Discrepancies between technology and legitimacy assumptions in the practice of public mobility surveillance

Paper presented to

The European Group for Public Administration (EGPA) Study Group on Information and Communications Technologies in Public Administration,
26 to 28 August 2015, IEP, Toulouse, France

Charlotte van Ooijen[1]

Centre d'Études et de Recherches de Sciences Administratives et Politiques (CERSA)
CNRS – Université Panthéon Assas | Paris II

Keywords:
Surveillance – Mobility – Legitimacy – Risk citizens – Social sorting

Abstract Mobile citizens attract the attention of government in various policy domains, such as traffic management, tourism, emergency services and policing. Government increasingly uses surveillance technologies, like GPS, mobile phones and automatic number plate recognition to collect geographical, temporal and personal data about citizens, in order to monitor and control this mobility. This paper addresses the question to what extent the legitimation of this public mobility surveillance is in line with the technological perceptions in the policy practice. The analysis of a case study in policing and one in traffic management suggests that a mere focus on privacy provides government agencies with insufficient means to collect and process mobility information about citizens in a legitimate way. Government should focus more attention on the grounds and procedures for the selection and definition of risks and groups of risk citizens.

1. Introduction

Who is where at what moment in time? Mobility information is essential in many domains of public administration. Where is suspect X? Which known hooligans are en route to 'enjoy' tonight's football match? Which categories of vehicles are usually found around traffic jams? Government uses technologies like automatic number plate recognition (ANPR), infrared cameras and Bluetooth to collect and process mobility data about citizens in various policy domains, such as traffic management (Brimicombe and Li, 2009), tourism (Calabrese and Ratti, 2006), emergency services (Gow and Ihnat, 2004) and policing (van Ooijen and Bokhorst, 2012). The concept of public mobility surveillance covers this kind of surveillance activities (van Ooijen, 2014).[2]

[1] As of September 2015, the author is no longer attached to the CERSA and will continue her research activities as an independent researcher. Charlotte can be contacted at: charlotte@cvano.com. She works as a consultant in the Directorate for Science, Technology and Innovation of the Organisation for Economic Co-operation and Development (OECD). This paper is not an OECD publication and does not in any way reflect the views or policies of the OECD.

[2] This concept was introduced to the Dutch speaking community in the author's PhD thesis.

The way in which public mobility surveillance manifests itself in the practice of public administration, depends on the technological possibilities and limitations and the legitimacy issues as perceived by policy actors. In the policy making process[3] concerning public mobility surveillance, there are two questions to be answered:

- Which possibilities does the surveillance technology offer in policy?
- Under which conditions can the application of surveillance technology be considered legitimate?

The assumptions that policy actors hold regarding technology and legitimacy shape the practice of public mobility surveillance. However, it is questionable whether there is always a sufficient connection between the ideas about what surveillance technology can accomplish in a certain policy practice and the suppositions about what can be considered legitimate. To what extent do the technology and legitimacy assumptions underlying public mobility surveillance match with each other?

In order to analyse the legitimacy and technology assumptions in the practice of public mobility surveillance, three theoretical perspectives on surveillance are distinguished: control, interaction and precaution. Each of these surveillance perspectives contains both assumptions about technology (possibilities in policy) and legitimacy (evaluation criteria in terms of legality, normative justification and social acceptability). Consequently, two policy practices of public mobility surveillance in the Netherlands are analysed regarding their underlying technology and legitimacy assumptions. The first case study focuses on the application of Automatic Number Plate Recognition (ANPR) by one of the Dutch regional police forces. According to a policy document by this police force, ANPR is 'a technique which involves mobile or static cameras equipped with underlying software scanning license plates in the streets and matching these directly to license plate numbers in a data file, a hotlist'.[4] The second case study involves innovation in the collection and processing of mobility data by the National Data Warehouse (NDW), which is part of *Rijkswaterstaat*, the Dutch executive agency for infrastructure and mobility policy. NDW started a public procurement procedure to find innovative technologies for gathering and processing mobility data about vehicles.

An interpretive-qualitative policy analysis was conducted, revealing how policy actors perceive technological possibilities and legitimacy issues concerning public mobility surveillance. Data generating methods included observation of interactions during meetings and outside the office, interviews with stakeholders and document study (policy documents; internal and external correspondence). Data generating took place between September 2008 and April 2009 for the police case study, and between December 2009 and October 2010 for the traffic management case study.

Finally, conclusions will be drawn regarding the degree of connection between the technology and legitimacy assumptions as observed in the case studies and the implications for surveillance policy-making.

[3] In this paper, policy-making is considered to be a non-linear process in which formal decision-making at the managerial level and work floor decisions at the implementation level influence each other. In reaction to the top-down approach of policy-making, this can be called a bottom-up approach in which policy implementation is viewed as part of the policy-making process rather than a separate process (Hill, 2009).

[4] Translation by the author

2. Surveillance in theory: control, interaction and precaution

2.1 The control perspective on surveillance

The control perspective is a dominant perspective in surveillance studies. It questions how panoptic surveillance, which controls and disciplines citizens, can be legitimised while protecting citizens' privacy at the same time. 'BIG BROTHER IS WATCHING YOU' (Orwell, 1949: 2) has become the adagio of the control perspective. The story of a society in which citizens, knowingly or unknowingly conform to the will of the state has several appearances in literature: from 'surveillance state' (Taylor, Lips and Organ, 2009) and 'control state' (Vedder et al., 2007) to 'panoptic state' (Bannister, 2005). Foucault's philosophical reflection on Jeremy Bentham's panopticon is a second powerful metaphor of surveillance (Haggerty and Ericson, 2007: 105). Haggerty (2006: 25) nicely summarises Foucault's adaptation of the panopticon: 'Panoptic schemes, following Foucault, become a principal means for managing a host of different populations through the dispersion of disciplinary power more generally'.

According to the control perspective on surveillance, Jeremy Bentham's brick panopticon is transformed into an electronic superpanopticon (Lyon, 2001). Poster (1990: 93) describes the superpanopticon as 'a system of surveillance without walls, windows, towers or guards'. In this system, the physical watch tower has been transformed into a data centre. The core principle of a knowledge asymmetry upholds in the electronic version and displays two elements. First, there's still a division between those who are watching and those who are being watched. 'Each individual [...] is seen, but he does not see; he is object of information, never a subject in communication' (Foucault, 1979: 303). It is the government who watches and the citizens who are watched and not the other way around. Criminal investigators can trace citizens by means of their mobile phones. Camera surveillance can serve to keep an eye on the public in the city centre. A second element of the knowledge asymmetry is that the government knows when it is and isn't watching. Citizens can only take a wild guess whether someone is actually present in the virtual watch tower. Are the traffic cameras on or off today? Is someone listening in on my phone conversation or not? This unequal knowledge is essential for the mechanism of discipline to work. Knowledge is a means of power for the government. 'Hence the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power' (Foucault, 1979: 303). Those who are under surveillance conform to the administered norms, because they may always be checked upon. ICTs enable the government to generate more and different knowledge about citizens than before. The knowledge government desires to have about citizens, concerning who deviates in what way, can be obtained in more ways than ever.

Technology and legitimacy assumptions

According to the control perspective, surveillance technology enables government to take on the role of 'the watcher' who monitors the watched citizens for deviant behaviour (sovereign power) and who disciplines them (disciplining power). Consequently, a central issue regarding surveillance as control is how the state's power can be controlled and checked upon. Next to the focus on checks and balances, the right to privacy is a prevailing issue in literature written from the control perspective. In the words of David Lyon (2007a: 460): 'in the case of the Orwellian and the panoptic imagery for capturing what surveillance is about, the language of privacy has popular cachet'.

Therefore, the control perspective supposes that there are two criteria for evaluating the legitimacy of surveillance: the grounds for the use of surveillance and the extent to which the privacy of citizens is

affected. Legal rules, normative principles and social support allowing or dictating the application of surveillance are balanced against legitimacy grounds protecting the privacy of citizens. Power in the relationship between the watcher and the watched is a central issue when theorizing surveillance from a control perspective. Does government or do citizens gain power in their surveillance relationship and how can this power be legitimised?

2.2 The interaction perspective on surveillance

The interaction perspective presents surveillance as a connection between different actors in society. Consequently, from this perspective the question is posed how access to surveillance systems and the value and quality of the produced information can be legitimised. Citizens share knowledge about themselves and others through the data clouds they increasingly produce (van den Boomen, 2007). This observation contradicts the control perspective that portrays the citizen undergoing government surveillance in the isolation of his cell in the panopticon. The fact that people do communicate with each other, is both a given and a prerequisite for democracy. Jurgen Habermas (1974) shows this clearly in his famous treatise on *Öffentlichkeit*, the public sphere. The public sphere is a domain in society in which citizens, facilitated by mass media, organise themselves to shape public opinion. All citizens have access to the public sphere and enjoy the freedom to express their opinions about issues that affect the public interest. Thus, the public sphere enables criticism and control of the actions of the state, thereby functioning as a mediator between society and state.

The acknowledgement that there is a public sphere in which citizens connect with each other and jointly interact, provides a fundamentally different starting point for studying surveillance than in the control perspective. Haggerty (2006: 27) notes that 'changes in surveillance processes and practices are progressively undermining the relevance of the panoptic model for understanding surveillance'. Facilitated by social media, surveillance appears to have become part of the public sphere. Social media seem to tear down the walls of the panopticon, and the lateral invisibility of citizens with it. Although some authors (Fuchs, 2011; Fuchs et al., 2011) show that surveillance on social media can be analysed from a control perspective, the dynamics of social media lead to a different perspective containing other issues. The interaction perspective on surveillance emphasises the communication between citizens instead of denying this fact.

The interaction between social media users focuses on creating content as well as establishing and maintaining social contacts. Both forms of interaction on social media may intentionally or unintentionally facilitate surveillance, which can be initiated by both citizens and government. Twitter, for example, offers a major platform for surveillance by citizen journalists: 'every day in the US, people randomly witnessing an exceptional or dramatic event (crime, protest or accident) use their mobile phone to broadcast real-time information from the field on Twitter [translated by the authors]' (Eudes, 2009). Government also uses social media for surveillance purposes. Mitchell, Wolakand and Finkelhor (2005) describe how police detectives pose as minors on the internet in order to track paedophiles. Additionally, there are several examples of how authorities use social media to engage citizens in the surveillance of other citizens (Frissen et al., 2008; Osimo, 2008; Bekkers and Meijer, 2010; Keymolen et al., 2010).

In the interaction perspective, surveillance information is created according to the logic of social media, in which users simultaneously take on the roles of producers and consumers of surveillance information and enter into social relationships with each other (Benkler, 2006; Keymolen et al., 2010: 26-27; Schoondorp, 2010). Not only do citizens connect with each other, but links between citizens and government arise as

well. The interaction perspective emphasises the democratisation of information and surveillance: information is accessible to many people, and is shaped, evaluated and modified by many. Pessimists claim that people will share the biggest nonsense with the world driven by an 'infinite desire for personal attention' (Keen, 2007: 7). Moreover, information is not corrected by other actors in the public space, such as citizens, government or experts like scientists or journalists. Optimists on the other hand have faith in 'the wisdom of the crowd' to always correct false information (Surowiecki, 2004; Keymolen et al., 2010: 20). Surveillance information is widely available as is the possibility to contribute to surveillance in the role of both watcher and watched. Everyone can watch (information about others) and be watched (based on information generated by themselves or others).

Technology and legitimacy assumptions

The interaction perspective supposes that technology serves to connect multiple actors in society. According to the logic of social media, all kinds of users create and evaluate information about themselves and each other. Because information is easily accessible to all, surveillance becomes of relevance to all. Surveillance technology enables both government and citizens to take on the role of watcher and to share what they see with everyone, including the watched. As such, the watched, along with other actors in society, can evaluate, supplement and correct the surveillance information which has been generated.

Legitimacy criteria involve the access to the surveillance system and the value and quality of surveillance information. Because technology facilitates anyone to participate in surveillance practices, the question arises when this access can be considered legitimate. On the basis of which legal, ethical and socially accepted grounds does a person have the right or obligation to participate in surveillance? The value and quality of surveillance information is a second criterion for legitimacy from the interaction perspective. Which information in the enormous pile of user-generated surveillance information is of relevance in a particular surveillance situation? And how can the quality of this information be evaluated? Which legal, ethical and social standards can help to evaluate these matters?

2.3 The precautionary perspective on surveillance

The precautionary perspective supposes that surveillance technology can serve to identify and contain risks. The legitimacy concern in this perspective is the evaluation of the grounds for defining risks and categories of citizens. 'Prevention is better than cure' is the motto of the precautionary perspective. Within the surveillance studies field, several authors suggest that surveillance increasingly operates within a society that wants to prevent disaster and discomfort as much as possible. Van Brakel and De Hert (2011), for example, point at surveillance as an integral part of police strategies aimed at preventing rather than punishing crime. According to Borgers (2007: 19), the logic of today's risk society is based on a strict and constraining interpretation of the precautionary principle. The author states that a strong perception of the threat of all sorts of risks has evoked the central idea that we should stay one step ahead of danger, and that therefore preventive measures must be taken, even if it is not certain whether the feared risk will be realised. The Dutch Scientific Government Council *WRR* also ascertains a moral imperative for preventive action by the government, not only to address known risks, but especially for early detection and evaluation of unknown risks (WRR, 2008).

From a precautionary perspective surveillance serves as a basis for interventions. Data are collected, categorised and analysed to look ahead and act prematurely: 'The leading trend, in most sectors, is towards classificatory, pre-emptive surveillance, that tries to simulate and anticipate likely behaviours'

(Lyon, 2001b: 103). According to Lyon, panoptic theory falls short in understanding the social classification of citizens, which is tied to the use of surveillance for identifying risks (Ibid.). Precaution is not focussed on perfecting the panopticon and disciplining citizens, but aims to protect society and provide the best service possible. Citizens expect government to take measures to eliminate risks (WRR, 2008). Categorisation of citizens is essential to gain insight in societal risks and to control them. Surveillance facilitates this process of social sorting, as David Lyon explains in various publications (Lyon, 2001b; 2007a; 2007b; 2010). A terrorism risk, a fraud risk and a risk of domestic violence are examples of categorisations a citizen can be subjected to. Depending on the specific interest of an organisation, surveillance technology helps to identify and isolate certain groups and individuals. Lyon cites the example of a security service which collects data about people and their activities, and performs secondary analyses (data previously collected by others) 'to surveil "suspects" who have been previously identified or who fit a particular profile, in the hope of building a fuller picture of such persons, keeping tabs on their movements, and forestalling acts of violence or terror' (2007a: 460). From a precautionary perspective, such 'risk citizens' deserve more surveillance attention than others. As Van Gunsteren (2008: 174) phrases it: 'For your and my safety, the safety of "us", it is therefore necessary to observe and classify them, and possibly intervene before the damage is done'.[5]

Technology and legitimacy assumptions

In the precautionary perspective, surveillance technology has a dual function: the identification and containment of risks. The analysis of existing surveillance data using data mining and profiling techniques helps government to identify hitherto unknown risks (Hildebrandt, 2008: 18). Surveillance technology can thus be considered as an actor having influence on the definition of risk groups by experts and thus the agenda of further surveillance with respect to the citizens involved. Risk citizens are confronted with the second function of surveillance: the containment of risks by keeping an extra eye on specific groups.

Since the prevention of disaster and discomfort is the central concern of precautionary surveillance, its legitimacy stands or falls by how disaster and discomfort are defined. The way in which risk groups are determined and the moral responsibility for the choices made are important. The precautionary perspective creates a division between risk citizens and non-risk citizens. Difference, rather than equality becomes the leading principle. Lyon (2010: 44) aptly refers to 'the Other' as the object of surveillance:

> 'But the new modes [of citizenship – CvO] […] tend to single out particular groups for less-than-favorable attention. Such groups may be thought of as Other – those whose existence stands as a warning and as a limit to those currently enjoying full citizenship entitlements, privileges, and rights.'

This ambiguity puts government in an awkward position. It is impossible to respect the rights of both categories of citizens in an equal manner. Self-proclaimed non-risk citizens try to get precaution regarding risks citizens on the public and political agenda. Risk citizens, in turn, require justification for the unequal treatment and its consequences. What must be prevented and who should be the object of surveillance to this end, are key topics of discussion when it comes to the legitimacy of surveillance. The precautionary perspective on surveillance pays attention to the complex and reciprocal relationship between government and citizens in a society full of potential risks. On the basis of which legal, ethical and socially desired grounds are citizens selected for surveillance and what are the consequences in terms of social inequality, exclusion and unjustified inclusion for the people concerned?

[5] Translation by the author

Table 1 summarises the technology and legitimacy assumptions in the three perspectives on surveillance.

CONTROL PERSPECTIVE	
Technology assumptions	*Legitimacy assumptions*
<u>Widespread control of citizens</u> Surveillance technology enables government to monitor citizens for deviant behaviour by providing the watcher with as many data as possible about the watched. <u>Disciplining citizens</u> Government is able to discipline citizens by letting them know there is a control system without providing the details about the way in which it is applied.	<u>Usage of surveillance versus citizens</u> a) Legal grounds to permit and/or dictate the usage of surveillance are of importance. b) Normative justification of the usage of surveillance is of importance. c) Social acceptance of the usage of surveillance is of importance. <u>Protecting citizens' privacy</u> a) Legal grounds for the protection of citizens' privacy are of importance. b) Normative justification of citizens' privacy protection is of importance. c) Social acceptance of citizens' privacy protection is of importance.
INTERACTION PERSPECTIVE	
Technology assumptions	*Legitimacy assumptions*
<u>Connecting government and citizens</u> Surveillance technology can connect government and citizens. <u>Joint creation of information</u> Surveillance technology enables government and citizens to create, evaluate and modify information about themselves and each other.	<u>Access to surveillance information</u> a) Legal grounds for acquiring access to surveillance information are of importance. b) Normative justification of acquiring access to surveillance information is of importance. c) Social acceptance of acquiring access to surveillance information is of importance. <u>Relevance and quality of surveillance information</u> a) Legal grounds for the evaluation of the relevance and quality of surveillance information are of importance. b) Normative justification of the relevance and quality of surveillance information is of importance. c) Social acceptance of the relevance and quality of surveillance information is of importance.
PRECAUTIONARY PERSPECTIVE	
Technology assumptions	*Legitimacy assumptions*
<u>Identifying risks and risk citizens</u> Surveillance technology enables government to identify risks and risk citizens. <u>Containing risks</u> Surveillance technology enables government to contain risks by keeping an extra eye on specific groups of citizens.	<u>Defining risks and categories of risk citizens</u> a) Legal grounds for the way in which risks and categories of risk citizens are defined are of importance. b) Normative justification of the way in which risks and categories of risk citizens are defined is of importance. c) Social acceptance of the way in which risks and categories of risk citizens are defined is of importance.

Table 1: Technology and legitimacy assumptions in the perspectives of control, interaction and precaution

3. Technology and legitimacy assumptions in two policy practices of public mobility surveillance

The analysis of ANPR policy making by a Dutch police force and innovation policy making by NDW shows that technology and legitimacy assumptions of all three surveillance perspectives can be found in the practice of public mobility surveillance. However, the theoretical assumptions manifest themselves in varying extent. Table 2 summarises the extent to which the technology and legitimacy assumptions pertaining to the three surveillance perspectives of control, interaction and precaution have been found in each of the two cases studies. Consequently, insight is gained into assumptions that influence decision-making about the application of technology for public mobility surveillance.

3.1 Manifestation of the control perspective

The control perspective on surveillance is particularly reflected in the criteria that the police and NDW find important in assessing the legitimacy of their practices of public mobility surveillance. Especially the normative justification of why surveillance technology should be allowed or is deemed necessary gets ample attention in both cases. Additionally, in both policy practices there is an awareness of the legal and public debate on privacy. The police, however, pay more attention to this issue in their ANPR policy than NDW does in its innovation policy. For NDW, privacy is less important, because they feel that the responsibility for this matter lies with the market players they intend to hire to implement the surveillance technologies. Regarding the technology assumptions of the control perspective, there is only one assumption strongly manifested in one of the case studies. The police have a strong view of ANPR as a means of gaining control and command over all major access roads to the police region. NDW doesn't consider the innovative traffic system in panoptic terms at all. It is notable that neither the police nor NDW in hint at the potential disciplining effect of the surveillance systems that they're implementing.

3.2 Manifestation of the interaction perspective

In neither of the surveillance practices policy focuses on forging new connections between government and citizens nor jointly creating surveillance information. No technology assumptions have been found that indicate an interaction perspective on surveillance. However, both the police and NDW appear to have an eye for legitimacy criteria that fit the interaction perspective on surveillance. Policy makers in both case studies pose questions about granting access to surveillance information and assessing the relevance and quality of surveillance information. In neither of the case studies, however, are these questions prompted by a concern about the possible influence of citizens on the surveillance system, but rather the influence of other parties, such as market players and other government organisations. Especially in the NDW case study, the interaction between government, market and technology itself is rather problematic.

In both policy domains, security and traffic management, it is to be expected that the interaction perspective will become more dominant in design of public mobility surveillance. In the security domain more and more practices arise in which the police involve citizens in their activities and even sometimes leave these up to them completely. For example, the Dutch *Burgernet* initiative prompts mobile citizens to engage in surveillance of fellow citizens in need of help, such as missing children, or of suspect citizens like burglars on the run (Politie en VNG, 2013). In the traffic domain, a trend can be discerned towards more interaction amongst vehicles and between vehicles and traffic management systems. Cooperative traffic systems and autonomous driving would be key technologies for more on-road interaction (Wilmink, Immers and Schuurman, 2011).

TECHNOLOGY AND LEGITIMACY ASSUMPTIONS	ANPR - POLICE	INNOVATION - NDW
Control		
Widespread control of citizens (technology assumption)	**Strong**	None
Disciplining citizens (technology assumption)	None	None
Usage of surveillance versus citizens (legitimacy assumption)	**Strong**	**Strong**
Protecting citizens' privacy (legitimacy assumption)	**Strong**	Weak
Interaction		
Connecting government and citizens (technology assumption)	None	None
Joint creation of information (technology assumption)	None	None
Access to surveillance information (legitimacy assumption)	Weak	**Strong**
Relevance and quality of surveillance information (legitimacy assumption)	Weak	**Strong**
Precaution		
Identifying risks and risk citizens (technology assumption)	Weak	Weak
Containing risks (technology assumption)	**Strong**	**Strong**
Defining risks and categories of risk citizens (legitimacy assumption)	Weak	None

Table 2: Empirical manifestation of surveillance perspectives

3.3 Manifestation of the precautionary perspective

The policy analysis of public mobility surveillance demonstrates that government associates surveillance technology to a great extent with risks posed by mobile citizens and to a lesser extent with the risks that mobile citizens might face. In both examined policy practices, government cautiously starts to identify unknown risks through targeted analysis of mobility data. Data mining and profiling techniques aren't employed yet. The second technology assumption within the precautionary perspective, containing known risks, is dominant in both policy practices. The police increasingly use ANPR to stop crimes and offenses committed by risk groups and on risk routes. Transport patterns of registered house burglars are analysed in order to increase the chance of catching them. In the NDW case study, the policy aims at using innovative traffic technology to get a grip on the risk of traffic congestion by recognising an imminent turning point in the traffic flow on risk roads. In both policy practices, public mobility surveillance implies

that government approaches mobile citizens as risk citizens. As she moves around in certain places at certain times, a citizen can be considered a risk to the rest of society, especially if she happens to have some other risky characteristics, such as a past as a home burglar (police case study) or an extra-long vehicle (NDW case study). Predicting the presence of certain groups of citizens at certain places and times is essential for preventive government policy.

The perception of the risk citizen is not the same in the two case studies. The police perceive mobile citizens purely as a potential security risk. The movements of known drug runners, house burglars and drunk drivers need to be mapped, because these groups represent a potential danger to society. NDW's innovation policy conveys a more ambiguous perception of mobile citizens. Road users are a potential traffic hazard and should be protected against this hazard at the same time. Remarkably, in neither policy practices is any effort made to legitimise the policy choices regarding the selection and definition of risks. Considerations about the legal, normative or social grounds for defining and rejecting risks are apparently not perceived as important for the legitimation of the surveillance policy. Defining risks currently seems to be a political or technocratic affair. Thus, the legitimacy grounds for surveillance of particular groups remain implicit.

4. Conclusion: discrepancies between policy developments and criteria of legitimacy

When looking at the elements of the three surveillance perspectives that emerge in the examined policy practices, no connection or a limited one is found between the technology assumptions and the legitimacy assumptions. In the police case study, both the control perspective and the precautionary perspective are characteristic of the technology assumptions underlying the ANPR policy. On the other hand, the legitimacy criteria that the police pay attention to, predominantly pertain to the control perspective. The definition and selection of risks and risk citizens is hardly legitimised. The quest for innovation in the NDW case causes a transition from a control perspective to a precautionary perspective regarding the use of traffic data. However, the legitimacy assumptions in the innovation policy are related to the perspectives of control and interaction.

The discrepancy between technology and legitimacy assumptions reveals that government supposes it can use public mobility surveillance to realise certain policy ambitions while using criteria of a different order to legitimise these technology applications. In other words, government focuses on legitimacy issues which aren't sufficiently appropriate for the envisioned technology applications. Whereas government puts more and more of an emphasis on prevention (of offenses, crimes and traffic jams) by identifying mobile risk citizens, it focuses on matters such as privacy protection and the quality of data in the legal, ethical and social legitimation of surveillance.

Given the dominance of the precautionary perspective in the practice of public mobility surveillance, the government should especially pay more attention to the grounds for marking someone as a risk citizen. It is of crucial importance that the process of selection and definition of risks is realised in a careful manner. Clear inclusion and exclusion criteria as well as sound procedures for the analysis of mobility data may help to evaluate the mobile citizen without arbitrariness and prejudice.

Literature

Bannister, F. (2005). The panoptic state: Privacy, surveillance and the balance of risk. *Information Polity*. 10 (1-2): 65-80.

Bekkers, V. & A. Meijer (2010). *Cocreatie in de publieke sector: een verkennend onderzoek naar nieuwe, digitale verbindingen tussen overheid en burger.* Den Haag: Boom Juridische uitgevers.

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom.* New Haven [Conn.]: Yale University Press.

Borgers, M.J. (2007). *De vlucht naar voren.* Den Haag: Boom Juridische uitgevers.

van Brakel, R. & P.J.A. De Hert (2011). Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. *Journal of Police Studies*. 20 (3): 163-192.

Brimicombe, A. & C. Li (2009). *Location-based services and geo-information engineering.* Oxford: Wiley-Blackwell.

Calabrese, F. & C. Ratti (2006). Real Time Rome. *Networks and Communication Studies. Official Journal of the IGU's Geography of Information Society Commission*. 20 (3&4): 247-258.

van den Boomen, M. (2007). 'Van gemeenschap via webnetwerk naar datawolk'. In Steyaert, J. and J. de Haan (Eds.) *Jaarboek ICT en samenleving*: Amsterdam: Uitgeverij Boom.

Eudes, Y. (2009). 'Twitter, les pirates et les diplomates', *Le Monde*, http://www.lemonde.fr/technologies/article/2009/08/24/twitter-les-pirates-et-lesdiplomates_1231380_651865.html (24 August 2009).

Foucault, M. (1979). 'Panopticism. From: Discipline and Punish: The Birth of the Prison'. In Webster, F. (Ed.) *The Information Society Reader*: 301-312. London: Routledge.

Frissen, V., M. van Staden, N. Huijboom et al. (2008). *Naar een 'User Generated State'? De impact van nieuwe media voor overheid en openbaar bestuur*. Delft, TNO.

Fuchs, C. (2011). New media, web 2.0 and surveillance. *Sociology Compass*. 5 (2): 134-147.

Fuchs, C., K. Boersma, A. Albrechtslund et al. (Eds.) (2011). *Internet and Surveillance: The Challenges of Web 2.0 and Social Media.* New York: Routledge.

Gow, G.A. & M. Ihnat (2004). Prepaid Mobile Phone Service and the Anonymous Caller: Considering Wireless E9-1-1 in Canada. *Surveillance & Society*. 1 (4): 555-572.

van Gunsteren, H. (2008). 'Burgerschap en veiligheid in Nederland'. In Alberts, G., M. Blankesteijn, B. Broekhans and Y. van Tilborgh (Eds.) *Jaarboek Kennissamenleving*: 169-183. Amsterdam: Aksant.

Habermas, J. (1974). 'The Public Sphere'. In Webster, F. (Ed.) *The Information Society Reader*: 350-365. London: Routledge.

Haggerty, K. (2006). 'Tear down the walls: on demolishing the panopticon'. In Lyon, D. (Ed.) *Theorizing surveillance: the panopticon and beyond*: 23-45. Devon: Willan Publishing.

Haggerty, K. & R. Ericson (2007). 'The surveillant assemblage'. In Hier, S.P. and J. Greenberg (Eds.) *The surveillance studies reader*: 104-116. Maidenhead: Open University Press.

Hildebrandt, M. (2008). 'Defining Profiling: A New Type of Knowledge?' In Hildebrandt, M. and S. Gutwirth (Eds.) *Profiling the European citizen: cross-disciplinary perspectives*: 17-45. Dordrecht: Springer.

Hill, M. (2009). *The Public Policy Process.* Harlow: Pearson Longman.

Keen, A. (2007). *The cult of the amateur: how today's internet is killing our culture.* New York: Doubleday/Currency.

Keymolen, E., B. van den Berg, J.E.J. Prins et al. (2010). *Vertrouwen in hybride ketens. Een onderzoek in het kader van de Alliantie Vitaal Bestuur*. TNO ICT - Erasmus University Rotterdam - Tilburg University.

Lyon, D. (2001). *Surveillance society: monitoring everyday life.* Buckingham: Open University Press.

Lyon, D. (2007a). 'Surveillance, Power, and Everyday Life'. In Mansell, R., C. Avgerou, D. Quah and R. Silverstone (Eds.) *The Oxford Handbook of Information and Communication Technologies*: 449-467. New York: Oxford University Press.

Lyon, D. (2007b). *Surveillance studies: an overview.* Cambridge: Polity Press.

Lyon, D. (2010). 'Identification, surveillance and democracy'. In Haggerty, K.D. and M. Samatas (Eds.) *Surveillance and democracy*: 34-50. Abingdon: Routledge.

Mitchell, K.J., J. Wolak & D. Finkelhor (2005). Police posing as juveniles online to catch sex offenders: is it working? *Sex Abuse*. 17 (3): 241-267.

van Ooijen, C.W. & M. Bokhorst (2012). 'Securing the Legitimacy of Surveillance. Automatic Number Plate Recognition in Dutch policing'. In Vande Walle, G., E. Van den Herrewegen and N. Zurawski (Eds.) *Crime, Security and Surveillance. Effects for the Surveillant and the Surveilled*: 123-144. The Hague: Eleven International Publishing.

van Ooijen, C.W. (2014). *Het risico van de mobiele burger. Publieke mobiliteitssurveillance voor informatie over het gaan en staan van burgers.* Den Haag: Boom Lemma uitgevers.

Orwell, G. (1949). *1984.* New York: New American Library.

Osimo, D. (2008). 'Web 2.0 in government: Why and how?'. *JRC Scientific and Technical Reports.* Seville (Spain), Joint Research Centre (JRC) - Institute for Prospective Technological Studies (IPTS).

Politie en VNG (2013). Burgernet. Samen voor een veilige buurt. https://www.burgernet.nl (17 November 2013).

Poster, M. (1990). *Mode of information: Poststructuralism and social context.* Cambridge: Polity Press.

Schoondorp, M. (2010). 'Social media en de kansen voor het onderwijs'. SURFnet/Kennisnet Innovatieprogramma.

Surowiecki, J. (2004). *The wisdom of crowds: Why the many are smarter than the few an how collective wisdom shapes business, economies, societies, and nations.* London: Little, Brown.

Taylor, J.A., A.M.B. Lips & J. Organ (2009). Identification Practices in Government: Citizen Surveillance and the Quest for Public Service Improvement. *Identity in the Information Society*. 1 (1):

Vedder, A., L.J.G. van der Wees, E.J. Koops et al. (2007). *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*. Den Haag, Rathenau Instituut.

Wilmink, I., B. Immers & H. Schuurman (2011). 'Toepassingsmogelijkheden van coöperatieve systemen en services in Nederland', http://www.verkeerskunde.nl/Uploads/2011/11/Bijdrage51.pdf (17 November 2013).

WRR, Wetenschappelijke Raad voor het Regeringsbeleid (2008). *Onzekere veiligheid. Verantwoordelijkheden rond fysieke veiligheid.* Amsterdam: Amsterdam University Press.