Version 10 February 2012
This is a pre-edited version of a book section. The final version is published as:

Grommé, Francisca. 2012. "Surveillance in the Supermarket: Technology and the Pluralisation of Crime Control." In *Crime, Security and Surveillance: Effects for the Surveillant and the Surveilled*, edited by Gudrun Vande Walle, Evelien Van den Herrewegen, and Nils Zurawski, 33–53. The Hague: Eleven International Publishing.

Surveillance in the supermarket: Technology and the pluralisation of crime control

Introduction

In 2007, a city in the Netherlands provided its shop owners with a facial recognition system to detect known shop thieves. The local government presented the project as a favour to the retail sector in the area to enable entrepreneurs to combat retail crime more actively and more resolutely. This smart camera system compared faces of individuals in the crowd with police photos of known local shoplifters. The shop owner was alerted when a match was established between a person having entered the shop and a database photo. The project started out with a one-year pilot in one supermarket to learn if and how the technology could be used for this purpose. In spite of the city's high expectations of this technology, the supermarket employees were critical of the favour presented by their local government: would a database with police photos contribute to their own knowledge? And would it make their work easier? Moreover, the retail sector in this city had no ambitions to increase its involvement in policing activities, despite the local government's encouragement. Given this discussion about the position of retail in crime control, the introduction of facial recognition in the supermarket raises questions about the use of technology to increase retail involvement in crime surveillance.

In this paper, I ask how facial recognition intervenes in the relations between the various actors involved in monitoring and controlling shop crime. In particular, I focus on the way in which technology affects the pluralisation of surveillance, understood here as the state's effort to mobilise new types of actors. State agencies increasingly assert themselves not as the main providers of security, but actively and openly seek the role of facilitators or partners in the provision of security (Rose, 2000). Consequently, the state should be understood as only one of the nodes in an extended crime control network that includes a variety of public and private agencies, relationships, programmes and techniques (Den Boer, 2004; Loader, 2000; Rose, 2000; Van Steden, 2007). The involvement of both state and non-state actors in crime control is not a new phenomenon (think, for example, of Rembrandt van Rijn's *The Night Watch*)[1]. However, the roles of private actors in crime control, including security agencies, retailers and technology suppliers, have nowadays become more formalised (Van Steden, 2007).

The pluralisation of surveillance in crime control is a significant development, because, as is often claimed, it can result in more 'intense' and 'ubiquitous' forms of monitoring and social control (Lyon, 2007; G.T. Marx, 2002). In the Netherlands various developments in the domain of surveillance and crime control have led to concerns about the infringement of new crime control measures on citizens' everyday lives. Since the 1980's

Dutch crime policy has increasingly prioritised security, safety, efficiency and service provision over privacy and proportionality. Crime policy has become more risk-driven, aiming for prevention, while a strict application of criminal law has replaced a tolerant approach (Boutellier, 2002; Koops, 2011). At the same time, the transfer of state responsibilities in crime control has become an explicit policy aim (Van Steden, 2007; Van Stokkom, 2009). As for the use of new technologies in the field of policing, Bert-Jaap Koops (2011) notes that a supply-driven line of thinking has become leading. Concerns about privacy, proportionality and legislation are now set aside to enable the use of new technologies in crime control. Thus, a technological advantage over criminals is prioritised over integrating new technologies into law and practice.

Despite increased attention to these issues, we know little about the interaction between the pluralisation of policing and the introduction of new technologies at specific sites. Recent scholarly work about surveillance suggests that technologies play an important role in this process, because they link different types of actors in 'networks' or 'complexes' of surveillance (Introna & Wood, 2004; Prainsack & Toom, 2010). Building on Gilles Deleuze and Félix Guatarri's (1987) notion of the rhizome, Kevin Haggerty and Richard Ericson (2000) have put forward one of the most prominent conceptualisations of the form and growth of surveillance: the surveillant assemblage. The metaphor of the rhizome refers to the root structure of weeds that grow independent of the main roots, but may shoot up in different locations and grow without a central order or hierarchy. In line with this notion, Haggerty and Ericson suggest that the surveillant assemblage is a heterogeneous gathering of loosely connected actors, such as people, institutions, technologies and knowledge. This assemblage can be considered as a unity to the extent that the actors may work together as a 'visualising device' for a target population.

In contrast to the idea of disciplinary surveillance (Foucault, 1995), this line of theory does not consider surveillance systems as discrete, institutional entities. Surveillance assemblages are expansive; they 'grow like weeds' (Haggerty & Ericson, 2000, p. 614) in the sense that they link ever more actors in fluid configurations. Ericson and Haggerty suggest that surveillance technologies play an important role in the enrolment of new actors. Technologies participate in translating the subject of surveillance into disembodied fragments, the 'data doubles'. By doing so, they create new target populations that may link actors in the surveillant assemblage. In addition, technologies make connections by integrating databases, for example when combining consumer databases, social security databases and police information systems to create a profile for a specific individual. These technologies do not necessarily need to be 'high tech' as, according to Ericson and Haggerty's line of argumentation, paper files may have the same effect.

Missing from this account is a comprehensive consideration of the ways in which surveillance technologies are implemented in their environment in order to visualise a target population. The assumption is that ready-made artefacts are flawlessly implemented in a new context. In practice, however, they need to be integrated within the relations, strategies, techniques, norms and preferences at a specific site, a process that can involve contingency and resistance (Akrich, 1992; Callon, 1986b). Only limited attention is paid to discrepancies and conflict among the actors, partly because the actors are granted limited agency; they have no capacity to change the world around them. Instead, agency is attributed to the theoretical concept of the assemblage itself (Prainsack & Toom, 2010). The observation that the effects of new technologies are not self-evident is demonstrated by Kelly Gates in a case study on a facial recognition pilot in Florida. In this case the technology served as a site of struggle over police competences in crime control (Gates, 2010). Moreover, ethnographic research shows that those who perform surveillance may be reluctant to accept more surveillance tasks, for example because they prefer to function as hosts or workplace coordinators (Helten &

Fischer, 2004), or because they experience monitoring activities as physically tiring (Smith, 2004).

In this paper, I use the notion of 'situated surveillance' to attend to the reconfigurations and contingencies that accompany the introduction of surveillance technologies. Christopher Gad and Peter Lauritsen (2009) suggest that surveillance is an event that only succeeds if various sources of information, devices and human actors act together. Consequently, 'the surveillant' is not a single operator, but a heterogeneous mixture of humans, artefacts and sources of information at a specific time and place (M'charek, 2008). Introducing a new technology, such as facial recognition, can involve a reordering of the relations between the actors that jointly operate to visualise a target population.

In line with Gad and Lauritsen's proposed approach towards surveillance of 'theoretical agnosticism',[2] my aim is not to develop a generalised argument for a model of the form or structure of surveillance, such as the surveillant assemblage or the Panopticon (Foucault, 1995). I rather intend to provide an in-depth analysis of the ways in which technologies are involved in the pluralisation of surveillance in the supermarket case. By studying surveillance as a situated practice of making shoplifters visible, I show how facial recognition was in this case part of an effort to further enlist the supermarket in monitoring petty crime. I furthermore attend to the contingencies of this process by showing that the supermarket was not mobilised as planned due to an inability to integrate the technology within the local surveillance practices. While surveillance technologies can potentially engage new actors, they do not necessarily do so as they may refuse to take part in a particular mode of surveillance. In other words, not only subjects of surveillance resist, resistances may also exist within the networks that perform surveillance.

Surveillance as a situated practice

Technologies are not passive entities in surveillance. As Amade M'charek (2008) argues with regard to the practice of making suspects visible on the basis of DNA, technologies may, depending on the context, lead to a reorganisation of the relations between actors. In a similar vein, facial recognition was designed to interfere with the existing relations between objects, devices and people that were embedded in the strategies and routines of monitoring shoplifting in the supermarket, but may in this context not have had the intended effect.

In order to show how facial recognition intervened in surveillance practices on the work floor, I approach surveillance as a situated, collective practice that introduces only partial 'visions'. In her argument for the partial perspective as a basis for a feminist practice of science, Donna Haraway (1988) proposes the metaphor of vision to refer to partial observations of the world that are mediated by bodies, instruments, culture and politics. When applied to the observations made in surveillance control rooms, it becomes clear that what surveillants see are not straightforward representations of the world out there. Instead, they constitute new, hybrid subjects (Haggerty, 2006). Consequently, making observations does not entail the creation of an overview of everything from nowhere, or doing 'a god trick' (Haraway, 1988, p. 581). In fact, in most control rooms operators make detailed observations by seeing as little as possible, because this is the only possible way to make sense of a complex world. In their study of 'oligopticons' in Paris, Bruno Latour and Emile Hermant (2006) show how observatories, marketplace coordinators, and police control rooms exclude most of the world in order to visualise what is relevant to them.

Surveillance practices are easily disturbed, because the various devices involved in making something visible may not act together (Dubbeld, 2005; Gad & Lauritsen, 2009). For example, Gad and Lauritsen show how fishermen might not be detected by radar, because

they found a way to block the signal. This is not to say that successful observations depend entirely on 'lucky circumstances' in which everything comes together. The notion of situatedness refers to the ways in which surveillance is embedded in specific artefacts, contexts and routines. In surveillance, visions are often constituted by professional groups. It is a skilled practice drawing on collective experiences, the trained use of artefacts, peer-to-peer negotiations, hierarchical relations, narratives, professional identities and tacit knowledge (Grasseni, 2007). As Cristina Grasseni suggests, these located practices are part of the negotiations that take place between standardisation (for example, Latour, 1990) and individual subjectivities (for example, Norris & Armstrong, 1999).

In the following I study surveillance as a professional practice that results in the performance of various contextual logics. As John Law (1992) argues, logics or strategies emerge from practices in which artefacts and humans take part, as opposed to practices that are imposed as 'top down' power mechanisms. I start out with an account of the contextual logics of supermarket surveillance before the start of the facial recognition pilot. Next, I show how facial recognition was meant to reorder surveillance practices to perform a different logic of surveillance that included the mobilisation of the supermarket to monitor a more broadly defined target population. Finally, I argue that in this case, the new artefact did not lead to the introduction of this ideal logic.

The logics of supermarket surveillance: Collecting strikes and care

The context: Anarchy in the supermarket

In the supermarket that is the subject of this case study,[3] the employees had adapted their surveillance strategies and routines to their local situation. The supermarket was generally thought of as a problematic site, where a disproportionate amount of stealing took place. This supermarket was located in the city centre, where it welcomed tourists, business people and other temporary visitors, as well as local residents. The employees felt they had little control over theft, because of the large surface of the store, the high number of visitors and the high racks that blocked their lines of vision in the store. A team of eight private security officers, working in shifts of two or three, were tasked with keeping order in the store.[4]

The supermarket was surrounded by a square known to local police officers as a site where drug dealers mixed with addicts, homeless people, tourists and locals. The security officers and the supermarket's local management regarded the group of people that often resided on this square as the supermarket's main source of nuisance. Commonly referred to by local management and employees as 'the community'[5] or 'the culture out there', this group was perceived as a constant threat to the supermarket. Accordingly, the official task of the guards was to 'prevent a state of anarchy in the supermarket'.[6] The security officers were instructed to prevent and detect shop crime in addition to their general task of making the employees and customers feel safer. In 2004 the supermarket implemented a banning order policy, comparable to the Anti-Social Behaviour Orders in the UK (see Donoghue, 2008). The banning order is essentially a means of local governments to reduce police intervention, because it allows the store's employees to impose the banning order themselves, provided they call in the police when they have arrested a suspect for theft or nuisance.[7] Individuals that break the house rules can be banned from the store for a year. Among this supermarket's house rules were: a prohibition of theft, harassment and substance use, but also the obligatory use of a shopping cart, a prohibition to eat inside the store and the obligation to follow staff instructions.[8] When a person with a banning order would attempt to enter the store again and refuse to leave, he or she could be arrested for trespassing domestic premises.[9] The banning order policy of this supermarket was very strict; every case of shop theft or misdemeanour

was followed by a banning order, even when the item stolen was only worth 50 cents.[10] For the supermarket the issue was not the value of the stolen products, but the repeated acts of shoplifting by some individuals at this location. The local manager expressed the problem of petty theft as follows: 'The incidents themselves are small, but what is small if you do it all the time? It becomes serious, as if somebody kicks you in the shins a thousand times'.

The logic behind this strict policy was that known shoplifters would 'collect strikes'. Local management and the supermarket's private security officers had set out to arrest 'their' thieves as often as they could, each arrest resulting in a strike. According to a national act that was passed at the time (the ISD Act), the more often a person is arrested and taken to the police station, the more likely this person will be detained for a longer period of time.[11] As a consequence, individuals that repeatedly commit minor offences can be detained for two years, whereas before they could only be 'kept of the streets' for a short period of time. In the supermarket, the shop ban was interpreted within the framework of the ISD Act. Collecting strikes within this framework was thought of by the supermarket's local management and security employees as the only effective method of diminishing crime and harassment, because offenders would be imprisoned for a longer period of time. In practice, this approach meant that the primary goal of the security officers was to catch as many thieves as often as possible, as opposed to preventing theft.

The collective work of detecting thieves

The logic of collecting strikes was the logic performed by the objects, knowledge, regulations and people in the supermarket in order to detect and arrest particular types of shoplifters. In this section I will take a closer look at the collective that performed this logic and the target groups that were watched. The primary focus of supermarket surveillance was to catch people in the act of stealing. In the supermarket, theft was only a fact when an individual passed the cash register without paying for an item. The security officers spent most of their days studying CCTV images. When the guards found a potential shoplifter, they followed their suspect's actions with several cameras. If they observed a person stealing, they followed this person until he or she had walked past the cash register, which allowed them to record the theft on video tape. Only then did they exit the control room, conveniently placed next to the cash register, and arrest the suspect. The supposed offender was then taken to a tiny cell next to the control room, where they photographed the suspect, registered his details and issued a banning order.

Various objects played a part in detecting theft. From a control room in the supermarket, security officers studied the monitors that displayed CCTV images. The store used 32 cameras, of which seven cameras belonged to a CCTV network that allowed for manually zooming in and out and changing the angle of view. Black-and-white photos of known offenders were attached to the wall. These photos showed individuals that were banned from the store, and were made by the private security officers using mobile phones. Underneath the photos, the guards had made handwritten notes of their names and possible risks (aggressive behaviour, for instance). In addition, fifteen colour photos showed the most notorious local offenders as defined by the police. These photos were given to the guards by the local police station. Furthermore, the security officers used paper files with information about the banned individuals and the circumstances in which they were banned. These files were used for a longer duration than the legal term of one year, in case the guards needed information about persons that had received a banning order more than a year ago.

Monitoring was done partly by the acquired skill of swiftly switching between the screens and by changing the camera's angle with a joystick. In addition, the security officers used their professional knowledge to detect suspect behaviour. In general, the practices of the guards focused on two target populations, each requiring a separate set of skills, knowledge

and devices to be identified. First, the guards tried to detect 'normal people that steal', or the Shoplifter/Normal person. The security officers acted on the principle that 'everybody steals': a thief does not necessarily look like a thief. This was a difficult task, and consumed most of the security officers' working hours. They were taught what to look for by their colleagues and through their professional education. While operating the cameras, the guards searched for suspicious behaviour, such as nervousness and hesitation. In addition, they paid attention to a number of markers, such as ragged clothing or a 'tourist outfit'. No strict guidelines existed, however. The guards did not only focus on individuals, but also paid close attention to the goods on the shelves. If a large stack of products suddenly went missing, this was a clue to search for suspect activity. The security employees made sure the cameras were not blocked, pointed at the goods in the right angle and that the grocery clerks continuously replenished the shelves. As a ground rule, the expensive products had to be placed at strategic places far away from the exit of the store and in view of the cameras.

Second, the guards kept an eye out for familiar faces, or the Shoplifter/Risky individual: those with a banning order and members of 'the community' that often loitered on the square just in front of the supermarket but were not necessarily banned from the shop. As the guards mentioned, their interaction with this group resembled playing 'cat and mouse games'. The guards pointed these individuals out to each other and they observed them from the doorpost of the store, occasionally having a chat with them. Because the guards worked in other supermarkets in the city, they also knew about the activities of this group in other places. This interaction worked both ways, however: the men and women in this group had supposedly also learned about the routines of the security officers and used this knowledge in their attempts at shoplifting.

Next to the logic of collecting strikes, the target group of Shoplifters/Risky individuals was important for the enactment of a second logic of surveillance of the security guards: care. At this location, the guards frequently experienced aggression and threats. To prevent future risks to their colleagues, they used photos, notes about earlier behaviour, outdated files and stories as resources of information. Updating each other on the group of Shoplifters/Risky individuals was essential, because in the guards' experience the appearances of people that live on the streets could change fast, e.g. they could gain or lose weight quickly.

Interaction with the police

To summarize, the supermarket's surveillant was a hybrid of the security guards, their knowledge of risky individuals and suspicious behaviour, cameras, paper files, photos and legislation. In addition, the guards organised the physical environment of the supermarket to ensure maximum visibility. They used their resources in line with the target populations they wanted to identify according to the logics of collecting strikes and care. With regard to the relation between the supermarket security team and the police, police interference in determining the target population had been limited to the supply of fifteen colour photos of police registered shoplifters.

The police, however, wanted to cooperate with the security guards more closely. Privacy regulations did not allow for sharing more police information with the supermarket, but local police officers were eager to expand the guards' activities to a wider target group of frequent offenders in the area around the supermarket. The police tried to motivate the security guards to keep an eye on 'the community' on the square and to report suspect activity to the police. At the same time, the police attempted to limit the guards' activities with regard to policing, repressive actions and the use of methods beyond their competences, such as the use of threat. Instead, their aim was to make sure the security officers complied with government guidelines on the use of the banning order, which included only limited

monitoring, preventive and proactive behaviour, approaching a suspect *before* he or she walks past the cash register and a minimum use of threat.[12]

In contrast, the security officers preferred the opposite situation: they refused police interference with their target populations and operated within the grey areas of what was permitted for private security officials. With regard to their target group, the guards defined the problem of shop crime as 'the outside coming in': problems in the world outside of the supermarket, like drug addiction, were considered causes of shop theft and nuisance. The security officers regarded these outside problems as police responsibilities and demarcated their area of activity at the entrance of the supermarket. At most, they watched the square from the doorstep of the supermarket. On busy days, they would drench part of the square with water to make sure that people would not 'hang out' there.

As for their methods of surveillance and policing, the supermarket security guards used the undefined rules of working in what they called a 'semi-public space' to their advantage. Not being tied to a strictly enforced code of conduct, as the police is, gave them a degree of freedom in tackling the diverse, and sometimes legally undefined, problem of shop crime. For example, issuing banning orders required that the security employees take and store photographs of the arrestee.[13] To do this required permission of the suspect. The guards would trick the arrestee into giving permission by using fake arguments ('otherwise we will call in the police' – which they would do regardless). Furthermore, the security guards were not allowed to search bags, but according to their own accounts, they would sometimes use threat to obtain permission. Thus, in terms of the surveillance of their target groups and the surveillance and policing methods used, the guards refused to become an 'extension of the police'.

Introducing facial recognition

Designing the system: One store, two databases

Facial recognition introduced an automated method to detect shoplifters. During the pilot, camera-captured, real-time images of the entrants were compared to a database with 'mug shots' of individuals that had received a banning order from the supermarket in the past year. The basic principle of this technology was feature extraction: the measurement of the distances between various facial points, for example the distance between the eyes.[14] This technology would ultimately establish a match between the algorithm that expressed the characteristics of the entrant and an algorithm in the database.[15] This was, and is, a challenging operation in an unregulated environment where people might suddenly turn their faces and where light conditions vary (Philips et al., 2005). Therefore, a match can never be established with a 100 per cent certainty. In the supermarket application, the match that was statistically most likely to be correct was presented to the supermarket employees.

In the eyes of the city and regional police management, facial recognition addressed a complaint about the banning order that the city was often confronted with: retailers simply had no time to be on the lookout for people with a banning order, and were unable to recognise them after a few months had passed. But this project did not only offer a tool to alert shop owners to the presence of the people to whom they had issued banning orders. The facial recognition system was also connected to a second database of police-registered frequent offenders.[16] The police database contained photos of individuals who had been repeatedly arrested for minor offences in the past years. It was composed of 1250 frequent offenders in the region who had been convicted for shoplifting at least once, in some cases in addition to other offences.[17] Some of these men and women might have been registered by both the shop and the police, but a check for double entries was not made. This second

database was exclusively police property. The hard disk was situated at the police station, and could not be searched by supermarket staff. Only when the system established a match between an individual in the supermarket and a police-registered offender would the photo and name be revealed to the supermarket employee on a hand-held palmtop.

As a result, new target groups were introduced to the supermarket. Ideally, this surveillance practice would focus on the frequent offender database in addition to the supermarket database of banning orders. The use of police information by private actors was presented as the main innovative feature of this project. Alongside its presumed usefulness on the shop floor, the inclusion of a frequent offender database legitimated the city's financial investment in this project. The local government was not allowed to invest in a project that only benefited the retail sector; the public good needed to be served as well.[18] The group of frequent offenders was generally held responsible for a variety of minor offences that affected the general public, like loitering and pick pocketing (Ferwerda et al., 2003). Connecting the supermarket to a frequent offender database would therefore not only solve a problem in the retail sector, but also contribute to decreasing disturbances caused by a group that was considered a societal problem.

As I argue here, this technology served as more than a practical tool. Facial recognition was designed to reorganise the collective of humans and artefacts so as to implement a new logic: 'deterrence'. In the following I will show that this logic involved another type of surveillance, in which the security officer would function as a host, carry more responsibility for preventing shop crime and monitor a larger target group.

A new logic: Deterrence

The logic of facial recognition was meant to introduce a new mode of operation in the supermarket. Starting in 2001, Dutch police had been trying to implement the deterrence (*tegenhouden*) method.[19] Working according to this concept required 'prevention before the preventive phase' (Raad van Hoofdcommissarissen, 2001). Facial recognition would be an instrument for deterrence, because it was not meant to catch people in the act of stealing, but to facilitate a proactive approach to shoplifting. As one of the policy advisors involved in the facial recognition pilot stated:

> 'It isn't some sort of sneaky camera that catches you in the act. That absolutely isn't the goal of this project, absolutely not. It's purely an instrument for deterrence, an instrument that empowers the shopkeeper to actively approach or stop a potential shoplifter. And when you stop it, it hasn't happened, it won't require any negative energy.'

The prevention of crime through proactive behaviour was to be a task of citizens and private organisations. While the paper banning order was an important means to accomplish this in retail crime, the retail sector continued to use its own methods rather than act in accordance with the banning order guidelines.

Facial recognition was intended to introduce a new order of surveillance into the supermarket that would redefine the security officer's work practices. First, as one of the city's policy officers put it, facial recognition was a 'sneaky method' to extend the knowledge of shopkeepers beyond the records about known offenders they kept themselves. The technology would bring a new target group of police-registered frequent offenders into the supermarket, without its explicit consent. Consequently, it would direct the gaze of the supermarket guards towards people and types of crime that they regarded as police responsibility. Second, the security officer would play the part of host to his customers. Third, surveillance would serve not to arrest, but to identify and establish contact with a person. The

supermarket's security guards would no longer wait until an item had actually been stolen, and consequently would not have to call in the police. A policy officer described the ideal mode of operation as follows:

> 'When somebody with a banning order walks in, an active strategy of guided shopping should be applied. This is to say you approach the person and request him to leave the shop, and only when this doesn't work, the police can be called in to make an arrest for trespassing …. As for the frequent offenders, if everything works as planned, you will not tell them: "you cannot shop here" or "oh, you're a frequent offender". No, as a security officer you will learn "that's a frequent offender, the police knows him, maybe I should get to know that person too", and you will actively remove this person out of the sphere of anonymity by suggesting to use a shopping basket, or by notifying him of discounts, walking along with him, or whatever. This will make this person think: "I'm not anonymous anymore, I'm being watched".'

Whereas the logics of collecting strikes and care required the use of CCTV images, knowing the local target group and operating in semi-legal domains, deterrence introduced a new organisational principle that required another type of surveillance. According to this approach, the security officers would no longer stay in the control room, but would be alerted to the target groups in the databases. Consequently, the target group categories of Shoplifter/Normal person and Shoplifter/Risky individual would be replaced by the new categories of Shoplifter/Banning order and Shoplifter/Frequent offender.

Facial recognition as a reordering device

In the following, I elaborate further on how the technology was used to mobilise the supermarket in the surveillance of a more broadly defined area of petty crime. In the first place, facial recognition offered the opportunity to share police information while complying with privacy regulations. According to the Police Registration Act,[20] sharing police data was only allowed under very strict conditions, including: a contract between public and private actors; timely deletion and updating of information; using the information solely for the purpose of crime control; and an inability of the police to solve the problem without interference of third parties (Internal report, 2005a).[21]

With regard to police-registered frequent offenders, the supermarket was already given fifteen colour photos and names of the most notorious frequent offenders in the neighbourhood known to the police. This was a very laborious method, however, because the paper photos had to be updated regularly and the police had to ensure that the information would not leave the premises of the supermarket. As a matter of fact, at the time of research this method was under debate in light of a court ruling against the use of card games and placemats with frequent offender photos in police canteens.[22]

Meanwhile, the police and the city were still eager to communicate about its risk groups with the retail sector. Facial recognition was thought to solve the problem, because it would only display information upon recognition, and the frequent offender database would be updated automatically. Consequently, this technology was regarded as an improvement of privacy. As a policy officer of the city's safety department stated:

> 'That [the frequent offender card game] was eventually forbidden by the Central Office for Personal Data, because a card game is made of paper and will just exist for ever …. And what we have now, the interesting thing about it is that we have a database that is not accessible for the retailer, he will only be presented a photo when the frequent offender enters the store and is recognised. He only knows what he looks

> like; he does not know his name, what he has done. He only knows: "watch out" …. So this database is also a black box for the retailer, he cannot snoop around in it. In comparison with paper this is an absolute improvement of privacy.'

Moreover, the signing of a contract stating that police information about frequent offenders could be shared on the basis of the Police Registration Act created a new basis for the use of paper posters. The policy staff of the police and the local government argued that if humans would update as rigorously as the computer and if the police would make sure that the paper files are stored in a safe place, there would be no obstacles to the large-scale use of police posters by the retail sector.

Furthermore, facial recognition could provide a legal basis for these practices by provoking a court case. During the pilot, the police hoped for a lawsuit on the issue of the production and storage of photographs. To this day, the quality criteria for the use of photos for automatic recognition and their storage in a database remain undefined. As a police participant to the project stated: 'a court ruling would give us all guidelines'. Facial recognition was expected to lead to a court case, because it was thought to provoke questions about the trustworthiness of the method, for example regarding the quality of the police photos and their suitability for automatic recognition. So far, no lawsuit has been filed against this practice or similar applications that make use of facial recognition.

On top of its interaction with privacy regulations, another issue concerning facial recognition was that it required a large number of entries to become effective, even in a pilot situation. In the early phases of the project, however, it was stated that the target group should be defined very strictly. Only 'very active frequent offenders', individuals that had gathered eleven or more police records in the previous five years, including one in the previous twelve months, would be admitted to the database.[23] The supermarket furthermore stated that it would not accept database entries of persons who had been convicted for violent acts, because it did not want to expose its security employees to potential harm.

Yet, when the police finally compiled the databases, these arguments were superseded by the argument that the technology 'needs hits', as the head of the project group that defined the target group explained. The chances that the technology would recognise somebody from the database would have been too small if it had only contained the fifteen individuals that the police registered for this area. To increase the chances of recognition, the criteria of admission to the database were relaxed. In the end, the police database included 1250 multiple, frequent and very frequent offenders from the region.[24] The minimum offence was one case of shop theft in the last twelve months and two police records in a lifetime. [25] Ultimately, no check for a violent background was included. So in order for the technology to work, it needed to include persons with a minimum of two offences in a lifetime, instead of eleven, notwithstanding the nature of the offence.

This suggests that facial recognition should not be considered as a neutral technology that simply links new actors to a network. By evading legal restrictions on the use of paper, this application would enable a reconfiguration of surveillance practices towards a logic of deterrence. In the ideal scenario the security officer would use a database of police information and would assert his presence on the shop floor as a host, thereby employing different monitoring skills than used in the logics of collecting strikes and care. In addition, the technology had a logic of its own. It needed hits and so required an enlarged target group, leading to a quantitative and qualitative redefinition of crime to be addressed by the supermarket. This way the supermarket became involved in the surveillance of petty crime beyond the store's doorstep. Therefore, the technology is not only a means to further implement the shop ban but it can also be a reordering device for crime control.

A favour that was not asked for

As a reordering device, however, facial recognition was subject to resistance. Also, it was put to use in unexpected ways. After a year of testing, the city council decided against funding the development of this application any further, because it was disappointed with the results of the pilot. During 161 measurement days four persons were recognised by the technology, so the evaluation report said. In reaction to this result, the local government stated that human recognition appears to be more effective, as the security officers arrested ten individuals with a banning order who remained undetected by the technology.[26] The consultants that supplied the technology disagreed. They claimed that these numbers were being misinterpreted; according to them, the technology itself worked well. In their view, the reason why a person with a banning order might not have been detected was because the security officers arrested him just before he walked into the camera's view. According to one of the consultants, this happened quite regularly due to the familiarity of the guards with their target group. Some homeless people might even approach the guards in order to be arrested, and obtain a place to stay for the night.[27]

The consultants` explanation indicates that this pilot is more than a story about technical failure. Even though this explanation may not fully account for the results of the pilot, they rightly observed that the old logics of surveillance had not been changed by the introduction of facial recognition. This suggests that the use of surveillance technologies does not necessarily lead to the pluralisation of policing and surveillance. In this case, the security officers held on to their old target groups: the Shoplifter/Normal person and the Shoplifter/Risky individual. The new databases of respectively the Shoplifter/Banning order and the Shoplifter/Frequent offender could not replace the advantages of the security officers' contextualised knowledge, because they only referred to the type of registration and not to local knowledge and experience. Consequently, these categories were unable to contribute to the performance of the logics of collecting strikes and care.

Moreover, the security officers and lower-rank management were simply not convinced that the logic of hosting would be an effective one for their target group. The guards were furthermore not interested in recognising individuals that were registered by the police for shoplifting and other offences in places other than their own supermarket. This would introduce the problems of the 'outside world' into the supermarket, so they claimed.

Nevertheless, the guards did think that some features of the technology were potentially useful. First, they reckoned that if the system had recognised more individuals, it could have helped to identify one of their target groups: the Shoplifter/Normal person. The guards argued that 'normal persons' that steal are difficult to recognise, so this is where facial recognition would have been useful. The guards did mention, however, that this would not solve the entire problem, because the technology 'does not recognise thieves', i.e. it cannot observe suspicious behaviour of people that are not part of the database. Second, the guards appreciated the system's computer as an administrative tool, helping them to store and browse their files.

Higher management at the supermarket head office also appreciated the technology in another way than planned. From the beginning, higher management felt uneasy about observing its own customers using facial recognition. It had nevertheless consented to the pilot, because it wanted to maintain good relations with the police and local government. Yet in the end the supermarket expressed its interest in using a smart camera system to monitor its goods, rather than its customers. As shown earlier in this paper, the visibility of products plays an important role in supermarket surveillance. Therefore, the supermarket's security department thought it would be more interesting to know if the technology could be used to

alarm the security guards when, for example, a large amount of toothpaste has disappeared from the racks. After the pilot project had officially ended, the supermarket and the consultant continued to test smart camera systems in the laboratory for the recognition of objects.

Conclusion

In this paper, the pluralisation of surveillance and policing was approached through the notion of situated surveillance, in which the articulation of the subject is understood as the outcome of a heterogeneous collective of objects and humans. I first described the logics of surveillance that were performed by the collectives in which the security officers of the supermarket took part: the logic of collecting strikes and the logic of care. The security officers used various artefacts and types of knowledge to monitor two target groups: the Shoplifter/Normal person and the Shoplifter/Risky individual. Moreover, the supermarket security guards carefully kept their distance from policing activities.

The facial recognition application observed in this case study was designed to implement an ideal type of crime control, according to the logic of deterrence. By sharing police knowledge, the supermarket would be mobilised to engage in a preventive mode of operation. On the one hand, police intervention would not be required as often and, on the other hand, the security guards would become an extension of the police surveillance of frequent offenders. Facial recognition was thus far from a neutral technology; it was designed to further involve the supermarket in the surveillance of petty crime. It could do so by adapting and evading privacy regulations, in order for the Shoplifter/Frequent offender to be observed by the supermarket's security officers. Moreover, the technology itself demanded an enlarged database of offenders that served to change the target groups of the supermarket.

Although facial recognition could potentially intervene in the relations between the various actors involved in monitoring shop crime, the technology could not be implemented in existing practices. This case consequently shows that it is crucial for those that study surveillance to attend to context and agency in order to understand how and why surveillance technologies may be resisted and adapted. The surveillant assemblage rightly draws attention to the diversity and multiplicity of actors that are pulled into networks of surveillance. What is more, Ericson and Haggerty usefully suggest that technology plays a role in drawing the actors together. However, by assuming a decontextualised logic of surveillance, the exact nature of the processes whereby new actors are drawn into surveillance networks cannot be fully understood. At times, configurations may be far from fluid. Instead, they can be rather viscous and resistant.

As M'charek (2008) argues, the manner in which technologies link actors and articulate suspects depends on the context of usage. This case study highlights several particular ways in which context plays a role. First, the interaction of the surveillants with their target group, 'the community', was an important aspect of the logics of collecting strikes and control. Thus, the surveillant is partly constituted by its subjects. Second, we learn that the mobilisation of new actors is also a process that can include resistance. Third, the notion that technologies never implement ideal strategies in a top-down fashion (Law, 1992) is illustrated by the renewed efforts of the supermarket to use a smart camera system for monitoring goods. In the practices of the surveillance guards, the products were also an important focus for surveillance.

An important critique of facial recognition is that the technology can contain a built-in preference for the recognition of certain ethnic groups over others. If applied in practice such (presumably unintentional) technological biases may be enforced by the existing discriminatory practices of the surveillants (Introna & Wood 2004). By assuming a focus on

the context of the surveillants' practices, I add another direction of critique to this concern. It should also be recognised that surveillance strategies emerge from coping with a complex situation. In this case shoplifting is part of a larger problem that includes poverty, homelessness and drug addiction. Policies that implement new regulations and technologies often act on simplified notions of the situation at hand, offering technological fixes that aim to trick new surveillants into assuming more tasks, while creating new grey areas of regulation at the same time. Taking into account the complexity of surveillance practices and how technologies affect these practices may open up new directions for analysis and critique.

References

Akrich, M. (1992). The de-scription of technical objects. In W. E. Bijker, & J. Law (Eds.), *Shaping technology/building society: Studies in sociotechnical change* (pp. 205-224). Cambridge, Massachusetts: MIT Press.

Board of Chief Commissioners (2006). *The police in evolution: Vision of policing*. The Hague. Retrieved April 11, from http://www.politie.nl/ImagesLandelijk/the%20police%20in%20evolution_tcm31-339858.pdf

Boutellier, H. (2002). *De Veiligheidsutopie. Hedendaags onbehagen en verlangen rond misdaad en straf.* Den Haag: Boom Juridische Uitgevers.

Callon, M. (1986a). Some elements of a sociology of translation – Domestication of the scallops and fishermen of St. Brieuc Bay. In J. Law (Ed.), *Power, Action, and Belief – A New Sociology of Knowledge* (pp. 196-233). London: Routledge and Kegan Paul Books.

Callon, M. (1986b). The sociology of an actor-network: The case of the electric vehicle. In M. Callon, J. Law & A. E. Rip (Eds.), *Mapping the dynamics of science and technology* (pp. 19-34) MacMillan.

Deleuze, G. & Guatarri, F. (1987). *A thousand plateaus.* Minneapolis: University of Minnesota Press.

Den Boer, M. (2004). *Out of the blue: Police perspectives on Europe, governance and accountability*. Amsterdam & Apeldoorn: Vrije Universiteit/Politieacademie.

Donoghue, J. (2008). Antisocial behaviour orders (ASBOs) in Britain: Contextualizing risk and reflexive modernization. *Sociology, 42*(2), 337-355.

Dubbeld, L. (2005). The role of technology in shaping CCTV practices. *Information, Communication & Society, 8*(5), 84-100.

Ferwerda et al. (2003). Veelplegers. *Tijdschrift voor Criminologie*, *2*(45), 110-118.

Foucault, M. (1995). *Discipline and Punish: The birth of the prison.* New York and Toronto: Random House.

Gad, C., & Lauritsen, P. (2009). Situated surveillance: An ethnographic study of fisheries inspection in Denmark. *Surveillance and Society, 7*(1), 49-57.

Gates, K. (2010). The Tampa "Smart CCTV" experiment. *Culture Unbound, 2*, 67-89.

Grasseni, C. (Ed.). (2007). *Skilled visions: Between apprenticeships and standards*. New York and Oxford: Berghahn Books.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology, 51*(4), 605-622.

Haggerty, K. D. (2006). Tear down the walls: On demolishing the Panopticon. In D. Lyon (Ed.), *Theorizing surveillance: The Panopticon and beyond* (pp. 46-68). Devon, UK: Willan Publishing.

Haraway, D. (1988). Situated knowledges: The science question in feminism and the privilege of partial perspective. *Feminist Studies, 14*(3), 575-599.

Helten, F., & Fischer, B. (2004). Reactive attention: Video surveillance in Berlin shopping malls. *Surveillance and Society, 2*(2/3), 323-345.

Introna, L. D., & Wood, D. (2004). Picturing algorithmic surveillance: The politics of facial recognition systems. *Surveillance and Society, 2*(2/3), 177-198.

Koops, B.J. (2011), The evolution of privacy law and policy in the Netherlands. *Journal of Comparative Policy Analysis: Research and Practice, 13*(2), 165-179.

Latour, B. (1990). Drawing things together. In M. Lynch, & S. Woolgar (Eds.), *Representation in scientific practice* (pp. 19-68). Cambridge, Mass. and London: MIT Press.

Latour, B. & Hermant, E. (2006) *Paris: Invisible City*. Retrieved November 11, 2010, from www.bruno-latour.fr/livres/viii_paris-city-gb.pdf

Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems Practice, 5*(4), 378-393.

Loader, I. (2000). Plural policing and democratic governance. *Social and Legal Studies, 9*(3), 323-345.

Lyon, D. (2007). *Surveillance studies: An overview*. Cambridge: Polity.

MacGillavry, E. C. (2005). Heeft u even voor de nieuwe wet politiegegevens? In A. Harteveld, D. H. De Jong & E. Stamhuis (Eds.), *Systeem in ontwikkeling, liber amicorum* (pp. 385-416). Nijmegen: Wolf Legal Publishers.

Marx, G. T. (2002). What's new about the new surveillance? Classifying for change and continuity. *Surveillance and Society, 1*(1), 9-29.

M'charek, A. (2008b). Silent witness, articulate collective: DNA evidence and the inference of visible traits. *Bioethics* 22(9), 519-528.

Norris, C., & Armstrong, G. (1999). *The maximum surveillance society: The rise of CCTV*. Oxford: Berg.

Philips, J.P. et al. (2005). Overview of the Face Recognition Grand Challenge. *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)*, 1, 947-954.

Prainsack, B., & Toom, V. (2010). The Prüm regime. Situated Dis/Empowerment in

transnational DNA profile exchange. *British Journal of Criminology, 50,* 1117-1135.

Raad van Hoofdcommissarissen (2001). *Misdaad laat zich tegenhouden. Advies over bestrijding en opsporing van criminaliteit.* Retrieved April 11, 2011, from http://www.politie.nl/ImagesLandelijk/misdaad%20laat%20zich%20tegenhouden_tcm31-66184.pdf

Rose, N. (2000). Government and control. *British Journal of Criminology, 40,* 321-339.

Schuilenburg, M., & Van Calster, P. (2009). De collectieve winkelontzegging: Een antwoord van willekeur op overlast. In H. Boutellier (Ed.), *Omstreden ruimte. Over de organisatie van spontaniteit en veiligheid* (pp. 137-155). Amsterdam: Van Gennep.

Smith, J. D. G. (2004). Behind the screens: Examining constructions of deviance and informal practices among CCTV control room operators in the UK. *Surveillance and Society, 2*(2/3), 376-395.

Van Steden, R. (2007). *Privatizing policing: Describing and explaining the growth of private security.* Den Haag: Boom Juridische Uitgevers.

Van Stokkom, B. (2009). Verwijderd van de straat. Over veiligheid door gebiedsverboden. In H. Boutellier (Ed.), *Omstreden ruimte. Over de organisatie van spontaniteit en veiligheid* (pp. 99-118). Amsterdam: Van Gennep.

Footnotes

[1] As Ronald van der Steden (2007) points out, the famous seventeenth-century painting *The Night Watch* by Rembrandt van Rijn portrays a group of guards that operated independently from the state.

[2] Gad and Lauritsen have adopted the original concept from Michel Callon (1986a) to denote a mode of analysis in which a search for general theory is replaced by a renewed focus on practices.

[3] In order to protect the identity of my informants, I refrain from mentioning the location of the pilot and the names of the organisations and persons that I interviewed for this paper. Moreover, citing the full titles of some policy documents and internal reports would reveal the names of the location and the involved organisations. In these cases, I do not cite the full reference in the bibliography. Instead, I refer to the type of document in the footnotes.

[4] This paper is based on fifteen in-depth interviews and twenty-eight hours of observation between April 2006 and February 2007. Also, I had access to project plans and reports. This information was complemented with policy documents and the minutes of city council meetings on this pilot. The interviews include conversations with all members of the project group that designed and executed the pilot (police, public prosecutor, local government, technology consultant); the local manager of the supermarket where the pilot was performed; the supermarket's higher management; and city councillors. The average length of the interviews was 90 minutes.

The observations include three visits to technology tests (twelve hours in total) at the supermarket, and two visits to the control room of the private security officers (two working days or sixteen hours). My aim was to gain an understanding of the security officers' routines by interacting with them in a setting they felt comfortable in and where they were the experts, as opposed to a more formal interview situation. Being in the control room also provided me with an insight into the various documents and tools the security officers use, and into the space they operate in.

[5] All quotes are translated from Dutch by the author, unless mentioned otherwise.

[6] Work manual private security guards, 2004 (internal document).

[7] In 2007, shop banning orders were only valid for individual supermarkets. At the time, this city had not yet introduced the collective banning order. For an analysis of the collective banning order, see Schuilenburg and Van Calster (2009).

[8] Work manual private security guards, 2004 (internal document).

[9] Dutch Code of Criminal Procedure, Article 53.

[10] Official reports on the number of banning orders that the supermarket imposed does not exist. The supermarket security guards and the manager estimated that one or two persons were arrested every day and police arrests for disturbance of domestic peace were carried out about five times a month. In contrast, a regular supermarket in a small town issued only one or two banning orders annually. The current arrest rate is, however, still a vast improvement over the estimated figure of forty arrests in one week before the implementation of the new banning order policy.

[11] ISD Act (*maatregel Inrichting Stelselmatige Daders*), Dutch Code of Criminal Procedure, Article 38m through 38u.

[12] Police information for local retail, police document, 2007.

[13] Police information for local retail, police document, 2007.

[14] Feasibility study of the project, technology consultant, 2005 (internal document).

[15] The significance of the match is based on a comparison with a mean algorithm of the population. For a description of the status and operation of this technology at this time, see Introna and Wood (2004).

[16] Final draft of the project plan, technology consultant, 2005 (internal document).

[17] Different definitions of the frequent offender circulate in policing practices in the Netherlands. In its most general definition, a frequent offender is a person that commits offences on a regular basis, ranging from non-violent offences to violent robbery. This group of offenders is thought to have a disproportional influence on crime rates. In this case, the minimum threshold for the database was one police record of shop theft in the previous twelve months and two police records in the individual's lifespan. The information was retrieved from the EDISON (*Electronisch documentatie informatie systeem voor opsporingnetwerk*) police database. It should also be noted here that like any category or label, the category of 'frequent offender', can be highly problematic. Here, I use the terminology that I encountered during my fieldwork. Although opening up this category (and indeed other categories used in crime control) for discussion would be a highly legitimate project, this is beyond the scope of this paper.

[18] Final draft of the project plan, technology consultant, 2005 (internal document).

[19] I follow the national Dutch police force in using the term deterrence as the English translation for *tegenhouden* (Board of Chief Commissioners, 2006).

[20] The Police Registration Act (*Wet politieregisters*) was replaced by the Police Data Act (*Wet politiegegevens*) in 2008. This did not affect the pilot discussed in this paper. For an analysis of the new legislation see MacGillavry (2005).
[21] Feasibility study of the project, technology consultant, 2005 (internal document).
[22] Local newspaper article, published on October 9, 2004.
[23] Final draft of the project plan, technology consultant, 2005 (internal document).
[24] Various categorisations of frequent offenders existed in Dutch crime policy during my fieldwork period. The categories used by my police informants in this case study were: 1) the first offender: one offence in a lifetime; 2) the multiple offender: two to ten police records in a lifetime, of which one record in the previous twelve months; 3) the frequent offender: more than ten police records in a lifetime, of which one record in the previous 12 months; 4) the very active frequent offender: more than ten police records in the previous five years, of which one record in the previous twelve months.
[25] I use the term 'police record' here to refer to the *proces-verbaal*. In Dutch criminal law, the *proces-verbaal* is used as a unit to measure offences. A *proces-verbaal* refers to the police document that reports the nature and details of the offence, the offender and the testimony. This document can report one or more offences. Nonetheless, in the administrative systems of the police the number of *proces-verbalen* is often equaled to the number of criminal records.
[26] Letter from the mayor to the councillors about the evaluation report, 2008.
[27] Press statement of one of the project's corporate consultants, 2008.