Surveillance and Privacy, Geography of

Till F Paasche, Soran University, Soran City, Kurdish Region Iraq
Francisco R Klauser, Institut de Géographie, Université de Neuchâtel, Neuchâtel, Switzerland

Abstract

Surveillance and privacy are mutually exclusive: if one increases, the other decreases. After defining these terms and their relation to each other, this article introduces key concepts in the field of surveillance studies, followed by a discussion of classical forms of surveillance and privacy invasion, namely, forms of visual surveillance. The second half of the article departs from the surveillance of individuals to new technological trends that represent new challenges to privacy concerns and the social sorting of populations through software algorithms.

Surveillance

Surveillance is a complex issue that has sparked a number of definitions. Because we have to start somewhere, we defer to two intellectual authorities in the field, Lyon (2007) and Marx (2012), who define surveillance in general terms outside the risk and security discourse in which it is often applied. Lyon (2007, p. 14) defines surveillance as follows:

> (...) the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction. Surveillance directs its attentions in the end to individuals (even though aggregated data, such as those available in the public domain, may be used to build up a background picture). It is focused. By systematic, I mean that this attention to personal details is not random, occasional or spontaneous; it is deliberate and depends on certain protocols and techniques.

Marx applies a similar individually focused angle to his definition:

> At the most general level surveillance of human (which is often, but need not, be synonymous with human surveillance) can be defined as regard or attendance to a person or to factors presumed to be associated with a person.
>
> Marx, 2012, p. xxv

While outlining various more detailed subfields of surveillance, Marx maintains a relatively strong focus on one individual or group attending to another individual or group. Thus,

> some common classificatory notion can be applied. In the case of surveillance social structures, for example, we can identify the *surveillance agent* (weather as watcher/observer/seeker/inspector/auditor/tester), while the person about whom information is sought or reported is the *surveillance subject*.
>
> Marx, 2012, p. xxv, emphasis in original

Inherently linked to these definitions is privacy, which we will discuss in the context of surveillance. The two terms can almost be understood as antipodes. The more (or less) surveillance there is, the less (or more) privacy there is. Thus, in an argument about omnipresent surveillance, we commonly speak about the death of privacy.

Privacy

Privacy is commonly seen as a good that needs to be protected against increasing surveillance activities. From this position, privacy is often defined in terms of access to information and control over this access. If surveillance is access to individual or personal information, privacy is the control over this access to information (Rössler, 2001). If we can decide who has access to what information about ourselves, we have full privacy. However, Rössler (2001), a key figure in privacy studies, argues that privacy is not only a desirable good but also a precondition for liberal democracies in which the autonomy to decide over one's own life according to one's abilities is of fundamental importance. To guarantee autonomy, a degree of privacy is needed to protect the individual. If, for example, an employer knew all the private details of an employee's life, such as mistakes in the past, diseases that do not impact the job, and relatives with criminal records, these details would likely influence employment and thus decrease autonomy. Nonetheless, as Rössler acknowledges, privacy in its purest form, i.e., complete control over all personal information, is impossible to achieve given participation in contemporary societies. The state, employers, banks, etc. will always possess some personal information about an individual that is beyond his/her control. Discussing surveillance and privacy is thus a question of balance; how much surveillance is needed to have, For example a functioning government able to provide security, and when is the invasion of the state into the privacy of its citizens unnecessary? Because many governments and governance bodies have a tendency to collect an abundance of data on their populations and thus tip this balance in one direction (Foucault, 2007), different parts of civil society, as well as many of the studies on surveillance and privacy, engage critically with the topic of increasing surveillance and its negative implications on privacy. However, as mentioned, this article approaches privacy in relation to surveillance. Therefore, we only refer to one of what Rössler (2001) calls the three dimensions of privacy. The first dimension, decisional privacy, is concerned, for example, with the freedom to decide what

clothes I put on in the morning. The dimension discussed in this article, informational privacy, is concerned with issues related to access to personal information. The last dimension, local privacy, is concerned with the ability to retreat into personal space, such as one's own home. Elements of this last dimension play a role when discussing visual surveillance in the form of drones.

Surveillance and Privacy Studies

In recent years, a rapidly developing international body of research has sought to explore the various causes, implications, and problems of the contemporary proliferation and intensification of surveillance. The emerging cross-disciplinary field of 'surveillance studies' (Lyon, 2007) has raised a number of critical issues with regard to the intensification and generalization of data gathering, transfer, and analysis in the information age. The resulting critical debates about surveillance fit largely into two complementary and often interrelated categories. The first category – predominant in sociology and urban studies – has sought to challenge the use of surveillance as a powerful tool for social sorting (Lyon, 2003) and is related to concerns of social exclusion and spatial justice (Coleman, 2004). The second category, traditionally predominant in regulatory approaches, has focused mainly on surveillance-related privacy and data protection issues.

In this article, we will touch on both categories. Following an introduction of the concepts and theories that explain surveillance, we introduce surveillance in its classical, human-focused form, drawing on the example of visual surveillance. We then shift our attention to the monitoring of the nonhuman, the foremost of which is urban aspects. As surveillance studies have shown, ubiquitous computing embodied by the various smart campaigns, can have a significant impact on the private even though the focus is not directly on the individual. We outline the social consequences of the various surveillance approaches in our final section.

Competing Concepts

There are different approaches to theorizing surveillance in its multiple facets, applications, and effects. Space does not permit an exhaustive review of the existing approaches, but some of the most important conceptual perspectives on surveillance shall be outlined here to add a more theoretical dimension to our discussion of surveillance and privacy that follows (for a more exhaustive discussion, see, for example, Lyon, 2006).

Surveillance scholars have found a range of conceptual tools in Michel Foucault's theorization of power and governmentality for dealing with the dynamics inherent in contemporary forms of control and regulation. Most notably, Foucault's analysis of disciplinary power, exemplified in his discussion of the Panopticon in *Discipline and Punish* (Foucault, 1977), has inspired a number of empirically and conceptually informed discussions on the normalizing prowess of novel surveillance technologies on individuals and social groups. For Foucault, the Panopticon exemplifies a particular economy of power that characterizes European modernity shaping, working through, and developing from a range of milieus such as hospitals, schools, army barracks, and prisons. The exercise of power in all of these settings implies a specific way of managing multiplicities through techniques of individualized surveillance and normalization.

However, while Foucault's Panopticon paradigm has been used prominently to problematize surveillance in its inherent power problems and implications, additional approaches have been mobilized to create a more conceptually and empirically accurate picture of the actual effects and limits of contemporary surveillance. For example, drawing on Deleuze's analysis of the contemporary shift from a Foucauldian 'disciplinary society' to a postmodern 'society of control' (Deleuze, 1992), various scholars have emphasized the changing modalities and functions of surveillance, from rigid and permanent monitoring and enclosure to more flexible and adaptable forms of regulation and control. Similar insights have been gained from Foucault's recently translated *Security, Territory, Population* lectures, given in 1977/1978 at the College de France (Foucault, 2007). Here, Foucault distinguishes between 'disciplinary' and 'security apparatuses' to capture the differing regulatory dynamics and mechanisms of power in the governing of men and things. A third source of inspiration in counterbalancing the Panopticon paradigm has been found in Michel de Certeau's work, who stresses the microtactics and strategies deployed by individuals and social groups to resist surveillance (De Certeau, 1984). On these grounds, the effects and implications of surveillance on social life (including privacy) have been found to be much more contingent and complex than initially expected.

While Foucault, Deleuze, and de Certeau allowed for the theorization of the effects and implications of surveillance, other theoretical sources have been mobilized to conceptualize the actual internal functioning, logic, and organization of specific surveillance systems. On a rather general level, approaches inspired by Marx and especially Giddens (1985) have portrayed (bureaucratic) surveillance as indeed a defining and constitutive feature of modern capitalist life. More specifically, rooted in an actor-network theory-based line of thinking, as developed by Bruno Latour and Michel Callon (Latour, 2005), various scholars have studied the complex actor networks underpinning and shaping the making of particular surveillance systems. Placing centrally the processes and relationships through which surveillance is conditioned and coproduced, this research has developed an understanding of surveillance in its complex sociotechnical associations and compositions that bring together, and are the result of, a wide range of actors, objects, instruments, intentions, and domains of expertise. This focus also resonates with the longstanding conceptual and empirical interest of Deuleuzian literature in the heterogeneous 'assemblages' of human and nonhuman entities that make up specific milieus or, more specifically speaking, surveillance systems (Deleuze and Guattari, 1987; Haggerty and Ericson, 2000). In terms of privacy, these studies have shown that the implications of surveillance depend on a variety of system-inherent factors, including not only its technical specificities but also resulting from the modalities, dynamic actor

networks, and interacting domains of expertise shaping the system 'in action.'

Visual Surveillance

CCTV

In this section, we discuss one of the most classic themes in surveillance and privacy studies, the CCTV (closed circuit television) camera, and some of its contemporary modifications, such as facial recognition software and drones. The first major boom in the use of CCTV cameras for surveillance and security purposes started in the late 1970s and continued into the 1980s. Particularly in the beginning, CCTV cameras in public space were hailed as a revolution in crime prevention, a claim that failed to manifest itself clearly in empirical data. Although the installation of surveillance cameras often results in a short-term reduction of crime rates, longer follow-up periods show that the cameras' long-term effects in deterring crime have to be interpreted more critically (Welsh and Farrington, 2002; Gill and Spriggs, 2005). Furthermore, a growing range of CCTV evaluations suggest that the efficiency of CCTV strongly depends on which type of crime is being analyzed. For example, CCTV is generally found to be effective in reducing vehicular crimes in car parks, whereas empirical research suggests that CCTV has little or no effect on vandalism and acts of aggression on public transportation systems and in city-center settings. The functioning and impacts of CCTV systems also depend on a variety of system-inherent factors, from collaborations between operators to technical dimensions of the cameras. Nonetheless, the number of cameras in various spaces continues to grow. In the United Kingdom, a country where the CCTV camera enjoys particular popularity, there are an estimated 1.85 m cameras ('The Guardian' http://www.guardian.co.uk/uk/2011/mar/02/cctv-cameras-watching-surveillance). Today, in many countries, high-resolution CCTV cameras can be bought in home improvement shops, and where they can be installed is only limited by national legislation.

Intelligent CCTV Systems

Throughout the 1980s and 1990s, CCTV systems were established and simply continued to exist more or less effectively; however, recent coded technologies have generated a new wave of excitement about CCTV cameras. The availability of large affordable digital storage facilities and fiber-optic cables has made cameras more effective for investigatory proposes and made intelligent networked CCTV systems possible. With continued research on increasingly sophisticated algorithms that can recognize faces, license plates, and even behavior patterns, cameras are becoming exponentially more effective (Graham, 2005). Where there used to be a human agent sitting in front of a wall of screens trying to detect suspicious individuals, code now automates this process. For example, by comparing faces to a database of terror suspects or registered hooligans, the algorithm can sound an alarm once a suspect is sighted or near a strategic facility. Although code is not yet capable of such sophisticated procedures, vast amounts of resources are being invested into the advancement of already existing recognition technologies.

Drones

Another technology that led camera-based surveillance into a new era is the unmanned aerial vehicle (UAV), commonly referred to as drones. UAVs further exemplify the close link between military and civilian surveillance technologies. During the War on Terror and various campaigns of counterinsurgency warfare, drones became increasingly popular and have undergone rapid development in recent years. UAVs are now integral to the warfare practices of technologically advanced armies. What started as surveillance tools soon became armed machines, as the latest versions of the Reaper drone show. Using drones in conflicts, intelligence can be collected and (extraterritorial) attacks carried out without putting pilots in danger (in fact, drone pilots can command their vehicles for a mission over Pakistan from their 'cockpits' in the United States). In their original function as surveillance tools that film or take images from high altitudes, UAVs thus complement satellites but are not bound to a single orbit. Like other developments originating in the military, UAVs soon caught the attention of law enforcement and other civilian agencies. As Graham argues,

> The crossover between the military and the civilian applications of advanced technology – between the surveillance and control of everyday life in Western cities and the prosecution of aggressive colonial and resource wars – is at the heart of a much broader set of trends that characterize the new military urbanism. (…) Fundamental to the new military urbanism is the paradigmatic shift that renders cities' communal and private spaces, as well as their infrastructure – along with their civilian populations – a source if targets and threats.
>
> Graham, 2010, p. xiii

With wars and conflicts being fought increasingly in urban areas, the line between military and civilian surveillance and other technologies is becoming blurred as technologies increasingly serve double functions. Today, UAVs come in all shapes and sizes, ranging from high-tech military drones with wingspans of well over 20 m to small surveillance UAVs that can land on the palm of a hand. Smaller UAVs are becoming increasingly popular with police forces all over the world for obtaining intelligence on armed suspects, groups of protesters, and sports fans or simply for monitoring deserted urban landscapes more efficiently. As mentioned above, UAVs constitute a quickly developing technological field whose development cannot be foreseen. Given their relative low costs and multifaceted functions for surveillance purposes, it is unlikely that drones will disappear from the CCTV/surveillance landscape soon. Combined with high-definition cameras and facial recognition software, drones are the latest high-tech advancement in a surveillance trend that started with the classic CCTV camera in the 1980s. Whereas the usual CCTV camera is stationary, although it may rotate, drones are highly mobile and able to survey many spaces previously unseen by CCTVs. In this context, local privacy, or the freedoms in one's own home, is under threat by the image of a drone hovering in front of a bedroom window (Rössler, 2001). As the technological possibilities increase exponentially, substantial further invasions of

privacy continue to be protected only by a critical civil society and the law, at least in Western democracies.

Computerization of Surveillance

Having outlined the more obvious forms of direct surveillance, we now focus on a more recent surveillance trend beyond the visual that focuses on the monitoring of the nonhuman. Today, we have reached an area of ubiquitous computing, where code penetrates most aspects of life and enables the management of urban environments, including both human and nonhuman objects. The logic of this approach of managing the urban environment is not new, although the first cases were human-oriented. The basic ideas of these current trends date back to the late nineteenth and early twentieth centuries and the first use of punch cards that enabled the structuring of relatively complex data on populations according to different characteristics. A similar logic was utilized by the German police in the late 1970s when *Rasterfahndung* (dragnet policing) was introduced in an attempt to identify members of the *Rote-Armee Fraktion* (Red Army Faction) and other left-wing terror groups. Using a state-of-the-art computer, various available sources of information, such as student loans, insurance, and registration data, were analyzed to obtain a manageable number of locations and suspects assumed to be typical for terrorists. In principle, the process included analyzing large data sets according to set parameters to generate a small number of individualized data.

However, only in recent years have computers and technologies such as GPS tracking and mobile phones become advanced and widespread enough to integrate algorithms into the functioning of everyday lives. Such advancements include RFID (radio-frequency identification) devices, which, by now, are ubiquitous in various trades and have become an unavoidable standard technology. RFID chips store information that is being transmitted via radio frequencies. If the chip comes close enough to a receiver from a few centimeters to hundreds of meters, the information can be read. RFID chips, some of which are not much larger than a grain of rice, can be found in access, food court and student cards, pets and livestock, shipping containers and other cargo, among other things. With a starting cost of just a few pence, the only reason RFID chips are not used even more extensively is data protection concerns, which are why chips have not been put in clothes (the washing machine would automatically know what temperature to use) or directly implemented in humans (this would make it impossible to forget ID cards and easier for police to identify individuals).

This increased computerization of life and dependenc on code led Dodge and Kitchin (2011) to formulate their code/space theory. Some years ago, code supported the functioning of space, as it eased daily operations. If the code broke away or malfunctioned, all operations could, although more slowly and less efficiently, continue. Although this coded space was supported by computing, it did not depend on it. In many instances, this has changed. Today, various spaces depend on code in a way that if the code breaks away, the whole space stops functioning. One example of such a code/space is the modern airport. If the various algorithms that enable check-in, baggage sorting, the functioning of the tower, or the functioning of the planes themselves stop working, the space is no longer an airport, but a chaotic agglomeration of hectic and panicking people. Dodge and Kitchin (2011) provide other examples of how we interact with more banal forms of code/space every day, including diaries in our smartphones, access to our e-mails, the engine of our car managed through the inboard computer, the electronic till of our favorite coffee place, and possibly even the entrance to our office building controlled by a swipe card or RFID chip. All of those examples are spaces that stop functioning in their designed purpose if the code breaks away.

Privacy and Contemporary Smart Surveillance

With the popularized smart city ambitions that are currently symptomatic for the management of urban environments, the idea of code/space is developed to a further extreme. In the context of the hyped smart city technologies, the linkages between increasing computerization and surveillances and privacy become clear. As explained with the example of punch cards and the *Rasterfahndung*, large data sets, are being combined and analyzed. In a process called data mining, linkages within data are made, and new information is extracted. Urban processes are managed on the basis of this new information, possibly resulting in the automation of parts of cities and buildings.

The smart city is currently one of the most prominent urban development technology and is being discussed around the world. Spearheaded by global IT companies, the smart city aims to optimize different aspects of urban space through algorithms. Targeted areas of cities include governance structures, water and electricity grids, traffic and transport, and the emergency services and police. Although part of different sectors, their automations all follow a similar logic, the analysis and interconnection of large quantities of data, including existing data being made available as well as the generation of new data either by digitizing analogous processes, such as electricity meters and sensors on highways or in public transport, or connecting different existing databases. Data are cumulated in vast databases, and once the data are centralized, algorithms can make the city, smart, by rendering the data usable for different optimization proposes, a process called data mining. Such optimization processes include more effective governance function as decisions can be based on the analysis of more data and thus be made faster, optimizing public and individual transport, for example in terms of travel time, or easing access to medical data.

Nonetheless, the data sets these mining algorithms analyze often comprise sensitive and private information. One example is the use of a smart grid, one component of the smart city. Smart grids are one technology experts see as the future of energy production and consumption; they are based on the analysis of the energy patterns of individual households through algorithms and, subsequently, the automation of some electronic appliances through code. The data collected in this process provide insights on individual habits and movement patterns (for example when one takes a shower, leaves the house, watches TV, uses electronic appliances).

The primary function of smart grids is the optimization of energy consumption and increases in alternative energy sources. Although these are honorable ambitions, to get there,

unrepresented amounts of private data are collected with increasing standardization of these technologies. Additionally, these data can potentially serve a secondary purpose; detailed personal information is of considerable value to the advertisement industry, which can create localized and personalized advertisements. This information could be of value to companies interested in the activities of their employees and police who would gain *Rasterfahndungs* capabilities that were unimaginable 30 years ago. Differing from the classical definition of surveillance of Lyon and Marx or the example of the CCTV camera that singles out suspicious individuals, the current trend of surveillance is to collect a variety of data on different aspects and to extract individualized information out of this data pool. Because they are not open or direct, these surveillance functions become blurred to the public eye and are ultimately trivialized by both the surveying agencies and the surveyed population.

Thus, the smart city exemplifies an increasing belief that cities cannot be managed without substantial invention by code and that the complexity of urban lives requires algorithms to regulate them. Indeed, there are arguments that underline the advantage of codes regulating and managing the urban space. However, these developments are rarely discussed with regard to surveillance, and the substantial invasion of privacy is of limited concern. In many contemporary examples, code/space issues of privacy and surveillance are deferred to the legal and institutionalized theme of data protection and detailed accounts on technical solutions against, for example hackers that want to invade privacy and/or abuse private data. What data are really needed in the first place is of lesser concern. Furthermore, with smart city ambitions, it is often automatically assumed that the state is immune to any form data abuse and thus can be trusted with vast amounts of very detailed personalized data, an assumption that was often contested in the past. In the concluding section, some of the implications of this trend are sketched out.

Social/Software Sorting

In this concluding section, we outline the consequences of surveillance, especially the impacts new coded forms of surveillance have on society and privacy. The increasing metamorphosis of space supported by code into code/space creates a situation where it is increasingly difficult, and in some parts impossible, to have control over personal information, who has access to this information, and how this information is being used. This difficultly is evident in our digital traces on the World Wide Web or mobile communication networks, the RFID chips in the cards in our wallets, and the sophisticated CCTV cameras that are watching us.

It is even more difficult for an individual to control his/her personal information with the spatial manifestations of smart cities and related visions based on data mining. By combining different information, code generates new data and information. Because we usually do not know the source information the data mining uses or the workings and capabilities of the code, we no longer have the chance to understand what knowledge about us exists. Linking this back to Rössler's privacy discourse, our autonomy is threatened by this development. In an environment of data mining and networked information, we cannot be certain what our opposite in a meeting might see on his/her screen about us; thus, we lose the ability to control our lives, and the chance of discrimination on the basis of private information grows concurrently. Privacy is increasingly no longer a right.

In addition to its implication on privacy, the computerization of space also enables an increasingly sophisticated sorting of populations along set parameters, as three examples outlined by Graham (2005), Lyon (2003), and Jones (2000) will show.

- Using code to control and regulate traffic flows: Utilizing software tools, road pricing becomes flexible and adaptable, different from the static vignette system some countries apply. Steering congestion through road pricing, the usage of streets during peak hours can become too costly for some at certain times. Although this is a specific example, it relates to the wider issue of managing space and populations, governing at a distance through code (Jones, 2000).
- Using codes to structure the city and manage police patrols: Using software such as geographic information systems (GIS), cities are becoming increasingly digitized. Attributing data to parts of the city, individual streets and so forth, space is being branded, identities are being created, or property prices are being influenced (Graham, 2005). A popular example is the online GIS-based crime mapping tool of the British police (http://www.police.uk/).
- Direct forms of coded exclusion and sorting: Code enables different form of exclusion. Although some of the following could theoretically be achieved, for example using ordinary keys, code eases processes and renders them useable, especially on a large scale. The most banal forms of exclusions include PIN codes, relatively cheap swipe cards, and using biometrics, such as fingerprints or iris scanners, to allow access to buildings. Here different levels of access can be allocated to individuals. The same can be applied to the virtual worlds of inter- and intranets. With the increasing importance of codes for access, the rejection of access privileges can be used in a disciplining way, punishing behavior.

This list could continue. However, the aim is not to produce a complete picture, but to indicate the issues that will arise with an increasing codification of live and space and rapidly advancing computing possibilities. However, the above is not a phenomenon that has emerged because of new possibilities in surveillance, but is rather a reflection of the long-existing desire of various agencies to survey and to manage the surveyed.

> If surveillance as social sorting is growing, this is not merely because some new devices have become available. Rather, the devices are sought because of the increasing number of perceived and actual risks and the desire more completely to manage populations – whether those populations are citizens, employees, or consumers.
> Lyon, 2007, p. 20

New code-based technologies support this desire for surveillance and data collection. What gives the development

a novel spin is that the omnipresence of a code, very different from CCTV cameras, begins to blur the line between surveillance and the invasion of privacy. This is especially true when the focus is not safety and security, but the improvement of urban space and the quality of life.

See also: Policing; Privacy: Theoretical and Legal Issues; Smart Cities; Surveillance Studies; Technology and Social Control.

Bibliography

Coleman, R., 2004. Reclaiming the streets: closed circuit television, neoliberalism and the mystification of social divisions in Liverpool, UK. Surveillance and Society 2, 145–160.

De Certeau, M., 1984. Practice of Everyday Life. University of California Press, Berkeley.

Deleuze, G., October 1992. Postscript on the societies of control, vol. 59. MIT Press, Cambridge, MA, 3–7.

Deleuze, G., Guattari, F., 1987. A Thousand Plateaus. University of Minnesota Press, Minneapolis.

Dodge, M., Kitchin, R., 2011. Code/Space. Software and Everyday Life. MIT Press, Cambridge, MA.

Foucault, M., 2007. Security, Territory, Population. Palgrave Macmillan, London.

Foucault, M., 1977. Discipline and Punish. Pantheon Books, New York.

Giddens, A., 1985. The Nation-State and Violence. Polity Press, Cambridge.

Gill, M., Spriggs, A., 2005. Assessing the Impact of CCTV, Home Office Research Study 292. Home Office, London.

Graham, S., 2005. Software-sorted geographies. Progress in Human Geography 29, 562–580.

Graham, S., 2010. Cities under Siege. The New Military Urbanism. Verso, London.

Haggerty, K., Ericson, R., 2000. The surveillance assemblage. British Journal of Sociology 51, 605–621.

Jones, R., 2000. Digital rule: punishment, control and technology. Punishment & Society 2, 5–22.

Latour, B., 2005. Reassembling the Social. University Press, Oxford.

Lyon, D. (Ed.), 2006. Theorizing Surveillance: The Panopticon and Beyond. Willan, Cullompton.

Lyon, D., 2007. Surveillance Studies. An Overview. Polity, Cambridge.

Lyon, D., 2003. Surveillance as social sorting: computer codes and mobile bodies. In: Lyon, D. (Ed.), Surveillance as Social Sorting. Privacy, Risk, and Digital Discrimination. Routledge, London, pp. 13–30.

Marx, G., 2012. "Your papers please": personal and professional encounters with surveillance. In: Lyon, D., Ball, K., Haggerty, K. (Eds.), International Handbook of Surveillance Studies. Routledge, London, pp. xx–xxxi.

Rössler, B., 2001. Der Wert des Privaten. Suhrkamp, Frankfurt a.M.

Welsh, B.C., Farrington, D.P., 2002. Crime Prevention Effects of Closed Circuit Television: A Systematic Review, Home Office Research Study 252. Home Office, London.