Cameratoezicht, privacy en veiligheid

Het verzorgen van veiligheid op een efficiënte en effectieve manier is een voortdurende uitdaging. De vraag om meer veiligheid lijkt nooit te stoppen, terwijl we resources te kort komen om mens en middelen aan te blijven dragen. Naast deze behoeftes die waarschijnlijk nooit volledig 'vervuld' zullen raken, zijn er ook verankerende beginselen zoals privacy, en beginselen die beschrijven hoe we deze zaken willen organiseren, zoals accountability en transparantie [WRR, 2011, iOverheid].

Afwijkend en verdacht gedrag
In deze context bouwt TNO kennis op over afwijkend en verdacht gedrag. Afwijkend gedrag is iets anders dan verdacht gedrag. Verdacht gedrag is gedrag waarvan bekend is dat het correleert met onveilige situaties, voor, tijdens of nadat dit gedrag vertoond wordt. Van zakkenrollers is bekend dat ze bij een kaartjesautomaat op een treinstation meerdere keren achteraan bij dezelfde rij aansluiten, zonder ooit vooraan een kaartje te kopen. Dit is bekend verdacht gedrag. Tegelijkertijd is het ook afwijkend gedrag. De meeste mensen gedragen zich niet zo. Dit laatste is relevant omdat heel veel dagelijkse omgevingen zo rijk zijn aan kansen voor mensen om zich onveilig of althans ongewenst voor anderen te gedragen, dat het meestal ondoenlijk is om alle vormen van verdacht gedrag af te tellen en te omschrijven. Het loont dan om een omschrijving te hebben van normaal gedrag, zodat de toezichthouder daar gericht minder aandacht aan kan besteden.

In een serie onderzoeken voor de NCTb [Lousberg, 2009, NCTb] zijn camera-operators geïnterviewd, en zijn opleidingen van operators geanalyseerd om er achter te komen waar ze op letten in bepaalde contexten. Daar zijn expliciete lijsten van gedragingen uit gekomen. We nemen aan dat het inzetten van menselijke operators om te kijken naar gedrag er voor zorgt dat het veiliger wordt. Dit is immers wat operators tegenwoordig aangeleerd wordt. Een goede onderzoeksvraag is dus hoe de relatie tussen operators die getraind zijn in afwijkend gedrag en de veiligheid in elkaar zit.

Gedrag in context
Sommige vormen van gedrag zijn overduidelijk verdacht, zoals het voorbeeld van de zakkenroller. Andere vormen zijn genuanceerder. Dan is het nodig om meerdere losse observaties met elkaar te verbinden. Een voorbeeld hiervan, die reeds is beproefd en wordt uitgevoerd door de politie, is de methode Search Detect React [Lousberg, 2009, SDR]. De bedoeling van deze methode is om bij mensen die verdacht gedrag vertonen, op een lichte manier te achterhalen of daar meer achter schuil gaat. Dit wordt gedaan door een prikkel te communiceren waarop de persoon op meerdere manieren kan reageren. Aan de concrete reactie is vervolgens meer af te leiden. Een enkele verdachte gedraging is zelden aanleiding voor welke aanvullende maatregel dan ook. De toezichthouder zal proberen om zo goed mogelijk de crimineel te onderscheiden van de goedgezinde burger. Daarbij kunnen meerdere observaties van een persoon hem helpen, om echt verdacht gedrag te onderscheiden van wie zich simpelweg een beetje afwijkend gedraagt.

Vrije wil en gedrag
Menselijk gedrag is een complex verschijnsel. Het wordt beïnvloed door bewuste en onbewuste intenties, door de fysieke mogelijkheden van het menselijk lichaam, door emoties en door allerlei omgevingsfactoren. Tegelijkertijd hebben we met betrekking tot ons gedrag een heel sterk gevoel van autonomie: ik bestuur mijn gedrag, in tegenstelling tot mijn huidskleur, etniciteit of identiteit. Het concept van *vrije wil* stelt dat er een deel aan ons is waar wij controle over hebben, en een deel waar wij geen controle over hebben. Als iemand ergens controle over heeft, dan heeft hij

daar ook een verantwoordelijkheid over. Mensen hoeven geen verantwoordelijkheid te nemen voor hun afkomst, etniciteit, huidskleur of andere aangeboren kenmerken. Dus tenzij een persoon zich met terrorisme of zware criminaliteit heeft beziggehouden, of op een andere manier een verhoogd risico vormt, is het niet geaccepteerd om zijn identiteit of achtergrond te lichten: gegevens moeten relevant zijn, en niet buitenproportioneel ten opzichte van het doel waarvoor ze worden verwerkt. Indien de toezichthouder geen reden en toestemming heeft om te zoeken naar specifieke personen, is het dus onnodig en ethisch onverantwoord om identiteit en achtergrond te achterhalen. Gedrag kan dan los beschouwd worden van identiteit en achtergrond.

Privacy-by-design

Het opbouwen van kennis over menselijk gedrag, en het –vooralsnog ten dele- automatiseren ervan helpt om kosten beheersbaar te houden, en een zekere mate van efficiëntie en effectiviteit te bereiken. Hier ligt een enorme verantwoordelijkheid met betrekking tot het misbruik maken van die kennis, maar ook een kans. Door kennis expliciet te maken, maken we ze immers ook controleerbaar. Hoe we met die verantwoordelijkheid en kansen om gaan, is een vraag waar we zelf bij zijn.

Bij het doen van onderzoek op dit gebied is het van belang om daar een aantal principes bij te hanteren, zoals transparantie, accountability, privacy en keuzevrijheid. De juridische, ethische en engineering vakgebieden zijn op deze vlakken enorm in beweging, mede naar aanleiding van enorme technologische sprongen van de moderne tijd. Er zijn weinig methodes of best-practices beschikbaar die tegelijkertijd voldoende specifiek zijn op ethisch gebied, en voldoende specifiek op praktische uitvoerbaarheid. Op het gebied van privacy geeft Privacy-by-design [Cavioukian, 2011] een verzameling van 7 uitvoerbare principes die bij het ontwerp proces richting geven. Hoewel onderzoek niet hetzelfde is als ontwerpen, geven deze principes wel al vroeg richting aan onderzoek.

Bij het doen van dit onderzoek ontstaat gaandeweg een beeld van een aanpak die doelmatig is en later vertaald kan worden naar concrete systeemeisen of een architectuur. Het ligt bijvoorbeeld voor de hand de losse observaties aan mensen te koppelen middels de identiteit van de persoon, of althans een persoonskenmerk waarmee de identiteit makkelijk achterhaald kan worden, zoals gezichtsherkenning of digitale wolk. Dat zou echter bovenmatig zijn in verhouding tot het doel, en dient dus ook vermijd te worden indien mogelijk. Dit is ook helemaal niet wat een menselijke operator zou doen. Deze heeft immers noch de geheugencapaciteit, noch de middelen om ad hoc identiteiten van passanten te achterhalen, noch heeft hij ze nodig om losse gedragingen aan elkaar te koppelen. Er bestaan meerdere technische manieren om meerdere gedragsobservaties van een persoon over een korte afstand aan elkaar te koppelen zonder daartoe gebruik te maken van persoonsgegevens waarmee identificatie ook makkelijk is.

De 7 principes van privacy-by-design zouden op de volgende manieren verwerkt kunnen worden in toepassingen op dit gebied:

- Proactive not Reactive; Preventative not Remedial – Identificeerbare stukjes data zoals gezichten en kentekens weg filteren uit de beelden, zodat anderen niet alsnog kunnen identificeren. Tracks van mensen pas vrijgeven als op individuele gedragingen afwijkingen zijn geconstateerd. Losse observaties kunnen pas gekoppeld worden, indien een individuele observatie daar aanleiding toe geeft.
- Privacy as the Default – Als je geen afwijkend gedrag vertoond, dan gebeurt er verder niets met jouw persoonsgegevens.
- Privacy Embedded into Design – We maken er een punt van om geen identificeerbare stukjes data, zoals gezichten, te gebruiken om gedrag over tijd en plaats te koppelen.
- Full Functionality – Positive-Sum, not Zero-Sum – Indien het gedrag van mensen aanleiding geeft, dan blijft het mogelijk daar nader naar te kijken. Dit wordt niet onterecht onmogelijk gemaakt door verkeerde design-choices.

- End-to-End Security – Lifecycle Protection – Indien er geen afwijkend gedrag is vertoond, dan worden de beelden verwijderd na verloop van de bewaartermijn.
- Visibility / Transparency – De lijst van gedragingen is te controleren door bijvoorbeeld CBP of het parlement.
- Respect for Users – Dit beginsel is wat vager omschreven, en is lastig te vertalen naar situaties waarin de “gebruiker”, in casu de geobserveerde, niet vanzelfsprekend zelf interactie heeft met het systeem.

De rol van TNO

TNO voert samen met allerlei partners onderzoek uit naar bovenstaande zaken. We publiceren over dit werk, en gaan op verschillende platforms de discussie aan. We definiëren en objectiveren de criteria waarop afwijkend gedrag wordt vastgesteld. [Lousberg, 2009, NCTb], [Burghouts, 2011] Daarmee wordt het expliciet welke gedragscriteria gelden en kunnen deze worden getoetst door degenen die de samenleving daarvoor aanwijst. We onderzoeken de meerwaarde van het koppelen van meerdere waarnemingen. [Lousberg, 2009, SDR]. We onderzoeken hoe de principes van privacy-by-design toegepast kunnen worden op intelligente camera’s. We onderzoeken manieren om mensen te volgen zonder gebruik te maken van persoonsgegevens [Hollander, 2010] [Rest, 2009] We onderzoeken systeemconcepten waarin observaties over tijd en plaats gecombineerd kunnen worden [Burghouts, 2009], [Burghouts, 2010], [Rest, 2009]. We maken het mogelijk observaties te koppelen, zonder dat iedere afzonderlijke observatie ook direct beschikbaar is [Nasrullah, 2009]. We onderzoeken ook manieren om identificeerbare persoonsgegevens zoals gezichten of kentekens uitmultimedia stromen te knippen, zodat voorkomen kan worden dat anderen alsnog identificatie plegen. [Roelofsen 2003]

[Roelofsen 2003] Patent WO 03/010728/A1 Method and System and Data Source for Processing of Image Data, februari 2003
[Munster, 2008], *Big Brother or Smart Sister? Completing the image…*, Presentation at HIDE project, http://www.hideproject.org/downloads/HIDE_FG-Embedded_Technology-Presentation_Ruud_v_Munster_FG1-20081031.pdf , oktober 2008
[Rest, 2009] Rest, J.H.C. van, et al, Safety and Security Systems in Europe 2009, Sensors and Tracking Crossing Borders, Proc Micromaterials and Nanomaterials
[Nasrullah, 2009] Nasrullah, I., 2009, *Hierarchical Query Mechanisms for Searchable Encrypted Databases*, TU Delft Master Thesis, 2009
[TNO Magazine januari 2009], *Privacy: Blijf wakker, denk goed na*, http://www.tno.nl/images/shared/overtno/magazine/tno_mag_1_jan_2009_06_07_08_09.pdf , Januari 2009
[Lousberg, 2009, NCTb] NCTb rapporten, Toolbox Afwijkend Gedrag, 2009
[Lousberg, 2009, SDR], Lousberg, *De sterke arm der Wet*, http://www.sdr.eu.com/news/item/3/tno-magazine-p-19, 2009
[Burghouts, 2009] G.J. Burghouts et al., ‘*Automated indicators for behavior interpretation’*, Int. Conf. on Crime Detection and Prevention, 2009.
[Burghouts, 2010] G.J. Burghouts, J-W. Marck, ‘*Reasoning about threats: from observables to situation assessment*’, IEEE Transactions on System, Man and Cybernetics, special issue on Pattern Recognition for Anti-terrorism Applications, submitted, 2010.
[Hollander, 2010] Hollander, R.J.M. den., Landsmeer, S.H., Eekeren, A.W.M. van., Bouma, H.; “*Appearance-based retrieval of persons in digital images of multiple cameras*”, Report TNO-DV-2009-D651, TNO, The Netherlands, 2010
[Cavoukian, 2011] Cavoukian, A. Privacy-by-Design, http://www.privacybydesign.ca/ , 2011
[Burghouts, 2011] G. J. Burghouts, R. den Hollander, K. Schutte, S. Landsmeer, J-W Marck, E. den Breejen, *‘Increasing the Security at Vital Infrastructures: Automated Detection of Deviant Behaviors’*, SPIE Defence, Orlando, 2011.

http://www.tno.nl/content.cfm?context=thema&content=innovatiegebied&laag1=893&laag2=910&item_id=910
[WRR, 2011, iOverheid] WRR, *iOverheid*, http://www.wrr.nl/content.jsp?objectid=5656