Gepseudonimiseerde data zijn te kraken, ook die van de CoronaMelder

Op de website www.security.nl verscheen op 2 november 2020 een interessant redactioneel artikel. Daarin maakt men duidelijk dat privacy-ontwerper en technologiecriticus Tijmen Schep een manier bedacht heeft waarmee elke geïnteresseerde met behulp van een programma kan achterhalen of gebruikers van de CoronaMelder-app in zijn of haar omgeving besmet is. Dat gebeurt met behulp van een door Schep geschreven programma op de website www.coronadectective.eu. Dat programma, CoronaDetective, vraagt dan toegang tot bluetooth en scant de directe omgeving op smartphones van mensen die de CoronaMelder geïnstalleerd hebben. Je hoeft niet eens zelf de CoronaMelder geïnstalleerd te hebben. Door die app worden codes(pseudoniemen) uitgezonden die geregistreerd worden door de CoronaDetective. Je kunt ermee zien of een persoon ver weg was of dichtbij, of hij net vertrokken is. Ook of een smartphone naar je toe komt of zich verwijdert. Je kunt zo identiteiten van mensen koppelen aan die pseudoniemen.

Corona

Zodra iemand in de CoronaMelder invoert dat hij/zij ziek is(positief getest) zal deze app de contactcodes gaan uitzenden naar de personen, onder pseudoniem, waarmee contact geweest is. Omdat zoals ik in de eerste alinea duidelijk maakte pseudoniemen aan personen te koppelen zijn is op dat moment voor de degene die CoronaDetective gebruikt duidelijk wie besmet is. Als er meer personen in de omgeving van dat indexgeval besmet worden en de gebruiker van de CoronaDetective deel uitmaakt van die omgeving kunnen andere

besmette personen ook gelokaliseerd worden.

Twee delen

Tijmen Schep maakt in een YouTube-filmpje duidelijk hoe dat allemaal kan. De CoronaMelder maar ook andere buitenlandse corona-apps die werken met het Google/Apple-protocol bestaat uit twee delen. Het deel dat door de overheid gebouwd is en het Google/Apple-deel. Omdat dat deel personen binnen bluetoothbereik een pseudoniem geeft, zit daar het zwakke punt. Niet in het overheidsdeel.

2014

Al vanaf april 2014 is door de uitspraak van de artikel 29 werkgroep van Europese privacy-toezichthouders duidelijk dat gepseudonimiseerde persoonsgegevens toch als (bijzondere) persoonsgegevens beschouwd te worden. Door intelligente koppelingen van databases, maar ook door een programma als CoronaDetective zijn pseudoniemen te kraken. Pseudonimiseren van data is dus geen veilige manier om persoonsgegevens te gebruiken.

Breed scala

Nog steeds denken overheden en andere instanties dat het gebruik van gepseudonimiseerde data een veilige manier is om met persoonsgegevens om te gaan. Even zoeken op deze website met de zoektermen “pseudonimiseren”, “pseudonimisering” en “pseudoniem” levert vele matches op. Pseudonimisering gebruikte de Stichting Benchmark GGZ met ROM-data. Het DBC-InformatieSysteem(DIS) gebruikt dit soort data. Het CBS werkt men op een dergelijke manier versleutelde data. Dit zijn nog maar een paar voorbeelden.

Naïef

Het is naïef om te veronderstellen dat niemand een poging zou

wagen om het achterhalen van persoonsgegevens op betrekkelijk simpele wijze aan te tonen. Het blijkt allemaal kinderlijk eenvoudig te zijn. Helaas is de CoronaMelder weer een vorm van cyberoptimisme. Men stelt vertrouwen in digitale oplossing die zelf niet meet of iemand corona heeft maar slechts een afgeleide ervan op een kraakbare wijze communiceert.

W.J. Jongejan, 2 oktober 2020

Afbeelding van congerdesign via Pixabay