Open Research Online

The Open University's repository of research publications and other research outputs

Experiences of accessing CCTV data: the urban topologies of subject access requests

Journal Item

How to cite:

Spiller, Keith (2016). Experiences of accessing CCTV data: the urban topologies of subject access requests. *Urban Studies*, 53(13) pp. 2885–2900.

For guidance on citations see [FAQs](#).

© 2015 The Author

<https://creativecommons.org/licenses/by-nc-nd/4.0/>

Version: Accepted Manuscript

Link(s) to article on publisher's website:

<http://dx.doi.org/doi:10.1177/0042098015597640>

Copyright and Moral Rights for the articles on this site are retained by the individual authors and/or other copyright owners. For more information on Open Research Online's data [policy](#) on reuse of materials please consult the policies page.

oro.open.ac.uk

Experiences of accessing CCTV data: the urban topologies of subject access requests

Keith Spiller

Open University Business School, Walton Hall, Milton Keynes, Mk7 6AA

Abstract

In this paper, I argue that careful attention needs to be paid to the handling of urban CCTV digital data. Since the early 1990s, CCTV has left an indelible mark on UK cities, and beyond. CCTV is a crime-reduction strategy, and its activation owes much to the laws and regulations that govern its function and the passivity with which it is often viewed. I consider the nature of security when CCTV signs, recorded images and the rights of citizens are interlinked in controlled urban spaces. Despite the regulatory powers of the Data Protection Act, the management of CCTV data is at times poorly operationalised and often obfuscated. The paper discusses my experiences of identifying 17 different CCTV cameras and being recorded and my attempts to access my images through subject access requests (SARs). In what follows, I draw on different topologies of experience in expanding upon the mutable, unpredictable and intensive relations that guide the management of CCTV data.

Keywords

CCTV, topologies, power, intensive relations, urban spaces, privacy, subject access request

Introduction

Police forces, governments, local councils and business owners, as well as many others, have long approved of the virtues of closed-circuit television (CCTV); cameras, we are told, keep citizens, streets, shops and cities safe (Ditton, 2000). Indeed, the use of CCTV in UK towns and cities recently celebrated its 25th anniversary and is now a mature mainstay in the UK security landscape. Estimates vary on the number of cameras in the UK, but figures seem to converge on approximately 6 million working cameras (BSIA, 2014). The attraction of the cameras has been in no small way encouraged by their impact on successful criminal investigations – CCTV evidence consistently encourages early ‘guilty’ pleas (Levesley et al., 2005). Indeed, local and central governments have placed a large amount of faith and investment in CCTV systems (Big Brother Watch, 2012). Recent innovations such as ‘smart CCTV’ are extending its use further; in these instances, algorithms detect unusual behaviours, for example where there is typically a lot of movement near certain stationary objects (Held, 2012). Not surprisingly, CCTV has generated much academic attention, particularly in the fields of urban studies (Fyfe and Bannister, 1996; Klauser, 2007; Murakami Wood et al., 2007) and surveillance studies (Norris and McCahill, 2006; Smith, 2007; Webster, 2002). What I want to push for in this paper is a broader discussion on the ambiguities evident in the dynamics of urban surveillance. The

proliferation of cameras has normalised CCTV; go to any UK city and it is reasonable to expect that you will be CCTV'd (McPhail et al., 2013; Surveillance Studies Network, 2010). It is also reasonable to expect your data will be managed correctly by those who are monitoring, recording and storing CCTV images. I challenge these expectations and in doing so draw on empirical findings and detail my experiences identifying 17 different CCTV cameras and then requesting my data or the images captured of me. The paper attempts to verify how CCTV data management and systems of data protection are at work in a UK city.

The CCTV cameras examined in this paper are those working in places of business and in public areas. The regulatory laws overseeing CCTV use in the UK are relatively complex; in brief, most CCTV use falls under the remit of the Data Protection Act (1998) (hereafter DPA) and Article 8 of the European Convention on Human Rights. These regulatory powers establish the protection of information and the right to privacy for individuals (Home Office, 2013). Cameras monitoring private and public spaces for security purposes must adhere to the DPA and Article 8; these include cameras used by public authorities, businesses and individuals. An exception, however, is made for domestic cameras, and, where cameras are used for personal purposes,

they do not fall under the remit of the above – even if these cameras happen to record public spaces. A central component to the development of my argument is the regulatory power of the DPA. The Act states CCTV operators (those monitoring cameras or screens or managing data) must notify people that they are being recorded, must store images with ‘integrity’ and must provide data to anyone requesting their images. The Act sets a clear code of practice that CCTV operators and data controllers are obliged by law to adhere to. I ask, what happens when this code of practice is operationalised? In answering this question, I consider the complexities that guide the normalisation of security (Amoore, 2009), but also the relations that sustain and challenge how security is performed. Here, I draw on topological ‘sensibilities’ (Hinchliffe et al., 2013) to explore the contested and uncontested relations in spaces observed and controlled by CCTV cameras. The premise, as with much of the topological work, is the spatial/temporal dynamics when objects or devices bind relationships. In these terms, CCTV data ties camera operators, data managers and urban publics. Those recorded by CCTV, I suggest, are distanced and to some degree de-personalised through the lens of the camera as CCTV staff remotely view, store and manage digital data of those who pass under the gaze of their cameras. I disrupt this relational dynamic through contact, or by deliberately seeking out CCTV operators and data managers in order to enact my data rights. The chain of events centres on

activities performed by urban publics, the recording and data management of these activities and finally gaining access to CCTV data. Three sets of actors are involved: firstly, CCTV operators or those sitting in-front of screens and monitoring live action or those responsible for the running of automatic camera systems; job roles include the retrieval and inspection of data; secondly, data managers or those responsible for the safe storage and protection of CCTV data (these roles are not exclusive and both positions require knowledge of DPA); and thirdly, my role as an inquisitive urban public member. In what follows I highlight five CCTV topologies to expose the social relations that underpin CCTV security and to examine the fluidity and variability with which CCTV operators and managers perform their roles. The paper proceeds by giving an overview of previous urban CCTV research, and then moves on to explore topological understandings of the dynamics of power and control, particularly those mediated over distance. I then comment on the methodological approach taken, before the empirical section which focuses on my experiences of digital capture in the urban environment. Finally, I offer some concluding thoughts on submitting subject access requests (hereafter SARs) and the difficult and intensive relations that often ensue.

Urban CCTV

CCTV has enjoyed a plethora of attention in urban studies literatures, regarding, for instance, its effects on fears of crime or the sensations of security enhanced by the presence of cameras. Indeed, central to urban CCTV arguments have been examinations of the socio-spatial implications of monitoring. Examples include research on the objectification of the female body through the focused targeting of women by CCTV operators for voyeuristic pleasure (Koskela, 2002). More recently, Brands et al. (2013) questioned perceptions of safety within public spaces when cameras are exposed to those they watch. As they suggest, urban publics are aware of the cameras and, as a result, do feel varying levels of safety, but the publics also acknowledge that the cameras will not stop a crime happening to them. Indeed, relations between publics and cameras are normalised and accepted (Graham, 1998); rarely outside of a significant incident or accident do urban, or other, publics contact CCTV data controllers. Instead, the presence of cameras is rationalised for the potential safeties the cameras may afford in deterring crime or solving crime *after the fact*. Safety in the city and the night-time has generated much recent discussion on urban CCTV. Security and safety play a key role, as the aspirations of those installing CCTV systems are attentive to protecting the revenues of bars, clubs and take-away establishments, as well as newer urban facets such as night markets or Christmas

markets (Pottie-Sherman and Hiebert, 2013). It is at these sites that the security relations between cameras, operators and urban publics coalesce in very real and applied ways, all of which is underscored by a social code of good and accepted behaviour, one encouraged by the presence of cameras and their operators. A new legitimacy, rather than the night-time economies of old (prostitution, drug dealing or drinking shebeens), is managed by CCTV, police, bouncers or even street pastors (Middleton and Yarwood, 2013) in order to placate, tame or discipline the potential harms of the night.

Urban CCTV focuses have also considered actual harms or more accurately reactions to events such as high-profile terror attacks. This has unsurprisingly spurred much reflection on the spatial logic of designing out threats. As Coaffee (2005) argues, events such as 9/11 stimulated the exposure of till-then habitually veiled security systems. Today it seems inconceivable to think of city design without serious consideration of terror, disaster or risk. The positioning of cameras and the spatial range and limitations of the images they capture are real and rationalised concerns. Protection and deterrence become interlinked with camera locations, positioning or zoomable qualities. Klauser (2004) uses the notion of territoriality to tease out relations between citizens and their physical environments. For him, CCTV is a

mediator of change as to how people use and enjoy public space; the presence of the cameras encourages order and discourages anti-social behaviour in CCTV-monitored zones. Indeed, the socio-technical order of cityscape is central to public policy discourse, as fear, crime and risk are designed out by ever-smarter cities and technologies (Kitchin, 2014; Townsend, 2013). Moreover, CCTV literatures have also been attentive to operators and those they observe; works have focused on the 'cat and mouse' of operator and surveyed, as those watched avoid areas or deliberately act suspiciously (see Armstrong and Norris, 1999; Ball, 2002). Other works, notably Norris and McCahill (2006), have been attentive to the social interaction and micro-sociologies of the control room and how operators interact with security systems and colleagues. However, I am interested in collapsing and unsettling the relations between observer and those observed, especially when the operator is called upon to act in ways that upset or surprise the normative structures, responsibilities and accountabilities of their roles and especially when operators are legally obliged to perform these disruptive tasks.

Intensive relations

Topological understandings are a useful concept to illuminate the complexity of power relations within CCTV security landscapes, because its central thesis is often exposure

of the working relations that bind and control disparate bodies. As Allen (2011) suggests, the mutating and shifting patterns of power cultivate insights into how distances become present and how power is mediated. Networks of control and networks of request pose a juxtaposition of sorts here, as the distances maintained by the data controllers are disrupted. I maintain these instances encourage understandings of the complex ways in which power influences and limits (Harvey, 2012). Indeed, it is the imperatives that guide normalisations and general understandings of CCTV and its practices, as felt by controllers and requesters, that are of importance here. I don't see topologies as a repository of all things relational; instead, I see a concentration on ambiguities and conflicts exposed by a disruption as providing greater depth to the workings and non-workings of power and security in urban CCTV contexts (Hier et al., 2006). The 'spatiotemporal coordinates', as Latham (2011) suggests, are known: if we enter a CCTV zone, a camera will watch and record. While Euclidean notions of geometry and topography do give rise to understanding of mathematical calculations of distance and space, there is a fixed rigidity to Euclidian geometry that does not encourage examination of the folded and distorted properties of relations and how these are mapped or how spaces and places are understood (Allen, 2011). The topological adds 'multidimensional models of happening' to the two-dimensional map (Vannini, 2011), as happenings etched onto the surface provide

informative detail. Moreover, as Appadurai (1986) suggests, 'scapes' build on the mathematical calculations of space and embrace the cultural imposition that disrupts the linearity and exactness of mathematical accuracy. DeLanda (2006), with a nod to Tuan (1974), asserts topological approaches allow for greater appreciations of the contrasting spatial relations evident within systems and relationships. Indeed, the rationality of technology or the passivity of those who come under the gaze of CCTV contributes to how surveillance is performed and comprehended (see Blair, 2013; Graham, 2012; Moore, 2011; Wagenaar and Boersma, 2012). Thinking beyond the lateral is the challenge addressed by topological approaches, one which encourages us to make sense of the complex ways in which, for instance, power transforms and influences the lives of those under the camera, as well as the relational contexts that involve multifarious security actors (Fussey, 2013).

For some commentators, topological approaches provide opportunities to explore moments of non-representation (Lury, 2013) or the co-constitution of objects, boundaries and devices (Ruppert, 2012). Various analogies have been used in demonstrating the topological 'turn' (Shields, 2012a); most popular are notions of the rubber mat or handkerchief that retains properties of space, power and interrelations

even with the advent of time–space compressions – or, when the handkerchief is crumpled up (Allen and Cochrane, 2010; Hetherington, 1997; Law and Mol, 2001). Looking to these works, it is clear that the problematic is understanding how relations move over time and space. As Murakami Wood (2008) suggests with reference to topologies of surveillance, computer data is ‘surveillable’ due to patterns of connectivity and the rules of flow between processors, computers and systems. Computer networks follow spatial protocols even within virtual spaces and these networks remain readable, traceable and influential. Indeed, Law (1986) speaks of the training of humans and technologies to enable control over distance. For him, the puzzle is how imperial expansions into the orient were accomplished. He argues that ‘it is not possible to understand this expansion unless the technological, the economic, the political, the social, and the natural are all seen as being interrelated’ (Law, 1986: p. 1). Strategies of durability, forcefulness and fidelity, Law suggests, are key. For Allen (2011), it is the modifying and shifting patterns of power that cultivate insights into how distances become present and how power is mediated and ‘intensive relationships’ bridge these gaps, a case in point being how governmental power in the UK emanates from London. In these instances, as we will see in the following sections, contact highlights relational composition of urban publics and data controllers.

The interplay between CCTV camera, its operators, CCTV regulations and urban publics demonstrates just some of these turbulent and unknown security potentials. There are after all a diverse set of actors that populate, control and influence the camera's line of vision; a surveillant relation, if you like, or one dominated by an overarching security function, yet it is also a relation interrupted by the legal rights and/or the proactive engagement of the surveilled. These instances complicate relations between operators, controllers and urban publics and highlight the incompetence and poor practices of those tasked with enacting digital rights. CCTV may offer reassurance of crime reduction and assurances of data protection compliance, yet rarely do 'connections between time, space, place and things ... have a simple narrative or simple spatiality' (Hetherington, 1997: p. 205). A CCTV sign, for example, is designed to signal the presence of a CCTV-controlled zone, which in turn may influence behaviour (Cole, 2002; Lippert, 2009). Nevertheless, as Clement and Ferenbok (2012) suggest, when we take a closer look at the wording on the signs, other indicators become apparent. While signs often declare 'For Your Security' or 'Shoplifters Beware', the researchers argue that these signs promote, particularly in commercial settings, the preservation of shopping prices. The overarching message is, if goods are stolen, prices will increase, and shoppers will incur the rising costs in their purchases. Elsewhere, CCTV operators perform roles of categorisations 'which they attempt to corroborate as

appropriate in negotiation with other bodies (such as CCTV managers, police, etc.)' (Neyland, 2004: p. 254). The images are at times manipulated to fit stories. As Neyland articulates, accounts of a man walking in a town centre with a knife change between the police, the media and a civil liberty group. Each group reads the CCTV images differently: the police view a man with mental health issues, the media see the benefits of CCTV and the civil liberties group council for better privacy protection. CCTV operators are complicit in the production of each of these stories. The point Neyland questions is how these images are made to speak and the fluidity to their interpretation. Indeed, the heterogeneity of security systems, devices and actors extends the heady mix of such networks of security, and how diverse and disparate functions are networked together. It is in these terms that topological approaches of making distant and overlooked influences present, and connecting bonds of power and agency become, more candid and knowable. The remainder of the paper details the story of CCTV operators, data controllers and me and the intensive relationships that ensued.

Getting caught on camera

The empirical work in the paper draws from data I collected as part of the EU-funded Increasing Resilience in Surveillance Societies (IRISS) project (2014). The project examined the development and employment of surveillance technologies and their impact upon citizen rights, as well as the social and economic costs of these advances. One focus was CCTV signage and subject access request for CCTV data across 10 European countries, and I focus on the UK example only. The UK city I chose was the one where I live. The city is in the south of England, has a population of 150,000 and is dominated by its large university. I chose the city for its ease of access, as I had expected most organisations to invite me to view footage in person and at their places of business, therefore necessitating follow-on contact. This was something that did not in fact occur; never was I invited to view footage in person.

Our approach and the template project partners agreed upon was to examine 20 urban sites. The first phase of the research was to appear on CCTV footage, and I began with a central building – in this case the town hall – where I stood under a visible camera. I also noted any contact information on signs and the ease or difficulty with which this was found. If information was not visible, I asked the nearest member

of staff if they could provide contact details. I also noted my time of arrival and the amount of time I spent at the site. I then repeated the process as I moved around the city. The city centre was easily covered on foot and all of the research sites visited, bar one, are within a 3-km radius. In total, 17 camera locations were identified: included were 2 shopping malls, 3 department stores, 4 banks, 1 stadium, 1 railway station, 1 bus station, 1 university, 1 open street system, 1 town hall, 1 government building and 1 museum. The locations, with the exception of the stadium, were visited on one day in late 2013 between 9.00 a.m. and 10.30 a.m. The 3 locations I did not find information for were: a children's playground, as no cameras were evident; the airport, as it is a small regional airport some distance away and could not be considered to be in an urban environment; and underground transport, as there is none in the city.

Following this collection phase, I began submitting SARs. However, a number of protocols had to be followed: namely, the request must be made in writing (on paper, not by email); details of the time and date of the footage must be included; and the requestor must also provide identification. The Information Commissioner's Office (ICO), which is effectively the UK data protection agency, provides a template letter on

their website which I used when making the requests (ICO 2014). Organisations are entitled to charge those making requests a £10 fee and must respond to the requests within 40 days. To avoid bias, I did not identify myself as a researcher – to have done so may have skewed results as controllers could have acted with undue favourability. I always used a non-university email address, did not use university-franked envelopes and used my mobile phone for communications. I suspect, judging by the marked increase in traffic to my academia.edu and researchgate webpages, that my name was searched online. Interestingly, when speaking to staff on the collection visits, I was never asked about my background or why I wanted the footage, whereas when speaking on the phone, at least 50% of organisations enquired as to why I wanted the footage. I always responded I was just curious to see if I could view my data. Throughout the research, I noted and compiled all site visits and all contact with controllers (dates and times), and kept records of all correspondence (see Table 1); I also photographed CCTV cameras and the signs that accompanied them. No specialist software and analysis was used in the results presented here; calculations simply focused on totals.

The topologies of surveillant relations under CCTV

In considering the spatial and relational complexity (Deleuze, 1993) of security networks and, as Allen (2011) suggests, to explore how relations retain veracity, despite the folds and twists of non-observable or non-measurable features, I advance the following five topologies of surveillant relations. I concentrate on the relations between data controller and me, a member of the urban public, in moments of distance reduction (Allen and Cochrane, 2010) and use this as an opportunity to explore the complexities and difficulties of these relations.

Curves of contact

Once I had located the position of cameras in each of the sites visited, I then stood for at least 2 minutes under the cameras in an attempt to make sure the camera would catch a clear view of my presence. Following this, I then searched for the signs accompanying the cameras. This is effectively the starting point of any SAR, because to secure data a person must contact the controller. At four locations (Department Store 2, Open Street, Bank 4 and Museum), I found a complete absence of signs. In each of these locations, cameras were clearly visible. Indeed, in three of the cases, when staff were asked about sourcing CCTV footage, they were forthcoming in directing me as to

where I could find contact details of the data controller – on each occasion a website was suggested. In two instances (Train Station and Stadium), signs were present but no contact information was included (see Picture 1). At the remaining locations, contact information was present but required some searching (see Picture 2) – I found signs at side entrances or on one occasion behind a mannequin.

Picture 1. Train station – contact information absent.

Picture 2. Shopping mall 2 – clear information with a telephone number.

Once contact information was collected, or all hope of finding it exhausted, I began making contact through the phone numbers that the signs provided. The results proved inconsistent; on five occasions, those I spoke to were not familiar with SARs and transferred my call or offered to ring back (Department Store 2, University, Government Building, Shopping Mall 1, Town Hall). On four occasions, the phone number provided was dead, no longer in use or rang out (Bank 1, Bank 2, Bank 3, Bus

Station). Following the limited success of my phone calls, I then resorted to organisation websites. These proved just as frustrating. I began the searches by entering 'data controller' or 'CCTV images' in the search boxes on the sites. On only one occasion did this provide the contact details; in the remaining 10 instances I searched with some difficulty, as information was often submerged in the site and required at least three clicks (or entries onto a new page) to obtain (see Table 1). I found the contact details of four data controllers using this method, and for the remaining requests I used the generic address of the organisations found at the bottom of their home pages. The difficulties compounded by dead telephone numbers or absent signs could highlight how distance between controller and me is maintained through processes that, for instance, contravene the authority of the DPA, all of which, I suggest, works toward an understanding of the relations of how things are tied together (Lury, 2013; Ruppert, 2012). In this case, distance is maintained through absence (Law, 1986) or the nonappearance of contact information. Nevertheless, once I did secure contact details for all 17 sites, I then wrote to each organisation.

Folds of refutation

Four organisations (Town Hall, University, Railway Station and Stadium) replied to my requests and confirmed I did not appear on any of their recordings. These results I found puzzling, as on each occasion I had stood under visible cameras and had spent a number of minutes at the locations. At the railway station, for example, I had spent at least 10 minutes in the station and had taken an extensive walk around looking for signs and information.

Within folds of refutation are some very real absences, notably my visibility. I make a presumption here, as quite possibly the cameras were not recording. However, the organisations' replies detailed the times and places I had specified in my SAR, and on each occasion the controllers stated the time sequence they looked at, i.e. 10 to 15 minutes either side of the time I gave. Adding to the perplexity of the situation is that, in each location, signs clearly identified cameras were in operation (some stating 24-hour coverage); therefore, the absence of data is possibly due to some form of oversight on the part of the recording technology or the CCTV operators – or quite possibly a form of incompetence as resistance (see Fleming and Sewell, 2002). Despite these possible shortcomings, what remains clear is that data was not obtained.

Twists of obfuscation

On a number of occasions, misleading or incorrect information was provided. These instances included, as mentioned, when the telephone numbers provided on signage were no longer in use. Other examples include:

Shopping Mall 1 – overcharging. This organisation replied to my SAR with a request for £20 (plus VAT) to process my request. I responded citing the DPA (1998) and that a standard charge of £10 applied. Three days later, I received a letter confirming that £10 was in fact the correct charge; the letter failed to offer any more information on the footage. Therefore I replied with a cheque and made clear I wished to gain access to my data. I then received a letter stating my cheque had been lost, but that they did have my footage. I telephoned and we agreed the easiest solution would be if I visited their security office to pay and collect. When I did this, I met the person with whom I had been corresponding and we had a quick conversation. During this, she mentioned that my request had actually done her a favour: ‘I never had to do this before, so at least now I know what has to be done.’

Bank 3 – time lapse. I had sourced this Bank's contact details through their website, where I found no mention of a processing fee, and therefore when I originally wrote, I did not include the fee. I duly received a letter requesting a fee; I replied and sent the fee. Finally, I then received a letter saying too much time had passed and the data had been deleted.

These twists impacted on my experiences and notably highlight a degree of ineptitude, for instance, operators' lack of familiarity with data regulations or the charge of fees – I am unsure where the fee of £20 plus VAT originated. Demonstrated is the ambiguity involved when making SARs and how 'stable' networks are easily disrupted through the delivery of information as a potential obstacle, whether intended or not (see Sewell and Barker, 2006).

Kinks of complaint

Four organisations (Museum, Shopping Mall 1, Department Store 2 and Bank 1) did not respond within 40 days to my initial requests. Therefore, I wrote to the ICO to register a complaint. The ICO provides a helpful and straightforward online system where the user can tick boxes indicating the nature of their complaint. The complainant may also

attach supporting documentation, such as copies of letters sent, etc. Once my complaint was made the ICO duly notified me, via email, that they would be contacting the organisations in question.

Shopping Mall 1. A member of staff from a London-based company which provides security to the mall rang early one Saturday morning, and he started with a slightly aggressive tone: 'This is a big company – I have no idea what this [my complaint to the ICO] relates to.' I then explained about my previous letter with the details of my site visit; after this, the caller was very courteous, and agreed to pass my information on to the relevant department. Within two days, I received a telephone call from the Operations Manager at the Mall, who asked for further details. I then forwarded a copy of the original letter. Two days later he responded via email:

There appears to be no record of receipt of your letter, so I can only assume that it has gone astray in the post.

Our CCTV system automatically deletes/overwrites footage after 30 days, and therefore I am unable to comply with your request ...

Bank 1 also claimed not to have received my letter of request, and stated that owing to a time lag, the information had been deleted. To this day, I have received no correspondence from the Museum.

Department Store 2 rang and explained their data controller had left the organisation and that the caller had taken over the role. He suggested he would look into the matter, and gave me a mobile number to contact him if anything else arose. After one week of no communication, I tried the number and left a message; the following week I left two more messages. At no time were these calls returned, and I am still awaiting a reply.

Kinks of complaint, I suggest, draw out some of the difficulties when relations are challenged or when the network of control embraces third parties. In this instance, I called for the assistance of the ICO because my requests were ignored, or hindered (allegedly) by postal and staff difficulties. As a consequence, for Shopping Mall 1, the introduction of the ICO instigated swift action; for others, the impact was less instantaneous. The kinks moved, pushed and cajoled the dynamic of the relationship in a progressive, or not, trajectory. Again, what I emphasise is the uncertainty in how

these relations are experienced and how the SAR progresses, as well as how participation and intention are often negotiated (Albrechtslund and Lauritsen, 2013). In this case, avoidance is part of the dynamic of the 'work-in-progress' that features in my relations with the data controller (Shields, 2012b).

Bends of competence

Despite the unpromising outcomes of some of my enquiries, I finish on a positive note; in three instances, I received good-quality CCTV footage on DVD, and in one instance still photographs. These examples demonstrate that making SARs does work and that when we condense or fold the distance between requestor and data controller, the object, as Latham (2011) argues, stays much the same, and what is important is the relationship that binds them. The relationship in this example begins with the fact that the three organisations had designed their own request forms. However, the initial stages of my requests were slightly less than straightforward as it was not clear that a form was needed, and only after my initial requests did I receive the form. Effectively, I had to provide the request twice because the times and dates provided in my initial request were replicated in the designated forms. What follows are the organisations that responded with the material I had requested.

Bus station and Open Street. I group these together as they had the same data controller. My initial requests were returned in a single envelope, and I was instructed to complete their SAR form. Both of the cheques for fees were also returned, and I was instructed only one payment was necessary. Once the form was completed and sent, I received a prompt reply which included footage from both incidents on one DVD.

Department store 1. In the store I had not been able to locate CCTV signs or contact details. After asking a store manager, he attempted to contact security and informed me there was 'a new form for this'. The manager was unsuccessful in locating the security person and took my name and address. I duly received a form from the organisation's 'Data Protection Paralegal', which I completed and returned with the requested fee. Three weeks later I received a DVD.

Bank 4. Again, this SAR started tentatively, as the bank displayed no contact details of their data controller on their signage. Upon seeking assistance from the bank's information desk, I was directed to their website, where I located the data controller's

address and found clear information on the request fee. On the 40th day after making my request, I received a DVD.

Department store 3. This request began badly, as I could not find any signage, and, when I asked the nearest member of staff, they directed me to the cashier, who then called security. Four security personnel arrived, all large and intimidating men. They were polite, but curt, and explained I would have to write to the store owner. Once the SAR was submitted, I received a prompt response outlining the £10 fee. Upon payment, I received 13 coloured sheets of still images from the footage (see Picture 3).

Picture 3. Department store – one sheet of stills.

Bends of competence emphasise that, even when the request proceeds successfully, there are still complexities in the relationship between CCTV staff and me. Again, in one instance, the irritation I obviously caused was lightly disguised, and, in each instance, the process of contacting the data controller was less than simple. Of

importance here is the converging of diverse actors and the tensions they generate; it is not the spatial distance or the SAR that poses most significance, but the interruption to the relationship that binds (Fussey, 2013; Hinchliffe et al., 2013). Good practice may be in evidence, but difficulties in operations remain.

Difficult relations

The folds, twists, kinks and bends of my experiences reveal a fluidity of interpretation as to how CCTV operators operationalise SARs, and also reveal the tensions and realities of how power is communicated and the allegiance in which it is held. Time and devotion are needed when pursuing personal data. The topologies of surveillant relations demonstrate some of the trajectories and intensities of the relations. Operators and data controllers, for the most part, seem ill-prepared to deal with the requests – or quite possibly delay is a form of denial, as on only one occasion did my initial requests result in getting the data. I spent over 20 hours making requests and dealing with follow-on letters and phone calls. In total I wrote 37 letters and made 31 phone calls. I also spent £60 making requests. Table 1 gives an indication of the success rates I experienced when sourcing contact details and the eventual success rates of the SARs.

Table 1. Subject Access Request (SAR) contact findings.

Location	Contact information on signs	Sign information that led to contact with data controller	Website information that led to contact with data controller	Requested information received
Shopping mall 1	X	X		
Shopping mall 2	X	X		X
Department store 1				X
Department store 2	X		X	
Department store 3			X	X
Bank 1	X		X	
Bank 2	X		X	
Bank 3	X		X	
Bank 4			X	X
Stadium			X	
Railway station			X	
Bus station	X		X	X
University	X	X		
Open street city centre system			X	X

Town hall	X	X		
Government building	X		X	
Museum				
Totals	10	4	11	6

Websites provided the most efficient source of information in my searches, and it remains surprising to me that this source is underutilised by organisations. Websites have the added advantage that they are easily updated and have no limits on the amount of information they can impart. The cost of processing fees for SAR forms, for example, could be placed on the websites. However, this overlooks the fact that the information should be evident on the signs that accompany the camera. On only four occasions did the signs effectively provide this information. As the Totals in the table suggest, despite the ICO's and DPA's clearly defined data access rights, the interpretation and action of data controllers is less clear. When faced with my requests, as well as the requests made with the support of the ICO, it would appear that technological expediency in deletion and organisational oversights in processing may offer glimpses of the propagation of ambiguity in how data rights are enacted. How power is circumvented, upheld, ignored and abused is striking in the refutation, obfuscation and competence of the data controllers. Forcing together the security

actors I have discussed reveals many inadequacies: specifically, normalised effects of security, where urban publics expect little interaction with CCTV, are disrupted, thus demonstrating the shortcomings and poorly operationalised practices employed by these security systems (Kettl, 2013; Wood and Webster, 2009). Mapping experiences and understanding them in terms of a spatial narrative embraces the elements that create distance but also compresses some of that distance.

Making sense of transference of power over distance highlights the potentials and propensities that contribute to relations around 'things' such as urban security data (Appadurai, 1986). The example of digital data may expose the inadequacies, digital transparencies or denials of security that shape the spatiotemporal relation of security in the city. Topologies as I see it draw on some of the complexities involved in CCTV and the control and monitoring of urban spaces. Certainly what I found in making SARs and chasing up contact information is that this is tedious and testing. Dealing with irate or less than accommodating staff and systems presents its own problems. Indeed, all too apparent is the power dynamic within how these relations are performed. Delay and refusal may have been a tactic of control - retribution, if you like, against the irritation caused by having to execute SARs. At issue here is the operationalisation of

the CCTV security networks: how organisations, staff and signs perform is not correlating with the intentions of the DPA. There is a power exercised by signs 'to signal a CCTV camera's presence in order to amplify its deterrent effects' (Lippert, 2009: p. 506). When the urban visitor enters a CCTV zone, such networks are operationalised in how that person's images are recorded and managed. However, what I have found in relation to, for example, contact numbers on signs is that, for the most part, they are inadequate.

Concluding thoughts

The happenings etched into the security landscape I have endeavoured to examine in this paper highlight the fragile nature of how security is performed and disrupted. These happenings, I contend, underscore how relationships between security operators and those who traverse city spaces can be understood. As the paper demonstrates, the intensive relations between data controller and urban publics are plain to see. The paper set out to examine what happens when we get closer and challenge the different types of power relations created by security dynamics. Fluidity of interpretation is key to understanding how operators respond to SARs and how they manage urban data. The distance traversed by the SAR was used to demonstrate the multifarious ways in which five topologies of surveillant relations illuminate how these

relations are put into practice. CCTV data remains the constant, but, as Latham (2011) or Hinchliffe et al. (2013) would have it, in topological terms it is not the object or the distance between things that is important, rather it is the relations that bind which are. The chains of events outlined in this paper touches upon these ambiguous, complicated and difficult relations, not least because as we have seen data controllers often fail to provide CCTV data – 11 out of 17 did not deliver. As has been stated elsewhere (see IRISS Policy Brief 2015), deeper considerations and indeed more robust policy analysis must be given to SAR procedures.

As I have also argued, urban studies can benefit from topological appreciations of the security relations that pervade UK cities. This, I contend, is reliant on viewing these relations as not bounded or putative, but as interruptible. An interesting and productive way to do this is to create unease and tensions in how power relations are performed and understood. The challenge, to some degree, forces some of the ambiguities to the surface. Power, as I have stressed, is important here and power is rarely absent from moments of surveillance (Armstrong and Norris, 1999: p. 92). Power lies in its omnipresent potential: 'do it and we will see it' is how security signs present themselves around any security-conscious city or town (see Cole, 2002). However, maybe the cameras don't see it and what then? Are we duped or have we

become accustomed to rationalising behaviour in the belief that deviant behaviour will be seen. The answer to which is something I do not know, but I suspect most of us simply carry on regardless. Disruption however may help to make sense of these security and spatial complexities (Deleuze, 1993). Making SARs challenges the normalisation of CCTV in the city by asking CCTV operators to do something they would, it appears, seldom have to do. Making sense of the topology of surveillant relations as I have argued illuminates the power that permeates the relations between watcher and watched, as well as providing some thought on the interplay between CCTV signs, operators, data controllers and urban publics.

Funding

This article was funded by the Seventh Framework Programme for research, technological the European Union's development and demonstration under grant agreement no 290492 and the project Increasing Resilience in Surveillance Societies (IRISS).

Acknowledgements:

I would firstly like to thank colleagues on the IRISS project, particularly Clive Norris and Xavier L'hoiry for their inspiration on WP3 and this aspect of the project. I would like to

thank the European Council for their support. In addition I want to thank Chiara Fonio and Kirstie Ball for their valuable comments on earlier drafts of the paper, as well as the audience at *City Materialities, City Securities*, (CRESC workshop), for their perceptive and challenging observations. In addition I would like to thank the 3 anonymous referees and the guidance of Urban Studies editor Jon Bannister for their critical, insightful and helpful comment.

References

- Albrechtslund A and Lauritsen P (2013) Spaces of everyday surveillance: Unfolding an analytical concept of participation. *Geoforum* 49: 310–316.
- Allen J (2011) Topological twists: Power's shifting geographies. *Dialogues in Human Geography* 1: 283–298.
- Allen J and Cochrane A (2010) Assemblages of state power: Topological shifts in the organization of government and politics. *Antipode* 42: 1071–1089.
- Amoore L (2009) Algorithmic war: Everyday geographies of the war on terror. *Antipode* 41: 49–69.

Appadurai A (Ed.) (1986) *The Social Life of Things: Commodities in Cultural Perspective*.

Cambridge University Press.

Armstrong G and Norris C (1999) *The Maximum Surveillance Society: The Rise of CCTV*.

London: Berg.

Ball K (2002) Elements of surveillance: A new framework and future directions.

Information, Communication & Society 5(4): 573–590.

Big Brother Watch (2012) The price of privacy: Councils spend half a billion pounds on

CCTV in four years. Available at:

<http://www.bigbrotherwatch.org.uk/home/2012/02/price-privacy-councils-spend-521m.html>.

Blair P (2013) Panopticons within panopticons: Surveillance inversions in Willie

Doherty's video installations. *Journal of Postcolonial Writing* 49: 539–551.

Brands J, Schwanen T and van Aalst I (2013) What are you looking at? Visitors'

perspectives on CCTV in the night-time economy. *European Urban and Regional Studies* 0(0): 1–17.

BSIA (2014) The picture is not clear. British Security Industry Association. Available at:

<http://www.bsia.co.uk/>

- Clement A and Ferenbok J (2012) Mitigating asymmetric visibilities: Towards a CCTV signage code. In: Doyle A, Lippert R and Lyon D (eds) *Eyes Everywhere: The Global Growth of Camera Surveillance*. New York: Routledge, pp.309–332.
- Coaffee J (2005) Urban renaissance in the age of terrorism: Revanchism, automated social control or the end of reflection? *International Journal of Urban and Regional Research* 29(2): 447–454.
- Cole M (2002) Signage and surveillance: Interrogating the textual context of CCTV in the UK. *Surveillance & Society* 2.
- Data Protection Act (1998). Available at:
<http://www.legislation.gov.uk/ukpga/1998/29/contents>
- De Goede M (2014) The politics of privacy in the age of preemptive security. *International Political Sociology* 8: 100–104.
- DeLanda M (2006) *A New Philosophy of Society: Assemblage Theory and Social Complexity*. London: Continuum.
- Deleuze G (1993) *The Fold: Leibniz and the Baroque*. London: Athlone Press.
- Ditton J (2000) Crime and the city. *British Journal of Criminology* 40: 692–709.
- Fleming P and Sewell G (2002) Looking for the good soldier, Švejk. Alternative modalities of resistance in the contemporary workplace. *Sociology* 36(4): 857–873.

- Fussey P (2013) Contested topologies of UK counterterrorist surveillance: The rise and fall of Project Champion. *Critical Studies on Terrorism* 6: 351–370.
- Fyfe N and Bannister J (1996) City watching: Closed circuit television surveillance in public spaces. *Area* 28: 37–46.
- Graham S (1998) Towards the fifth utility? On the extension and normalisation of public CCTV. *Surveillance, Closed Circuit Television and Social Control*. Aldershot: Ashgate.
- Graham S (2012) Olympics 2012 security: Welcome to lockdown London. *City* 16: 446–451.
- Harvey P (2012) The topological quality of infrastructural relation: An ethnographic approach. *Theory, Culture & Society* 29(4–5): 76–92.
- Held C (2012) Intelligent video surveillance. *Computer* 45: 83–84.
- Hetherington K (1997) Museum topology and the will to connect. *Journal of Material Culture* 2: 199–218.
- Hier SP, Walby K and Greenberg J (2006) Supplementing the panoptic paradigm: Surveillance, moral governance and CCTV. *Theorizing Surveillance: The Panopticon and Beyond*. Cullompton, Portland: Willam Publishing, pp.230–244.

Hinchliffe S, Allen J, Lavau S, Bingham N and Carter S (2013) Biosecurity and the topologies of infected life: From borderlines to borderlands. *Transactions of the Institute of British Geographers* 38: 531–543.

Home Office (2013) Surveillance Camera Code of Practice. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

ICO (2014) CCTV. Information Commissioner's Office. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/>

IRISS (2014) Increasing resilience in surveillance societies. FP7 EU project. Available at: <http://irissproject.eu/>

IRISS (2015) 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-Final.pdf>

Kettl DF (2013) *System under stress: Homeland security and American politics*. New York: Sage.

Kitchin R (2014) The real-time city? Big data and smart urbanism. *GeoJournal* 79(1): 1–14.

- Klauser, F (2004) A comparison of the impact of protective and preservative video surveillance on urban territoriality: The case of Switzerland. *Surveillance & Society* 2(2/3).
- Klauser FR (2007) Difficulties in revitalizing public space by CCTV: Street prostitution surveillance in the Swiss city of Olten. *European Urban and Regional Studies* 14: 337–348.
- Koskela H (2002) Video surveillance, gender, and the safety of public urban space: “Peeping Tom” goes high tech? *Urban Geography* 23(3): 257–278.
- Latham A (2011) Topologies and the multiplicities of space-time. *Dialogues in Human Geography* 1: 312–315.
- Law J (1986) On the methods of long distance control: Vessels, navigation, and the Portuguese route to India. In: Law J (ed.) *Power, Action and Belief: A New Sociology of Knowledge?* Henley: Routledge.
- Law J and Mol A (2001) Situating technoscience: An inquiry into spatialities. *Environment and Planning D: Society and Space* 19: 609–621.
- Levesley T, Martin A and Britain G (2005) *Police Attitudes to and Use of CCTV*. London: Home Office.
- Lippert R (2009) Signs of the surveillant assemblage: Privacy regulation, urban CCTV, and governmentality. *Social & Legal Studies* 18: 505–522.

- Lury C (2013) Topological sense-making: Walking the Mobius strip from cultural topology to topological culture. *Space and Culture* 16: 128–132.
- McPhail B, Ferenbok J, Dehghan R and Clement A (2013) “I’ll be watching you”: What do Canadians know about video surveillance and privacy? *iConference*.
- Middleton J and Yarwood R (2013) ‘Christians, out here?’ Encountering street-pastors in the post-secular spaces of the UK night-time economy. *Urban Studies* 52: 501–516.
- Moore D (2011) The benevolent watch: Therapeutic surveillance in drug treatment court. *Theoretical Criminology* 15: 255–268.
- Murakami Wood D, Lyon D and Abe K (2007) Surveillance in urban Japan: A critical introduction. *Urban Studies* 44: 551–568.
- Murakami Wood, D. (2008). Towards spatial protocol: the topologies of the pervasive surveillance society. In Aurigi, A and De Cindio, F (eds.) *Augmenting Urban Spaces: Articulating the Physical and Electronic City*. Aldershot: Ashgate, pp93-106.
- Neyland D (2004) Closed circuits of interaction? *Information, Communication & Society* 7: 252–271.
- Norris C and McCahill M (2006) CCTV: Beyond penal modernism? *British Journal of Criminology* 47: 97–118.

- Pottie-Sherman Y and Hiebert D (2013) Authenticity with a bang: Exploring suburban culture and migration through the new phenomenon of the Richmond night market. *Urban Studies* 52(3): 538–554.
- Ruppert E (2012) The governmental topologies of database devices. *Theory, Culture & Society* 29: 116–136.
- Sewell G and Barker JR (2006) Coercion versus care: Using irony to make sense of organizational surveillance. *Academy of Management Review* 31(4): 934–961.
- Shields R (2012a) Cultural topology: The Seven Bridges of Königsburg, 1736. *Theory, Culture & Society* 29: 43–57.
- Shields R (2012b) Feral suburbs: Cultural topologies of social reproduction, Fort McMurray, Canada. *International Journal of Cultural Studies* 15(3): 205–215.
- Smith G (2007) Exploring relations between watchers and watched in control(led) systems: Strategies and tactics. *Surveillance & Society* 4: 280–313.
- Surveillance Studies Network (2010) An update to a report on the surveillance society. UK Information Commissioner.
- Townsend AM (2013) *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*. New York: WW Norton & Company.
- Tuan Y-F (1974) *Topophilia: A Study of Environmental Perception, Attitudes, and Values*. Columbia University Press.

Vannini P (2011) *Ferry Tales: An Ethnography of Mobility, Place, and Technoculture on Canada's West Coast*. New York: Routledge.

Wagenaar P and Boersma K (2012) Zooming in on 'heterotopia': CCTV-operator practices at Schiphol Airport. *Information Polity* 17: 7–20.

Webster WR (2002) The diffusion, regulation and governance of closed-circuit television in the UK. *Surveillance & Society* 2: 230–250.

Wood DM and Webster CWR (2009) Living in surveillance societies: The normalisation of surveillance in Europe and the threat of Britain's bad example. *Journal of Contemporary European Research* 5(2): 259–273.