Door dr. Wouter Teepe, verbonden aan de Security of Systems groep van de Radboud Universiteit Nijmegen, naar aanleiding van zijn onlangs verschenen proefschrift "Reconciling Information Exchange and Confidentiality" te vinden op http://www.teepe.com/phdthesis/ en op www.nanomagazine.nl

De privacy van de patiënt: hoe combineer je gegevensuitwisseling met geheimhouding?

Van gevoelige gegevens wil je niet dat ze in de verkeerde handen terechtkomen. Opsporingsgegevens van politie en medische dossiers horen niet op straat te liggen. Tegelijkertijd is het nodig dat deze gegevens wél op de juiste momenten beschikbaar komen, daar waar dat nodig is. Wanneer je van tevoren kunt voorspellen wie welke gegevens nodig zal hebben, is dat relatief makkelijk te organiseren. Maar hoe zit dat met gegevens waar je van tevoren niet van weet wie ze nodig zal hebben?

Soms kan je van tevoren wel zeker weten wie gegevens ***niet*** nodig zal hebben. Wie niet bij de politie werkt hoeft geen opsporingsgegevens te zien en wie geen medisch beroep heeft geen medische dossiers. Met een beetje moeite kun je de groepen nog wat verder afbakenen, maar dan blijven er nog steeds heel veel mensen over die wél toegang hebben tot gevoelige gegevens. Bij de politie zijn er enkele duizenden beëdigde opsporingsambtenaren en in de medische sector is het aantal mensen dat op regelmatige basis zulke gevoelige gegevens kan inzien en verwerken nog veel groter.

Daarmee wordt het tijd voor een retorische vraag: hoeveel van die politiemensen zijn er corrupt? Nul, of meer? Zouden corrupte politieambtenaren opsporingsgegevens lekken naar criminelen? Zouden medici van laag allooi medische dossiers doorverkopen aan screening-bureaus, van verzekeringsmaatschappijen bijvoorbeeld? Puur op basis van de aantallen mensen waar het om gaat die toegang hebben tot deze gegevens, kan je er vergif op innemen dat zoiets gebeurt. Kortom, het hebben van de juiste rol en functie, zoals een baan waarbij een lange opleiding en ook nog een beroepseed hoort, is onvoldoende garantie voor een integere behandeling van gegevens. De infrastructuur waarmee de gevoelige gegevens opgeslagen en uitgewisseld worden, moet er dus voor zorgen dat de kans op oneigenlijk gebruik van die gegevens zo klein mogelijk wordt gemaakt.

De logische vraag is dan: hoe ziet die infrastructuur er in de praktijk uit? Zowel bij de politie, als in de medische wereld wemelt het van de "full-access" systemen. Als je eenmaal toegang tot het systeem hebt, kun je er in grasduinen dat het een lieve lust is. Regelmatig zijn dit zelfs systemen waarin verschillende gezondheidszorginstellingen binnen een gemeente al hun gegevens op één grote hoop gooien. Ik heb eens een lange middag gediscussieerd met een ontwerper van zo'n systeem, en het bleek hem niet aan zijn verstand te peuteren dat enkel de beroepseed van de gebruiker toch een wat zwakke garantie levert, als je meetelt dat je duizenden gebruikers hebt.

Gelukkig zijn er ook systemen die wat minder slecht zijn opgezet. Zowel binnen de politie, als binnen de medische wereld zijn de "verwijsindexen" in opkomst. Een verwijsindex is een soort telefoonboek, waar achter elke naam een contactgegeven staat van mensen of organisaties die meer informatie over de desbetreffende persoon hebben. Wanneer ik nu bij mijn lokale academische ziekenhuis bij de balie mijn pasje aangeef, ziet de telefoniste niet welke ziektes ik allemaal onder de leden heb. Wat ze nog wel kan zien is bij welke afdelingen van het ziekenhuis in de afgelopen jaren ben geweest, en wanneer precies. Maar je hoeft maar een klein beetje ingevoerd te zijn om aan de hand van een dergelijk lijstje een ruwe schatting te kunnen maken van iemands gezondheid. Bij de politie is het al niet veel anders: als ik bij iemands naam de contactgegevens van verschillende narcoticabrigades vind, dan kan ik ook een ruwe schatting maken van de aard van iemands bijverdiensten.

Het lijkt erop dat het geheim houden van gegevens, en het uitwisselen ervan, niet goed samen kan gaan. Dat je, de argumenten afwegende, een (politiek) compromis moet sluiten over hoeveel gegevens je precies uitwisselt en

hoeveel niet. Immers, óf je wisselt gegevens uit, óf je doet dat niet. Als je uitgaat van dit principe, dan lijkt de verwijsindex het best haalbare.

Maar het principe klopt niet. Het uitwisselen van gegevens kan heel goed samen gaan met het geheim houden van gegevens. Het is misschien moeilijk voorstelbaar, maar de gangbare 'leken-intuïtie' over gegevensverwerking klopt niet.

In mijn recent voltooide proefschrift "Reconciling Information Exchange and Confidentiality" heb ik een serie cryptografische protocollen ontwikkeld waarmee het mogelijk is om de overlap tussen twee lijsten te bepalen, zonder de lijsten zelf prijs te geven. Om een aansprekend voorbeeld te geven: de EU kan een lijst vliegtuigpassagiergegevens aan de VS geven, en met behulp van het protocol de privacy van de niet gezochte passagiers garanderen.

Een ander resultaat uit mijn proefschrift is dat het goed mogelijk is om "bestanden te koppelen" zonder dat daarbij wederzijds toegang tot gegevens hoeft te worden gegeven. Sterker nog: het koppelen van bestanden kan, mits op de juiste manier gedaan, de privacy van de mensen over wie de gegevens gaan juist verhogen.

Dit schreeuwt om toepassing in de praktijk, maar daar is méér voor nodig dan alleen maar een toepasbare methodiek. Het is nodig dat beleidsmakers ervan doordrongen raken dat privacy en gegevensuitwisseling op zich geen tegenstrijdige belangen zijn en dat we niet "aan de grenzen van wat mogelijk is" zitten.

Niet alleen de beleidsmakers kunnen een heroriëntatie gebruiken, ook de architecten van de IT-infrastructuur zelf. De "nieuwste" systemen bevatten vaak technologiën die conceptueel gezien al in de late jaren 70 beschikbaar waren. Wat snellere computers, nieuwe software, en internet in plaats van supertrage modems maken het allemaal wel gelikter, maar dat betekent niet dat de nieuwste inzichten op het gebied van gegevensbeveiliging ook worden toegepast in de infrastructuur die nu gebruikt wordt. Zelf ben ik in de late jaren 70 geboren. Moet het nu een hele menselijke generatie duren voordat de nieuwste inzichten in privacybescherming ook worden toegepast? Ik hoop van niet. Als we nu 30 jaar doorgaan met het klakkeloos digitaliseren en uitwisselen van gegevens, dan worden we op een goede morgen wakker met de vraag of we het nou allemaal zo gewild hadden. Of we het, als we ons eerder hadden gerealiseerd dat het anders had gekund, ook anders zouden hebben willen doen. Ik vermoed dat het antwoord op de laatste vraag zeker "ja" zal zijn.

De kritische lezer zal misschien geneigd zijn te denken: "Ach, weer een academicus die denkt dat zijn werk de wereld verandert." Zulk een scepsis is nogal eens terecht. Ook ik heb geen slangenolie in de verkoop, die alle problemen omtrent privacy oplost. Wat ik wel kan leveren is een (existentieel) bewijs dat het beter kan. In een wereld waar de communis opinio is dat het zeker niet kan, lijkt mij dit een waardevol gegeven.

Of mijn eigen technologie nou de doorslag blijkt te geven of die van anderen, doet niet ter zake. Wat wel ter zake doet, is dat de baat hebbende domeinen (politie, gezondheidszorg) open zouden moeten staan voor nieuwe ideeën en nieuwe oplossingen.

Laat de wetenschappers die zich met informatiebeveiliging bezighouden maar binnen! Vertel ze over uw problemen, op die manier stimuleert u hun onderzoek. Zo maakt u het mogelijk dat er oplossingen gevonden worden voor úw domeinspecifieke problemen. Als u dat niet doet, dan zou het zomaar eens 30 jaar kunnen duren voordat ze in de praktijk worden opgelost. Dat is doodzonde, want het kan veel sneller. De medische wetenschap is een goed voorbeeld van hoe technieken en behandelmethoden uit de academische wereld zo snel mogelijk toegepast worden, zij het uiteraard met de nodige voorzorgsmaatregelen en waarborgen.

We hebben nu en later te maken met een nieuw ingeschreven patiënt: de privacy van uw klant. Wanneer gaan we diagnose plegen? Wanneer gaan we hem behandelen?