zorgvuldig met hun gevoelige informatie omgaat." Verder vindt de AP dat anonimiteit bij apps voorop moet staan. "Kan het niet anoniem, dan is er een aparte wet nodig."

- Voorzitter Aleid Wolfsen: "Een app kan alleen als de privacy daarbij van Nederlanders goed is gewaarborgd. Daar moeten we zeker van zijn. Het gaat om zorggegevens en je wordt de hele dag gevolgd. Mensen moeten er absoluut zeker van zijn en op kunnen vertrouwen dat zorgvuldig wordt omgegaan met hun gezondheidsgegevens. En daarom zullen we daar ook strak en alert op toezien. We hebben nog geen ontwerpen voorgelegd gekregen van het ministerie. Het maakt ons extra alert omdat het juist om zorggegevens gaat, om gezondheidsgegevens. Mensen moeten erop kunnen vertrouwen dat informatie niet weglekt naar de overheid, bedrijven of anderen waarvan jij niet wil dat dat gebeurt. (...) Mocht het op een of andere manier verder gaan dan we zouden willen. Dan moet het absoluut tijdelijk zijn zodat het over een paar maanden ook weer uit de lucht wordt gehaald. Als privacy niet kan worden gewaarborgd, en mensen er

niet op kunnen vertrouwen dat de zorggegevens niet weglekken naar de overheid, bedrijven of andere instanties dan kan de app er om die reden niet komen."

Bits of Freedom:

- Bits of Freedom op Twitter: "Minister @hugodejonge en @MinPres benadrukken dat er ook privacyvriendelijke manieren zijn om contactonderzoek te doen via een app. Maar: het is zeker geen vanzelfsprekendheid. Eerste stap? Nodig de juiste mensen uit om mee te denken. Als blijkt dat een veilige, privacyvriendelijke, niet-verplichte contact tracing app de data oplevert die nodig is om #corona te bestrijden, dan heeft Nederland de expertise in huis om die te maken. Of de app er onder menswaardige voorwaarden komt is een politieke beslissing."

Ancilla van de Leest:

- Privacy-expert Ancilla van de Leest "Ik moet eerlijk gezegd even bekomen van de schrik. Zal weldra een inhoudelijke reactie geven. (...) Today the Dutch government proposed the use of severely privacy violating apps. This is happening worldwide. Tomorrow around 8pm Amsterdam time utc +2 I'll be doing a periscope about this for you. Send me your thoughts and questions and I'll see if I can answer them."

IT-deskundige 5.1.2e :

- IT-deskundige 5.1.2e, voorheen eigenaar van cybersecuritybedrijf FOX IT: "Om de privacy van deelnemers te beschermen, krijgt iedereen een unieke code die niet gekoppeld is aan je identiteit. Het systeem houdt ook niet bij waar je bent geweest, alleen maar wie je hebt ontmoet. "Een dergelijk systeem, daar zou ik niet fel op tegen zijn. De snelheid waarmee het wordt ingevoerd, kan wel tot problemen leiden. Zulke apps kunnen in opzet goed zijn, maar tijdens het programmeren kunnen foutjes worden gemaakt. Normaal test je daar maanden op en laat je hackers proberen in te breken, maar daar is nu weinig tijd voor." Meteen nadat het kabinet bekendmaakte een dergelijke app te overwegen, kwamen op internet de eerste privacyprotesten los. Is de overheid niet stiekem uit op onze locatiegegevens? Volgens Prins is dat niet het geval. "De politie en inlichtingendiensten hebben al genoeg bevoegdheden en mogelijkheden om dat te achterhalen, dus daar hebben ze deze app niet voor nodig. Maar als het een bezwaar is, zou je nog een extra garantie kunnen bieden door de gegevens te laten beheren door een speciaal hiervoor op te richten stichting." Prins ziet niet veel bezwaren tegen een dergelijke app. "Zeker niet als het gebaseerd is op vrijwilligheid. Ook al zou 70 of 80 procent de app installeren, dan zou dat de virusbestrijders al enorm kunnen helpen. Ik denk dat de animo er best voor zal zijn. Rutte pakte het in de persconferentie slim aan, door de koppeling te maken dat we wellicht de teugels wat kunnen laten vieren als er meer grip is om het virus te bestrijden."

Privacy-onderzoeker verbonden aan de Radboud Universiteit Nijmegen Jaap-Henk Hoepman:

- De regering wil een app laten ontwikkelen die vertelt je of je in de buurt bent geweest van een andere gebruiker die besmet blijkt te zijn, en sluit niet uit dat die app verplicht wordt. De privacy moet wel gewaarborgd worden, zegt de regering. Vraag is wat dat betekent. In technische termen is het doel van een dergelijke app *contact tracing*, of *proximity tracing*. Achter de schermen is een groot Europees consortium (PEPP-PT) bezig met het ontwikkelen van een dergelijke app. Hoe de PEPP-PT app werkt is niet duidelijk: er is geen duidelijke beschrijving van de architectuur beschikbaar, laat staan dat de broncode beschikbaar is. Het lijkt er op dat bepaalde landen in dit consortium aansturen op een zogenaamd *gecentraliseerd* systeem. In zo'n systeem worden de personen die in de buurt zijn geweest van een andere gebruiker die besmet blijkt te zijn doorgegeven aan de centrale autoriteiten (bijvoorbeeld de GGD). Deze nemen vervolgens contact op met deze potentieel besmette mensen en leggen maatregelen op. Een dergelijk systeem zet de deur wagenwijd open voor volledige surveillance van wie waar op welk moment is. Er wordt past sinds kort nagedacht over privacy vriendelijke varianten van dergelijke gecentraliseerde systemen, maar die maken vooralsnog wel aannames die misbruik niet uitsluiten. Een alternatief is een *gedecentraliseerd* systeem. Hierin is er *geen* centrale autoriteit die inzicht krijgt in de locatiegegevens van gebruikers die de app hebben geïnstalleerd. Daarmee is een dergelijke app, qua privacy, duidelijk in het voordeel. Bij een gedecentraliseerde app krijgen gebruikers *zelf* direct van het systeem een seintje als ze in de buurt zijn geweest van een andere gebruiker die besmet blijkt te zijn. Ze kunnen er voor kiezen om dan contact op te nemen met de GGD. Maar als ze dat niet doen, weet de GGD niet wie deze potentieel besmette personen zijn. Een grote groep Europese wetenschappers (waarvan sommigen, verwarrend genoeg, ook onderdeel zijn van het eerder genoemde PEPP-PT consortium) hebben een ontwerp van zo'n gedistribueerd systeem (DP-3T) afgelopen vrijdag gepubliceerd. En iedereen gevraagd mee te kijken, mee te denken, om zo het systeem nog beter en privacy vriendelijker te maken. Zo is voor iedereen duidelijk hoe zo'n systeem werkt en wat de risico's zijn. Dat is te prefereren boven de heimelijke en gesloten manier waarop het PEPP-PT vooralsnog te werk gaat. Nader onderzoek is zeker nog nodig, maar vooralsnog gaat mijn voorkeur uit naar zo'n gedecentraliseerd systeem. Onder een essentieel voorbehoud: dat duidelijk onderbouwd wordt *waarom* een dergelijk systeem voor contact tracing vanuit epidemiologisch perspectief noodzakelijk is, zeker gezien de grote aantallen false positives (je was helemaal niet dicht genoeg in de buurt om besmet te raken) en false negatives (je bent wel besmet, maar het systeem heeft je niet waargenomen) die zo'n systeem

noodzakelijkerwijs opleveren. Een dergelijk app kan hooguit schatten hoe dicht je bij iemand in de buurt bent geweest, en kan niet rekening houden met zaken als besmetting via enige tijd na elkaar aangeraakt oppervlakken, om maar even twee voorbeelden te noemen. Wat verplichting betreft: dat lijkt me onmogelijk, en onwenselijk. Niet iedereen heeft een smartphone, of een smartphone waarop een dergelijke app geïnstalleerd kan worden. En uiteindelijk is zo'n app een digitale enkelband die, ondanks alle eventuele waarborgen en bezweringen, mensen het gevoel gaat geven dat de overheid over hun schouder meekijkt met iedere beweging die ze maken. In landen als China, waar zo'n app verplicht is, leidt dat er al toe dat mensen maar liever niet meer de metro nemen. Omdat het risico als potentieel besmet aangemerkt te worden te hoog is, en de consequenties daarvan te zwaar.

Hoogleraar artificial intelligence en privacy Rob van den Hoven van Genderen:

- Het is levensgevaarlijk om dit soort data te laten verzamelen door de overheid. Wie garandeert dat de overheid er niet op een andere manier gebruik van gaat maken?" De data zou geanonimiseerd worden, maar volgens Van den Hoven van Genderen is er sprake van 'pseudonimisering'. Met behulp van artificiële intelligentie kan van de geanonimiseerde data alsnog achterhaald worden waar de data vandaan komt. In Europa wordt over een initiatief gesproken om de app verder te ontwikkelen en de data te analyseren om in de toekomst voorbereid te zijn. "Dat betekent dat de gegevens worden opgeslagen." Hij vreest eveneens voor andere 'slechtwillenden'. Om die buiten te houden, zal de overheid "hele sterke beveiligingsbarricades moeten opwerpen".

Oud-hoogleraar publieke gezondheid 5.1.2e :

- Schrijvers stelt voor om het gebruik van de app te starten met vrijwilligers. "Stel ik krijg een coronabesmetting en de huisarts vraagt mij of ik deze app wil installeren." Met toestemming mag de besmette persoon dan gevolgd worden, ook om bijvoorbeeld te controleren of de quarantaine wordt opgevolgd. "Ik verwacht dat een groot deel van Nederlandse het belang voor de volksgezondheid ziet en de privacy even opschort." Daarmee wordt volgens Schrijvers voorkomen dat een klein deel dat tegen is, van schande gaat spreken. "Die hoeven niet." Wanneer er eenmaal een groot draagvlak is, zou de app altijd nog verplicht gesteld kunnen worden. Schrijvers ziet het voordeel van de app, omdat veel onzeker is rondom corona – zoals de 'kudde-immuniteit'.

Productmanager Thijs Niks:

- Ik maak me zorgen over de effectiviteit van de voorgestelde traceringsapp, want het is ongeteste technologie die — samen met het verhogen van de testcapaciteit — voorlopig het enige concrete voorstel is voor onze transitiestrategie. Het OMT/RIVM verwijst specifiek naar "technieken die de privacy van eindgebruikers waarborgen conform de AVG-wetgeving (zie bijvoorbeeld het recente https://pepp-pt.org initiatief)." Maar dat ziet er vooralsnog uit als een project met veel logo's en weinig resultaten. Minister De Jonge, 7 apr: "Engeland heeft een app, Duitsland ook. Dus we kijken goed over de grens" https://youtube.com/watch?v=-j3_mmZcBZU&t=25m08s... Minister Bruins, 13 mrt: "Ik wil leren van landen dichterbij. Daar verwacht ik de beste leerervaringen" https://youtube.com/watch?v=wo2ig7iBwLs&t=5h55m22s... Blijven we Azië negeren? In Singapore gebruiken ze inderdaad nu een app, die net als het Nederlandse voorstel, Bluetooth tracering gebruikt. Maar dat is een gloednieuw project, waar we nog geen resultaten van hebben. Het Singapore project voor Bluetooth tracering klinkt mooi, maar er zitten nogal wat praktische haken en ogen aan. Zo werkt het alleen op iPhones als je verder stopt met het gebruiken van je telefoon... https://tracetogether.zendesk.com/hc/en-sg/articles/360044846854-Does-TraceTogether-need-to-be-in-the-foreground-to-work-Can-I-use-other-apps-... https://youtu.be/6n9ZsHSc4YA In landen waar ze traceringssystemen voorbereid hadden, hebben ze niet voor Bluetooth gekozen. Zowel Taiwan als Zuid-Korea zijn voor lokalisering gegaan op basis van het telefoonnetwerk. "The monitoring system in Taiwan is described as a 'digital fence,' whereby anyone required to undergo home quarantine has their location monitored via cellular signals from their phones" https://qz.com/1825997/taiwan-phone-tracking-system-monitors-55000-under-coronavirus-quarantine/ "Nearly all potential patients can be found [in South Korea] and tested this way. A new patient's movement can be compared against those of earlier patients. That comparison reveals exactly where, when and from whom the new patient was infected." https://theconversation.com/coronavirus-south-koreas-success-in-controlling-disease-is-due-to-its-acceptance-of-surveillance-134068 Naast Bluetooth kan een app natuurlijk ook GPS tracering gebruiken. Daarmee heb je een grotere kans dat je iets van ruwe data hebt, maar dat verhoogt waarschijnlijk wel het aantal foutpositieve meldingen als je het op telefoons met gelimiteerde rekenkracht verwerkt. Hier is een aardig overzicht van de verschillende apps die overwogen worden: https://gdprhub.eu/Projects_using_personal_data_to_combat_SARS-CoV-2 In plaats van een app, zou Nederland natuurlijk ook netwerklokalisering kunnen overwegen. Voordelen: - Werkt nagenoeg altijd voor elke telefoon Kun je aan de achterkant blijven verbeteren - Mensen hoeven niks te installeren. Nadeel: - Mogelijk privacy risico. De transitiestrategie leunt sterk op meer testen en traceren. En de magische app lijkt nu het enige voorstel om de traceercapaciteit te vergroten, maar op basis van Bluetooth en GPS is dat onwaarschijnlijk. Hoe lang totdat we netwerklokalisering gebruiken? Nog eens 5 weken?

Internetexpert, innovatie-expert, technologie-expert 5.1.2e :

- Corona tracking app: één uniek ID is nog steeds een uniek ID. Dan heet ik geen Danny, maar ben ik 1234. Los je qua privacy helemaal niks mee op. Beter is het om regelmatig het ID van telefoons te veranderen, zoals bijvoorbeeld https://pepp-pt.org/content doet. Stel dat je tel 4x per uur een ID genereert, dat zijn er 96 per dag. Symptomen treden op binnen 14 dagen. Neem een zekerheidsmarge van 7 dagen (totaal 21d), dan zit je op 2016 ID's per besmetting die je zou moeten broadcasten. Snap ik [met 10.000 besmettingen per dag en een anonymous ID van 512 bit heb je dan al gauw een gigabyte per dag die je binnen moet hengelen], daar moet je dus iets op verzinnen. Je zou het proces kunnen omdraaien: dat jouw telefoon de random ID's die hij gesignaleerd heeft checkt met een centrale lijst. Dat scheelt veel data. Maar ook dan moet je de privacyimplicaties goed uitdenken. Conclusie: een privacyvriendelijke app bouwen is moeilijker dan het lijkt. Maar, gelukkig, hebben we mensen die daar veel ervaring in hebben en die volgens mij met hele mooie privacyvriendelijke oplossingen gaan komen. Daarom [bang dat partijen die schaalbaarkunnen denken geen rekening houden met privacy en de partijen die privacy vriendelijk denken moeilijk schaalbaar kunnen denken] op zich goed dat @hugodejonge onderzoek laat doen. Ik hoop alleen dat ze iets verder kijken dan het standaardlijstje van ICT-leveranciers en ik hoop heel erg dat technische universiteiten hier hun rol gaan pakken.

Privacy Consultant Mitchell Hendriks:

- Nederland overweegt om apps in te zetten om de verspreiding van corona te beperken. Minister De Jonge gaf daarbij wel aan dat privacy daarbij gewaarborgd moet worden. De vraag is wat dat betekent. Naar mijn idee is het volgende in ieder geval van belang: Op de juiste manier kijken naar mensenrechten. Niet: privacy óf gezondheid/veiligheid, maar wel: privacy én gezondheid/veiligheid. Privacy en effectieve bestrijding sluiten elkaar niet uit. In tijden van crises moeten we waarden en mensenrechten juist versterken, niet afbreken. Het grootste privacyrisico is datakwaliteit: op welke wijze borg je privacy én krijg je bruikbare data? Uitdaging: 'false positives' (iemand was niet dicht genoeg in de buurt om besmet te raken) en 'false negatives' (iemand is wel besmet, maar heeft de app dit niet waargenomen). Voorkomen of beperken van 'function creep'. Kortgezegd houdt dat in: wetten, beleidsinstrumenten, maatregelen en programma's – maar ook apps – hebben dan een geheel andere uitwerking (soms ook op een totaal ander terrein) dan waarvoor ze oorspronkelijk zijn bedoeld.

Appontwikkelaar 5.1.2e :

- Het voorstel wat ik richting DH heb gestuurd gaat over een app die we kunnen ontwikkelingen en die vanuit de app store kan worden geïnstalleerd. Vervolgens genereert de app een uniek ID waar geen persoonlijke informatie in zit of telefooninformatie. ID wordt via bluetooth uitgezonden zodat andere gebruikers dat kunnen oppikken. Mocht iemand dan besmet raken met corona dan kan die de app openen en vrijwillig aangeven dat hij besmet is en dan wordt de unieke ID opgestuurd naar een officiële instantie zoals het ministerie of RIVM. Daarna wordt de ID doorgestuurd naar de apps, en app kijkt intern of ID in de buurt is geweest en als dat zo is dan krijg je keurig een melding dat je in de afgelopen periode met iemand in aanraking ben geweest die besmet is. Het wordt intern opgeslagen niet in een Cloud. Alleen als iemand is besmet, dan geeft de gebruiker zelf toestemming om zijn ID door te zetten naar de andere apps. Nooit te herleiden wie de persoon is die bij de ID hoort. Alleen melding dat je in de buurt bent geweest niet wanneer en waar. App is redelijk snel te bouwen. De app kan in stores gezet worden door ministerie of RIVM (moet officiële instantie zijn). Als we groen licht krijgen, dan zou het eind van de maand af kunnen zijn.

Beveiligings- en privacy-expert 5.1.2e :

- Ok dan.... Laat je testen op Corona en krijg twee apps om al je contacten inde gaten te houden. Pijnlijk dat net de Wet op de inlichtingen en veiligheidsdiensten is opgerekt. Dit is een potentiële goudmijn. Dus afweging is testen en geen persoonlijke levenssfeer of niet testen...OMG Hugo de Jonge kijkt naar Bluetooth voor de apps. De apps zijn er al en dan gaan ze nadenken over privacy... geen privacy by design likt het. Wat een een privacy en security nachtmerrie. Je mag hopen dat Hugo de Jonge gewoon niet deskundig blijkt. De apps lijken echt zeer riskant. Ze mogen echt wel bewijs aanleveren. Oei. Als het kabinet de app verplicht gaat stellen dan ga je echt een grens over. Dan komt de vraag op: moet je je nog laten testen. Daarnaast is het heel makkelijk zo'n app te frustreren. Dat moet je zo niet willen. Regel het goed (dat kan) en overtuig:https://www.computable.nl/artikel/nieuws/zorg/6910520/250449/kabinet-wil-desnoods-verplichte-app-bij-coronatesten.ht

Directeur Waag 5.1.2e

- Hier 10 vereisten voor contact tracing. @hugodejonge @MinPres @bitsoffreedom @FD_Nieuws @Nieuwsuur https://twitter.com/francesca_bria/status/1247193696665288706

Techniek Filosofe Martijntje Smits:

- Smits onderschrijft de zorgen betreffende de privacy die veelal ongemerkt is weggegeven. Daarbij wordt voorbijgegaan aan dat de apps ingezet zouden worden om rechten op vrije beweging weer te vergroten. "Wat je ziet is een dilemma tussen verschillende rechten." Ze pleit daarom voor strikte voorwaarden indien

de app daadwerkelijk ingezet zou worden. Bijvoorbeeld een duur over hoe lang de regelgeving wordt opgeschort, hoe lang privacy wordt weggegeven, een adviesraad die op het gebruik toeziet en het openstellen van de data. De haast die eventueel geboden is bij de inzet van de app om corona te bestrijden, is volgens haar geen geldig argument. "Het mag niet zijn dat een tijdsargument wordt gebruikt om belangrijke rechten op te schorten."

Data scientist bij het Den Haag Centrum voor Strategische Studies Paul Verhagen

- Er zijn wel degelijk manieren om de data binnen de regels van de AVG te behandelen. Er zijn wel degelijk manieren om de data binnen de regels van de AVG te behandelen. 'Dit is iets waar andere landen al een tijd lang naar hebben zitten kijken. Het werd eigenlijk hoog tijd dat we deze kant op gingen en een gesprek hebben over hoe we die apps gaan gebruiken. De data worden alleen lokaal opgeslagen, dus er zijn zeker manieren om het te doen binnen de richtlijnen.'

Partner BDO Menno Verweij

- Vanuit privacy-oogpunt is het is goed ons te realiseren dat het om twee apps gaat: een track & tracing-app en een app die de GGD-taken gaat ondersteunen. De eerste app richt zich dus op locatiegegevens, de tweede op medische gegevens. Ik kan me niet aan de indruk onttrekken dat de voorzitter van de privacy-waakhond, Aleid Wolfsen, dit niet helemaal scherp heeft.' De deuren voor een track en tracing-app worden op EU-niveau door relevante spelers al open gezet, zegt Weij. 'De privacy-toezichthouder op EU-instellingen, de European Data Protection Supervisor, heeft al gepleit voor een pan-Europees model 'COVID-19 mobiele applicatie', gecoördineerd op EU-niveau. En ook de European Data Protection Board is bezig met guidance op dit punt, maar heeft al verklaard dat privacy en gezondheid hand in hand gaan.'

RTL tech-journalist 5.1.2e :

- De Nederlandse overheid bouwt een app waarmee de verspreiding van corona kan worden getracked. De details zijn nog onduidelijk. In Singapore boekt zo'n app veel succes en werkt hij relatief privacyvriendelijk door gebruik van anonieme ID's. Zo werkt het: https://www.youtube.com/watch?v=buj8ZTRtJes&feature=youtu.be Ik krijg veel vragen: > Hoe werkt de app? > Is het geen inbreuk op de privacy? > Mag dit onder de AVG? > Wordt 'ie verplicht? > En wat vind ik ervan? Geen idee, heb hem nog niet getest. Maar reken maar dat zowel experts als ik hier heel grondig naar kijken. To be continued.

NOS tech-journalist 5.1.2e :

- Hoe ernstig is de privacy-inbreuk van een app die meet of je in de buurt van coronapatiënten bent geweest? Dat hangt sterk af van de onderliggende techniek. Het klinkt als een forse privacy-inbreuk: de overheid die precies weet met wie je in contact bent geweest. Als dat zo was. Maar het kan ook op een relatief privacy-vriendelijke manier. Je kúnt ervoor kiezen om alle locatiedata van alle burgers linea recta naar de overheid over te hevelen en daar centraal uit te vogelen wie bij wie was. Dat doet bijvoorbeeld Israël, waar je een sms'je krijgt van de geheime dienst dat een van je contacten corona heeft.Maar het kan ook anders, via bluetooth. Yup, dat brakke protocol waar je op loopt te schelden als je AirPods verbinding maken met het verkeerde apparaat. Is een shit-protocol, maar om onbegrijpelijke redenen heeft vrijwel elke telefoon het. En dat heeft nu een voordeel. Je kunt daardoor een lijst bijhouden van alle telefoons waarbij je in de buurt bent geweest, op basis van een uniek nummer per bluetooth-verbinding. Die lijst kun je lokaal bijhouden, zonder dat bijvoorbeeld de overheid of de GGD hoeft te weten bij wie je in de buurt was. Als dan achteraf blijkt dat een van de mensen met wie je in contact bent geweest het virus bij zich draagt, worden die unieke nummers met elkaar vergeleken. Dat kan zonder dat iemand weet wie bij wie in de buurt was. Sterker nog: dat kan zonder dat jíj dat weet. Die vergelijking kun je namelijk lokaal op je apparaat maken. De smartphone-app laadt een lijst met unieke nummers van bluetooth-ontmoetingen tussen mensen die mogelijk een coronarisico waren. Jouw apparaat vergelijkt die 'vieze' lijst met de lijst op je apparaat. Als er ergens een match is, weet je dus dat je in contact bent geweest met een coronapatiënt, en kun je bijvoorbeeld het advies krijgen om zelf in thuisisolatie te gaan. Dat alles zonder dat ergens centraal je locatie of ontmoeting is geregistreerd. Die unieke nummers kun je ook weer afschermen voor verdere anonimiteit, bijvoorbeeld via hashing. (Hashing is de bom, hier meer daarover: https://dekennisvannu.nl/site/artikel/Wat-is-een-hash/6380...) Wil dat zeggen dat de app per se veilig is? Of dat dit de manier is waarop de overheid het gaat doen? Nee, dat moet allemaal nog blijken. Bluetooth gaat wel een rol spelen, maar hoe het precies zit, weten we nog niet. Of het een goed idee is? Of de privacy-inbreuk gerechtvaardigd is? Dat is niet aan mij om te zeggen. Dit draadje was vooral om uit te leggen hoe je een 'contact tracing'-app kunt bouwen zonder dat je als overheid per se hoeft te weten wie met wie contact heeft. Nog een verduidelijking. Er is dus wel één moment dat er iets centraal moet worden geregistreerd: als je het virus blijkt te hebben. Op dat moment zou in jouw app moeten worden geregistreerd dat je het virus hebt, om zo jouw bluetooth-ontmoetingen als risico aan te merken. Wel een belangrijke vraag: hoe gaat de app werken? Werkt ie makkelijk en simpel? Qua functionaliteit lijkt het Nederlandse idee op TraceTogether, de app die in Singapore is uitgerold. Maar die app heeft wel een belangrijk nadeel voor iPhone-gebruikers: je moet de app bewust in de voorgrond laten draaien. Niet echt gebruikersvriendelijk. (Op Android hoeft dat niet)

• Of het een goed idee is? Of de privacy-inbreuk gerechtvaardigd is? Dat is niet aan mij om te zeggen. Dit draadje was vooral om uit te leggen hoe je een 'contact tracing'-app kunt bouwen zonder dat je als overheid per se hoeft te weten wie met wie contact heeft.

5.1.2e |
Ministerie van Volksgezondheid, Welzijn en Sport | 5.1.2e Flex|Pro |
Parnassusplein 5 | 2511 VX | Den Haag |
Postbus 20350 | 2500 EJ | Den Haag |
Tel.: 5.1.2e E-mail: 5.1.2e @minvws.nl |