# Digitale politieagent moet onze privacy beschermen

**Met grote regelmaat verschijnen berichten in de pers over het onderwerp privacy. Uit deze berichten blijkt vaak hoe genuanceerd de belangen van een gebruiker en een dienstenleverancier verstrengeld kunnen raken. Dit artikel gaat nader in op de nieuwste ontwikkelingen betreffende privacy verhogende technieken.**

*Ir. J.J.H. Meijers* *

Privacy is moeilijk te definiëren. Toch is het belang ervan op indirecte wijze wel duidelijk te maken. Zeker is in ieder geval dat privacy slechts betrekking kan hebben op gegevens van bestaande personen. Maar daarmee is nog niet alles gezegd.
De meeste mensen zullen in eerste instantie niet veel bezwaar hebben tegen het feit dat instanties hun persoonlijke gegevens verzamelen. Ze menen niets te verbergen te hebben. Anderen zijn ervan overtuigd dat het belang van privacy ondergeschikt is aan het doel waarvoor de betreffende organisaties de gegevens verzamelen en registreren. Te denken valt aan bestrijding van fraude met belasting of sociale uitkeringen.
Het belang van privacy krijgt een andere inhoud als op basis van de verzamelde gegevens belangrijke beslissingen genomen worden. Stel dat tijdens een sollicitatiegesprek het via het klantenpasje van de supermarkt verkregen boodschappenlijstje van de kandidaat ter sprake komt. "U houdt er wel erg ongezonde eetgewoonten op na!"

## Profielen van GSM-gebruikers

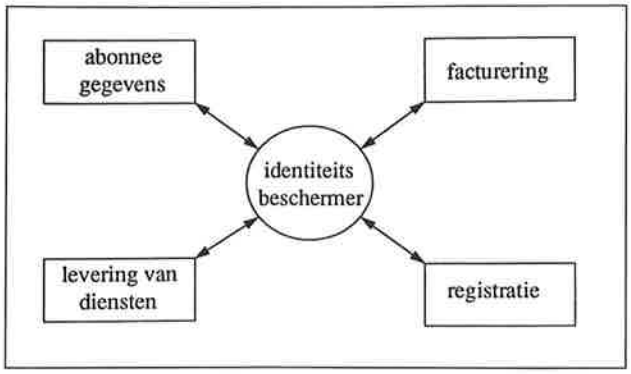
Het bovenstaande voorbeeld is gechargeerd. In werkelijkheid is het niet altijd duidelijk wat de voor en tegens nu eigenlijk zijn. Deze controverse rond privacy blijkt eens te meer uit een bericht in de Automatiseringsgids (19/01/96). Om fraude met GSM-telefoons op te sporen stellen enkele grote Amerikaanse en Engelse telecommunicatieaanbieders profielen op van het telefoongebruik van hun abonnees. Als het belgedrag van een abonnee op een gegeven moment sterk afwijkt van zijn profiel, kan dit duiden op misbruik van het abonneenummer door anderen. De telecomaanbieder neemt dan ter controle contact op met de abonnee.
De abonnees reageren tweeslachtig. Als inderdaad blijkt dat anderen een telefoonnummer misbruiken, reageert de abonnee verheugd. Het kan echter ook zijn dat de abonnee gewoon veel meer is gaan bellen. Hij ervaart de controle door de GSM-exploitant dan als inbreuk op zijn privacy.
De GSM-exploitant staat hier voor een lastige keuze. Of het garanderen van privacy door het niet opstellen van profielen of het hebben van een belangrijk middel voor fraudebestrijding.

De Registratiekamer [1] heeft, in haar streven de discussie en meningsvorming rond het begrip privacy te stimuleren, een studie verricht naar de mogelijkheden van privacy-bevorderende technieken. De geïnteresseerde lezer kan in het rapport 'Privacy-Enhancing Technologies: the path to anonymity' uitgebracht door de Registratiekamer, meer informatie over privacy-bevorderende technieken vinden.

## Nieuwe oplossingen

Door de hedendaagse technische mogelijkheden raakt de privacy vaker in het geding. Het is nu technisch veel makkelijker om meer en gedetailleerdere gegevens te verzamelen, te vergelijken en te interpreteren dan vroeger. Een voorbeeld hiervan is het koppelen van twee databases ten behoeve van het opsporen van fraude. Verder wordt informatie steeds vaker elektronisch opgeslagen. Wil een dienstenaanbieder zowel de privacy van zijn afnemers garanderen als fraudebestrijding mogelijk maken, dan zal hij nieuwe oplossingen moeten bedenken. Zo heeft hij in principe geen abonneegegevens nodig om gebruikersprofielen op te stellen en te analyseren. Deze hoeft hij pas te hebben als hij contact wil opnemen met een abonnee. Voor enkel het opstellen van profielen is het voldoende om elk telefoontoestel (of nummer) een uniek label te geven, zodat twee verschillende toestellen (of nummers) van elkaar onderscheiden kunnen worden. Voor elk label is vervolgens een profiel op te stellen.
De meest voor de hand liggende keuze voor een label is het abonneenummer of een andere code die direct gerelateerd kan worden aan een abonnee. In dat geval heeft de telecomaanbieder continu inzage in het telefoongebruik van zijn abonnees. Het is dan niet ondenkbaar dat de analist, die de profielen opstelt, toegang heeft tot de gegevens van het telefoongebruik van zijn buurman. Bovendien heeft, afhankelijk van de situatie, niet alleen de analist inzage in belprofielen van abonnees, maar iedereen met toegang tot de computersystemen waarop deze analyses uitgevoerd worden. Deze systemen zullen daarom weer goed beveiligd moeten worden en dat is op zich al een probleem.
Een andere, minder voor de hand liggende keuze voor het label is een willekeurig gegenereerde code. Dit label kan in de abonneegegevens opgenomen worden of is

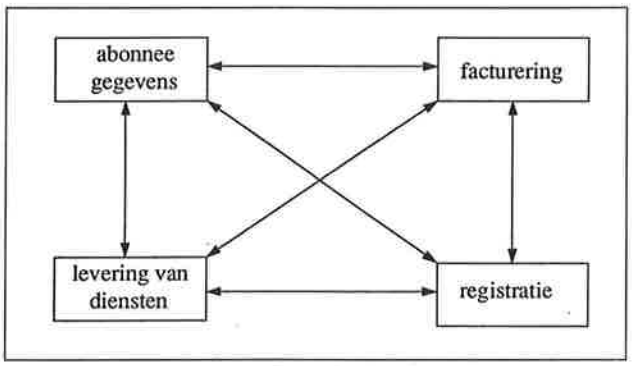
afzonderlijk van de abonneegegevens op te slaan. Het voordeel van deze keuze is dat het opstellen van gebruikersprofielen nu geheel anoniem kan geschieden. Het systeem waarop de analyses uitgevoerd worden bevat geen abonneegegevens meer en de analisten hebben nu geen toegang tot persoonlijke gegevens.
Het voorgaande voorbeeld illustreert dat er verschillende keuzen mogelijk zijn bij het ontwerpen of inrichten van een informatiesysteem. Het gros van de huidige informatiesystemen houdt geen bijzondere rekening met de belangen van de privacy van de gebruiker. Persoonlijke informatie wordt net zo behandeld als andere gegevens in het systeem. Wellicht waren er eisen voor het efficiënt en effectief verwerken van gegevens, maar niet voor het privacy-bewust behandelen ervan. Persoonsgegevens of andersoortige gegevens die de privacy van een gebruiker raken, kunnen vrij door andere elementen van het systeem benaderd worden (zie figuur 1).




**Figuur 1. Alle processen binnen een informatiesysteem kunnen ongecontroleerd de abonneegegevens benaderen, waardoor persoonlijke gegevens vrij door het systeem circuleren.**

## Digitale politieagent

Een voor de hand liggende manier om ongecontroleerde informatiestromen te kanaliseren, is het inzetten van een soort digitale politieagent, een identiteitsbeschermer die de informatiestromen binnen het systeem controleert en begeleidt. Processen, functies en andere delen van het systeem kunnen dan niet zonder meer de identiteit van de gebruiker benaderen, maar moeten dit via de identiteitsbeschermer doen (zie figuur 2).
Door het concept van de identiteitsbeschermer op te nemen in de specificatie en het ontwerp van nieuwe systemen, kan de privacy-gevoeligheid van het systeem verlaagd worden. De situatie geschetst in figuur 2 is de ideale situatie. Alle gegevensstromen lopen via de identiteitsbeschermer. Het is ook mogelijk dat slechts enkele delen of processen van het systeem afgeschermd zijn van de abonneegegevens. De figuur laat verder in het midden of de identiteitsbeschermer onder controle staat van het systeem (en dus de dienstenaanbieder) of van de abonnee zelf. In ieder geval moet de identiteitsbeschermer door beide partijen vertrouwd kunnen worden.




**Figuur 2. Een identiteitsbeschermer voorkomt dat andere processen ongecontroleerd de abonneegegevens kunnen benaderen.**

## Trusted Third Party

De bedreiging van de privacy is door de groeiende technische mogelijkheden sterk verhoogd. Aan de andere kant levert de techniek ook de mogelijkheden om de bedreigingen van de privacy sterk terug te dringen.
De meeste privacy-bevorderende technieken zijn gebaseerd op cryptografische algoritmen, zoals die voor het genereren en controleren van digitale handtekeningen. In theorie kunnen deze technieken nog veel verder doorgevoerd worden. Het is technisch mogelijk dat een gebruiker zijn identiteit bij een Trusted Third Party (TTP) in bewaring geeft en onder een digitaal pseudoniem gebruik maakt van allerlei elektronische diensten. Pas als deze gebruiker zijn verplichtingen ten aanzien van een leverancier niet nakomt, kan de TTP zijn identiteit onthullen. Een aantal van deze technieken wordt al toegepast op het Internet, namelijk bij 'anonieme' elektronische betalingssystemen.

Deze nieuwe technieken, met de verzamelnaam Privacy Enhancing Technologies, zijn nu nog vaak onbekend bij systeemontwikkelaars en opdrachtgevers, maar daarin komt geleidelijk aan verandering. Ook praktische bezwaren, zoals gebrek aan zekerheden, worden steeds meer weggenomen. Een identiteitsbeschermer in de vorm of als onderdeel van een smartcard of PCMCIA-card ligt voor de hand.
Helaas zijn er, afgezien van de technische aspecten, nogal wat organisatorische problemen rond het invoeren van PET-technieken, zoals het inrichten van een Trusted Third Party. Welke onafhankelijke instantie wil en kan deze taak op zich nemen, en wat is de juridische positie van zo'n organisatie?
Gezien de belangstelling van gebruikers voor hun privacy en de toenemende bekendheid van het fenomeen, lijkt het echter een kwestie van tijd voordat de eerste privacy-bewuste informatiesystemen zullen verschijnen. ◄

*** Is werkzaam bij TNO-FEL als informatiebeveiligingsdeskundige.**

**[1] De Registratiekamer is belast met het registreren van en het toezicht op persoonsregistraties in het kader van de Wet Persoonsregistraties (WPR).**