Column uitgesproken in De Balie in Amsterdam, op de discussie-avond "Nederland Controlestaat?" op 17 nov. 2006.

Bart Jacobs, www.cs.ru.nl/B.Jacobs

Privacy, dames en heren, is de bron van alle goeds! Deze stelling is denk ik goed te verdedigen. Privacy is de bron van alle goeds. Het is echter niet wat onze politici, beleidsmakers en ambtenaren op het gebied van openbare veiligheid ons de afgelopen jaren hebben laten horen. Hun beeld is vooral: privacy is de schuilplaats van het kwaad. Deze omslag is op zijn minst opmerkelijk te noemen. Het bijbehorende mensbeeld is ook opmerkelijk negatief: wanneer je burgers even uit het oog verliest leidt dat alleen maar tot narigheid.

Wie niks te verbergen heeft, heeft ook niets te vrezen! Deze oproep tot transparantie van burgers probeert een positievere draai te geven aan dit negatieve mensbeeld. Ik beschouw mijzelf echter als een brave burger die zich netjes aan allerlei regels en wetten houdt, en desondanks heb ik toch veel te verbergen. Ik wil een overheid die dat respecteert, zonder mij direct in een criminele hoek te plaatsen.

Onze privacy moet opgeofferd worden voor veiligheid. Nog zo'n kreet die kenmerkend is voor het huidige tijdsbeeld. De noodzaak van deze opoffering heb ik echter nooit goed begrepen. De vooronderstelling lijkt te zijn dat privacy en veiligheid niet samengaan. Is dat wel zo? Ik wil een overheid die voor allebei zorgdraagt, zonder een geforceerde tegenstelling te creëren.

Privacy is juist essentieel voor persoonlijke veiligheid. Vrouwen in een blijf-van-mijn-lijf huis weten wel waarom. En politici worden juist om die reden zo nerveus wanneer de precieze locatie van hun privéwoning via Google-earth duidelijk zichtbaar op het web verschijnt—zoals onlangs bij casabobo.nl, maar inmiddels onder druk weer snel verwijderd. Er bestaan op dit moment veel ondoordachte plannen om onze identificeerbaarheid te vergroten. Een voorbeeld zijn zogenaamde RFID-chips in nummerplaten, zodat de identiteit van uw auto op afstand snel herkend kan worden. Dit lijkt allemaal mooi en handig. Maar het kan ook makkelijk misbruikt worden, bijvoorbeeld om een bom automatisch te laten afgaan wanneer de "juiste" auto passeert. Reken maar

dat men in het criminele circuit daar dankbaar gebruik van gaat maken. Transparantie is niet noodzakelijk goed voor persoonlijke veiligheid.

Ook via biometrisch paspoorten komen mijn biometrische gegevens, zoals vingerafdrukken, wereldwijd in allerlei databanken terecht. Het is niet iets wat in mijn persoonlijk belang lijkt te zijn. Misbruik van die gegevens kan tot identiteitsfraude leiden, waarbij iemand anders zich als mij voordoet, waar ik weer veel last van kan hebben.

Maar natuurlijk, ik weet het ook wel, al deze maatregelen zijn niet gericht op mijn persoonlijke veiligheid, maar op de collectieve veiligheid, voor ons allemaal. Het verbaast mij echter dat zulke maatregelen in het kader van openbare veiligheid ingevoerd worden zonder een uitgebreidere afweging van de impact op uw en mijn persoonlijke veiligheid. Soms kan ik me niet aan de indruk onttrekken dat het gehele perspectief ontbreekt van privacy als essentieel voor persoonlijke veiligheid.

Wat kunnen we hier voor de toekomst nog aan doen? Ik wil vanavond twee dingen noemen, waarvan één slechts kort. Het eerste, korte punt is een radicale decentralisatie van gegevensbeheer, waarbij burgers zelf veel meer zeggenschap krijgen over hun gegevens en over hoe ze op welk moment hun identiteit aan de omgeving laten zien (en bewijzen). Hoe dit technisch en organisatorisch geregeld zou moeten worden is een grote uitdaging aan mijn vakgebied computerbeveiliging. Daar wil ik het nu verder niet over hebben.

Mijn tweede punt is wat ik meestal aanduid met de kreet *select before you collect*. Traditioneel is het zo dat je eerst geselecteerd moet zijn als verdachte, op basis van een redelijk vermoeden, voordat jouw privacy rechten geschonden mogen worden bij het verzamelen van informatie, bijvoorbeeld in een strafrechtelijk onderzoek via telefoon- of internettaps. Met de toegenomen technische mogelijkheden zien we steeds vaker een omkering van selecteren en verzamelen. De moderne werkwijze is *collect before you select*: eerst van iedereen informatie verzamelen, en dan pas selecteren van wie gegevens gebruikt gaan worden. Dat is duidelijk te zien bij het Europese besluit om de zogenaamde verkeersgegevens van alle 450 miljoen Europese burgers voor langere tijd op te slaan. Dit omvat onder andere de locatiegegevens van alle

mobiele telefoons, en bijvoorbeeld ook of en hoe vaak ik de website `erectieproblemen.nl` bezoek. Die informatie lijkt mij nauwelijks relevant bij het verijdelen van terroristische aanslagen.

Deze omdraaiing van *select* en *collect* verloopt sluipenderwijs, zonder veel discussie, maar is in mijn ogen zeer fundamenteel. Ik wil er hier expliciet voor pleiten om te zeggen: dat doen wij in Nederland **niet**, puur omdat we een fatsoenlijke overheid willen die niet al haar burgers wantrouwend als criminelen benadert! Dit is een kwestie van niet alles willen wat ook technisch mogelijk is. Nederland bouwt ook geen kernbom.

Vasthouden aan het principe van *select before you collect* vereist een nadrukkelijker onderscheid tussen *good guys*—die weloverwogen met rust gelaten worden—en *bad guys*—tegen wie een redelijk vermoeden bestaat, en tegen wie wat mij betreft de volledige staatsmacht zonodig ingezet mag worden. Ik wil er dus voor pleiten het vergaande middel van data-surveillance niet breed voor iedereen in te zetten, maar alleen gericht op *bad guys*, en bijvoorbeeld ook als sanctie. Na veroordeling kunnen mensen in bepaalde gevallen onder verscherpt data-toezicht blijven, in lijn met het huidige gebruik van huisarrest via elektronische pols- of enkelbandjes. We kunnen ook creatief en selectief, in plaats van lomp en breed, gebruik maken van de technische mogelijkheden.

Maar, zo hoor ik sommigen van u denken, pak je met dat fraaie *select before you collect* principe wel terroristen? Ik ben daar redelijk van overtuigd—waarbij ik moet toegeven dat ik geen *inside knowledge* heb van terrorismebestrijding. Echter, wat ik wel weet is dat in alle publiekelijk bekende gevallen van terroristische aanslagen, of van pogingen daartoe, de inlichtingendiensten de daders van te voren al in de smiezen hadden. Ze waren dus al geselecteerd, maar het probleem is dat hun risico niet altijd juist ingeschat is. Bevolkingsbrede data-surveillance voegt hier niks aan toe, en maakt het misschien alleen maar moeilijker om de ruis weg te filteren. De effectiviteit van grootschalige data-opslag en privacy-aantasting is volstrekt niet bewezen.

Terroristen, dames en heren, dagen ons uit juist die waarden te ondermijnen waarvan we het hardste roepen dat we ze willen verdedigen.

Mijn voorzet voor de verdere discussie vanavond is dus de concrete vraag: willen wij Nederland als controlestaat, of willen wij vasthouden aan het basisprincipe van *select before you collect*?

Dank voor uw aandacht.