The Dynamics of Impersonal Trust and Distrust in Surveillance Systems

Abstract

Empirical research concerned with the trust individual's may or may not have in surveillance systems has largely been gauged through opinion poll and survey type research. Although these may be useful in augmenting broad patterns of trust based attitudes, this article argues that they tend to harbour theoretically weak conceptualisations of trust which may produce misleading results. We draw on relevant concepts related to notions of 'impersonal trust' (for example, 'access points', 'facework' and 'complexity-suspension') to facilitate a qualitative analysis of semi-structured interviews which concerned Londoners trust related experiences, perceptions and understandings of living in a so called 'surveillance society'. We form a number of preliminary conclusions which are of interest to sociological research on trust and surveillance studies: contrary to prior research on trust and surveillance, trust related positions may be neither static nor polarised, but processual and situational; the suspension of certainty bridged by impersonal trust is particularly problematic in surveillance systems as they especially lack access points; and impersonal trust related positions are likely to be considerably weak as information about the systems requires specialist information.

Introduction

Trust is a primary constituent of the relational dynamic of most surveillance systems. Issues concerned with trust are often the catalyst for the implementation of a surveillance system[i]; for example, citizens need to be surveilled as they are untrustworthy (at least some of them), in turn citizens may feel that the surveillors are untrustworthy. Norris argues that increasing forms of mass surveillance sends a clear message to the public "that everybody is untrustworthy. If we are gathering data on people all the time on the basis that they may do something wrong, this is promoting a view that as citizens we cannot be trusted" (House of Lords 2009: 29). Additionally it is considered to profoundly negatively affect "social cohesion and solidarity", "fosters suspicion", and thus can be understood as committing a "slow social suicide" (Ball *et al*. 2006).

Even though trust is clearly a key component of surveillance, there is very little empirical analysis in the surveillance studies context which thoroughly accounts for the dynamics of trust. Indeed Raab suggests that 'trust' is the second main concept (after the concept of 'risk') which needs revisiting in the surveillance and privacy protection context to further understand its practical implications (Raab 2002). He states,

> Alongside face-to-face and other interactions amongst mutually known actors, virtual transactions with strangers and abstract systems extend chains of (inter)dependence into new territory in which familiar ways of establishing trust are absent and the reliability of new mechanisms remains to be tested (Raab, 2002: 112).

Indeed, throughout the trust literature there is very little empirical analysis of citizens' perceptions and experiences of trust in abstract systems (what we refer to here as impersonal trust). Much of the research in these contexts has been conducted through quantitative analysis (such as surveys and opinion polls); although these are informative they incur a number of limitations. For example, they are not able to

sufficiently address the complex dynamics of what they seek to understand and they often draw on overly simplistic notions of trust.

To facilitate a detailed analysis of the dynamic ways that positions of impersonal trust are negotiated and produced in these contexts we incorporate relevant concepts associated with impersonal trust: Lhumann's (1979) understanding of *trust* and *distrust* as being distinct but potentially coexistent mechanisms for managing complexity; Giddens' (1990) conceptualisation of 'access points', Goffman's (1967) 'facework', and Möllering's (2006) 'complexity suspension'. These conceptual tools facilitate a qualitative analysis of an empirical study that consisted of 31 semi-structured interviews of Londoners' trust related experiences and perceptions of living with everyday surveillance.

The analysis reported here is structured by three concerns. Firstly, we draw on the concept of impersonal trust to examine accounts of trust in abstract systems of surveillance (this includes incorporating the concepts of 'access points', 'facework' and 'complexity suspension'). Secondly, we investigate how citizens dynamically produce trust-related positions in the surveillance context. Finally, we attend to the range of ways in which participants construct trust. We focus on how participants discuss trust in relation to three domains of surveillance: e-commerce; e-government; and CCTV. These different domains give rise to a number of different dilemmas in relation to privacy: consumer convenience versus privacy; efficiency versus privacy; and security versus privacy.

Trust and Surveillance Studies

Surveillance is often thought of as primarily involving visual data that is captured through Closed Circuit Television (CCTV). However, surveillance is increasingly conducted through a wide range of means particularly as communication occurs progressively more over the internet. Hence much of surveillance nowadays is of a digital nature which equates to more and more forms of personal data being stored on large databases. The term 'dataveillance' has been coined to denote this form of data-gathering (throughout this article we will use the term 'surveillance' to indicate the multifarious forms of personal data collection processes). With this acceleration, academic interest in surveillance has gained momentum and has now more formally emerged as a trans-disciplinary community of interests headed under the umbrella term 'surveillance studies' (for example, see Ball *et al*. 2012). Scholars in this field argue that surveillance has emerged as "the dominant organizing practice of late modernity" (Ball *et al*. 2012: 1). Even though trust is clearly one of the central components of surveillance systems it is astonishing that the term does not even appear in the index of the aforementioned *Routledge Handbook of Surveillance Studies*. This is possibly because trust in this context has yet to receive sufficient suitable scholarly theoretical and empirical consideration.

Empirical research in relation to surveillance and trust has mostly been conducted through surveys, opinion polls by governments and industry reporting on citizens' trust related attitudes towards surveillance. For example *The Surveillance Project* (Zureik *et al*. 2009), the *Flash Euroberometer*, (Gallup Organisation, 2010), *YouGov/Telegraph* (2006), *Big Brother Watch* (2009), and *Joseph Rowntree Reform Trust Ltd*., (Anderson *et*

al. 2009) have all developed opinion polls and surveys which relate to trust and surveillance. The questions that such surveys ask respondents, for example, whether they would like to see CCTV increased in certain areas, are relatively reductionist. Such questions do not address for example 'why they would or would not like to see them increased'. And polls such as *The Surveillance Project*, the *Flash Eurobarometer YouGov/Telegraph,* and *Big Brother Watch*, tend to ask overly generalised questions concerning the collection of personal information and trust, which does not allow for insights into to *why* there is or is not trust in these areas. Questions pertaining to whether respondents feel safer with particular systems often only require a negative or positive response. This is also the case in 'likert' forms of surveys, as these only inquire into the levels of agreement or disagreement by, for example, inquiring into the degrees of trust. However, it has been found that citizens can feel quite ambivalent about increasing surveillance infrastructure as for example this may increase security but is likely to infringe upon one's privacy. An individual may feel simultaneously safer and therefore trusting of the implementation of a surveillance system and equally feel distrusting of the surveillors (Koskela 2000). Surveys therefore do not have the ability to inquire into the nuanced ways that people may respond to and experience surveillance systems; such as, how might they feel and negotiate distrust and/or trust positions. Additionally, trust positions can fluctuate as they are not as static as often depicted, but are likely to have processual characteristics which are situationally specific (Dibben 2000).

Conceptualising Trust and Distrust in the Surveillance Context

In many of the surveys that we have cited, 'trust' is usually treated as being opposite to 'distrust'. For example, the following question was asked in *The Surveillance Project* "When it comes to the privacy of personal information, what level of trust do you have that your government is striking the right balance between national security and individual rights?" (Zureik *et al*. 2009). From this question respondents can tick one of the following responses: a) very low level of trust, b) fairly low level of trust, c) reasonably high level of trust, and d) very high level of trust. The lower levels of trust are often reported as representing 'distrust'. It has been argued that trust and distrust are not simply at opposite ends of the same spectrum (Harrison *et al*. 2001; Sinaceur 2010). For example, Jones in the *Routledge Encyclopaedia of Philosophy* (Craig 1998) states that there is wide agreement that, "[T]rust and distrust are contraries but not contradictories. Just because one does not trust, it does not follow that one thereby distrusts" (8689). Similarly, in the context the games theory and trust, Ullmann-Margalit (2002) analyses versions of the prisoner's dilemma (a well-worn model for looking at the rational choices between trust and distrust, see Hardin (2006) for overview and critiques). She looks at how trust can logically emerge out of forms of distrust, even in relation to a Hobbesian understanding of humans in the so called 'state of nature', trust can be formed without resorting to an external Sovereign. Elsewhere Ullmann-Maralit makes the point that while the concepts of trust and distrust are not mutually exhaustive (2002); Stoneman explains this by stating that just because a person does not find a particular person trustworthy does not necessitate that s/he finds that person untrustworthy. Similarly, if a person does not find another person untrustworthy does not necessitate that s/he finds that person trustworthy (2008: 23). Stoneman goes on to suggest that a position is often not formed between the two due to a lack of information and thus a stage of 'agnosticism' occurs between trust and distrust.

In illustrating the conceptual distinctions between trust and distrust, Harrison *et al*. argue that the emotions that relate to trust are not on the opposite spectrum of the emotions that relate to distrust. Distrust constructs often include such emotions as wariness, caution, cynicism, defensiveness, anger, fear, hate, feelings of betrayal, uncertainty and a lack of confidence; whereas trust often include such emotions as hope, safety, assurance and confidence; "[T]hese sets of emotions may be more orthogonal than merely at different ends of the same scale from each other" (46). Thus, Harrison *et al*. state that "trust and distrust are separate constructs that may exist simultaneously" (p. 29). Lewicki, McAllister and Bies (1998) argue that the 'normative view' of trust is often understood as being opposite to distrust in the same way that *good* is seen as being opposite to *bad* on a single continuum (Lewicki *et al*. 1998). Indeed Lewicki *et al*. argue that this normative view tends to associate trust with the good and distrust with the bad. In this article we find it useful to side with the views that trust and distrust are not necessarily opposites and do not necessarily have fixed good or bad valences.

Additionally, Luhmann (1979) has drawn attention to the important relational dynamic of trust and distrust in the negotiating of a dis/trust position, through the suggestion that trust and distrust are distinct but are also potentially coexistent mechanisms for managing complexity. Luhmann argued the rather intriguing point that increases in trust or distrust – apart from increases in the other – may do more harm than good. For example, trust without elements of distrust is likely to lead to vulnerability and distrust without elements of trust can lead to paranoia. Dawes and Thaler (1988) developed a simple effective illustration of how trust and distrust work hand-in-hand in the most basic of systems.[ii] Lewicki *et al*. contend that "organisations are rife with mixed-and multiple-motive conditions" (1998: 454) and they call for a richer understanding of the dynamics of trust and distrust relations.

Thus the forms of trust that we discuss and analyse throughout this article can be allied to what has elsewhere been termed 'institutional-based trust' (Zucker 1986) which concerns institutions as sources of trust; and 'systems trust' (Luhmann 1979; Barber 1983; Giddens 1990) which concerns trust and confidence that individuals have in (abstract) systems (also see Lane 2000: 15). Both of these concepts can be understood as inextricably linked to processes involving 'impersonal trust'. Although both institutional and systems trust may involve aspects of interpersonal trust (as will later be discussed), because of an increasing dependence on ICT infrastructure, the forms of trust that citizens develop in many institutions and systems arise through the absence of interpersonal (face-to-face) factors. For example, Giddens states that trust in abstract systems may entail no "encounters at all with the individuals or groups who are in some way "responsible" for them" (1990: 83).

This is quite problematic for some trust researchers as it can be envisaged as a dispassionate form of trust which does not involve the forms of emotion and affect that many trust researchers see as important to the dynamics of trust processes (for example, Lewis & Wiegert 1985; McAllister 1995). Hardin (2006) stresses that "[T]he nature of a personal relationship involving trust is far richer and more directly reciprocal" (65). And yet Levi (1998) has argued that while trust exists between people, trustworthiness can be attached to both people and institutions. Our past experiences

with a particular individual or institute inform us as to whether he, she or it is worthy of our trust. For example, according to Luhmann (1979), system-trust is developed and maintained through the functioning of a system which facilitates generalizations and indifference (Möllering 2006: 364). Similarly, Zucker (1977) stresses that impersonal trust is enabled through institutionalised norms and beliefs. Additionally, impersonal trust is achieved through the systems having functioning controls maintained by experts that the actors can trust rather than the experts or people themselves. However, trust in an abstract system or institute cannot solely be based on previous experiences as for example, we may not have had any experiences to draw upon. In this respect trust is seen to be facilitated for Luhmann in the assumption that it is normal to trust such a system, as everybody else does.

In this way the complexity of the system is held, one does not need to have expert knowledge or previous experience. Thus trust and distrust here for Luhmann are what he terms 'functional equivalents' but entail different means. Both allow the containment of social uncertainty and complexity (simplification). Trust allows undesirable outcomes to be removed from consideration and allows desirable outcomes to be viewed as likely – *beneficial expectations*. While distrust allows for undesirable outcomes to be viewed as likely – *injurious expectations.*

However, following Shapiro's (1987) article discussing 'The social control of impersonal trust', Möllering (2006) argues that Luhmann does not appropriately account for a 'suspension of doubt' between distrust and trust. Rather than simply trust or distrust in a system, actors either accept "a given level of assurance" or look "for further controls and safeguards" (364). Similarly, McKnight *et al*. (1998; 2002) suggest that impersonal trust has at least two dimensions. These are *situational normality beliefs* and *structural assurances*. The former implies that trust is given as everything is as it should be: things are properly ordered in such a way to bring about desired outcomes. While the latter implies that trust is generated through such things as contracts, guarantees, and regulations that are in place. The seeking of 'controls and safeguards' when doubt is suspended is particularly well conceptualised, according to Möllering, through Giddens' (1990) notion of an abstract system's "access points". In everyday interpersonal trust activity, trust between individuals is seen to be enacted in part through 'facework', a concept borrowed from Goffman's (1967) influential writings concerned with interpersonal impression management. Goffman defines the term face as,

> the positive social value a person effectively claims for himself by the line others assume he has taken during a particular contact. Face is an image of self delineated terms of approved social attributes (1967: 5).

In this respect, according to Misztal, interpersonal trust is based on,

> our ability to express and read the intentions behind people's behaviour; thus trust is the essential background of everyday interaction, and as such it helps us to simplify information, reduces the complexity of signals, and protects us from the ambiguity and uncertainties of many situations (2001: 323).

Thus, abstract systems are essentially faceless (impersonal) but obtain a trusting face (or not so trusting) through their access points (Giddens 1990). The access point of an abstract system is where citizens encounter professionals and experts who are representative of the particular abstract system; for example, a doctor who regularly meets a patient is an access point of the health service he or she works for.

The terms thick and thin trust are usually applied to interpersonal forms of trust; thick trust denotes strong ties between individuals and thin trust denotes weak ties (Putnam 2000). We apply the terms thick and thin to what is denoted here as thick and thin institutional and abstract systems trust. The argument we make above suggests that the forms of trust and distrust that the citizen has in an institute (or abstract system) which does not have access points is likely to be thin. This is because it is unlikely then to have undergone the kinds of dynamic processes that facework facilitates. In contrast, access points offer the citizen the chance to develop the dynamic forms of trust discussed above, improving the citizens' chance to develop more thick forms of trust and distrust.

Facework then is especially problematic in the context of surveillance systems, as the access points are often very restricted and may need to remain essentially faceless, abstract and impersonal for them to be effective. Accordingly the affective impacts of these systems are likely then to remain complex, ambiguous and uncertain. Given this, the process of trust requires quite lofty, what Möllering (2006) describes as, 'suspensions of doubt' in relation to the perceived intentions of the surveillors, wherein perhaps other forms of controls and safeguards need to be sought. In contrast to the trust suspension, there may be indifference towards the abstract systems, or there may be various forms of lacks of trust, distrust and suspicions. For example, the vacuum ensued by the facelessness of the surveillor may propagate fantasies of the other, such as through the development of conspiratorial thinking. Thus impersonal trust in the surveillance context can be viewed as particularly problematic and merits a detailed micro analysis, something which is presently missing in the literature.

Such detailed analysis cannot be instituted through opinion poll type research but requires qualitative analysis. Thus we produce a qualitative, analysis of the sections of semi-structured interviews that concerned issues of dis/trust in surveillance systems. Additionally, the theoretical concepts discussed above, namely access points, facework, and complexity suspension are employed to further theoretically inform the analysis of the dynamics of impersonal dis/trust in surveillance systems.

Methodology

After the study had gained ethical approval by a university's ethics committee, thirty one adult participants residing in London and the surrounding area were interviewed by two research assistants (one male and one female). Nineteen of the participants were female and twelve were male with an average age of 41.2. The participants were recruited by a number of strategies (e.g. payment of participants (£20 shopping voucher), targeted distribution of flyers in public places, in local businesses, approaching university staff and students). The participants were made up of a range of ethnicities: fourteen identified as white British, six white other, three black British, two as black African, two as British dual heritage, one as black other, one as black Caribbean, and one as Sri Lankan. Three of the participants did not declare their employment status, seventeen were employed, six were students, three were full-time carers and two were unemployed. The educational attainment was a lot higher than the national average as five had Masters Degrees, twelve had degrees, one had a BTEC, three had A levels, six had CSE/GCSEs, and one had none.

The semi-structured interviews took place either in the University or a public place convenient to the participants (following a risk assessment). The duration of the

interviews were on average 45 minutes each. The interviews generally focused on citizens' knowledge of the different forms of surveillance systems, their everyday experiences of them, the role they believed surveillance systems play in contemporary society, and their views on balancing desires for security with desires for privacy. The interview data was then transcribed and anonymised. Although the semi-structured questions sought information concerning trust in surveillance systems this was not the sole focus of the interviews, however it emerged as a dominant theme throughout the analysis.

Data analysis

According to the discourse analytic approach, the interview transcripts were initially coded in relation to talk concerning trust and distrust. The participants may not have explicitly used the words 'trust' or 'distrust' but to be included in the data-set, they would have to have stated something which we regard as trust or distrust related expressions. For example, the statement "CCTV makes me feel safer" would be considered as including an expression of 'trust in CCTV'. If an entity influences a person to feel, for example, safe or insecure this tends to imply that the entity is trustworthy or untrustworthy respectively.

The initial coding enabled the identifying of material relevant to these issues, and was deliberately open-ended and inclusive (Potter & Wetherell 1987). Following the initial stage of coding a 'cyclical process' (Potter & Wetherell, 1987) was undertaken, which involved moving between stages of coding and analysis. During the cyclical stage, coding and analysis become related processes, in which early themes are fed back into codes, which then inform subsequent analysis; this in an iterative process that increases the depth and sophistication of analysis.

What was of particular interest to analyse in relation to the present study were the parts of the interviews through which the discussion of the surveillance systems entailed nuanced dis/trust related positions which could not easily have been categorised as fitting singularly into either a trust or distrust based stance. For example, participants may fluctuate between positions, and thus were quite ambivalent.[iii] These are not all necessarily contradictory or indeed irrational, but demonstrate how trust related positions can be fluid and processual. The interviews allowed participants to think through the dilemmas of for example needs for security balanced against needs for privacy. The space of the interviews allowed for positions to be constructed broken down and reconstructed. As discussed earlier, Luhmann (1979) suggests that trust and distrust positions can work dialectically to support each-other. For example, ambivalent dis/trust related positions that a person may have of one of the surveillance systems can contrast and differ for the varying aspects and contexts of the system. Overall, ambivalences highlighted how notions of generalised forms of trust in a particular system can be misleading; as the abstract systems become increasingly complex and impersonal they are likely to produce equally complex trust related affects. The below analysis attempts to develop insights into these multifaceted dynamics in relation to three specific surveillance systems which were discussed by the participants in relation to trust and distrust: E-Commerce, E-Government, and CCTV.

Table 1

Trust in:	CCTV	Internet shopping	Government
Number of participants	27	24	22
Number of references*	388	163	60

Table 1 shows the amount of participants who spoke about each theme and how many references were made about the theme overall.
*'Number of references' relates to the amount of interview dialogue segments that are dedicated to the theme.

Results Sections

E-Commerce Trust

'Trust in internet shopping' was an issue that seemed to particularly concern the participants. Their experiences of it were portrayed as invariably negative and we heard a variety of concerns; for example stories of credit card fraud, related issues of identity theft and concerns with the surveillance that occurs through E-transactions. For example Susan does not shop on-line because she distrusts it for a number of reasons. When asked if she shops online she stated:

> Extract 1: Susan
> S: I don't I should but <I: should do?> [laughter] but I do have this kind of distrust to kind of like the data information on it <I: ok> and it can be kind of like erm what's the word hacked downloaded and whatever abused <I: m-hm> so I'm a bit kind of like I haven't fancied it yet.

While Susan was concerned about the potential illegal use of her data, Sharon discusses how her diminishing trust is due to the various ways companies can use her data:

> Extract 2: Sharon
> S: what I would like to change personally is to make people aware of the DVLA, the shopping habits, basically just to make people aware that these people who up until now I've always trusted I don't anymore <I: mm, ok> you know just think the DVLA (2) they can sell my erm information to a wheel company . . . the public should be more aware of the circle of trust they have in people just basically isn't there.

However, participants did not always simply come down on one side or the other in terms of trust and distrust. What was of particular interest to our analysis was when participants discussed nuanced and ambivalent trust related thoughts and feelings. In the following 'extract 3', Mohammed discusses how he recognises features of a website that he portrays as facilitating the type of trust that he requires to shop online.

> Extract 3: Mohammed
> <I: Do you do any online shopping? In terms of bank details bank accounts> M: yes I do <I: Do you trust online shopping?> Erm I can trust online, I don't but I can (.) if I see some features on that website that I'm aware of that ok this proves

> there is safety like there is a padlock, there is lock and there is SSL and all these technologies implemented on that website then I'll feel safe using my financial card or whatever in that sense (.) but if there is if I suspect the website to be dodgy like the link that your personal details would be going to when you click and submit or check out or whatever if I don't trust that link then I wouldn't shop <I: ok so you are cautious?> yeah I m cautious

Clearly Mohammed portrays some insight into internet security technology. This knowledge is constructed as helping him to feel safer and more trusting of internet shopping. Interestingly he answers the question whether 'he trusts online shopping' by stating that he "can trust online" but he doesn't. Trust here is configured as something that is not passively gained but involves an active engagement of delineating criteria to evaluate whether a system is trustworthy. He suggests that at times he does not trust a website as he "suspects" it "to be dodgy". This is, for example, through noticing the padlock sign and/or the SSL which is a protocol developed by Netscape, short for Secure Sockets Layer, which increases the security for transmitting private documents over the internet. *Suspecting* the *dodginess* of a website then requires an active engagement of looking for signs and clues to verify its authenticity. Here then trust is developed through a duality relationship between distrust and trust. Trust and distrust are simultaneously engaged with; not trusting facilitates the active engagement which will either solidify one or the other position. However, in contrast to Luhmann's notion of the withholding of complexity, Mohammed's engagement here actually calls into play some complex understanding of internet shopping systems.

It would be incorrect to simply surmise that Mohammed distrusts or indeed trusts internet shopping; his trust and distrust are contextually specific and attuned through experience and the acquisition of particular forms of knowledge. It can be related to what Giddens refers to as an 'active trust' (1994) which develops gradually in processes which require active forms of agency and what Möllering (2006) refers to as processes of 'reflexive trust'. This can be associated to a form of facework or what we term 'interfacework'. The access points of the impersonal system are not embodied through the physical features that are displayed on an organic face, but are rather manifest, to some degree, through a B2C corporations website interface which may or may not harbour the forms of security technologies which facilitates a kind of trusting impression management for Mohammed. Thus what we have coined as interfacework here is the agent actively seeking controls and safeguards on websites to help produce a suspension between ignorance and certainty.

It is worth noting however, that Mohammed is not representative of the general population who uses or decides not to use the internet for shopping. He is a 27 year old male who has a degree in Information Technology and so is very likely to be a refined user of the internet. Margaret, a 53 year old female carer, did not state what her highest academic qualification is, but states that she has used her computer to shop (a few times) but does not anymore as she does not trust it.

> Extract 4: Margaret
> <I: Right, do you do any shopping online?> Margaret: Occasionally <I: right> I've bought erm a pram for my daughter but that's about it and a couple of silly things I don't really do it I don't use my computer to shop I don't trust it I just don't

> trust it I wouldn't wanna put my bank details in the computer <I: ok> I just don't I don't know why maybe it's 'cause I'm I don't go on computers a lot anyway (.) probably my age really that you know its a technology I'd rather just I'd do it on the phone to companies that I use that I know that I trust
>
> Extract 5: Margaret
> M: I just don't do it on a computer 'cause it's just, you know I'm not used to the computer yet I've only just got a laptop (.) we've had a computer in the house for years but it got quite old and it got viruses on it my son you know my son used to use it all the time but I've just got a laptop so once I've (.) get a bit more confident with it <I: Ok so it's not because of> It's not because of the credit thing cause I've got a security thing on my computer and everything <I: Is it erm is it because you don't want to give up your personal data online though?> Yeah and I think well it's cause I'm not confident doing it yet <I: ok, alright> it's just me <I: right> I mean I think once I get start to use it a lot more and I get more confident then I probably will because I know my computer's all got security thing on it and I've obviously you know passwords and things

Margaret repeats the refrain "I don't trust it" twice near the beginning of the first segment of the interview, portraying a sense of distrust in internet shopping. She presents herself as being unclear as to why this is but then suggests this may be because she is not familiar with the technology of computers which she attributes to her age. Hence she does not have the technical insight required to seek the forms of controls and safeguards instrumental in developing the impersonal trust relationship. A technology that she appears to be more familiar with is the telephone as she presents a sense of the processual growth of trust over time which has come about through an active or reflexive engagement with certain companies through this medium; processes which are still in embryo in relation to the internet. The telephone as an access point of B2C commerce are, perhaps, much better at facilitating trust. What would otherwise be impersonal trust through internet shopping may now be considered as a form of interpersonal trust. However, this access point does not, again, facilitate facework in the traditional sense, but is much more about 'voicework'. The controls and safeguards utilised to acquire trust here (the impression management) are communicated vocally, through which concerns are potentially alleviated instantaneously through the question and answer format.

However, a little later in the interview Margaret portrays some awareness of the controls and safeguards that she needs to become more familiar with. She uses terms such as "viruses", "security thing", and "passwords" in a form of acknowledgment that she may eventually be able to actively engage in more trust work or what she considers as "confidence" in giving over personal information through internet shopping. Thus she moves from a position of not being able to trust *it* (the internet), to a lack of confidence in *herself* in relation to *it* through the statements from "I don't trust it" to "it's just me". In contrast to Mohammed, Margaret presents a low engagement with internet security technology which gives way to vulnerability, inhibiting internet shopping experiences. This engenders two positions that she portrays chronologically: firstly, a distrust of the internet and secondly, a lack of confidence in the self (self-confidence, or self-trust (Lehrer, 1997)) in relation to the internet. However, through the process of actively engaging with these issues in the context of the interview, Margaret presents a sense of

developing the resources to move between the two positions, portraying a much more fluid sense of impersonal trust positioning.

Coles-Kemp *et al*. (2010) found through surveys that factors such as 'gender', 'age', and 'years of experience on the internet' produce significant differences in relation to 'privacy concerns' on the internet. For example: females, respondents with less than 10 years of internet experience, and respondents aged 41 and above, all demonstrate a higher level of concern with internet privacy, a demographic which Margaret fits into while Mohammed fits into the opposite demographic. Although Margaret presents as being concerned about giving over personal information on the internet, it is not so much due to distrust in internet security technology than it is a lack in self-confidence in using this technology appropriately, which may subsequently make her vulnerable to cybercrime. This lack of self-confidence is therefore likely to be related to, what has been identified in a variety of literature, as aspects and combinations of: 'computer anxiety' (Cambre & Cook 1985), 'technology anxiety' (Meuter *et al*. 2003), 'perceived ease of use' (Venkatesh 2000), 'computer confidence' (Levine & Donitsa-Schmidt 1998), 'computer self-efficacy' (Bandura 1997) and so on, all of which are likely influence trust related phenomena of internet shopping. Hence for Mohammed a form of routine trust is portrayed as being enacted, he knows what to look for through experience to develop a trust position. Yet for Margaret the internet is an unfamiliar terrain, but Margaret opens up to the idea of developing trust in this system perhaps because as Luhmann suggests, it is 'normal' to trust in it, as many others do; for example, as Margaret's daughter does.

E-Government Trust

Trust in government forms of surveillance was an area that was often discussed by the participants. A number of issues here were raised. For example, anti-terror forms of surveillance were discussed by Samantha as suspicious:

> Extract 6: Samantha
> S: Erm I think there is erm I think that there is a big drive to prevent crime and to prevent terrorism and I think a lot of the surveillance has to do with terrorism erm but I think that the objective behind it is not necessarily erm an anti-terrorist or a democratic objective and I think that erm once once you have to view that you have a right to people's personal data that gives the government and the state a great deal of power a great deal of power and that power is open to misuse (.) I think erm foreign policy the government's foreign policy and the policy of the United States (.) erm against other countries and against Palestinians and I think that all of these things are are the real issues I don't think you're gonna stop crime by putting people under surveillance

The economic benefits of CCTV (e.g. parking fines) was also an issue that was of concern. For example Eugenie spoke of her concerns that politicians may be benefitting from CCTV contracts:

> Extract 7: Eugenie
> E: some people make money because they keep selling all these cameras and the new systems to government so they make profit from that I don't know who it is it might be Siemens that gives all these cameras to Britain so Siemens might be

> one of the biggest companies ever so maybe politicians who make the deal with that company to install all these cameras might have had some benefit too so for what? To tell lies to the public that now they are safer with all those cameras watching them? I don't believe that.

Among other issues distrust in government databases were frequently discussed (which we refer to here as e-government trust). In the following extract, Terry begins to discuss his dislike in third parties collecting his personal information, particularly without his consent and without information as to what it is to be used for. He then goes on to depict distrust in the government. However, this distrust creates a bit of a dilemma for Terry, on the one hand he wants the government to place further regulations on internet activity, but on the other hand he does not trust the government.

> Extract 8: Terry
> T: Erm, I don't think it's ok to have my data collected unless I have said to people that they can have my data, collected (.) and what what they going to be collecting my data for*?* That is what I would want to know who's collecting it or what are they collecting it for <I: yeah erm, any exceptions to that rule?> I don't think there's any exceptions to that rule I mean I don't care if it's the police I don't care if it's the er you know the Cameron the government whoever I don't want people collecting data on me unless I'm I'm told and what it is going to be used for and who's using it and things like that (.) no I just want controls placed on this sort of thing <I: ok> before it gets outta hand (.) that is what worries me I know there are criminals that use this stuff but the government you know I think if we ask most people do you trust the government that's leading this country I think most people if you asked them honestly they'd say no (.) they don't even trust this government and they'll take this information and use it back against people and Big Brother or whatever things that they're not even supposed to know about people

Some of the problems associated with dataveillance and impersonal trust are well represented in the above extract. As discussed earlier, Luhmann (1979) argues that impersonal trust in abstract systems is often established through processes of normalisation. For Terry, the inverse seems to be enacted. He portrays *distrust* in the government as a normative position by stating that "most people . . . don't even trust this government". In the UK, the government's fallibility in relation to the security of personal information has become so widely reported that it is now unusual to state that one has trust in this area of government responsibility. Terry's distrust is also portrayed as difficult to overcome. Firstly, he alludes to the lack of access points through which he can determine what his personal information may be used for; and secondly he alludes to the lack of instituted controls and safeguards "placed on this sort of thing". Thus the government's dataveillance systems remain abstract with no apparent means of them being reembedded. Indeed the one way gaze remains hidden; a gaze which he can only assume sometimes passes his way, which in turn fuels suspicions, distrust and conspiratorial thoughts. He relates the government to "Big Brother", a government to be feared, thus, people may not be 'honest' when asked if they trusted the government through fear of retribution. Additionally this "Big Brother" type government is represented by Terry as invading people's privacy and obtaining information on people "that they're not even supposed to know".

Interestingly, Terry is not only concerned about the personal information that is held on government related data-bases, he is also concerned about the government using personal information that is uploaded onto the internet by anybody. He immediately qualifies this statement in the following way.

> Extract 9: Terry
> T: like for instance right now I can put I can put things on Google about you for instance, is that fair? Is it fair for me to be able to take your name and put things on Google about you and you can't take those things off of Google and unless you come to me and say take those things off I can turn around and say no (.) Is that fair? That's not fair is it? <I: no, no> and it doesn't seem as if anything can be done about that

Terry implies that if citizens' internet usage is not regulated, the result would be increased distrust between citizens. It is generally an argument against libertarian positions that argue for lowered government regulation. The flow between impersonal trust and (social) interpersonal trust appear fluid here. Terry implies that he trusts neither, in this context, the government nor citizens. The ability to publish details of somebody's personal information is now not only activities employed by experts such as academics and journalists, indeed virtually anyone with access to the internet can do this. Although this is not uploaded directly up onto the Google website, as implied by Terry, he seems to be intimating that once information is uploaded onto the internet, one only need to Google a name (input a name onto the Google search engine) in order to retrieve any information that is written about that name that is publically accessible. This information then is easily obtained through government surveillance systems, seems to be Terry's line of argument: the information may then in turn be used against a person.

Terry's distrust of the government's motivation and ability to regulate the internet is quite hot topic presently, particularly in relation to the kind of cyber defamation that Terry seems to be referring to. The UK 1996 Defamation Act theoretically empowers victims of cyber defamation to take legal action against suspected perpetrators. However, this is an emerging area of law which is growing in complexity (Edwards & Waelde, 1997), partly due to the fact that cyber defamation is becoming an ever increasing problem. Due to the relatively recent development of Web 2.0 technologies such as Facebook, it is arguable that free speech has never been so abundant. Kariniel states,

> The idea of free speech has ceased being an abstract ideal, a general aspiration or rhetoric shared by philosophers and judges, and has been transformed into a complex, sometimes merciless, daily reality on the internet. (Karniel, 2008)

Historically, defamation proceedings were the domain of the wealthy who could afford to bring such actions to a court of law. However, Davies and Lee (2008) make the point that there is the willingness now of some law firms to act in internet defamation cases under conditional fee agreements. The public awareness of such laws and legal resources is likely to be extremely limited. For example, they state that there is anecdotal evidence which suggests that law students on degree programmes tend to study internet defamation law at an early stage and find it,

> a sobering experience when they come to realise that they may be the unwitting perpetrators of tort, with the potential of having imposed upon them an order for damages and legal costs. (Davies & Lee, 2008, p. 276)

So, although everyday users of the internet, such as Terry, may be unaware of such laws, Terry appears to have a sense that presently this area is a growing problem that has yet to be appropriately addressed. Trust, and indeed we could also add 'distrust', is often conceptualised as "a type of tacit knowledge we use to reduce the complexity of situations" (Luhmann 1979: 4). Thus the suspension vacuum that is filled with distrust here, works to simplify and reduce the need to understand the complex laws relating to internet defamation. Perceptions, or what Luhmann refers to as 'tacit knowledge', are likely to be fuelled by the popular media which tends to report on high profile cases of the wealthy and famous taking out proceedings. Research by the Legal Services Research Centre suggests that nothing is done in one in five civil law problems and a third of these cases are due to inaction as people do not understand their legal rights (Pleasence *et al*. 2006). However, it is conceivable that even when a thorough understanding of internet defamation laws are acquired, one is likely to take on a distrusting position in relation to the government's ability to regulate it, as law in this area is still developing, conviction rates are relatively few and although, as mentioned, there are some conditional fee arrangements, Davies and Lee state that "the current legal investigation of internet defamation claims can be extremely costly and time consuming" (2008: 278). Indeed Giddens (1990) notes that to maintain the trust a citizen has in an abstract system, it is often important that the citizen does not have expert knowledge of the system as this will enlighten him or her to its fallibility (86-87). In this case however, the knowledge gap (suspension) does not work to increase impersonal trust, but perhaps increases imaginations of tyranny.

CCTV trust

Surveys and polls tend to suggest that there is widespread support for the implementation of CCTV cameras, even though the evidence of their efficacy is far from clear. About a third of the participants in this study explicitly stated or implied their distrust in CCTV for a range of reasons.

> Extract 10: Julie
> J: I think it's a way of raising revenue <I: mm> you know I honestly think (.) I'm under that impression that if I fell victim of crime out in the street there right now I would be very unlikely to benefit from the cameras and catch the criminal (.) park a car on a double yellow line I'll immediately get a ticket through the post (.) so I think the streets in this city are being watched to raise revenue

Julie in the above extract presents her distrust in CCTV in two senses. Firstly in relation to CCTV being used by governing bodies (not explicitly mentioned) as a source of income and secondly, distrust in its ability to prevent crime. About a quarter of the participants who spoke about this issue either stated explicitly that they trusted it or implied their trust in it through such comments as 'CCTV makes me feel safer'. A typical refrain can be seen from the below extract, relating to a trusting position:

> Extract 11: Sharon

> S: I personally think they're a good idea because at the end of the day if you're not doing nothing wrong you've got nothing to worry about <I: ok> they are there I believe for people's safety and security

The refrain 'if you're doing nothing wrong then you have got nothing to hide' is a well-worn argument for pro-surveillance positions. However quite often when the participants were probed further, concerns in relation to CCTV and privacy are raised. For example, later in the interview Sharon states the following:

> Extract 12: Sharon
> S: I think in residential areas like around here <I: m-hm> for example erm I think they invade people's privacy <I: m-hm> erm (.) but in shopping areas I think they're fine

Indeed, many of the participants represented complex, ambivalent and ambiguous trust related positions towards CCTV cameras. In the below extract, Roger begins his discussion about CCTV by stating that "they are very very helpful"; however, as the interview continues, as we later see, there is a positional shift which then verges on distrust.

> Extract 13: Roger
> R: erm , CCTV for instance <I: mmhm> erm I think it's a good thing, you know, just you knowing that you're being monitored, kind of make you conscious of what you do, you know, if you plan to be a menace in a public place you probably be just, that one little thing like ok I might be maybe someone's watching me, maybe I shouldn't act the way I'm about to and <I: so that's a good thing?> it's a good thing I mean we live in a society where things happen and and when things really bad happen you need to be able to trace it back to be able to find the right person who committed say crime for instance <I: ok> so for those reasons surveillance are very very helpful

Roger starts by making two optimistic claims in relation to CCTV surveillance. Firstly, he states that CCTV cameras have the potential to regulate public behaviour positively. This works, for Roger, by people recognising that they are being monitored and so are likely to think twice, in Rogers words "maybe I shouldn't act the way I am about to", before being "a menace in a public place". His second optimistic claim is that CCTV footage can be used retrospectively to catch criminals. He states that "when things really bad happen you need to trace it back to be able to find the right person who committed say crime for instance" which he states CCTV can be "very, very helpful" for.

CCTV systems are complex and widespread; for example, operated by private individuals, commercial corporations and local and central government, access points thus maybe thought of as multiple and yet are more often, ironically, inaccessible (for example we are unlikely to encounter a CCTV operator). Instead the distribution of information about CCTV is most likely to come through the media. In the UK context, a public attitudes survey in 2005 attempted to investigate perceptions of CCTV in areas that it was at the time being implemented. 82% of respondents stated that they were 'happy' with the installation of CCTV and only 17% agreed that it would be an invasion of privacy. The study suggests that it is likely that the public awareness and acceptance

of CCTV is due to both its increasing familiarity across towns and cities and a perceived success rate in identifying some offenders, such as the highly publicised James Bulger case and the Brixton nail bomber (Spriggs *et al*. 2005). However, there have been many criticisms of the efficacy of CCTV (see Webster 2009). A report by Big Brother Watch in 2009 stated: it has no demonstrable equivalent success in reducing crime, cameras are regularly turned off and footage is deleted before it can be used, pictures are often of insufficient quality for court purposes, it serves as a placebo to appease neighbourhoods, it has implications for personal privacy and data security, funds are diverted from conventional policing budgets and so it has a considerable negative impact on the public purse. Despite these reports, discourses and consequent perceptions, such as Rogers, in relation to its role in regulating anti-social behaviour and retrospectively facilitating solving "the really bad" crimes, are likely to be prominent as it is argued the misconceptions or 'myth' of its power tends to continue (Webster 2009). The rather more complex picture of its fallibility is not so prominent a discourse, as the various polls suggest. The suspension of uncertainty is widely held here and in its place a misplaced impersonal trust patches over the complexity to act as a form of placebo, which placates the public.

However, unlike opinion polling research, qualitative interviewing allows for further consideration by the respondents of their trust in CCTV. Thus as suggested above, many of our participants went on to portray ambivalent and fluctuating positions. For example, Roger then went on to state,

> Extract 14: Roger
> R: but the downside is (2) nobody really knows what happens with the data that they record all those things that they get like all those videos, nobody really knows what happens to them and how long do they keep them is there a law that abides them to how long they're supposed to keep those peoples' er data they store, through the CCTV?

The placebo thus wears thin throughout the course of the interview and Roger begins to depict some of the underlying complexity behind CCTV phenomena which is centred on issues of distribution and retention. Roger generalises his distrust by making the claim that "nobody really knows what happens to the data", which portrays this lack of information as common. Of course Roger is probably doing some rhetorical work here to normalise a lack of knowledge concerning the regulatory laws of CCTV, perhaps to reduce his accountability for appearing uninformed. But his question is valid, as the regulatory laws are presently quite arbitrary in the UK wherein organisations can virtually make up their own rules in relation to retention periods and how restricted the access is.[iv] The controls and safeguards in this case, are instituted and driven by what Shapiro (1987) refers to as the "guardians of impersonal trust" (623) (in this case the ICO) which she argues can result in a spiral of mistrust through which the guardians also require guardians *ad infinitum.*

So in this section we see the suspension bridged by impersonal trust begin to be dismantled. The trust that is initially portrayed is shown to be a rather weak position (thin trust) which soon fluctuates when rather more complex issues are raised. Although this is not a simple move to distrust in CCTV, but rather results in a questioning of the ethicalities of its procedures. It is worth noting here that the seeking

of safeguards and controls in the CCTV surveillance context is less likely than in the other two contexts that we have looked at. This is because our engagement with CCTV cameras does not require us to do anything, we are passive recipients of a system that is extremely difficult (if not impossible) to avoid. Whereas internet shopping and being included on a data-base often (although of course not always) requires partial consent and choice, we have very little choice as to whether or not information is recorded and stored on most CCTV systems. Thus, there is simply a fundamental requirement for a large measure of impersonal trust in this sphere in order to be able to function on a day to day basis in London. Alternatively one can adopt positions of impartiality, indifference and apathy.

Discussion

So the point of this study was to investigate how citizens dynamically produce trust related positions in the surveillance context. To facilitate this we employed the concepts of 'access points', 'facework' and 'complexity suspension' in relation to impersonal trust. We developed an analysis by firstly identifying some of the dynamic processes related to impersonal trust. This illustrated the processual and fluid quality of impersonal trust processing and positioning. This is an area of trust research which Luhmann (1979) distinguishes as an important and integral aspect of developing dis/trust positions and Lewicki *et al*. (1998) suggest requires further empirical investigation. Our preliminary analysis suggests that this indeed was evident throughout the data.

Perhaps what we have identified as 'interfacework' in the Internet shopping context will be something which has the potential to facilitate impersonal trust. This led to an illustration of how impersonal trust can be developed through negotiating a variety of trust and distrust related positions. This form of impersonal trust does require some specialist knowledge, something which goes quite against the notion of trust being developed on the basis of 'complexity suspension'. As the website interface becomes ever more important as an access point, functional tools which promote assurance and confidence require continued development to accommodate these processes.

While impersonal trust in e-commerce was something which involved active negotiations between trust positions, impersonal trust in e-government surveillance appeared to have less actively engaging access points and so involved more passive processes. For example, the processes of giving consent to having personal data-collected and stored upon data-bases was an issue which involved some strong feelings. Access points in relation to consent and access to information about what personal information is held and for what purposes, appeared particularly opaque for participants. Additionally concerns about the intentions, integrity and benevolence of the government in relation to the use of personal data, alongside the ability and competence of the government to safeguard the confidentiality of the data are issues which are likely to increase distrust here. The example of ambivalence used in the analysis in relation to e-government trust, concerned the need for the government to regulate defamation on the internet. This exemplified a way in which the dynamics of impersonal trust ambivalence can meet an impasse and affect a spiralling decent of distrust. The suspension of complexity here served the distrust position, as Luhmann (1979) suggests, undesirable outcomes (in relation to the collection of personal information) were viewed as likely. Where there are no apparent access points people

are likely to rely on popular myths and discourses that are circulated via the popular press.

This appears also to be the case in relation to CCTV trust wherein its efficacy has been determined by a number of reports and studies as quite limited, yet it is often reported by the media as being effective (Webster, 2009). Hence public trust in CCTV is internationally recorded as high. However the nature of the semi-structured interview requires individuals to think in some depth about issues, this allowed for alternative positions to emerge. This was certainly the case when thinking about CCTV. A position of what may be considered as rudimentary (thin) seems to occur when the complexity of a phenomenon is suspended. Yet when more complex issues are considered, the primary position is likely to be challenged and so a trust dynamic is produced, which Luhmann suggests is central to the development of a dis/trust position that is effectual. Yet without access points through which forms of facework can occur, the possibilities and opportunities for individuals to enter into trust related negotiations to produce a thick trust are likely to diminish.

Extracts of data were chosen for the analyses that were particularly representative of the dynamics of dis/trust from the data-set which consisted of interviews enquiring into citizens' perceptions, knowledge, opinions and everyday experiences of surveillance. The participants who were interviewed lived in the South East of England (mostly in the London area). In relation to these factors there are two general points that need to be discussed here. Firstly, this article is published in an international journal so what relevance does it have seeing the study took place in a particular part of England? And secondly, this article concerns trust and the interview data was not solely focused on this, does this significantly limit the findings?

Perhaps this is quite a restrictive sample and indeed as a lot of qualitative research, it suffers from its lack of generalisability. However, London is of particular interest in relation to understanding the impacts of surveillance on the dynamics of trust processing as it is known as one of the most highly surveilled populations in the world after certain cities in China and North Korea. London is therefore rather an interesting case to study for Western democracies, as policy makers and governments of cities are likely to look to London to scrutinise the effects increased surveillance has before considering developing measures to increase their own systems. Although this is a relatively small study (only involving 31 participants) we have been able to micro analyse some of the processes involved in producing impersonal trust positions of surveillance systems and specifically draw attention to some of its processual qualities. This is of particular relevance to the surveillance studies literature as there is a dearth of academic empirical analysis and theorisation of trust in this context. The concepts of access points, facework and suspension were particularly useful tools to think through and analyse impersonal trust in this context. The lack of conventional access points of the surveillance system tends to produce lofty suspensions of complexity and explicitly draws attention to some of the limits of impersonal trust in abstract systems and institutions.

This should have wider appeal to trust researchers in other contexts. As suggested, ICT systems are increasingly reducing the need for individuals to develop fact-to-face relations. For example, many people now shop on-line rather than visit a store, bills are

increasingly paid electronically, more and more people are able to work from their home computer, telephone system access points are increasingly becoming automated services, and indeed all manner of information can be obtained from the home on-line without the need, for example, to check with the local doctor. Additionally, in an age of austerity institutions are very likely to turn to e-systems as access points in bids to cut costs on the reliance of relatively expensive human resources. Thus systems and institutions will need to be considerably more creative in developing and maintaining trust with increasingly less forms of traditional access points involving interpersonal interaction. This is well exemplified in our case study of the surveillance in the UK wherein CCTV reduces police officers on the street, e-government reduces civil servant costs and e-commerce replaces high street shopping.

ANDERSON, R., Brown, I., Dowty, T., Inglesant, P., Heath, W., and Sasse, A. (2009). Database state. *Joseph Rowntree Reform Trust Ltd*.

BALL, K., Haggerty, K., and Lyon, D. (2012). *Routledge Handbook of Surveillance Studies.* Routledge: Taylor and Francis

BALL, K., Lyon, D., Murakami-Wood, D., Norris, C., and Raab, C. (2006). Report on the Surveillance Society. In D. Murakami-Wood (Ed.): Wilmslow.

BANDURA, A. (1997). *Self-efficacy: The exercise of control*: Worth Publishers.

BARBER, B. (1983). *The logic and limits of trust.* New Brunswick, N.J.: Rutgers University Press.

BIG BROTHER WATCH. (2009). *4 in 5 people believe freedoms are being eroded in Britain*. Big Brother Watch Press Resease.

CAMBRE, M. A., and Cook, D. L. (1985). Computer anxiety: Definition, measurement, and correlates. *Journal of Educational Computing Research, 1*(1), 37-54.

COLES-KEMP, L., Lai, Y. L., Ford, M., and Hyperion, C. (2010). Privacy on the Internet: Attitudes and Behaviours. *A survey by VOME*.

CRAIG, E. (1998). *Routledge Encyclopedia of Philosophy: Questions to sociobiology* (Vol. 8): Taylor & Francis.

DAVIES, M.R., and Lee, B. A. (2008). The legal implications of student use of social networking sites in the UK and US: current concerns and lessons for the future. *Education and the Law, 20*(3), 259-288.

DAWES, R.M., and Thaler, R.H. (1988). Cooperation. *Journal of Economic Perspectives, 2*, 187-197.

DIBBEN, M.R. (2000). *Exploring interpersonal trust in the entrepreneurial venture*. MacMillan: London.

EDWARDS, L., and Waelde, C. (1997). *Law and the Internet: regulating cyberspace*: Hart Publishing: London.

FRIEDERSDORF, C. (2011). London Is the Surveillance Society's Biggest Test Yet, *The Atlantic*. Retrieved from http://www.theatlantic.com/technology/archive/2011/08/london-is-the-surveillance-societys-biggest-test-yet/243445/

GIDDENS, A. (1990). *The consequences of modernity*. Stanford University Press: Stanford.

GIDDENS, A. (1994). Risk, trust, reflexivity. In: Beck, U., Giddens, A., Lash, S. (eds.). *Relexive Modernization*. Polity Press: Cambridge.

GOFFMAN, E. (1967). *Interaction Rituals*. Garden City: New York.

HARDIN, R. (2004). *Distrust*. Russell Sage Foundation.

HARDIN, R. (2006). *Trust*. Polity Press: Cambridge, Malden.

HARRISON, D., McKnight, D., and Chervany, N. (2001). Trust and distrust definitions: One bite at a time. *Trust in Cyber-societies*, 27-54.
HOUSE OF LORDS. (2009). Selected Committee on the Constitution, *Surveillance: Citizens and the State*, HL Paper 18-1, 2nd Report of Session 2008-2009, Volume I: Report.
KARNIEL, Y. (2008). A new proposal for the definition of defamation in cyberspace. *Communications law, 13*(2), 38-46.
KOSKELA, H. (2000). ' The gaze without eyes': video-surveillance and the changing nature of urban space. *Progress in Human Geography, 24*.
LANE, C. (2000). Introduction: Theories and issues in the study of trust. Chapter in C. Lane & R. Bachmann (eds): *Trust within and between organisations: Conceptual issues and empirical applications*. Oxford University Press: Oxford.
LEHRER, K. (1997). *Self-trust: A study of reason, knowledge, and autonomy*: Wiley Online Library.
LEVI, M. (1998). A state of trust, in M. Levi and V. Braithwaite (eds) Trust and Governance, pp. 77-101. Russell Sage Foundation: New York.
LEVINE, T., and Donitsa-Schmidt, S. (1998). Computer use, confidence, attitudes, and knowledge: A causal analysis. *Computers in Human Behavior, 14*(1), 125-146.
LEWICKI, R.J., McAllister, D.J., and Bies, R.J. (1998). Trust and distrust: New relationships and realities. *The Academy of Management Review, 23*(3), 438-458.
LEWIS, J.D. and Weigert, A. (1985). Trust as a Social Reality. Social Forces, 63, 967-985.
LUHMANN, N. (1979). Trust and power. John Wiley and Sons: London.
MCALLISTER, D. J. (1995). Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal, 38,* 24–59.
MEUTER, M. L., Ostrom, A. L., Bitner, M. J., & Roundtree, R. (2003). The influence of technology anxiety on consumer use and experiences with self-service technologies. *Journal of Business Research, 56*(11), 899-906.
MISZTEL, B.A. (2001). Normality and trust in Goffman's theory of interaction order. *Sociological Theory, 19*(3), 312-324.
MOLLERING, Guido. (2006). *Trust: Reason, routine, reflexivity*. Elseiver: Amsterdam.
GALLUP. (2010). Data protection in the European Union. Citizen's perceptions. Analytical report, Survey conducted by the Gallup Organization Hungary upon the request of Directorate-General Justice, Freedom and Security. Flash-Eurobarometer no. 225. 2008.
PLEASENCE, P., Balmer, N., and Buck, A. (2006). *Causes of action: Civil law and social justice*: The Stationery Office/Tso.
POTTER, J. and Wetherell, M. (1987). Discourse and Social Psychology: Beyond attitudes and behaviour. Sage: London.
PUTNAM, R. (2000). *Bowling alone. The collapse and revival of American community.* New York: Simon and Schuster.
RAAB, C. (2002). Electronic Confidence: Trust Information and Public Administration. In I.Th.M. Snellen & W.B.H.J. van de Donk (Eds.), *Public Administration in an Information Age: A Handbook*. IOS Press: Amsterdam.
SHAPIRO, S. P. (1987). The social control of impersonal trust. *American journal of Sociology*, 623-658.
SINECEUR, M. (2010). Suspending judgment to create value: Suspicion and trust in negotiation. *Journal of Experimental Social Psychology, 46*(3), 543-550.

SPRIGGS, A., Argomaniz, J., Gill, M., and Bryan, J. (2005). *Public Attitudes Towards CCTV: Results from the Pre-intervention Public Attitude Survey Carried Out on Areas Implementing CCTV*: Home Office.

STONEMAN, P. (2008). This Thing Called Trust: Civic society in Britain. Palgrave Macmillan: London.

ULLMANN-MARGALIT, E. (2002). Trust out of Distrust. The Journal of Philosophy, 99(10), 532-548.

ULLMANN-MARGALIT, E. (2004). Trust Distrust and In Between, In R. Hardin, R. (Ed.) *Distrust*. Russell Sage Foundation.

VENKATESH, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information systems research, 11*(4), 342-365.

WEBSTER, C. W. R. (2009). CCTV policy in the UK: Reconsidering the evidence base. *Surveillance & Society, 6*(1), 10-22.

YOUGOV/TELEGRAPH. (2006). Survey Results. Retrieved from http://www.yougov.co.uk/extranets/ygarchives/content/pdf/TEL060101024_3.pdf

ZUCKER, L.G. (1977), The Role of Institutionalization in cultural Persistence. *American Sociological Review.* 42, 726-43.

ZUCKER, L. G. (1986). Production of trust: Institutional sources of economic structure, *Research in organizational behavior,* 1840–1920.

ZUREIK, E., Harling-Stalker, L., Smith, E., Lyon, D., and Chan, Y. (2009). *Privacy, surveillance and the globalization of personal information: international comparisons.* McGill-Queen's University Press: Kingston.

---

[i] They can additionally be used to appease voters' fears and concerns regarding safety.

[ii] In many parts of the world farmers may sell their produce on a table beside a road which are often unmanned. Customers are expected to take the produce desired and pay for it through a cash box with a small slit in it for posting the money which is secured to the table. At a preliminary glance one may conclude that this is a very trusting system (which indeed it is). But on closer inspection we can see how both trust and distrust is built into the system. Primarily the farmer trusts the customers to pay for the produce, but distrust simultaneously facilitates the working of the system through the small slit in the money box which stops people from taking the money out of the box and the screws which affix the box to the table make it difficult for people to make off with the money box. Thus trust and distrust here work to make the system viable.

[iii] However we do point out a note of caution, ambivalence throughout the interviews is perhaps not that surprising given that the participants may not have given such matter this much conscious deliberation in the past, and there may also have been an interviewer effect wherein the participants could have felt some pressure to produce a variety of reflection.

[iv] The regulatory laws of CCTV used in the UK are set out through the *Information Commission Office's* (ICO) 'CCTV Code of Practice', which is written to help guide operators to comply with their legal obligations under the Data Protection Act (DPA). The ICO states that CCTV data needs to be safely stored and access to it must be restricted. Although confidentiality remains a general rule there are exceptions: the apprehension or prosecution of offenders, the prevention and detection of crime; and issues of national security (see sections 28 and 29 of the Data Protection Act 2008). The amount of time that the data is to be stored for is broadly left up to organisation to decide. The ICO recommends that "retention should reflect the organisation's own purposes for recording images" and that they should "not keep images for longer than strictly necessary". In 2007, CameraWatch issued a report which was widely reported in the press, stating that over 90% of CCTV cameras in the UK are in breach of the DPA. The ICO subsequently made a statement in response to the CameraWatch report claiming,

> 'We are not aware of any evidence that supports the suggestion that 90% of CCTVcameras are not complying with the ICO Code of Practice. We don't believe there is any such evidence' (ICO, 2007).

There have, however, been many calls for more regulatory powers of CCTV which the present Conservative Liberal Democratic Government of the UK is purportedly responding to. There is presently a Protection of Freedoms Bill which includes a new code of practice for surveillance camera systems. This bill has been through the House of Commons and waiting to undergo a second reading in the House of Lords.