Track-and-Trace is voor pakketten, niet voor personen

Door Rens Philipsen en Annabel Broer van de Jonge Democraten

In tijden van crisis moeten we waken voor onze principes, want juist dan komen deze snel in gevaar. Zo ook in deze corona-crisis, waar het kabinetsvoorstel om via apps besmettingen te volgen de deur wagenwijd openzet voor het volgen van personen. Met toegang tot medische gegevens als kers op de taart. In deze crisis moeten we alle technologische middelen aanwenden om het virus te lijf te gaan. Maar een GGD-app die automatisch gegevens verzamelt over locatie en sociale contacten is buitenproportioneel, ook in crisistijd.

Voor het automatisch functioneren van een corona-app zouden onze telefoons continu met elkaar moeten communiceren. Onze telefoons zenden dan uit hoe lang we bij elkaar in de buurt zijn en op welke afstand we ons van elkaar bevinden. Niet alleen naar andere telefoons met de app, maar naar elk luisterend apparaat. Dit betekent dat het voor derden kinderspel wordt om bij te houden op welk moment een telefoon passeert. Het medicijn krijgt zo een vervelende bijwerking: het biedt de mogelijkheid om nauwkeuriger dan ooit bij te houden wie zich wanneer waar bevindt. Een goudmijn voor iedereen die om welke reden dan ook alles over ons te weten wil komen.

Als deze gegevens niet aan personen kunnen worden gekoppeld, dan valt het nog enigszins mee. Helaas is dit niet zo: locatiegegevens zijn niet anoniem. Ze bieden een volledig beeld van ons leven. Immers, er is maar één telefoon die zich ‘s ochtends thuis, en ‘s middags op uw werkplek bevindt. De New York Times liet eind vorig jaar zien hoe, uit de locatiegegevens van twaalf miljoen telefoons, individuen persoonlijk konden worden geïdentificeerd, van senator tot automonteur. De combinatie van tot de persoon herleidbaar locatiegegevens met een handig GGD-bericht als iemand ziek wordt, maakt een inbreuk op onze levenssfeer die geen precedent kent.

De lat voor een digitaal hulpsysteem moet daarom hoog liggen. Een app die mensen ondersteunt bij het bijhouden van hun sociale contacten kan zeker het werk van de GGD makkelijker maken. Maar dit kan ook minder ingrijpend. Gerichte registratie, in plaats van blind communiceren. Met QR codes en NFC, net als bij contactloos betalen. Met volledige controle voor de gebruiker over wat zij wanneer met wie communiceert en deelt. Laten we ook hierin vertrouwen op de medewerking van alle burgers die zich zo goed aan hun isolement hebben gehouden, die zich bekommeren om hun naasten, en die maar al te graag weer naar buiten willen treden.

Het is een gemakkelijke gedachte om tijdens een crisis als deze onze kritische houding richting privacyschending los te laten. Bijzondere tijden vergen immers bijzondere maatregelen. Maar laten we niet te gemakkelijk onze privacy inleveren. De keuzes die we in deze tijden maken leggen de basis voor elke discussie over digitalisering, ethiek, en privacy, en elke keuze die we de komende jaren maken. We moeten kiezen voor burgerrechten en verworven vrijheden. Juist in tijden van crisis.

Ten tweede, gegevens mogen niet centraal worden verzameld, door welke partij dan ook. En ten derde, de burger dient ook beschermd te worden tegen derde partijen die maar al te graag meeluisteren. Dat betekent dat informatie in de openbare ruimte rondsturen geen optie kan zijn. *Privacy by design and default*, in plaats van hopen dat het wel mee zal vallen. De keuzes die we in deze tijden maken leggen immers de basis voor elke discussie over digitalisering, ethiek, en privacy, en elke keuze die we de komende jaren maken.

In Nederland, maar ook breder in Europa, worstelen we al langere tijd met dilemma’s over digitalisering. Juist daar moeten onze Europese waarden van vrijheid en respect voor het individu de boventoon voeren. Een nee tegen een wereldwijd Amerikaans sleepnet. Een nee

tegen totalitaire Chinese controle. Een ja voor burgerrechten en verworven vrijheden. Ook, of eerder juist, in crisistijd.

Uitwerking eisen app, mede obv https://www.veiligtegencorona.nl/ (uitstekend stuk), en deels geinspireerd door breach notification sites als www.haveibeenpwned.com .

1. Data blijft lokaal
2. Data wordt vrijwillig uitgewisseld
3. Data wordt alleen uitgewisseld met noodzakelijke partijen
4. Data wordt zsm verwijderd

Het doel van de app is het vergemakkelijken van het antecedentenonderzoek door de GGD. Minimale eis voor functionaliteit is dat een persoon op de hoogte gesteld kan worden als er contact is geweest met een patiënt in de besmettelijke fase. Bluetooth-gebaseerde communicatie vereist broadcasting naar nabije omgeving (enkele tientallen meters). Hierbij is een telefoon zichtbaar voor elk apparaat. Hiermee is een persoon identificeerbaar op deze tijd en deze locatie. Hierdoor wordt niet voldaan aan eis 3.

Voorstel:

- App bevat een identifier, welke getoond kan worden in QR code, of gecommuniceerd via NFC (bereik < 1 meter ipv 60 meter)
- Sociale contacten kunnen worden bijgehouden door elkaars QR code te scannen, of token uit te wisselen via NFC. Dit is in essentie je telefoon als geheugensteun gebruiken wie je wanneer ontmoette. Te doen voor kleine settings. Voor uitwisseling is hierdoor elke keer expliciete actie (en dus toestemming) nodig van de eigenaar van de telefoon.
    a. Bij een besmetting communiceert de GGD niet wie besmet is, maar wie zich zou moeten laten testen.
    b. Lokale apps controleren of zij op de lijst met te testen identifiers staan
        i. Dit kan anoniem, op eenzelfde manier als hoe je kan controleren of een wachtwoord of mailadres voorkomt in een gelekte/gehackte dataset (zie bv https://arstechnica.com/information-technology/2018/02/new-tool-safely-checks-your-passwords-against-a-half-billion-pwned-passwords/)
        ii. Open vraag: hoe te garanderen dat alleen de eigen identifier opgezocht kan worden? Blijf je voldoende anoniem richting de server als je verzoeken ondertekent, bv via publiek-private versleuteling?
- Groepsbijeenkomsten kunnen worden bijgehouden door een snapshot (dus niet doorlopend) van tijd en locatie op te slaan.

. Bij een besmetting communiceert de GGD welke tijd/plaats gevaarlijk was.

a. Dit identificeert enkele tijd/locatie punten van een besmet persoon. Bij een klein aantal besmettingen zijn die mogelijk tot een persoon te herleiden. De vraag is of dit proportioneel is.

b. Lokale apps controleren of hun lijst met tijd/locatie overeenkomsten kent met de gepubliceerde lijst, op de methode zoals hierboven beschreven.