Surveillance & Society

Article

Video Surveillance and the Right of Access: The Empirical Proof of Panoptical Asymmetries

Robert Rothmann

University of Vienna, Austria.
robert.rothmann@univie.ac.at

Abstract

This interdisciplinary paper examines visual power relations in urban settings under video surveillance and the right of access as a central feature of privacy regulation. The aim is to analyze whether citizens can actually exercise their legally stipulated right to access, and how data controllers react to and handle such requests. The deeper focus is on revealing normative perceptions in regard to visual privacy and surveillance in everyday life. From the theoretical point of view, the concept of panopticism is critically examined as a simplifying and overused approach. Thus, this study represents a micro-sociological assessment of panoptical power asymmetries as a normative order of surveillance. Employing the methodological approach of *"breaching experiments"* by Garfinkel, a series of access requests were carried out with an overall number of 29 locations analyzed. By applying the right of access as a legal corrective measure, opposing the idea of one-sided surveillance, the panoptical power structure is challenged. However, the empirical analysis shows that the right is refused, denied and largely undermined by data controllers and their representatives. The legal entitlement to access one's personal data is often not recognized, whereas rejecting and shielding is a key coping strategy used by surveilling entities. Thus, the socio-technical asymmetry of surveillance prevails and the normative figure of panopticism becomes evident in the monitored routines of everyday life.

Introduction

In contemporary societies, video surveillance has become an integral part of everyday urban life (Graham 1998). Presented and advertised as a security measure (Rothmann 2010), the practical use of the technology has become widely accepted and is seemingly not questioned by the affected population (Honess and Charman 1992; Bennett and Gelsthorpe 1996; Ditton 2000; Reuband 2001; Hempel and Töpfer 2004; Spriggs et al. 2005; Kudlacek 2015). People seem to have forgotten that video surveillance is still a surveillance technology, which does not constitute normalcy, but rather a legally justifiable intervention in the privacy of the citizens concerned. In this context, the fundamental right to privacy has a defence function. Whenever personal (image) data are processed, protective rights are defined for the affected data subjects.[1]

[1] Cf. Articles 12 and 14, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Union *L 281*.

Rothmann, Robert. 2017. Video Surveillance and the Right of Access: The Empirical Proof of Panoptical Asymmetries. *Surveillance & Society* 15(2): 222-238.
http://library.queensu.ca/ojs/index.php/surveillance-and-society/index | ISSN: 1477-7487

The aim of this study is to examine the right of access to one's personal data in the case of video surveillance as an essential aspect of privacy and data protection.[2] It focuses on the practical enforceability of the legal entitlement and the normative perception held by the data controllers and their representatives. The paper investigates how system operators react to such access requests and how they handle them formally. The underlying assumption is that questioning such a widespread and predominantly positively perceived surveillance practice such as video surveillance will be regarded as an offence and a breach of norm in the social structure. This, by implication, would mean that the panoptical asymmetry has already become a somewhat normal phenomenon in everyday urban life.

The article is structured as follows. First, a theoretical framing takes place, in which the social dimensions of visual privacy are explained. Secondly, the concept of panopticism is critically discussed, in which the simplified visual inequality is qualified by different practices and types of counter-surveillance. In this context, access requests are defined as emancipatory engagement and a right of control to counterbalance the power asymmetries of surveillance. Subsequently, the legal basis is outlined and the provisions of the data protection law in the case of video surveillance are presented as a guideline for the practical application of access requests. Building on that, the methodological approach of *"breaching experiments"* (Garfinkel 1967) is introduced as a possibility to make social norms and expectations tangible. Finally, the empirical section provides an overview of the examined locations and a detailed discussion of the findings and reactions of the data controllers and their representatives. The analysis is followed by a broader socio-legal discussion of problematic aspects and difficulties in the enforcement of a person's right to access their personal data. In closing, the paper provides some practical and legal recommendations and concludes with a summary and the theoretical embedding and explanation of the key findings.

Theoretical Framing

Visual Sociality in Everyday Life

To look at and observe each other is a form of social interaction. Georg Simmel describes moments of visual face-to-face interaction as *"maybe the purest social interdependences which generally exist"* (1908/1992: 724) already in the beginning of the 19th century. According to him, even the slightest hint of avoiding somebody's eyes and *"looking away"* interrupts this unique character of social reciprocity. It is obvious that visual aspects affect and shape social situations and gatherings in everyday urban life (Goffman 1971; Rammert 2002). The search for and avoidance of eye contact, the brief exchange of glances, hiding behind sunglasses or looking away at short spatial distance like in the subway or on the elevator (Simmel 1908/1992; Rammert 2002; Hirschauer 1999)—all these visual elements can initiate and terminate interactions and define social order. The appropriate time and intensity for looking at fellow humans is a matter of delicacy and greatly depends on the setting (Goffman 1971). People may feel provoked and react aggressively when stared at. In this sense, a person's gaze has the potential to be a visual and informational form of privacy intrusion into someone else's *"Territory of the Self"* (Goffman 1971: 28). Moreover, in various social situations power is exercised by visual hierarchy and (one-sided) monitoring. In times of American slavery, for example, *"[...] looking at a white person, especially a white woman or person in authority, was forbidden for those classified as 'colored' [...]."* (Mirzoeff 2011: 482). Hence, lowering one's eyes can be understood as a gesture of humility and submission, whereas looking down on others can be an indication of sovereignty, control and domination.[3]

---

[2] The right of access is probably the most important right for the affected citizens because if they are barred from accessing information about themselves, it is not possible to exercise other rights such as the right to rectification or deletion of data. Cf. IRISS (2015): European Policy Brief: Recommendations to the Council of the EU and the European Parliament on access rights, in the context of the European data protection reform. Available at: http://irissproject.eu/wp-content/uploads/2015/02/IRISS-POLICY-BRIEF.pdf (accessed 05/10/2016).

[3] Goffman (1971: 40 f) further states that the greater the power and the higher the social rank, the greater the size of all territories of the self and the greater the control across the boundaries.

Panoptical Asymmetries and Participatory Culture

The above considerations on visual sociology likewise apply to video surveillance in the sense of unequal dimensions of being looked at and looking through the medium of a camera. In this context, the German sociologist Werner Rammert (2002) speaks of a technical disturbance of the natural observation regime. He holds that the socio-technical constellation of video surveillance causes an imbalance in the visual order of everyday life.

Visual and informational imbalance is a fundamental characteristic of the model of panopticism (Foucault 1975: 195). Although this article is not about a simplified adoption of the concept, it can nevertheless be said that panopticism is a central theoretical approach in the field of Surveillance Studies. The model postulates a prison building whose circular architecture allows for an observation of the inmates in their cells at all times. Simultaneously, the centrally located observation room is equipped with one-way mirrors, making the surveillance unidirectional and seemingly omnipresent to the inmates. According to Foucault (1975: 201), the *"... Panopticon is a machine for dissociating the see/being seen dyad: in the peripheric ring, one is totally seen, without ever seeing; in the central tower, one sees everything without ever being seen."* Following the principle that power must be visible but opaque, panoptical surveillance appears permanent and automated even if it is only sporadically executed. The model of panopticism and its visual and informational asymmetry is considered to be typical for surveillance processes and is also apparent, for example, in the design of so-called *"dome cameras."*[4] Treatises on the topic of video surveillance therefore frequently make reference to Foucault and his illustrations.

While the dominant influence of the concept is broadly acknowledged, increasing criticism has been voiced regarding its non-reflective and inflationary adoption (McCahill 1998; Norris and Armstrong 1999; Lyon 2001, 2005; Haggerty 2006; Kammerer 2008; Boyne 2000; Han 2014). It is assumed that video surveillance differs from the panoptical ideal in various aspects. For example, the observed persons are not spatially confined like prisoners, but free to move into and out of the monitored area. Another point is the rigid structural inequality between the watcher and the watched, which, as it seems, no longer applies in everyday life.

Current developments suggest that the distinction between the surveilling entity and the subject of surveillance has become less absolute (Koskela 2011). The ongoing neoliberal privatization and a shift in the *"culture of control"* (Garland 2001) have led to an interweaving of public (governmental) and private (citizen-led) sectors (Pöschl 2015), resulting in a tendency to utilize civil society as participants in the *"surveillance work"* (Koskela 2011).

In addition, progress in the field of digitization seemingly entails a kind of technical emancipation. The difference between surveillance cameras and other equipment has blurred and the low cost of procuring video and surveillance equipment has led to more and more private persons using these devices for their own ends as a vehicle for empowerment (Koskela 2011). Thus, the active role of citizens in the production of video footage turns the concerned subjects into surveillance entities themselves (Koskela 2011; Han 2014; Schaefer and Steinmetz 2014). Moreover, the prevalence of *"Web 2.0"*-based internet services and the ubiquitous dissemination of (image) data have seemingly altered the discourse of one-sided surveillance in terms of a voluntary *"Participatory Culture"* (Fuchs 2014: 52). Surveillance has changed from a predominantly top-down control mechanism to a practice to which almost anyone can contribute (Koskela 2011). This not only means a strong increase in the operation of video surveillance systems by

[4] A *dome camera* is a special type of video surveillance camera with a semi-spherical tinted dome around the lens, which makes it difficult for passers-by to see the actual direction in which the camera is pointing.

private companies and citizens, but also variants of self-monitoring[5] and self-staging[6] (Koskela 2004: 2011; Kammerer 2008; Han 2014) and raises significant new legal questions regarding the distribution of responsibility in regard to the provision of content and the related processing of personal data (Mülleder 2014; Pöschl 2015).

Sousveillance, Counter-Surveillance and Access Requests

The easy access to video and surveillance technology has also led to forms of surveillance targeted at the supposed authority. When this happens intentionally, it is usually referred to as *"sousveillance"* or "*counter-surveillance*" in scientific literature (Mann et al. 2003; Monahan 2006, 2010; Schaefer and Steinmetz 2014).

In contrast to surveillance in the traditional sense, the approach of "*sousveillance*" by Mann et al. (2003) is a sort of "*surveillance from below*," meaning that sousveillance is the surveillance of the surveilling entity by the surveilled subject(s). Sousveillance is a reflexive process to mirror and confront the organizations of surveillance. Its fundamental notion is based in part on the movement of the Situationist International, but it is also viewed as a form of democratic participation. As a performative strategy, sousveillance inverts the controlling gaze of institutions, with the intent of both a form of resistance by evidence and technologically supported interaction at eye level: *"It is a model, with its root in previous emancipatory movements, with the goal of social engagement and dialogue"* (Mann et al. 2003: 347).[7]

Monahan (2006: 516), in turn, defines counter-surveillance as *"intentional, tactical uses, or disruptions of surveillance technologies to challenge institutional power asymmetries."* In his article, Monahan refers to activities like disabling or destroying surveillance cameras, mapping paths of surveillance and publishing this information online, or staging public plays to draw attention to the prevalence of surveillance in society.

An early example of sousveillance or counter-surveillance in the form of "*cop-watching"* (Schaefer and Steinmetz 2014) is provided by the Rodney King case of 1991, in which violence by police officers against a vehicle driver in Los Angeles was filmed by a witness using a handheld video camera.[8] Another example with regard to car traffic comes from Ukraine, where corruption among police has recently caused a rise in sousveillance by automobile drivers: when stopped by the police, they record the proceedings of the identity check using a small video camera affixed to their car dashboard.[9]

Such practices and strategies are inconsistent with a simplistic adoption of the theoretical concept of panopticism and its underlying idea of power distribution. The same applies to the right of access, whose effectiveness and social anchorage in everyday life is discussed and analyzed in this study. Access requests can be understood as *"emancipatory engagement"* with the entities of surveillance and

---

[5] Lifecaster Jenny Ringley (JenniCam), who began publishing her life on the internet using a webcam in 1996, is often considered a progenitor of this trend—Cf. Jennifer Ringley (JenniCam), http://en.wikipedia.org/wiki/JenniCam (accessed 05/10/2016).

[6] More current variants of self-staging are the party videos by Boiler Room or the phenomenon of *"selfies,"* which has—not least—emerged through the proliferation of mobile computing and smartphones, cf. Boiler Room (06/06/2015): Peter Kruder Boiler Room Vienna DJ Set, https://www.youtube.com/watch?v=eZh2vhmype4 (accessed 05/10/2016).

[7] A radical example of sousveillance and breaching the norm of visual privacy is provided in the videos by the *"Surveillance Camera Man,"* http://www.liveleak.com/c/surveillancecameraman (accessed 05/10/2016).

[8] The subsequent acquittal of the officers sparked urban riots lasting several days ("LA Riots"). Cf. multishowtvweb (published on 03/12/2015): RODNEY KING BEATING VIDEO Full length footage SCREENER, https://www.youtube.com/watch?v=sb1WywIpUtY (accessed 05/10/2016).

[9] Cf. ORJEUNESSE (uploaded on 01/24/2011): ГАИпостнаМ4 ШахтыпопыткаразводаИДПСнаскорость, http://www.youtube.com/watch?v=Kr6tQ9FFroY (accessed 05/10/2016).

theoretically framed as a legally supported variation of *"sousveillance"* or *"counter-surveillance.*" They question the ongoing monitoring and serve as a possibility of controlling the system operators in charge. But there are also crucial differences: conducting a single access request is not necessarily a form of (counter-)surveillance, especially because it is possible that the data controller refuses the request.[10] The most important distinction between subject access requests and the activities discussed by Monahan (2006) and Mann et al. (2003) is the explicit foundation in data protection law. While sousveillance or counter-surveillance can also be seen as a kind of resistance or even as an illegal act (Monahan 2006), access requests have a legal basis. The law grants citizens access to their own data, if they are affected by a privacy intrusion. This ultimately also means that—in contrast to various more or less artistic forms of sousveillance and counter-surveillance—access requests must be performed in compliance with legal provisions. In this sense, the data protection regulations serve as a methodological guideline on how to perform access requests in everyday life.

Legal Framing and Requirements

Privacy as a Fundamental Right

From a legal point of view, citizens are in principle protected against (visual) surveillance by their right to privacy and data protection, which is established and codified, for example, by the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights (ECHR) or the European Data Protection Directive.[11] In Austria, the Directive has been implemented and transposed to the national level by the so-called Data Protection Act (DSG 2000), which includes a specific section on video surveillance.[12] All these regulations provide citizens with a fundamental legal framework that is intended to ensure freedom from arbitrary (visual) privacy intrusion.[13] Interference in these rights may only occur under certain predefined legal conditions.[14]

The Right of Access as Legal Corrective

Whenever personal (image) data are processed, additional protective rights apply to persons affected. In this regard, the right of access is a key feature of data protection and regulates the relationship between citizens and the surveilling organizations.[15] The entitlement to access is also closely linked to the right of rectification, deletion, and the right of objection. The Charter of Fundamental Rights, for example,

---

[10] This also depends on how the request is conducted, recorded and documented.

[11] Cf. Articles 7 and 8, Charter of Fundamental Rights of the European Union (2000/C 364/01), Official Journal of the European Communities, C 364/1, 12/18/2000; Cf. Article 8, European Convention on Human Rights (ECHR); Cf. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Union *L 281;*www.ris.bka.gv.at.(accessed 05/10/2016).

[12] Cf. Section (9a); Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000), BGBl.I Nr. 165/1999 idgF; see: Rechtsinformationssystem (RIS), www.ris.bka.gv.at. (accessed 05/10/2016).

[13] In addition, visual data are considered to be sensitive information as personal aspects such as ethnicity, religious affiliation or the (state of) health can be identified (via video footage). Cf. § 4 (2) Austrian Data Protection Act (DSG 2000).

[14] Such conditions are, for example, vital interests or the consent of those affected, but also overriding legitimate interests of third parties. Legitimate purposes are the protection of the monitored object, the protection of the monitored person, and the fulfilment of legal due diligence. This usually requires a private-law legal relationship to the monitored object (ownership structure or tenancy) or to the monitored person (by legal or contractual due diligence). Private video surveillance operators are generally not permitted to monitor foreign property or third parties (without consent). In addition, the operation of a video surveillance system must be covered by appropriate legal powers and may only be conducted in the necessary (proportionate) extent (Ennöckl 2014).

[15] Cf. IRISS (2015): European Policy Brief: Recommendations to the Council of the EU and the European Parliament on access rights, in the context of the European data protection reform. Available at: http://irissproject.eu/wp-content/uploads/2015/02/IRISS-POLICY-BRIEF.pdf (accessed 05/10/2016).

stipulates that *"[e]veryone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."*[16] In addition, Recital 41 of the European Data Protection Directive clarifies that *"[...] any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing [...]."*[17] Hence, the entitlement to access personal data is essential for uncovering illegitimate or illegal surveillance practices and can therefore be seen as a legally backed opportunity to scrutinize the socio-technical power asymmetry produced by video surveillance. The right of access provides the data subjects with a possibility to equalize the above-mentioned reciprocity of interaction and (partially) restore or at least improve transparency in regard to the ongoing processing of personal data.

Regulations on Video Surveillance

In Austria, video surveillance is legally defined as the systematic and, in particular, continuous detection of events related to a specific object or a specific person by way of technical image recording or transmission devices.[18] If a video surveillance system records image data, the system must be registered in the Data Processing Registry.[19] The data must generally be deleted within 72 hours.[20] So-called real-time monitoring, i.e., video surveillance without recording, as well as storing of the image data on analog media (video tapes) are excluded from the reporting obligation.[21] In addition, a labeling requirement is defined. The signage (labeling) has to make clear who operates the video surveillance system. Furthermore, the labeling must be applied locally in such a way that any affected person has the possibility to avoid the surveillance.[22]

Finally, the right of access in the case of video surveillance is legally defined as follows:

- Every person affected has the right of access to their personal data processed by the video surveillance system after providing proof of identity and specifying the time and place of surveillance.[23]
- The answer to such a request must include any processed data, information about the origin of the data, any recipient of the data, the actual purpose of the data processing and the related legal basis.[24]
- Access shall be provided within eight weeks; otherwise a written justification must be given stating why the information was not or not completely handed over.[25]
- Access shall be free of charge as long as the applicant has not submitted another request to the same operator in the same matter in the current year.[26]

---

[16] Cf. Article 8 (2) Charter of Fundamental Rights of the European Union (2000/C 364/01), Official Journal of the European Communities, C 364/1, 12/18/2000.

[17] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Union *L 281*.

[18] Cf. § 50a (1) DSG 2000.

[19] With the exception of video surveillance by the police, which is statutorily regulated primarily by the Security Police Act (Sicherheitspolizeigesetz – SPG). Cf. §§ 17 ff and 50c DSG 2000, Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000), BGBl.I Nr. 165/1999 idgF; (Data Processing Registry = Datenverarbeitungsregister – DVR).

[20] Cf. § 50b Austrian Data Protection Act (DSG 2000).

[21] Cf. § 50c (2) Austrian Data Protection Act (DSG 2000).

[22] Cf. § 50d Austrian Data Protection Act (DSG 2000).

[23] Cf. § 1 (3) and § 26 in connection with § 50e Austrian Data Protection Act (DSG 2000).

[24] Cf. § 26 in connection with § 50e Austrian Data Protection Act (DSG 2000).

[25] Cf. § 26 (4) Austrian Data Protection Act (DSG 2000).

[26] Cf. § 26 (6) Austrian Data Protection Act (DSG 2000).

— From the time an access request becomes known, the related personal data must not be destroyed within a period of four months, and in the case of a legal complaint until its final conclusion.[27]
— The operator of the video surveillance system must arrange the handing over or delivery of a copy of the processed personal data in a customary technical format. The applicant may also request inspection of the data directly on site.[28]
— In the case that visual access cannot be granted due to overriding legitimate interests of third parties affected, the applicant is entitled to receive a written description of the monitored situation or a copy of the data with third parties blanked out or anonymized.[29]
— In the case that no personal data have been processed, it is sufficient for data controllers to point out this fact.[30]
— Lastly, the right of access does not apply in case of real-time monitoring.[31]

Research Questions

Based on these considerations, the aim of this study is to examine how the right to access is exercised in practice and how data controllers react to and handle such requests in everyday life. Thus, the research focus is, on the one hand, on the analysis of discrepancies between statutory provisions and their actual implementation and enforceability. On the other hand, the study aims to reveal implicit normative perceptions held by the data controllers and their representatives in regard to visual privacy and panopticism as a theoretical approach to surveillance.

Methodological Approach

Breaching Experiments

The practical conduct of subject access requests and the associated sociological analysis of normative expectations can be methodologically based on Harold Garfinkel's (1967) *"breaching experiments."* According to Garfinkel's ethnomethodology, social reality is understood as a complex arrangement of mutually referential interpretations of meaning based on the subjective horizons of experience of the involved individuals. In this sense, the acting individuals themselves are to be viewed as constructors of reality (Schütz 1932). In regard to the micro-sociological analysis of these generalized and socially shared spheres of meaning—Garfinkel also speaks of *"background features of everyday scenes"* and a *"world known in common and taken for granted"* (1967: 37)—relevant moments of interaction are those at which indexical reference is made to underlying, latent meanings and assumptions about the respective lived-in world. In order to reveal these common expectations of everyday life, he asks *"what can be done to make trouble"* (1967: 37). His approach is about mechanisms that make such life-world-constitutive assumptions visible. The systematic creation of irritation and confusion in situations of social gatherings demonstrates normative expectations and makes them tangible.

In a practical experiment, for example, Garfinkel (1967) asked his students to behave towards their parents as if they were guests visiting their home for a given time, i.e., to be overly polite and somewhat distant. Persons confronted with such irritation practices will generally attempt to fend off the role applied to them, and to maintain or restore their own conception of normality. The intensity of the reaction to the

[27] Cf. § 26 (7) Austrian Data Protection Act (DSG 2000).
[28] Cf. § 50e (1) Austrian Data Protection Act (DSG 2000).
[29] Cf. § 50e (2) Austrian Data Protection Act (DSG 2000). Cf. Fragen and Antworten https://www.dsb.gv.at/web/datenschutzbehorde/fragen-und-antworten (accessed 05/10/2016).
[30] Cf. § 26 (1) Austrian Data Protection Act (DSG 2000).
[31] Cf. §50e (3) Austrian Data Protection Act (DSG 2000).

irritation can be interpreted as an indicator of the power of the underlying norm. While Garfinkel (1967) himself speaks of *"demonstrations,"* this method came to be known as *"breaching experiments."*

In reference to this methodological approach, it is assumed that video surveillance as a widely distributed technology is a largely accepted and socially expected condition of urban life (Graham 1998). Thus, the related socio-technical asymmetry is something common and taken for granted. The questioning of video surveillance by access requests therefore represents a normative irritation and can be perceived as a breach of the panoptical norm as the underlying power structure of surveillance. Thus, making access requests has the potential to reveal the implicit ideas and perceptions of surveillance held by the data controllers and their representatives. Seen from this perspective, the "*inquiry-in-performance*" (Mann et al. 2003) not only provides empirical insight into the practical enforceability of access requests, but also discloses the normative mindset of data controllers and the actual social anchoring of the legal entitlement in everyday urban life.

In-Field Strategy

The access requests were carried out according to the following procedure: similar to the approach of sousveillance, the monitored settings are first documented with short videos and/or photos to record the labeling of the system and the positioning of the surveillance cameras.[32] This is also the moment at which the researcher himself becomes visible to the cameras and the actual demand to access the personal data originates. In the second step, the nearest responsible contact person is sought and the template form, provided on the website of the Austrian Data Protection Authority, is handed over including all relevant legal information, the time and place of the monitored situation, and contact data for further correspondence.[33] In addition, proof of identity is provided by presenting an ID card (passport or driving license). Finally, the entire course of each request is recorded by way of field notes.[34]

Empirical Findings

Sample

The following list shows all 29 locations at which access requests were made. The aim was to achieve a heterogeneous selection that is close to everyday life. The sample therefore includes large and typical as well as small and unusual sites and system operators. The requests were conducted in Vienna in two phases, from August to October 2013 and from March to June 2014.

Table 1: Locations and Findings

Setting/location of request	Image data received	Legal information received	Legal violations identified
Public transport (railway station concourse)	No	Incomplete	(8)
Public transport (metro station)	no (RT)	Incomplete	(8)
Shipping line (boardwalk)	No	No	(1, 3)

[32] Passers-by sometimes try to evade the photographical documentation of the setting by changing their direction to avoid walking into the picture or by covering their faces with their hands.

[33] Model form of the Austrian Data Protection Authority, https://www.dsb.gv.at/dokumente (accessed 05/10/2016).

[34] A complaint procedure with the Austrian Data Protection Authority or a data protection lawsuit before a civil court is explicitly not part of the present study. The scientific aim is the description, documentation and analysis of practical and legal problems encountered in the course of access requests.

Car park (entrance, parking level)	no (D)	No	n. s.
University building (entrance, corridors)	no (RT)	incomplete	n. s.
City library (reading room)	no (RT)	incomplete	n. s.
Museum of Applied Arts (exhibition rooms)	No	Yes	(8)
Zoological garden (koala house)	No	incomplete	n. s.
Public aquarium (entrance, information desk)	No	No	n. s.
Public art and culture space (entrance, courtyard)	No	Yes	(8)
Disco/night club (entrance, corridors, chill-out area)	Incomplete	No	(1, 4)
Bank branch office A (entrance, ATM area, information desk)	incomplete (S)	incomplete	n. s.
Bank branch office B (outdoor ATM area)	incomplete (S)	incomplete	n. s.
Post office (entrance, salesroom)	No	No	n. s.
Jeweler's store (entrance area, salesroom)	No	No	n. s.
Fast-food chain A (seating area, cash desk area)	Yes	Yes	(6)
Fast-food chain B (entrance, cash desk area, seating area)	no (RT)	No	(6)
Restaurant (entrance, seating area)	Yes	No	(1, 4, 5, 6)
Sausage stand (cash desk area)	No	No	n. s.
Supermarket A (entrance, salesroom, cash desk area)	No	No	n. s.
Supermarket B (entrance, salesroom, cash desk area)	No	incomplete	n. s.
Supermarket C (entrance, salesroom, cash desk area)	No	incomplete	n. s.
Shoe store (salesroom)	no (D)	No	n. s.
Clothing store A (underwear section)	no (RT)	No	n. s.
Clothing store B (entrance, salesroom, cash desk area)	No	No	n. s.
Tobacconist A (entrance, salesroom, cash desk area)	Incomplete	No	(1, 4, 6, 7)
Tobacconist B (salesroom, cash desk area)	no	No	(2)
Pharmacy/drugstore (salesroom, cash desk area)	no	incomplete	n. s.
Social welfare/addiction treatment center (entrance, corridors)	no (RT)	incomplete	n. s.

Key:

Image data received:

yes = all relevant cameras; complete video footage was received
no = no video footage or image data were received
incomplete = missing cameras; missing time
RT = real-time monitoring (without recording)
D = dummy
S = screenshot

Legal information received:

yes = full information about the processed data, their origin, recipients or groups of recipients, the purpose of use and the legal basis were received
no = no information about the processed data, their origin, recipients or groups of recipients, the purpose of use and the legal basis were received
incomplete = missing information; not all legally relevant aspects were received

Legal violations identified:

n. s. = not specified
(1) = neglect of labeling obligation
(2) = storage time exceeded
(3) = premature deletion of video footage in case of ongoing access request
(4) = missing anonymization of third parties
(5) = neglect of reporting requirement
(6) = performance monitoring of employees
(7) = audio surveillance
(8) = referring to DPA decision K121.605/0014-DSK/2010 of 2010. According to the decision, the enforcement of access requests violates the privacy of third parties captured on video. Therefore, the right of access is not exercisable in cases where the footage is only recorded and stored but not watched/analyzed/utilized by staff (see further discussion of the decision below).

Initial Contacts and Course of Requests

In general, it can be said that the course of requests was not exactly predictable. The dynamics in the field were often surprising, each situation developed differently, rendering the abundance of empirical contacts difficult to generalize.

In some cases, the challenge began with difficulty in identifying the data controller operating the system. The labeling often did not clarify who is actually responsible. There were also video surveillance systems which were not registered and officially labeled.[35] Overall, this made it difficult for the affected applicant to submit a request.

Once a contact person was found, the further handling of the request sometimes included up to ten or more involved persons, from the cashiers in the sales room to department managers and external providers like private security firms, as well as internal legal departments forwarding the e-mail correspondence to their superior in copy. Bureaucratic procedures and accountability issues came into play. Even security employees in front of surveillance monitors claimed *"... we have nothing to do with this ..."*[36]

[35] The actual purpose of the signage, namely to inform potentially affected individuals about the ongoing video surveillance in order to allow them to evade it, is largely lost in practice.

[36] Mann et al. (2003) likewise report such responsibility rejections, drawing a parallel to the so-called "Eichmann defense strategy," in which the accused claim to have only done what the next-higher authority ordered them to do. On the strategy of delegating responsibility to higher levels in hierarchical contexts – frequently encountered in everyday situations – also see Scott and Lyman (1968).

Data controllers seldom reacted and responded proactively. Instead, a multitude of restrictive practices emerged. The persons responsible did not reply to e-mails, claimed that the request had not been filed correctly, or referred to cameras that did not belong to them or were not part of the access request. Access was often hard-earned and the data subjects had to show persistence and confidence to exercise their right.[37]

The research further reveals a lack of awareness among data controllers. Despite having implemented video surveillance systems, most of the data controllers did not know about the associated legal duties. The representatives in charge often reacted as surprised and overwhelmed. Some operators used the opportunity to ask the applicant about the actual legal situation. The study shows that the majority of data controllers were faced with access requests for the first time.

Although in some cases the contacts in the field were quite helpful and even accommodating, the basic tenor of the conversations was characterized by latent tension. The analysis shows that the initial field contacts were usually the toughest in terms of refusal. Requests were frequently denied even before the access form was submitted to the person in charge. Statements like *"... I cannot provide any information on this issue," "... only the police are allowed to inspect the video footage"* or *"... we can't name the manager or any contact person in charge"* were made. It was often conveyed quite clearly that the requests were perceived as a nuisance and illegitimate impertinence.

In addition, open distrust towards the applicant was expressed in statements such as "*... your ID could be fake…"* or *"... perhaps the request is in fact an excuse and you are secretly planning a burglary..."* Thus, citizens interested in the surveillance system are viewed with skepticism. In the case of the request in the jewelry store, for example, an official *"criminal record extract"* for the applicant was demanded (which is legally not necessary). Such reactions clearly display the underlying normative assumptions in everyday life. Data subjects are not considered to be legally entitled to gain access to their files, but are instead eyed with suspicion.

The access requests were sometimes also perceived as an inspection situation (*"... are you from a government agency?"*), causing contact persons to behave overly formally. In addition, assuagement was sometimes attempted and the functionality and use of the system were downplayed (*"…it is only for determent, so that people know they are being filmed"*). In three cases, employees complained about being concerned about the ongoing monitoring of their workplace. Occasionally, lively conversations about privacy, surveillance and technology unfolded. The relevance of the topic was generally conceded, but this also occurred in cases where the requests were rejected or legal violations were apparent. This sometimes resulted in interesting contradictions: in the case of the request at the disco, for example, a strict no-photo policy was in effect within the premises of the club. Thus, the photographic documentation of the setting by the applicant was immediately prohibited by the security staff. In the further course of the request, the management of the club justified the policy with the argument that the privacy of guests (in excessive party mood) must be protected. Nevertheless, the night club operates a video surveillance system for security reasons. The system was reported to have been utilized only once, when there was a scuffle, but the situation in question had not been captured by the cameras. The access request was eventually answered—in apparent contradiction to the club's own policy—by handing over several gigabytes of uncut and non-anonymized video footage, much of which did not pertain to the request, on two USB flash drives.

[37] For similar experiences cf. IRISS (2015): European Policy Brief: Recommendations to the Council of the EU and the European Parliament on access rights, in the context of the European data protection reform. Available at: http://irissproject.eu/wp-content/uploads/2015/02/IRISS-POLICY-BRIEF.pdf (accessed 04/26/2016).

Case Analysis and Strategies of Denial

A total number of 29 access requests were performed for the study. In only six cases, image or video data were delivered, with complete data only provided in two of those cases. In 14 out of 29 requests, some legal information (purpose of use, legal basis, etc.) was provided, but in only three cases to the full extent required. Ultimately, only one system operator responded correctly on all points.

In all other cases it was not possible to gain access for various reasons: six times it was stated that the system did not record, but merely operated via real-time monitoring, which is excluded from the obligation to provide access. In one of these cases it was acknowledged that the surveillance system was able to save image data if required, but that at the actual time of the request this had not been the case. In two other cases it was claimed that the cameras were only dummies.

Another data controller deleted the footage despite the ongoing request. The reason provided was that all data were in fact backed up on DVD, but unfortunately the camera affected by the request had been forgotten. In other cases, the operators lacked the technical skills to handle the video device and deliver the footage. In general, the data controllers (system operators) frequently lacked technical knowledge. Either the video footage could not be exported and stored on external devices without professional help, or post-processing in terms of cutting or anonymization of third parties presented a challenge. Delivery of the footage, it was sometimes claimed, required external service technicians, causing additional costs.

Another operator, in turn, denied access on the grounds that the video surveillance system was simply not in operation. The system had been installed for several years, but due to technical problems it had de facto never been active. The operator stated *"... that maybe it will work in a week or so."* In another case it was similarly claimed that due to technical problems a few days before it had not been possible to store any video data at the time of the request. The person in charge professed that an attempt was being made to fix the problem, and said that *"... the system should be working again soon."*

Other operators simply did not reply after receiving the template letter and apparently ignored the subject's access request. Even follow-up calls (by telephone) after the 8-week time limit had elapsed did not bring about any progress in these cases. In some of these cases it was stated that the template letter would be passed on to another department within the company, but this department then claimed not to know anything about the request and not to have received any documents, or simply declared not to be responsible.

Finally, in four cases the requests were rejected with reference to the jurisprudence of the Austrian Data Protection Authority.[38] In the mentioned decisions, the Data Protection Authority holds that the privacy of third parties captured on video could be affected by chance if the video footage is watched to enforce the right of access. For this reason, these operators claimed that the video footage could not be handed over to the applicant (see the discussion of the DPA decision below).

The analysis shows that real-time monitoring and the assertion that no data were recorded (due to technical problems) are the most frequently stated reasons for denying access requests. In some cases, there were indications that false statements were made to avoid granting access. By using such explanations, the data controllers sought to prevent any further discussion. However, the statements had to be accepted—whether a system is out of order or truly not recording could not be verified. Even bringing a complaint before the Data Protection Authority would, in most cases, not serve to clarify these situations retroactively.

[38] DPA decision, reference number: K121.385/0007-DSK/2008, 12/05/2008; DPA decision, reference number: K121.605/0014-DSK/2010, 07/30/2010; DPA decision, reference number: K121.698/0004-DSB/2013, 07/09/2013; DPA decision, reference number: K121.605/0003-DSK/2013, 09/06/2013.

The reactions of data controllers can partially be explained by the fact that the requests entail additional effort for the operators. For this reason, at the very least, access requests are not welcome. This also raises the question what would happen if access requests become a daily practice. The amount of additional work would be difficult to manage for most data controllers. Post-processing of video footage, in particular, appears to be time-consuming and costly. Thus, large numbers of requests could have serious consequences, especially for smaller system operators.

As the statements cited above show, there were cases in which the requests were also perceived as a kind of threat. By submitting an access request, negative legal consequences were at least implied, which led to corresponding counter-reactions by the system operators. Aside from possible legal consequences, access requests were regarded as a potential security risk: data controllers were concerned about being spied on.

Moreover, it became clear that the larger the data controller (or company), the more people and departments were involved in a request and the more remotely an access request was handled. Larger companies tend to have their own legal departments or enough financial means to employ a law firm, which leads to more or less slick rejections. Denials with reference to the DPA decision, for example, only happened in such cases. On the contrary, smaller data controllers and companies where managers themselves are available to speak with applicants are often rather poorly informed about the legal situation and disclose unlawful practices.

Socio-Legal Reflections

Obvious Grievances and Curtailing of Entitlements

Operators of video surveillance systems are not the only ones who handle data protection regulations loosely. A look at the legal development over the past few years shows a successive easing of various regulations: real-time surveillance, for example, was exempted from the registration requirement, and the regular period of allowed storage was extended from 48 to 72 hours. In addition, the standard application *"SA032"* was introduced, removing the registration requirements for banks, jewelers, antiques and art dealers, gold- and silversmiths, tobacconists, gas stations, and private property with buildings. These measures are in part an attempt to more efficiently administrate the increasingly unmanageable number of new video surveillance installations by private operators and the accompanying registration procedures.[39]

In this context, it is also questionable that according to the Austrian Data Protection Act, real-time monitoring (without recording) is not considered privacy-invasive.[40] In addition, real-time monitoring is excluded from the right of access, and real-time monitoring and analog video surveillance are excluded from the registration requirement. This actually appears to contradict a decision by the Austrian Supreme Court.[41] According to this ruling, even dummies can pose a *"serious interference"* in the fundamental right to privacy. In addition, both real-time monitoring without recording and analog video surveillance are subject to the legal principle of proportionality (König 2007). Moreover, for the citizens affected, it is impossible to know whether they are faced with a dummy camera, real-time monitoring or high-resolution recording and algorithm-based analysis. Thus, for the data subjects in everyday life, any camera is a real camera, and therefore—at least from a sociological point of view—any subject access request would appear to be legitimate.

[39] Cf. Standard-und Muster-Verordnung 2004, BGBl. II Nr. 312/2004 idgF; see: Rechtsinformationssystem (RIS), www.ris.bka.gv.at.
[40] Cf. § 50a (4) 3 DSG 2000.
[41] Cf. OGH 30.01.1997, 6 Ob 2401/96y; 7 Ob 89/97g; 6 Ob 6/06k.

Access Requests as Privacy Violation

Furthermore, the above-mentioned decisions by the Data Protection Authority are of interest.[42] They restrict the access to image data citing the argument that the viewing of footage could violate the privacy of third parties captured in the video. This is especially the case when the video footage is watched and utilized for the first time by a human (the representative of the data controller) as a consequence of the access request. According to the Data Protection Authority, such screening may not necessarily lead to personal identification of third parties, but there may be accidental findings. Applicants are therefore denied to access their image data. The DPA decisions refer to Viennese subway cars and city commuter trains. In these cases, the video footage is recorded and stored locally on a hard drive in the respective car, but not watched or *"utilized"* by staff. Thus, only so-called *"indirectly personal data"* are processed and the right of access does not apply.[43] In the course of this study, however, these decisions were also cited by some data controllers in reference to different situations in which video footage is constantly viewed on screens by humans in control rooms. This further leads to the problem that the term *"utilization"* is not legally defined by the Data Protection Act. It could be argued that *"utilization"* means any watching of the video footage on screens or just the act of taking a closer look in order to, for example, count people by their gender. Does *"utilization"* only refer to a kind of technical handling and modification of the footage, like playing the video in slow motion? Is so-called *"intelligent"* or *"smart"* algorithm-based video analysis a kind of *"utilization"* even if the video footage is not watched by humans? The mentioned jurisdiction seems legally ambivalent and raises serious questions about the actual purpose of the right of access and its practical enforceability. From a sociological perspective, these tendencies and decisions at least undermine the possibility of visual adjustment and balancing the power asymmetry between data controllers and affected citizens.

Practical Recommendations and Legal Means

Against this background, the question arises as to how such an imbalance can be countered in practice and how the enforceability of the legal entitlement can be improved. Firstly, it is important to point out the insufficient signage, which should be standardized for all video surveillance systems and include an official regulatory registration number which would make it possible to locate and contact the data controller. Furthermore, organizations which operate a video surveillance system should train their responsible employees and provide a manual on how to react correctly in such situations.[44] Data subjects, in turn, are advised to obtain the necessary legal information and official documents (using the model form for access requests) from the competent data protection authority in advance. Preparation and knowledge of the prevailing legal situation increase the chance of successfully enforcing one's right of

---

[42] DPA decision, reference number: K121.385/0007-DSK/2008, 12/05/2008; DPA decision, reference number: K121.605/0014-DSK/2010, 07/30/2010; DPA decision, reference number: K121.698/0004-DSB/2013, 07/09/2013; DPA decision, reference number: K121.605/0003-DSK/2013, 09/06/2013.

[43] In addition, the Data Protection Authority points to Article 13 of the European Data Protection Directive (95/46/EC), which allows the definition of exceptions to the right of access to provide necessary legal protection of others.

[44] Rammert (2002) mentions two other ideas to compensate for the disturbed visual reciprocity in the case of video surveillance. Firstly, he argues that screens could be set up additionally on which the data subjects can see and control the images of their behavior themselves. Secondly, screens could be set up on which the data subjects can observe the observers in the concealed control room during their work (Rammert 2002: 15). It must be said that in the first case, the panoptic asymmetry is not necessarily abolished. Rather, the data subjects become aware of the surveillance (like in the case of labeling/signage) and are thus prompted to adjust their behavior. The second proposal would amount to a kind of workplace surveillance, which, again, is legally problematic. In the end, it can be said that the surveillance of the entities of surveillance may lead to *"equal firepower"* but does not lead to more privacy.

access.[45] Finally, people should be made aware of the fact that if their right of access is violated, it is possible to initiate a formal legal procedure at the data protection authority or to bring an action to court.[46]

Conclusion

The legally intended purpose of the right of access is to provide a corrective measure. It gives citizens affected by video surveillance the possibility to check the surveillance of their person and verify its lawfulness. Besides general legal information on the purpose and functionality of the monitoring, this also includes the entitlement to demand the video footage created during data processing. The detailed configuration of the legal right reflects the legislator's conception in regard to the balancing of visual privacy in everyday life. However, the study shows that an equalization of the visual interrelationship—as described by Simmel (1908/1992) and Rammert (2002)—cannot be achieved in practice. The analysis reveals the partial reading of the law by the data controllers and their strategies in evading and negating accountability. While the data subject's right of access exists on paper, it seems nearly impossible to exercise in everyday life.

Failure to comply with a request is apparently not always intentional, but often occurs due to a lack of technical and legal competence. But besides the more or less practical aspects and explanations, there is a basic lack of social understanding as to why citizens should be granted access to their personal (image) data. According to Goffman (1971: 60), informational and territorial self-determination is crucial to one's sense of what it means to be a full-fledged person. Thus, the conducted access requests show how self-determination in the sense of visual privacy is denied by the data controllers, turning the citizens into subjects of surveillance without rights. Instead, data controllers seek to protect their own *"information preserve"* (Goffman 1971: 28), maintaining their own ideas of how video surveillance should be performed. To grant access is obviously not part of these assumptions.

Citizens' right to access is refused and not considered legitimate by the data controllers and their representatives. Due to the fact that there was no actual security-critical scenario and—from the operator's point of view—no convincing reason was specified, the access requests were perceived as a kind of annoying game and a normative irritation to everyday life expectations (Garfinkel 1967). The questioning of video surveillance was considered absurd. Data controllers and their representatives asked for the underlying motivation or a legitimate reason for requesting the respective (personal) data, but justifications like *"... because I'm curious about"* or *"... I have the right to it"* were perceived as insufficient and met with refusal. Establishing contact and inquiring about the person in charge of the ongoing surveillance was perceived (and treated) as an unwanted deviation and potential threat. The applicants were faced with skepticism and suspected of planning or preparing criminal acts. The communicative negotiation during the requests was in most cases detrimental to the data subjects concerned.

The empirical assessment of the right of access discloses the normative mindset of the data controllers and shows that the panoptical asymmetry of surveillance has, to some extent, already become a normal condition in the micro-sociological structures of surveilled locations. The legal entitlement to receive more information about the ongoing surveillance of oneself is not commonly anchored in everyday life—

[45] For further recommendations see IRISS (2015): European Policy Brief: Recommendations to the Council of the EU and the European Parliament on access rights, in the context of the European data protection reform. Available at: http://irissproject.eu/wp-content/uploads/2015/02/IRISS-POLICY-BRIEF.pdf (accessed 05/26/2015).

[46] In the case of a violation of the right of access, three different procedures are possible: an ombudsman procedure before the data protection authority (§ 30), a complaint procedure before the data protection authority (§ 31) or a legal action before a civil court (§ 32 Austrian Data Protection Act/DSG 2000), Cf. Austrian Data Protection Authority, https://www.dsb.gv.at/rechte-der-betroffenen (accessed 05/10/2016).

instead, the social norm is to maintain the power asymmetry. The overall socio-technical constellation ultimately leads to a situation that can be described as panoptical (Foucault 1975). Lack of signage or inadequate labeling of video surveillance systems and the associated difficulty in finding the actual person responsible can lead to Kafkaesque situations of opaque hierarchies and anonymous powers. Although more information about the data processing can be obtained through access requests than would be available to a normal passer-by, overall the requests cannot be said to open up the *"closed circuits"* of surveillance. In technical and informational terms, at least, the data controllers are in the position of power, despite the intention of the lawmakers to disrupt this structural inequality. Rather, it is the attempt to execute the legal right to access that makes the requester's inferiority truly tangible. Thus, the socio-technical asymmetry of surveillance prevails and the normative figure of panopticism becomes visible in the monitored routines of everyday life.

Acknowledgments

Funded by the Cultural Department of the City of Vienna, MA7—Science and Research Funding; Project no. 363800/13. Special thanks to Professor Alfred Smudits for everything he has made possible. Furthermore, I would like to thank the students of the "Visual Surveillance" course at the Institute of Sociology (University of Vienna), who courageously conducted access requests in summer 2014.

References

Bennett, Trevor and Gelsthorpe, Loraine. 1996. Public attitudes towards CCTV in public places. *Studies on Crime and Crime Prevention* 5: 72-90.

Boyne, Roy. 2000. Post-Panopticism. *Economy and Society* 29 (2): 285-307.

Ditton, Jason. 2000. Crime and the City. Public Attitudes towards Open-Street CCTV in Glasgow. *British Journal of Criminology*. 40: 692-709.

Ennöckl, Daniel. 2014. *Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung*. Habilitationsschrift, Schriftenreihe Forschung aus Staat und Recht. Verlag Österreich.

Foucault, Michel. 1975. *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books.

Fuchs, Christian. 2014. *Social Media: A critical introduction.*London: Sage Publications Ltd.

Garland, David. 2001. *The Culture of Control: Crime and Social Order in Contemporary Society*. Oxford: Oxford University Press.

Graham, Stephen. 1998. Towards the fifth utility? On the extension and normalisation of public CCTV. In: *Surveillance, Closed Circuit Television and Social Control*, eds Clive Norris, Jade Moran and Gary Armstrong, 89-112. Aldershot: Ashgate.

Garfinkel, Harold. 1967. *Studies in Ethnomethodology.* Cambridge: Polity Press.

Goffman, Erwing. 1971. *Relations in Public: Microstudies of the Public Order.* New York: Penguin.

Haggerty, Kevin D. 2006. Tear down the walls: on demolishing the panopticon, In: *Theorizing Surveillance: The Panopticon and Beyond*, ed. David Lyon, 23-45. London and New York: Routledge.

Han, Byung-Chul. 2014. *Psychopolitik – Neoliberalismus und die neuen Machttechniken.* Frankfurt am Main: Fischer Verlag.

Hempel, Leon and Töpfer, Eric. 2004. *On the Threshold to Urban Panopticon? Analysing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts*. Berlin. Urban Eye Project.

Hirschauer, Stefan 1999. Die Praxis der Fremdheit und die Minimierung der Anwesenheit. Eine Fahrstuhlfahrt. In: *Soziale Welt* 50: 221-246.

Honess, Terry and Charman, Elizabeth. 1992. *Closed Circuit Television in Public Places: It's Acceptability and Perceived Effectiveness.* In: Police Research Group. Crime Prevention Unit Series: Paper No. 35. London: Home Office.

Kammerer, Dietmar. 2008. *Bilder der Überwachung*. Frankfurt: Suhrkamp.

Koskela, Hille. 2004. Webcams, TV Shows and Mobile Phones: Empowering Exhibitionism. *Surveillance & Society* 2(2/3): 199-215.

Koskela, Hille. 2011. Hijackers and Humble Servants: Individuals as Camwitnesses in Contemporary Controlwork. *Theoretical Criminology* 15(3): 269-282.

König, Gregor. 2007. Videoüberwachung und Datenschutz – Ein Kräftemessen. *Aktuelle Fragen des Datenschutzrechts*, eds Dietmar Jahnel, Stefan Siegwart, Natalie Fercher, 109-147. Wien: Facultas.

Kudlacek, Dominic. 2015. *Akzeptanz von Videoüberwachung. Eine sozialwissenschaftliche Untersuchung technischer Sicherheitsmaßnahmen.* Wiesbaden: Springer VS.

Lyon, David. 2001. *Surveillance society: monitoring everyday life*. Buckingham, UK: Open University Press.

Lyon, David. 2005. Interview. "Wir haben gerade erst begonnen." Überwachen zwischen Klassifikation und Ethik des Antlitzes. In: *Bild-Raum-Kontrolle: Videoüberwachung als Zeichen gesellschaftlichen Wandels,* eds Leon Hempel and Jörg Metelmann, 22-32. Frankfurt am Main: Suhrkamp.

McCahill, Michael. 1998. Beyond Foucault: towards a contemporary theory of surveillance. *Surveillance, closed-circuit television and social control*, eds Clive Norris, Jason Moran, and Gary Armstrong, 41-65. Aldershot: Ashgate.

Mann, Steve, Nolan, Jason and Wellman, Barry. 2003. Sousveillance: Inventing and Using Wearable Devices for Data Collection in Surveillance Environments. *Surveillance & Society* 1(3): 331-355.

Mirzoeff, Nicholas. 2011. The Right to Look. *Critical Inquiry* 37 (3): 473-496.

Monahan, Torin. 2006. Counter-Surveillance as Political Intervention? *Social Semiotics* 16(4): 515-534.

Monahan, Torin. 2010. Surveillance as governance: social inequality and the pursuit of democratic surveillance. In: *Surveillance and Democracy*, eds Kevin D. Haggerty and Minas Samatas, 91-110. New York: Routledge-Cavendish.

Mülleder, Lisa. 2014. Datenschutz und Privatsphäre in Social Networks am Beispiel von Facebook. In: *Spektrum der Rechtswissenschaft*, 471-499. Wien: Jan Sramek Verlag.

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

Pöschl, Magdalena. 2015. Sicherung grund- und menschenrechtlicher Standards gegenüber neuen Gefährdungen durch private und ausländische Akteure. In: *Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer (VVDStRL)74*, Referate und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Düsseldorf vom 1. bis 4. Oktober 2014, De Gruyter: 406-452.

Rammert, Werner. 2002. *Gestörter Blickwechsel durch Videoüberwachung? Ambivalenzen und Asymmetrien soziotechnischer Beobachtungsordnungen.* Technische Universität Berlin, Technology Studies, Institut für Soziologie, Working Papers TUTS-WP-9-2002.

Reuband, Karl-Heinz. 2001. Videoüberwachung. Was die Bürger von der Überwachung halten. *Neue Kriminalpolitik*, *Forum für Praxis, Wissenschaft und Politik* 13(2): 5-9.

Rothmann, Robert. 2010. Sicherheitsgefühl durch Videoüberwachung? Argumentative Paradoxien und empirische Widersprüche in der Verbreitung einer sicherheitspolitischen Maßnahme. *Zeitschrift Neue Kriminalpolitik (NK), Forum für Kriminalwissenschaften, Recht und Praxis* (3): 103-107.

Schaefer, Brian. P. and Steinmetz, Kevin F. 2014. Watching the Watchers and McLuhan's Tetrad: The Limits of Cop-Watching in the Internet Age. *Surveillance & Society* 12(4): 502-515.

Schütz, Alfred. 1932. *Der sinnhafte Aufbau der sozialen Welt. Eine Einleitung in die verstehende Soziologie.* Wien: Springer.

Scott, Marivn B. and Lyman, Stanford M. 1968. Accounts. *American Sociological Review* 33(1): 46-62.

Simmel, Georg. 1908/1992. *Soziologie. Untersuchungen über die Formen der Vergesellschaftung*. Gesamtausgabe Bd. 11. Frankfurt: Suhrkamp.

Spriggs, Angela, Argomaniz, Javier, Gill, Martin, Bryan, Jane. 2005. *Public attitudes towards CCTV: results from the Pre-intervention Public Attitude Survey carried out in areas implementing CCTV*. University of Leicester. Home Office Online Report 10/05.