Innovation: The European Journal of Social Science Research
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ciej20

Privacy issues in public discourse: the case of "smart" CCTV in Germany

Norma Möllers [a] & Jens Hälterlein [a]
[a] Faculty of Social Sciences, Department of Sociology of Organization and Administration II , Potsdam University , August-Bebel-Str. 89, D-14482 , Potsdam , Germany

Published online: 13 Nov 2012.

To cite this article: Norma Möllers & Jens Hälterlein (2013) Privacy issues in public discourse: the case of "smart" CCTV in Germany, Innovation: The European Journal of Social Science Research, 26:1-2, 57-70, DOI: 10.1080/13511610.2013.723396

To link to this article: http://dx.doi.org/10.1080/13511610.2013.723396

Innovation: The European Journal of Social Science Research, 2013
Vol. 26, Nos. 1–2, 57–70, http://dx.doi.org/10.1080/13511610.2013.723396

RESEARCH NOTE

Privacy issues in public discourse: the case of "smart" CCTV in Germany

Norma Möllers* and Jens Hälterlein

Faculty of Social Sciences, Department of Sociology of Organization and Administration II, Potsdam University, August-Bebel-Str. 89, D-14482 Potsdam, Germany

(*Received 30 October 2011; final version received 20 August 2012*)

In dealing with surveillance, scholars have widely agreed to refute privacy as an analytical concept and defining theme. Nonetheless, in public debates, surveillance technologies are still confronted with issues of privacy, and privacy therefore endures as an empirical subject of research on surveillance. Drawing from our analysis of public discourse of so-called "smart" closed-circuit television (CCTV) in Germany, we propose to use a sociology of knowledge perspective to analyze privacy in order to understand how it is socially constructed and negotiated. Our data comprise 117 documents, covering all publicly available documents between 2006 and 2010 that we were able to obtain. We found privacy to be the only form of critique in the struggle for the legitimate definition of smart CCTV. In this paper, we discuss the implications our preliminary findings have for the relationship between privacy issues and surveillance technology and conclude with suggestions of how this relationship might be further investigated as paradoxical, yet constitutive.

Keywords: smart CCTV; video surveillance; privacy; data protection; sociology of knowledge; discourse analysis

The persistence of privacy

Privacy is a controversial issue in surveillance scholarship because it meets political, thematic and conceptual difficulties. Regarding privacy as a policy instrument, Stalder (2002, 123), for instance, has expressed doubts as to whether privacy can effectively keep surveillance in check, because sanctions of information misuse are not strong enough. On the other hand, Bennett (2011, 493–494) claims that privacy regulations remain flawed but necessary, simply because they are the only actual mechanism to control excessive surveillance. To varying degrees, these positions exemplify a broadly shared conviction that privacy is a fairly weak means for political activism. On a related matter, Lyon (2003a, 1), van der Ploeg (2003, 66–67), and others insist that focusing too much on privacy as a scholarly theme means ignoring more pressing issues that may result from surveillance practices, such as discrimination, social inequality or even shifting conceptions of bodily integrity. The rejection of privacy as a defining theme is widely shared in surveillance research because it is regarded as too narrow to grasp the entirety of the social consequences resulting from surveillance practices. Finally, several scholars have pointed out serious difficulties when privacy is applied as a theoretical concept to analyze whether we have less privacy now than in the past. In response to these conceptions

*Corresponding author. Email: norma.moellers@uni-potsdam.de of privacy, Lyon and Zureik (1996, 13) pointed out that understandings of what is private and what is public differ across cultures, and Haggerty and Ericson (2006, 11–12) added that they are also relative to institutional and organizational contexts. They then conclude that such a static definition of privacy is largely inappropriate to the factual complexities of surveillance in present societies.

While we sympathize with the claim that researching surveillance technology exclusively through the lens of privacy is inadequate, we nevertheless face the problem that it cannot be ignored because of its regular occurrence in empirical data. If privacy endures as a substantive empirical subject in surveillance research, we must find an adequate perspective to work with it. The critiques of privacy as a theoretical concept can help guide this perspective: if understandings of privacy are culturally relative, then they are also historically relative, and we can trace their development across time and analyze how they relate to other topics in surveillance research. This means that we can treat privacy as an empirical phenomenon that is constructed and negotiated in social processes, and thus open it up for sociological analysis. This approach somewhat resembles Steeves's understanding of privacy as "a dynamic process of negotiating personal boundaries" (Steeves 2009, 193). However, we would prefer to treat the ends of this negotiation as an open-ended question because personal boundaries are not necessarily the only parameters that are construed under the title of privacy. This shift in perspective decenters privacy and focuses on other issues such as the development and employment of surveillance technology, the organization of labor, or shifts in social control. This perspective might bring privacy back into surveillance research in a useful way, for example, by scrutinizing how the public debate on privacy might affect the development of surveillance technology, or how privacy regulations and their interpretations in practice might affect the organization of surveillance work.

Thus taking a social constructionist stance, this paper analyzes a small portion of the relationship between privacy and surveillance technology. Technology studies have demonstrated that the technical properties of a technological system cannot determine its legitimate use, but that technology is better understood in a mutually constitutive relationship with the social worlds in which it is embedded (MacKenzie and Wajcman 1999, 23). This means that meanings attached to a technology are achieved to an important extent by the social processes relevant to its development and employment. Whereas early technology studies focused on the social shaping in design and appropriation of technologies (Pinch and Bijker 1984; Bijker 1995; Kline and Pinch 1996), subsequent contributions pointed out the importance of the cultural conditions under which a technology is developed (e.g. Klein and Kleinman 2002, 40–46; Jasanoff 2005, 247–249). Applied to surveillance technology, this means that discourses of privacy also shape the circumstances for which it is regarded an appropriate means. Although these negotiations constitute only one facet of social processes, their analysis might nonetheless help understand why surveillance technologies enjoy their immense popularity, even though there is no strong evidence for their effectiveness or a general increase in crime.

This paper suggests that the privacy discourse might have helped the emergence of new surveillance technologies. We outline this seemingly contradictory relationship between privacy critiques and surveillance technology by discussing preliminary results of our analysis of the public discourse of so-called "smart" closed-circuit television (CCTV) in Germany between 2006 and 2010. First, we state our working definition of smart CCTV. Second, we briefly sketch the institutional context in which actors struggle over the legitimate definition of smart CCTV. Third, we delineate our research design by laying out the theoretical and methodological assumptions on which our results are based. Fourth, we briefly summarize the overall structure of the public discourse of smart CCTV, pointing out the various core issues that emerged between 2006 and 2010. Finally, we focus on how privacy issues have been discussed in public discourse, and elaborate on some of our findings. We conclude with some suggestions of how the relationship between privacy and surveillance technology might be further investigated as paradoxical, yet constitutive.

"Smart" CCTV

Scholars still grapple with finding an appropriate term for the new CCTV systems that are currently being developed in the Euro-American world because they come with a variety of functionalities and applications. Functionalities may range from classification, storage and retrieval of video footage, through object tracking, to data mining and the prediction of events based on the captured data (Introna and Wood 2004, 181; for a more detailed overview in terms of technical features see Gouallier and Fleurant 2009). The new CCTV systems are also not limited to one single purpose. Desired applications range from automatic detection of criminal behavior, identification of search-listed criminal or unwanted individuals, through the prosecution of traffic offenders, to prediction of traffic jams and mass panic, as well as the statistical analysis of consumer behavior (e.g. in supermarkets). Although these projected functionalities and applications may seem disparate, the common idea that runs through them is that operators are not required to watch the video screens at all times, but are notified by the system in case of an event of interest. In other words, the shared feature of the new CCTV systems is that all of them are built around the computer, not the camera.

The shift from camera to computer is nicely captured by the term *algorithmic surveillance*, originally coined by Norris and Armstrong (1999) and adapted by Introna and Wood (2004) for facial recognition systems. Some of the more commonly used alternatives are *semantic video surveillance* (Musik 2011), *second generation CCTV* (Surette 2005), and *smart CCTV* (Gates 2010; Ferenbok and Clement 2011). However, none of these terms are entirely satisfying: *algorithmic surveillance* does not discriminate visual from non-visual surveillance and thus might be better used as an umbrella term for all kinds of computer-based surveillance technologies; *second generation CCTV* collapses the complex entanglement of social and technical processes to a linear and evolutionary logic of technological development; and *smart CCTV* might be understood containing a strong normative connotation of technological progress.

For the sake of brevity and owing to the lack of a better term, throughout this paper we apply the term *smart CCTV*, while acknowledging its flaws. Our working definition of smart CCTV refers to *visual surveillance systems* that analyze and interpret video footage by using *pattern recognition technologies*. Because we take a social constructionist stance, the systems' actual properties were less important; instead, we collected documents if they defined the emerging technology as new, smart, autonomous or in similarly descriptive terms. Also, our definition ultimately guided our selection of articles in which we restricted the data collection to articles that (1) discussed visual surveillance, and (2) referred to these surveillance systems as somehow "doing things autonomously".

Situating the controversy

The development of surveillance technology is accompanied by struggles over their legitimate definition. Governmental institutions might strongly demand and extensively fund research and development because global risks, such as terrorism and organized crime, seemingly necessitate more efficient countermeasures. Nevertheless, privacy advocates criticize surveillance technologies because they are seen to pose threats to individual liberties. To varying degrees, these contrasting positions are stabilized in Germany's institutional landscape.

Governmental institutions are often a crucial driving force for the development and implementation of new surveillance technologies because provision and protection of public safety fall under their area of responsibility. In 2007, Germany's Ministry of Education and Research set up extensive funds to stimulate research of smart surveillance technologies. Similarly, the various police offices that are affiliated with the German Ministries of Internal Affairs each have their own in-house research facilities for these technologies. Alongside considerations of security, the flourishing market for security technology strongly motivates governmental institutions to push research and development; of course, this interest is widely shared by private corporations within the industry for surveillance technology. However, smart CCTV systems, similar to analog systems, encounter serious socio-technical problems, as exemplified by the facial recognition project of the Federal Police Office (Bundeskriminalamt) in 2006, in which false alarm rates proved to be problematic for police in terms of effectiveness. More importantly, failures frequently have elicited harsh criticism, weighing the systems' low effectiveness against considerable infringements of privacy rights. Thus, in spite of massive efforts to push research and development, government institutions are probably pressured to justify the appropriateness of smart CCTV against opponents' objections.

In 1970, protection of privacy was formally institutionalized in German law following a decision in the federal state of Hessen. Mayer-Schönberger (1997, 221) claims that a major reason for this was the introduction of electronic data processing into governmental bureaucracies. Since then, the juridical literature on privacy and data protection has expanded significantly and numerous legal regulations have been passed in Germany to protect guidelines and sanction their violations, which is an effect presumably due to the expansion of computer-based work in public and private sectors. Privacy advocates may be organized in non-governmental organizations (NGOs), and privacy is on the agenda of political parties, but with varying degrees of importance. Although privacy is addressed in a range of institutions, control of privacy guidelines is mainly provided by data protection commissioners at communal, federal and national levels. The commissioners' mandate is to assess organizations' surveillance practices and pressure them to meet legal requirements. Yet the legal regulation of CCTV in public spaces remains extremely complicated because it varies not only along Germany's national laws, but also along those of the 16 federal states. In semi-public spaces such as public transportation, the problem is even more intricate because the employment of CCTV not only falls under police regulations, but is also subject to civil law. Similarly, legal regulations are also required to consider the great variety of surveillance technologies and keep track of the critical differences between old and new technologies. Thus, despite considerable efforts to control the use of surveillance technologies, requirements specific to the sovereign rights of the federal states and rapid technological advances of emerging surveillance technologies challenge legal frameworks, courts and data protection commissioners.

Theoretical framework

Our project uses the "sociology of knowledge approach to discourse" (SKAD) which was mainly developed by Keller (2011a, 2011b, 2011c) over the course of the past decade. As its name implies, the most distinctive feature of SKAD, compared with linguistic or ethnomethodological traditions of discourse analysis, is that it draws heavily from the sociology of knowledge traditions.[1] Another distinctive feature of SKAD is that it is compatible with inductive strategies of qualitative research, most importantly grounded theory in the tradition of Strauss (Strauss 1987; Strauss and Corbin 1998). Although SKAD's conceptualization of the relationship between the material and the social could be better elaborated, we contend that it is a framework particularly well suited to exploring the cultural conditions of the development of surveillance technology.

Keller developed the theoretical framework by integrating Berger and Luckmann's (1966) approach to the sociology of knowledge and Foucault's (1972) concept of discourse. It attempts to overcome the shortcoming of both approaches, which is the analytical gap between structure and agency. On one hand, it uses Berger and Luckmann's approach to conceptualize how knowledge shapes and is shaped by social practices, which is a pitfall in Foucault's early structuralist writings. On the other hand, SKAD deems Foucault's concept of discourse to be beneficial because it focuses on the extent to which large-scale knowledge regimes, entrenched in powerful institutions, structure social practices. Keller points out that this is a conceptualization of large-scale social aggregation that was not sufficiently elaborated in Berger and Luckmann's theory. According to Foucault (1972, 49), these large-scale sign structures, which he calls discourses, do not represent the objects to which they refer, but systematically produce them. Translating Foucault's well-known concept into sociological terms, SKAD understands discourses as knowledge that forms patterns of interpretation and action. This knowledge is understood as institutionalized in social and material structures within specific socio-historic contexts. SKAD thus tries to adapt Foucault's (1979) later material-semiotic understanding of the social and material worlds as inextricably linked to each other because there is no practice independent of discourse; simultaneously, discourses exist only by means of practices and artifacts.

Referring to Berger and Luckmann (1966), SKAD agrees that society is an "objective reality" that is institutionalized in social stocks of knowledge. Actors in turn internalize knowledge in socialization processes, and then reproduce and transform knowledge in their everyday practices. For example, when we read in the daily press about plans for a new CCTV system in our neighborhood, it certainly shapes our attitudes towards these technologies: some people may feel safer in monitored spaces, while others might try to avoid them or even engage in organized public protest. It is of crucial importance that these practices do not occur in an arbitrary way, but are bound to the finite number of alternatives provided by shared ways of knowing. Thus, if knowledge structures the ways in which individuals act, think and speak, it is useful to scrutinize which knowledge is acknowledged and accepted as true. A second reason for analyzing discourses in terms of SKAD is that it allows for particular attention to claims that are marginalized or excluded from dominant discourses. If discourses determine what is known to be true, truth-claims that contradict dominant discourses but cannot draw on powerful resources (e.g. degree of organization, public visibility) generally have great difficulty in being acknowledged. Disadvantaged social groups are often excluded from dominant discourses, and the analysis of their exclusion informs us about the distribution of power. Finally, even within the arena of dominant discourses, phenomena often remain contested over longer periods of time; the discourses of surveillance technology are prominent examples of such struggles. Consequently, dominant discourses might compete for the legitimate definition of a phenomenon by seeking to include or exclude issues, or controlling a controversy (Keller 2011b, 47; also see Foucault 1982). Applied to our research, the configuration of negotiations in relation to what they exclude then constitutes the cultural conditions that afford the development of smart CCTV.

Methods

Data collection

In order to link theory and methods, we chose to analyze public documents in which the production and reproduction of social stocks of knowledge could be found. In public arenas like the mass media, discourses not only struggle over the legitimate definition of smart CCTV; they also reach a significant audience whose relation toward smart CCTV they are likely to shape. We thus considered only publicly available documents that explicitly discussed smart CCTV. Among our data set first were daily and weekly newspaper articles on regional and national levels. On the national level we selected widely circulated newspapers, whereas on regional levels we pre-selected newspapers of areas in which smart CCTV was either piloted or officially planned. To cover the widest possible range of discourse, we also collected articles from blogs and online magazines because we assumed that they might present smart CCTV in different ways. Finally, to cover explicitly political discourse, we collected transcripts of parliamentary debates and other parliamentary documents at regional and national levels.

We accessed our source material via online archives of the aforementioned formats. We began with a set of three keywords – "intelligent video surveillance", "smart CCTV" and "automated video surveillance" – which unfortunately returned only about 20 articles. Having subsequently learned that the technical community has a much wider vocabulary for smart CCTV, we expanded the keywords to terms such as "machine learning" and "video analytics", among others. Our expanded list then had 34 combinations of different keywords for smart CCTV, and returned about 400 articles. After two readings of the entire data set, we discarded articles that were clearly not related to smart CCTV as stated in our working definition, or which only mentioned smart CCTV in passing. Our final data set (Table 1) then comprised 117 documents, covering the years between 2006 and 2010.[2] We can see that the public discussion is relatively small, which is probably because smart CCTV in Germany is still in the development phase. Also note that there are only eight parliamentary documents, which indicates that the issue has not yet been widely discussed in the legislative branches of government. We want to emphasize that our focus on these formats was not to disregard other sources, such as documents of NGOs, lobbies and unions, or radio and TV productions, but rather because qualitative analyses, including discourse analysis, are time-intensive.

Table 1. Final data set covering 2006–2010

	Daily and weekly newspapers	Parliamentary documents	Blogs and online formats
2006	8	4	10
2007	20	0	15
2008	7	0	20
2009	3	0	5
2010	6	4	15
Total	**44**	**8**	**65**

Data analysis

We analyzed the material using qualitative methods, drawing heavily on strategies developed in grounded theory (Strauss 1987; Strauss and Corbin 1998). The aim was not to deductively assume that there are discourses in opposition to or in favor of smart CCTV, but to inductively analyze how smart CCTV was problematized. Since we wanted to understand the different meanings of smart CCTV in public discourse, the roles it would play could not be set in advance, but had to be treated as open-ended questions. This blending of theoretical assumptions and inductive methods leads to a common problem in qualitative research: because the analysis iterates between empirical concepts and relevant theoretical sources, a complete rendition of the process would involve a somewhat lengthy and unintelligible chronological presentation of data and concept building. For the sake of clarity, we suspended this option in favor of an exemplary description of the coding process.

We began our analysis with a close line-by-line reading of the material, during which we developed codes to describe every syntactic unit. In the terms of grounded theory, we broke down the text by developing empirically grounded concepts (Strauss and Corbin 1998, 102). While the codes at first were closely attached to the manifest meaning of a syntactic unit, they quickly became increasingly abstract. We grouped codes that seemed to belong to a category and, if possible, assigned new codes to already established categories. For example, it soon became clear that our codes "attention span problems of security personnel" and "high staff expenses" were framed as dimensions of a bigger problem that we termed "inefficient surveillance strategies". When we found complaints about the poor quality of video footage, we then could assign them as an additional dimension to this category. Problems of unsatisfactory surveillance strategies again referred mainly to one set of proposed solutions, which was the integration of different kinds of smart CCTV components. Thus we developed a category that was called "proposed solutions to inefficient surveillance". We repeated this process, simultaneously grouping and regrouping our codes and categories, until it became apparent that the structure of problems, solutions and respectively accorded actors also fit the logic of other reoccurring themes, as well as enabled the agreement of our other categories. Consequently, we used them as core categories for organizing and comparing the entire data set:

(1) causes attributed to a problem;
(2) actors held responsible as the cause of a problem;
(3) solutions and strategies to a problem proposed;
(4) actors held responsible to solve a problem;
(5) values referenced.

Whenever the content of these categories diverged significantly – for example, when one text fragment framed an institution as the cause of a problem, whereas the same institution was framed to be a solution in another fragment – we interpreted them as respectively belonging to distinct discourses. These distinct orders were not necessarily coherent with the organization of one document: while some documents contained only a single discourse fragment, many contained several fragments belonging to different discourses. By rearranging the material according to the discourses' respective logical structures, we thus obtained different meanings of smart CCTV.

Thus, although our categories are informed by social theory, we did actually develop them from our data. Of course, our reading is not the only possible one; readings obviously differ according to the respective research questions and alternative readings should therefore be encouraged. However, we hope that our mapping can nevertheless provide useful insights into the various issues connected to smart CCTV.

"Smart" CCTV in public discourse

Mapping the controversy

Before we elaborate on our findings in terms of the negotiations of privacy, we briefly outline the various issues that emerged in public discourse. This overview must remain partial owing to the scope of this paper, but it is necessary to understand how negotiations of privacy contribute to the meanings of smart CCTV in public discourse. We distinguished four types of problematizations that reoccurred steadily between 2006 and 2010. They represent the core meanings of smart CCTV available in public discourse, and can be described as the following ideal-type statements:

(1) Crime and terror pose threats to public safety, but can be regulated by developing and employing smart CCTV systems.
(2) Simple CCTV systems are inefficient in terms of resources, but can be improved by developing and employing smart CCTV components.
(3) Mass panic is unpredictable and uncontrollable for human security personnel, but can be predicted and regulated by smart CCTV systems.
(4) Smart CCTV systems pose a threat to personal liberty; therefore, data protection commissioners must control and sanction infringements of laws and guidelines.

The *first discourse* above constitutes smart CCTV as an appropriate and working solution for problems of crime and terrorism. It presumes a very specific model of criminal behavior, as something of natural and evenly patterned appearance, which is a precondition for the functionality of smart CCTV systems. Criminal behavior here is exclusively defined by its consequences, not its causes. The emphasis on the potential harms and dangers of criminal behavior constructs the plausibility that technology could effectively predict and detect these dangers. Thus, the legitimacy of smart CCTV in this context is established by a managerial-regulative definition of crime. The *second discourse* listed above produces the plausibility of smart CCTV systems by contrasting them to simple CCTV systems. It defines smart CCTV's appropriateness by means of managerial arguments as well, but in contrast to the first discourse, the "true" field of intervention is said to be the surveillance practices required by non-computed CCTV. Smart CCTV is hence established as a plausible technology by framing the poor quality of human labor as the main reason for simple CCTV's inefficiency. The *third discourse* also frames smart CCTV as an appropriate solution, yet again for different reasons and in a less elaborated way. Smart CCTV's plausibility here is co-produced by making the irrationality of collective behavior and limited cognitive capacities of humans a mere fact of nature (as opposed to socially shaped). The discourse then rests on contrasting inevitable human failure with the calculative superiority of smart CCTV systems. It is worth mentioning that these three discourses, among other rhetorical strategies, strongly emphasize technological agency over "inferior" human security work. Finally, the *fourth discourse* constitutes smart CCTV as an inappropriate technology. Evoking Orwellian metaphors, this discourse mobilizes privacy and data protection violations to admonish smart CCTV's threats to personal liberty.

Discourses (1), (2) and (4) were reproduced across all media, while discourse (3) remained somewhat fragmented. If these discourses struggled for the legitimate definition of smart CCTV, this took place mainly between discourses (1), (2) and (4). Furthermore, the interpretive stability of the first two discourses refuted our initial assumption that blogs present the topic differently, suggesting that it is a dominant interpretation of smart CCTV.

Personal liberty, privacy and the problem of smart CCTV

According to the data, the core problem of this discourse was that the employment of smart CCTV systems might pose threats to the value of personal liberty (Table 2). Criticism sometimes admonished the compromise between security and personal liberty. Similar criticism again weighed the effectiveness of CCTV systems in terms of crime prevention against constraints of personal liberty. Thus, large parts of this discourse established smart CCTV as an inappropriate technology by stressing the tensions between public safety and personal liberty.

Although the logical structure of this discourse explicitly referenced personal liberty as a value to be protected, descriptions of actual or possible liberty constraints

Table 2. Problematization of smart CCTV as a threat to personal liberty

Causes attributed to a problem	● Violation of data protection guidelines by employing smart CCTV ● Compromise between security and personal liberty
Actors held responsible as the cause of a problem	● Police bureaus (who employ smart CCTV) ● Politicians of the governments (who disregard civil rights by introducing smart CCTV) ● Researchers and developers of smart CCTV (both universities and corporations)
Solutions and strategies to a problem proposed	● Enforcement of guidelines and sanctioning of data protection infringements ● Public supervision of research and development
Actors held responsible to solve a problem	● Data protection commissioners ● Germany's Federal Constitutional Court ● Political parties (of the opposition)
Values referenced	● Personal liberty as a fundamental right

remained vague. If ever there were descriptions, they predominantly referred to infringements of privacy regulations. Our point here is that there seems to be quite a gap between the idea of personal liberty and privacy regulations. Whereas the broad idea of personal liberty usually denotes the absence of excessive constraints on human action, privacy in Germany is far more specific. Privacy in Germany, which we use synonymously with data protection, is institutionalized as the protection of the right to "informational self-determination". This somewhat unwieldy term means that an individual cannot be coerced to disclose personal information, and can freely decide on its use (Mayer-Schönberger 1997, 229). Accordingly, privacy regulations order the timely deletion of data, provision of information security or signposting of monitored spaces. What privacy regulations protect, then, is only a small fraction of personal liberty: individuals' control over the release and use of their personal data. The important difference is in the range of constraints these concepts encompass: data protection guards personal liberty only by restricting control over personal information, it cannot protect liberties harmed by discrimination, physical assaults or other constrictive actions. Thus, how this discourse defined personal liberty was reduced to infringements of privacy regulations.

A possible consequence of this discourse restricting the meaning of personal liberty to privacy might be that it could have displaced other discourses critical of surveillance technology (for a similar assessment, see Steeves 2009, 192). In fact, infringements of privacy regulations were the only forms of critique. The privacy critique framed smart CCTV as inappropriate, but this was not in relation to the problems that the other discourses posed. For example, the privacy critique did not oppose the proposition of the second discourse, which was to overcome the poor quality of human labor by automating it with smart CCTV. Automation of labor, as Noble (1986) points out, allows for deskilling and reorganization, sometimes disempowering the employees while privileging managerial authority. Because this is not merely an academic concern, we expected criticisms in relation to labor issues to appear in public discourse. Instead, voices of security staff were excluded from public discourse, and their roles were largely defined as an obstacle to greater public safety. Furthermore, the necessity of regulating crime by technical means – the first discourse's central claim – was hardly ever questioned. This is best exemplified by criticisms that referred to simple CCTV's low effectiveness. The argument here was that privacy infringements could not be tolerated, especially when considering the failure of simple CCTV to prevent crime. This argument shows that the privacy discourse did not consider technical regulation of crime as an undesirable aim in itself. In relation to this purpose, it did not question smart CCTV's legitimacy. The relationship between privacy and smart CCTV was thus not defined as mutually exclusive; instead, privacy was framed as a necessary *condition* of its legitimacy. This suggests that, if smart CCTV systems consider privacy regulations, then the privacy discourse would consider them to be legitimate. Finally, the privacy discourse did not refer to the variety of social consequences that surveillance practices might entail for the monitored individuals. For instance, the classification and discrimination of social groups is a major concern among surveillance scholars (e.g. Gandy 1993; Lyon 2001; and the contributions in Lyon 2003b) because of the likelihood that individuals are targeted based on bias. Again, because discrimination based on race, sex or age is not a merely academic concern, we expected it to appear in public discourse. Instead, these concerns were not addressed and targeted individuals were framed in generic terms such as "hooligans" or "terrorists", broadly defining them as potential threats to public safety. In consequence, critiques of social inequality were largely absent, while the public critique of smart CCTV was mainly concerned with infringements of individuals' privacy.

With the emphasis on privacy infringements, it is no surprise that this discourse attributes potential deficits of smart CCTV systems to violations from police bureaus, political actors and smart CCTV developers. Stronger legal control and enforcement of already existing data protection guidelines were deemed the appropriate strategy to regulate the employment of smart CCTV. The roles of data commissioners were thus defined as the main carriers of public accountability, with their trustworthiness based on their legal expertise and affiliation with data protection bureaus. The confidence in expert rationality resonates with Jasanoff's observation that, in Germany, regarding science and technology, public accountability is understood as a product of trustworthy institutions rather than "proven personal service to citizens or the state" (Jasanoff 2005, 262). Paradoxically, she observes, the strong cultural belief that expert bodies can map the entire terrain of relevant social groups renders the need for additional reasoning unnecessary, thereby potentially excluding additional concerns from the wider public (Jasanoff 2005, 269).

In summary, personal liberty in the context of smart CCTV was discussed in Germany predominantly as a regulative problem of privacy rights. This discourse staged its claim by referring to the expertise of data protection commissioners, whereas references to the potential social consequences of surveillance practices remained mostly excluded. References to public administration's promises of control underlined the project of regulating constraints of liberty through sensible legal instruments. However, by making it a matter of effective bureaucratic control, the privacy discourse, in consequence, did not question the legitimacy of smart CCTV in general; rather, it configured meeting privacy requirements as its major necessary condition.

Preliminary conclusions and suggestions for further research

If public understandings shape technology development, and the privacy discourse framed smart CCTV as inappropriate, then why did the privacy critiques not prevent the emergence of smart CCTV (or other surveillance technology, for that matter)? This is not a trivial question because, as Klein and Kleinman (2002) remind us, success and failure of technology depend not only on their social meanings, but also on structural factors, such as the distribution of power between social groups, the organization of labor, the role of the state, and of course technological preconditions. With these limitations in mind, we can begin to answer this question by pointing to the way in which the public discourse relates privacy to smart CCTV.

First, the privacy discourse interpreted the employment of smart CCTV as a potential threat to privacy requirements, but not as a threat to ideals of social equality. To answer our question, we might thus consider that the privacy critique was not able to create the same political pressure that critiques of social inequality and discrimination possibly would have achieved. At least in present-day Germany, privacy infringements for the sake of public safety seem somewhat compatible with Germany's self-image. This self-image includes political sensitivities about social inequality, which precludes open and public discussions about discrimination. Thus, we might suspect that privacy infringements do have a basic compatibility with Germany's present political culture, and that this might be one reason why the privacy discourse did not prevent the emergence of smart CCTV.

Second, although the privacy discourse defined smart CCTV as a potentially inappropriate technology, it did not define the relationship between privacy and smart CCTV as mutually exclusive. Instead, if smart CCTV systems consider privacy regulations, then the privacy discourse would consider them to be legitimate. This might be an important point in understanding smart CCTV's emergence. As Haggerty (2009) points out, opponents of surveillance technology inadvertently encourage further research and development because their critiques help guide developers toward perceived flaws in the systems. This dynamic of critique and development might also apply to the privacy discourse. Recent German technology policy indicates that the critiques seem to have pressured government into making it obligatory for most projects to include privacy experts in the development process. Privacy regulations again are explicit enough for programmers to integrate into smart CCTV systems. Thus, the participation of these experts might satisfy the privacy critique, especially because the meaning of personal liberty has already been reduced to privacy. Although it may seem paradoxical to privacy advocates who assume that their critique hinders technological development, the privacy critique actually might have contributed to the development of smart CCTV.

Qualitative research always seems to be useful in raising more focused questions, and our preliminary findings call for further comparative and historical empirical research. First, to substantiate our hypothesis concerning the differences between privacy critiques and critiques of social inequality, it would be helpful to compare our findings with the public discourse of alternative surveillance technologies. Although recent research on surveillance discourses in the UK suggests that differences between technologies are of minor importance (Barnard-Wills 2011), the perception of technological differences in Germany may also be influenced by cultural differences. Second, historical research on the German census that was planned for 1981 could prove to be helpful in understanding the cultural transformation of privacy across time. In 1981, privacy issues related to the census led to the formation of massive resistance, but today privacy seems to be regarded as a mere matter of bureaucratic regulation. Third, we encourage research on how privacy issues shape various social worlds relevant to surveillance. This would contribute to understanding the relationship between surveillance technology and its critique. In our opinion, a sociology of knowledge approach is conceptually helpful to accomplish such a disentanglement of historical and institutional configurations regarding new and emerging surveillance technologies.

Acknowledgements

We would like to thank our student assistants Anna Binder, Sophia Gredig and Livia Mattmüller for their invaluable help in organizing the data, Reini Joosten for her support putting together the source material, as well as Maja Apelt and the anonymous reviewer of *Innovation* for helpful comments on earlier drafts of this paper.

Notes

1. Note that we use a specific notion of discourse that differs considerably from other concepts, such as Habermas's discourse ethic, the post-Marxist Essex School (Laclau and Mouffe), critical discourse analysis (Fairclough, Wodak and Jäger), or ethno-methodological discourse analysis (for a discussion see Keller 2011a, pp. 20–62).

2. The first German article that explicitly and prominently discusses a smart CCTV system was published on 17 May 2006, in the electronic newsletter *heise-online* (available from: http://www.heise.de/newsticker/meldung/Flughafen-Helsinki-setzt-Software-fuers-Video-Monitoring-ein-125378.html). Also in 2006, the Bundeskriminalamt (Federal Police Office of Germany) introduced a smart CCTV pilot project that tried to combine a CCTV system with biometric facial recognition software. Because smart CCTV is an emerging technology, it might be necessary to extend the analysis to documents up to the present day.

References

Barnard-Wills, D. 2011. “UK News Media Discourses of Surveillance.” *The Sociological Quarterly* 52 (4): 548–567.

Bennett, C. J. 2011. “In Defence of Privacy: The Concept and the Regime.” *Surveillance & Society* 8 (4): 485–496.

Berger, P. L., and T. Luckmann. 1966. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. Garden City, NY: Doubleday.

Bijker, W. E. 1995. *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change*. Cambridge, MA: MIT Press.

Ferenbok, J., and A. Clement. 2011. “Hidden Changes: From CCTV to ‘Smart’ Video Surveillance.” In *Eyes Everywhere: The Global Growth of Camera Surveillance*, edited by A. Doyle, R. K. Lippert, and D. Lyon, Abingdon: Routledge, 218–233.

Foucault, M. 1972. *The Archeology of Knowledge*. London: Tavistock.

Foucault, M. 1979. *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books.

Foucault, M. 1982. *I, Pierre Rivière, Having Slaughtered My Mother, My Sister, and My Brother: A Case of Parricide in the 19th Century*. Lincoln, NB: University of Nebraska Press.

Gandy, O. H. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview.

Gates, K. 2010. “The Tampa ‘Smart CCTV’ Experiment.” *Culture Unbound* 2: 67–89.

Gouallier, V., and A.-E. Fleurant. 2009. *Intelligent Video Surveillance: Promises and Challenges: Technological and Commercial Intelligence Report*. Montréal: Centre de recherche informatique de Montréal.

Haggerty, K. D. 2009. “Methodology as a Knife Fight: The Process, Politics and Paradox of Evaluating Surveillance.” *Critical Criminology* 17: 277–291.

Haggerty, K. D., and R. V. Ericson. 2006. *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press, 3–25.

Introna, L. D., and D. Wood. 2004. “Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems.” *Surveillance & Society* 2 (2): 177–198.

Jasanoff, S. 2005. *Designs on Nature: Science and Democracy in Europe and the United States*. Princeton, NJ: Princeton University Press.

Keller, R. 2011a. *Diskursforschung: Eine Einführung für SozialwissenschaftlerInnen* [Discourse Analysis: An Introduction for Social Scientists]. 4th ed. Wiesbaden: VS Verlag für Sozialwissenschaften.

Keller, R. 2011b. “The Sociology of Knowledge Approach to Discourse (SKAD).” *Human Studies* 34 (1): 43–65.

Keller, R. 2011c. *Wissenssoziologische Diskursanalyse: Grundlegung eines Forschungsprogramms* [The Sociology of Knowledge Approach to Discourse: Foundations of a Research Perspective]. 3rd ed. Wiesbaden: VS Verlag für Sozialwissenschaften.

Klein, H. K., and D. L. Kleinman. 2002. “The Social Construction of Technology: Structural Considerations.” *Science, Technology & Human Values* 27 (1): 28–52.

Kline, R., and T. J. Pinch. 1996. “Users as Agents of Technological Change: The Social Construction of the Automobile in the Rural United States.” *Technology and Culture* 37 (4): 763–795.

Lyon, D. 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

Lyon, D. 2003a. “Introduction.” In *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, edited by D. Lyon, 1–9. London: Routledge.

Lyon, D., ed., 2003b. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge.

Lyon, D., and E. Zureik. 1996. "Surveillance, Privacy, and the New Technology." In *Computers, Surveillance, and Privacy*, edited by D. Lyon and E. Zureik, 1–18. Minneapolis, MN: University of Minnesota Press.

MacKenzie, D. A., and J. Wajcman. 1999. "Introductory Essay: The Social Shaping of Technology." In *The Social Shaping of Technology*, 2nd ed., edited by A. MacKenzie and J. Wajcman, 3–27. Milton Keynes: Open University Press.

Mayer-Schönberger, V. 1997. "Generational Development of Data Protection in Europe." In *Technology and Privacy: The New Landscape*, edited by P. Agre and M. Rotenberg, 219–241. Cambridge, MA: MIT Press.

Musik, C. 2011. "The Thinking Eye is only Half the Story: High-Level Semantic Video Surveillance." *Information Polity* 16 (4): 339–353.

Noble, D. F. 1986. *Forces of Production: A Social History of Industrial Automation*. New York: Oxford University Press.

Norris, C., and G. Armstrong. 1999. *The Maximum Surveillance Society: The Rise of CCTV*. Oxford: Berg.

Pinch, T. J., and W. E. Bijker. 1984. "The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit each Other." *Social Studies of Science* 14 (3): 399–441.

Stalder, F. 2002. "Privacy is not the Antidote to Surveillance." *Surveillance & Society* 1 (1): 120–124.

Steeves, V. M. 2009. "Reclaiming the Social Value of Privacy." In *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*, edited by I. Kerr, V. M. Steeves, and C. Lucock, 191–208. Oxford: Oxford University Press.

Strauss, A. L. 1987. *Qualitative Analysis for Social Scientists*. Cambridge: Cambridge University Press.

Strauss, A. L., and J. M. Corbin. 1998. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. 2nd ed. Thousand Oaks, CA: Sage.

Surette, R. 2005. "The Thinking Eye: Pros and Cons of Second Generation CCTV Surveillance Systems." *Policing: An International Journal of Police Strategies & Management* 28 (1): 152–173.

van der Ploeg, I. 2003. "Biometrics and the Body as Information: Normative Issues of the Sociotechnical Coding of the Body." In *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, edited by D. Lyon, 57–73. London: Routledge.