Bart Jacobs,
hoogleraar computerbeveiliging Radboud Universiteit Nijmegen (www.cs.ru.nl/~bart)

Pas op: **in je blootje vat je kou!**

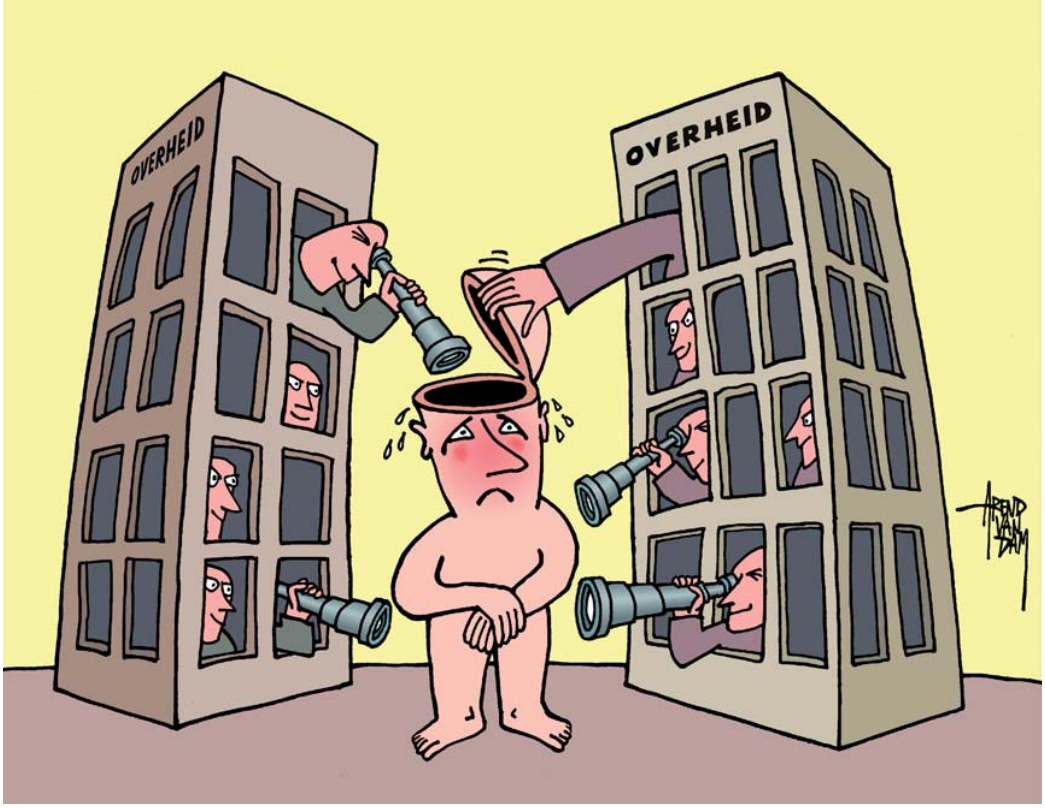
Begin september 2009 waarschuwde de Amerikaanse president Obama jongeren om vooral geen gekkigheden over zichzelf op sociale netwerken te plaatsen, zeker als ze de ambitie hebben om ooit president van de Verenigde Staten te worden. Als jongere doe je soms domme dingen, zei Obama, die je online kunnen blijven achtervolgen, zoals bij sollicitaties. Dit geldt voor veel ambten, en niet alleen voor het hoogste.
De Nederlandse overheid was er in de zomer van 2009 eerder bij. Toen werd de campagne "Veilig Internetten" in gang gezet om de eigen burgers voor soortgelijke risico's te waarschuwen (zie website www.veiliginternetten.nl). Vanaf een camping gaf minister van Justitie Hirsch Ballin het startschot voor een serie van TV-spotjes om mensen beter bewust te maken van de persoonlijke gegevens die ze op internet zetten en van de kwetsbaarheden die ze daarmee mogelijk creëren. Een voor de hand liggend voorbeeld is het openlijk vermelden van niet alleen het eigen huisadres maar ook de vakantiedata op sociale netwerksites zodat inbrekers daar hun voordeel mee kunnen doen. Dit is een zinvolle en hoognodige campagne.
Toch schuurt en jeukt er iets.
Diezelfde overheid heeft de afgelopen jaren wetgeving en maatregelen ingevoerd waardoor velerlei gevoelige persoonlijke informatie van ons burgers vastgelegd en ingeleverd moet worden, via bijvoorbeeld dataretentie (van email en telefoonverkeer), elektronische slotgrachten (waarmee autokentekens automatisch geregistreerd worden), centrale opslag vingerafdrukken (uit paspoorten), opslag van openbaar vervoersbewegingen (voor 7 jaar, via OV-chipkaart), elektronische `smart' meters (die iedere 15 minuten het elektriciteitsgebruik automatisch doorgeven), etcetera. Eerst worden ons door de overheid de kleren van het lijf getrokken, en vervolgens krijgen we te horen: "pas op, in blootje vat je kou!".
Is hier sprake van hypocrisie?

Good guys en bad guys

Impliciet bij deze ontwikkelingen is een aantal vooronderstellingen, met name over wie *good guys* en *bad guys* zijn. De overheid waarschuwt ons tegen *bad guys* die mogelijk misbruik maken van onze persoonsgegevens, maar beschouwt zichzelf nadrukkelijk onderdeel van de *good guys*. De situatie zou als volgt explicieter gemaakt kunnen worden. De overheid zegt: "Brave burger, verspreiding van persoonsgegevens maakt u kwetsbaar; daar kan op allerlei manieren door kwaadwillenden misbruik van gemaakt worden. Maar die persoonsgegevens moet u wel bij ons in leveren zodat we u beter kunnen helpen en beschermen; overheden zijn goedwillend en maken nooit misbruik van zulke gegevens." Deze formulering schuurt en jeukt al veel harder.
Om te beginnen is het een positieve ontwikkeling dat de overheid burgers waarschuwt voor de risico's van slordige omgang met persoonsgegevens. Vroeger was het zo dat je vooral zelf een sukkel was in geval van slordigheid. Identiteitsfraude kan echter zodanige vormen aannemen dat het maatschappelijk ontwrichtend kan werken, bijvoorbeeld wanneer grootschalige administraties en bestanden vervuild raken door propagatie van fouten. Dit zou mogelijk kunnen optreden bij identiteitsfraude in de zorg (door onverzekerden) waardoor foutieve medische gegevens zich via landelijke koppelingen voortplanten. Ook is de huidige infrastructuur voor financiële dienstverlening in hoge mate afhankelijk van adequate authenticatie van personen, bijvoorbeeld bij internetbankieren. Indien deze authenticatie in een significant aantal gevallen faalt, hebben we nauwelijks meer een alternatieve infrastructuur om op terug te vallen. Daarnaast kunnen zaken die geheim zouden moeten blijven, mogelijk uitlekken door ondoordachte verspreiding, zoals bij voorbeeld de identititeit van de chef van de Britse geheime dienst MI6, die normaal alleen als "C" bekend is, maar deze zomer door toedoen van zijn echtgenote slechts in zwembroek te zien was op Facebook.
Er is dus alle reden voor terughoudendheid met persoonsgegevens. In feite behoort het aanleren van dergelijke terughoudendheid tot de basisvaardigheden die (jonge) mensen zich eigen moeten maken in het digitale tijdperk.

Burgers leveren in

Des te wranger is het dat de overheid in steeds sterkere mate aanstuurt op transparantie van burgers – en veel minder andersom, overigens. Om vage redenen worden zware inleververplichtingen opgelegd, zonder dat daar duidelijk meetbare doelstellingen, evaluaties, of inschattingen met betrekking tot risico's of misbruik tegenover staan. Heeft de politie bijvoorbeeld een meetbare doelstelling om aantoonbaar X procent meer zaken op te lossen door de digitale slotgrachten, en is ze bereid om in geval dat percentage niet gehaald wordt de kenteken-camera's weer te verwijderen? Natuurlijk niet. Het gebrek aan een dergelijke kritische context versterkt het wantrouwen en het risico op steeds uitgebreider gebruik, veel verder dan de oorspronkelijke doelstellingen – *if any*.
Een goede illustratie van dergelijke *function creep* vormen de vingerafdrukken in paspoortchips. De oorspronkelijke



Overheid: "good guys" of "bad guys"...?

doelstelling om daarmee de band tussen een paspoort en de drager ervan beter te kunnen controleren is goed te verdedigen. Gaandeweg zag de overheid echter nieuwe "kansen" en besloot de vingerafdrukken zelf op te slaan in een centrale database. Daarvoor werden gekunstelde redenen bedacht, zoals het voorkomen van het aanvragen van twee paspoorten onder verschillende naam – zonder te onderzoeken hoe groot dat probleem eigenlijk is – of identificatie van slachtoffers bij grote rampen – waarvoor gebitten natuurlijk veel geschikter zijn dan vingerafdrukken. Na enige tijd kwam de aap uit de mouw: inlichtingendiensten en justitie willen ook in de database kunnen zoeken! In de wet zoals die er nu uitziet staan nog allerlei procedurele beperkingen voor toegang door justitie. Maar je hoeft geen helderziende te zijn om te weten dat die beperkingen er snel van af gaan. Het scenario is voorspelbaar: eerst komt er een hoofdcommissaris van politie op TV vertellen dat zware-jopie-de-serie-baby-verkrachter op tijd gepakt had kunnen worden als men zonder beperkingen toegang tot de database had gehad en vervolgens gaat de politiek door de knieën. Binnen een paar jaar fungeert deze centrale database met vingerafdrukken als een kenteken-register voor alle burgers – en niet alleen de criminele. Onduidelijke doelstellingen en vormen van *function creep* bij informatieverzameling dragen niet bij aan vertrouwen en maken het minder vanzelfsprekend dat de overheid tot het kamp van de *good guys* behoort.

Bescherming van burgers

Natuurlijk worden wij burgers geacht de overheid tot de *good guys* te blijven rekenen, bij wie wij dus zonder aarzeling en zorgen onze persoonsgegevens wel kunnen inleveren. Het lijkt het voorstellingsvermogen van veel Haagse politici te boven te gaan dat burgers misschien ook tegen de eigen overheid beschermd zouden moeten worden. Het is zorgelijk wanneer de overheid zonder duidelijke motivatie zo sterk inzet op het in de gaten houden van de eigen burgers met middelen die niet anders gekwalificeerd kunnen worden dan als instrumenten van een politiestaat. Een eventuele minder welwillende overheid komt hierna in een gespreid bedje. Maar, zult u misschien tegenwerpen, al deze maatregelen zijn toch niet tegen burgers gericht maar worden juist ingevoerd om de veiligheid te vergroten en de burger te beschermen. Dit pad van steeds ingrijpender surveillance en controle, via instrumenten van een politiestaat, heeft echter een eigen logica en dynamiek, waarbij we aan het eindpunt mogelijk tevreden kunnen constateren dat een politiestaat voor veel mensen veiliger is dan een democratie. Onze tijd vraagt om een heldere visie met bijbehorend toetsingskader, om grenzen te kunnen en durven stellen en om een balans te vinden tussen enerzijds door angst en effectiviteitseisen gedreven surveillance en controle en anderzijds bescherming van individuele autonomie. Misschien is het voor de overheid een zinvolle aanvulling op de campagne om de technologische voortgang ook (en vooral) in te zetten om die autonomie te beschermen en te versterken.
Het is een belangrijke stap dat de huidige overheid de risico's van onzorgvuldige verspreiding en gebruik van persoonsgegevens inziet en burgers daar nadrukkelijk tegen waarschuwt. Geloofwaardigheid van deze waarschuwing legt de overheid zelf ook de nodige verplichtingen op, niet alleen in handelen maar ook in verantwoording. Om de impliciete vooronderstelling bij deze waarschuwing dat de overheid zelf tot de *good guys* behoort en blijft behoren waar te maken is een andere houding en werkwijze nodig dan de afgelopen jaren ten toon gespreid is.
Anders wordt het tijd voor een nieuw type waarschuwingsspotje.