Beyond 'nothing to hide': When identity is key to privacy threat under surveillance

Avelie Stuart and Mark Levine

Psychology, University of Exeter

Author note:

Avelie Stuart

Psychology, University of Exeter

Washington Singer Laboratories

Perry Road

Exeter UK EX4 4QG

Email: a.stuart@exeter.ac.uk

Phone: +44 (0)1392 4694

This is an author pre-print of a paper accepted for publication in the European Journal of Social Psychology, please do not freely distribute.

This research was supported by the Engineering and Physical Sciences Research Council research grant: EP/K033433/1

The authors declare that there are no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Abstract

Privacy is psychologically important, vital for democracy, and in the era of ubiquitous and mobile surveillance technology, facing increasingly complex threats and challenges. Yet surveillance is often justified under a trope that one has "nothing to hide". We conducted focus groups (*N*=42) on topics of surveillance and privacy, and using discursive analysis, identify the ideological assumptions and the positions that people adopt to make sense of their participation in a surveillance society. We find a premise that surveillance is increasingly inescapable, but this was only objected to when people reported feeling misrepresented, or where they had an inability to withhold aspects of identities. The (in)visibility of the surveillance technology also complicated how surveillance is constructed. Those interested in engaging the public in debates about surveillance may be better served by highlighting the identity consequences of surveillance, rather than constructing surveillance as a generalised privacy threat.

Keywords: surveillance; privacy; resistance; identity; impression management

Beyond 'nothing to hide': When identity is key to privacy threat under surveillance

Privacy has moved to the centre of the political and social agenda. Just a few of the recent developments include the revelations of whistle-blower Edward Snowden (Greenwald, 2013), increasingly sophisticated algorithmic face, emotion and age detection software (e.g. Farfade, Saberian, & Li, 2015; Jeni et al., 2012; Microsoft, 2015), and controversy over social media and dating websites covertly experimenting on their customers (Kramer, Guillory, & Hancock, 2014; Rudder, 2014). There has been considerable debate and research from the social and technology sciences about such developments, yet we have heard little from social psychologists. Margulis (2003) argued that this is a persistent problem with privacy and psychology – it is often acknowledged as an important social and political issue, but not as particularly important for the development of psychological theory. Moreover social psychologists have been slower to pay attention to social media and mobile technologies despite them being a key site in which to study classic social psychological questions (Kende, Ujhelyi, Joinson, & Greitemeyer, 2015) – such as privacy. In this paper we revisit how people construct privacy, when privacy threat becomes salient in discourse about surveillance, and make contributions to how the theorisation of the social psychology of privacy can be pursued in socially networked and surveilled societies. Using discourse analysis we identify when surveillance is constructed as privacy threatening, in a context where the presence of surveillance is often assumed. We identify an assumption that surveillance is always present but has no self-consequences, however when an overreach of existing power relationships is identified (e.g. students and their university administration), or when surveillance is said to be narrowing in on individuals' specifically, this position becomes unsettled, particularly if it involves misrepresentation of identity.

Privacy in Socially Networked Societies

Privacy is psychologically important because it allows people to maintain feelings of self-control, of relaxing away from others, and of personal autonomy (Goffman, 1961; Margulis, 2003; Schwartz, 1968; Solove, 2002). Privacy is also about the freedom to share with whom we want and

to maintain chosen boundaries around who we share with (Altman, Vinsel, & Brown, 1981; Livingstone, 2006; Petronio & Reierson, 2009). Thus privacy research should consider practices of both sharing and withholding, and how they are situated in interpersonal practices (Antaki, Barnes, & Leudar, 2005).

Much of the work employing a conceptualisation of privacy as situated in interpersonal practice draws on Goffman's work on impression management. In *The Presentation of Self in Everyday Life* (1959) Goffman argues that by acting in a certain way, we make claims to be a particular kind of person and expect others to treat us in that way. At the same time we can have difficulty in up-keeping such performances when our audience changes, or in the presence of different audiences. We attempt to be authentic in these self-presentations, but this is complicated by the multiple social roles that we possess. Similarly in self-categorization theory is the notion that people find it important to maintain identity multiplicity and compartmentalisation (Roccas & Brewer, 2002; Turner, Hogg, Oakes, Reicher, & Wetherell, 1987). The complexity of managing separate identities, and upholding the associated norms, is anxiety provoking (Barreto & Ellemers, 2003; Hirsh & Kang, in press). Developments in technology are the primary way in which new possible identities are created (Gergen, 1991). In social media and mobile technology, people use online spaces to carve out their identities, to test out ways of expressing themselves, and of connecting to others (McMahon & Aiken, 2014). For example, Marwick and boyd (2011)'s study of Twitter users illustrates how people attempt to convey themselves in a certain light to their audiences, but also try to maintain authenticity in their self-expression.

Privacy has been theorised as relating to impression management in the moments when people fail to manage or correctly imagine their audiences, resulting in revealing aspects of themselves to an unintended audience (Acquisti & Gross, 2006; Tufekci, 2008). For instance, being labelled as a member of a particular social category could produce privacy concern if people are in a context where they feel that categorization is not relevant, or if the identity is stigmatised (see Ellemers & Barreto, 2006). Consistent with this, Nissenbaum (2004) conceptualises privacy as

contextual integrity – explaining that the "normative roots of uneasiness over public surveillance" (p. 102) rest on notions that there are places (or spaces or domains) that are personal to the individual (e.g. their home). Despite the complexity and contested nature of these domains, people operate under shared assumptions that everything that happens, happens within contexts that have conventions and cultural expectations about appropriateness and where information should flow. When those expectations are violated – through "context collapse" – privacy can be socially understood to have been violated also (boyd, 2012; Davis & Jurgenson, 2014). Norms of appropriateness (of sharing information) are then governed by the relationships between the people exchanging information in a given context (Nissenbaum, 2011; see also Petronio, 2002).

It is the difficulties in impression management and maintaining contextual integrity that often underpin so-called failures to maintain privacy. Yet a lack of understanding of what motivates people's sharing behaviour online has led to a widespread perception that people posting personal information, or actively participating in technologies that facilitate their own surveillance, are incapable of managing their privacy, or do not care about their privacy. This problem has been labelled the "privacy paradox" – a contradictory finding where people report being concerned about their privacy but (appear to) do little to protect their privacy (e.g. Cranor, Reagle, & Ackerman, 2000; Norberg & Horne, 2007; Smith, Dinev, & Xu, 2011). Such behavioural inconsistency lends favour to the rhetorical justification of privacy "invasions" on the basis of service exchange arguments. For example, Facebook justifies experimenting on people as one of the conditions that they consent to upon signing up for their service (Kramer et al., 2014), despite criticism that such experiments are unethical (e.g. Chambers, 2014). Privacy advocates and academics have been keen to promote an alternative story, which claims that people do care about their privacy and that the inconsistencies arise from measurement problems (e.g. Dienlin & Trepte, 2015), and misunderstanding impression management strategies (boyd & Marwick, 2011), social exchange negotiations (Tufekci, 2008), or situational factors (Ellis, Harper, & Tucker, 2013b; Joinson, Reips, Buchanan, & Paine Scholfield, 2010).

In this paper we explore accounts of privacy in the context of surveillance. We consider how concepts of impression management and context collapse are relevant in accounts of privacy under surveillance. Are similar privacy preserving strategies as described in social media contexts also discussed in the context of surveillance? Literature on surveillance resistance has typically examined top-down hierarchical surveillance relations (Martin, van Brakel, & Bernhard, 2009). However, what has received less attention is the more 'everyday' practices – that is, the threat posed by surveillance to people's ability to manage impressions of them, and to maintain contextual integrity.

When is Privacy Threatened by Surveillance?

Surveillance studies have extensively drawn on Foucault's invocation of Bentham's panopticon - where self-discipline is produced in reaction to feeling as if one is under surveillance (Foucault, 1977). This self-discipline replaces the need for authoritative power; power is encoded through us rather than upon us (Foucault, 1977; Spears & Lea, 1994). Thus most of the surveillance resistance literature has examined hierarchical power relations and how people comply even if they are unsure if they are being watched (Martin et al., 2009). Yet others argue that the panopticon metaphor has been overextended (Haggerty, 2011; Haggerty & Ericson, 2000).

In this paper we are not concerned with debates about surveillance and self-discipline. Instead we focus on a surveillance culture where people know they are under surveillance even though they cannot (for the most part) see the surveillance technology. More specifically, we explore surveillance conditions where people know they are under surveillance but say it has no impact on them – that they have 'nothing to hide'. The reason for our interest in the explicit articulation of privacy is because work on surveillance (e.g. CCTV) has noted that people are now so accustomed to being under surveillance that they do not necessarily engage with it. The lack of noticing is in part due to the technological design; many technologies are designed to fit seamlessly into our environment (Hjelm, 2005), and online surveillance is largely imperceptible (Acquisti, Brandimarte, & Loewenstein, 2015; Tucker, Ellis, & Harper, 2012). Ellis et al (2013a) propose that

surveillance promotes “affective atmospheres” – an unsettled feeling of being watched but one that is difficult to engage with or articulate.

Following from this, one avenue taken in surveillance resistance work is to find the conditions under which surveillance changes from being unnoticeable to noticeable – such as by probing people’s beliefs about situational normality (McKnight & Chervany, 2001). An example is that you might think it is normal have CCTV in a public place, but it is abnormal in your private residence. Thus when surveillance appears in places that people do not expect it, they might notice it. The presence of surveillance alone may not be a problem, however. It is important to consider the consequences of being seen (Levine, 2000). For the (implied) surveillance to have an effect there must be some punishable behaviour – laws or social norms to which one must abide. The problem is that one of the most prevailing public discourses on surveillance - the “nothing to hide” argument (Solove, 2007) – posits that if an individual is doing nothing wrong then they have no reason to worry. Subsequently, one suggestion for raising awareness about surveillance made by Solove (2007) is to make people aware of their current privacy practices – like asking the simple question, does your house have curtains? The realisation that one does indeed have curtains might cause them to reassess their need for privacy even if they are doing nothing wrong.

Despite these efforts, however, the nothing to hide argument has shown to be persistent and appears to invalidate attempts to warn people of panopticon or “Big Brother” futures. It is concerning because it represents a false trade-off between security and privacy which blankets over the damaging consequences of collective surveillance (Solove, 2007), and this is at least in part because some consequences are intangible - we do not know who can see us and what is done with our information (Acquisti et al., 2015).

Another potential way in which to increase surveillance awareness, one that we explore in this research, is based on the finding that surveillance becomes unsettling to people when it links to their identity (Tucker et al., 2012). This process was amusingly illustrated in John Oliver’s TV show *Last Week Tonight* (2015) when he ‘surveyed’ people on the streets and found them disinterested in

government surveillance, until they were told that the government had access to pictures of their genitals – making the self-relevance and consequences of surveillance apparent. The capacity of digital technologies not only to capture but also to reveal intimate aspects of self can be constructed as a plausible threat to our personal identity. However, it is not only personal identity threat that can affect surveillance awareness. For example, social psychology research indicates that people accept the presence of surveillance when they see it as being for their (shared) benefit – linking social identity and group processes to the acceptance of surveillance (O'Donnell, Jetten, & Ryan, 2010a, 2010b; Subašić, Reynolds, Turner, Veenstra, & Haslam, 2011). The surveillance becomes less acceptable, more intrusive and subject to micro-resistance, when it compromises a shared vision of the social group. For example, when workers feel they should be trusted in a particular work context, but are nevertheless subject to surveillance by management, then the presence of surveillance becomes a live concern.

It seems therefore that in order to understand people's response to surveillance we need to examine how the technology interjects itself into everyday social relations, and opens up or restricts people's opportunities for identity construction, impression management, and selective withholding. Based on this promising line of work on surveillance and identity, in this study we examine further how and when, in talk about surveillance, privacy threats relating to identity become salient.

The Current Study

According to the literature on social media and impression management, privacy does matter to people, but to capture this requires an awareness of the context in which information is created and shared, and the consequences for revealing or withholding. Privacy is a fluid regulatory process (Altman, 1974; Altman et al., 1981), and the values and expectations of privacy are being actively constructed and negotiated as new technologies open up new forms of social relations and identity construction opportunities. It is within the context of social network (and surveillance-capable) technologies that we aim to understand how people construct their privacy when under surveillance.

A discursive approach seemed particularly well suited to our research topic. It is through language that ideological assumptions are made explicit, and the positions that people can adopt within existing power relations emerge (Edley & Wetherell, 2001). We do not treat participants talk as an accurate (or inaccurate) reflection of their behaviour online; this is not a survey of people's opinions or a report of their experiences, but an analysis of the discursive resources that are used to acquire a position in resistance or acceptance of surveillance.

In particular, we analyse where people reported noticing (or even objecting to) the presence of surveillance in their lives with the aim of uncovering what could underpin the unsettling of the notion that they have "nothing to hide". The participants in this research are young adult university students, who all report actively engaging in social network sites and other mobile technology. Their constructions of surveillance demonstrate their investment in their ongoing participation in these technologies, and the expectation that they are already under some surveillance. Indeed, the 'flavour' of these discussions is dismissal of surveillance as being a significant concern. However, we analyse the points where this dismissiveness no longer worked, and why – this is where we connect to the prior literature on impression management, contextual integrity, the debate around whether the literal presence of surveillance is sufficient enough to cause people to be concerned about their privacy, and more general concepts of privacy and identity, where relevant. We also examine where privacy is made explicit (or implicit) within talk about surveillance, and whether privacy is constructed as immutable or exchangeable.

We chose focus groups rather than interviews because in focus groups people engage in collective sense-making (Wilkinson, 1999). We believe it is well suited to discussions of privacy because it can be considered both an (elusive) individual need but also an important social value that requires collective regulation (see Goffman, 1972, on privacy in public spaces). Talk in a focus group is interactive and constitutive of the subject being discussed, meaning that people within the group can question each other and this can lead to further unpacking of assumptions and the elucidation of alternative formulations.

Our discussions of surveillance technologies move between government or corporate surveillance of social network sites (SNSs), tracking people with mobile location tools, and the use of wearable technologies (specifically Google Glass). Although these different technologies have different uses and consequences, we do at times blur them together here because they work together as a surveillant assemblage (Haggerty & Ericson, 2000).

Method

Participants

Forty-two participants (26 female) attended 7 focus groups (of between 4-10 people) which all ran for approximately 1 hour. Ages ranged from 18-46 (M=21.2, SD=6.18, 7 missing). All were students recruited from a British University, and the majority of participants were British (n=23), with others including other European (5), Chinese (4), other Asian (2), and Russian (1) nationalities. All participants reported having a Facebook account.

Procedure

Participants were all presented with an information and consent form before audio recording commenced. They were informed that all identifying information would be kept out of transcripts, and that only the authors would have access to the audio recordings. The first author facilitated the focus groups. The questions followed a semi-structured format covering a range of topics including inquiry about what different apps and social network sites they use, rules or norms of privacy and sharing amongst their friends, whether they think about who can see or access information they upload (such as photographs) and whether different types of data are more private than others. They were asked for anecdotes of situations where they or someone they know had had their privacy breached, and what they did to rectify privacy in that situation. In the final set of questions a couple of scenarios were explained to participants: one about a high school in the USA that had hired a firm to monitor students' public social media posts, and another scenario about

their university introducing location-tracking tools to monitor student's movements while they are on campus. They were asked how they felt about these scenarios.

Analytic Method

The style of discourse analysis adopted here is informed by the work of Wetherell and colleagues (Edley & Wetherell, 2001; Wetherell, 1998, 2007), described as a combination of ethnomethodology and conversation analytic techniques, informed by the work of Foucault and post-structuralism. In simpler terms, this involves analysing the local organisation of talk within an interaction and identifying patterns in talk that indicate where participants are drawing on shared discursive resources that reveal normative assumptions and indications of power relations (Edley & Wetherell, 2001). We analyse the functionality of rhetoric and how it is formulated within the focus group interaction, and the trajectories of these rhetorical formulations within conversations, as per the discursive psychology method (Edwards & Potter, 1992). Then we identify assumptions that are made about surveillance technology, when privacy is identified as being threatened by surveillance, and how such threats appear, or when they are dismissed as unimportant. This involves identifying the ways that participants investment in their identities (e.g. as students or consumers of media) informs their constructions of surveillance and privacy.

The transcripts were transcribed verbatim and coded with descriptive codes, but it was not our intent to report on the most commonly occurring themes or categorise the data. In some of the extracts we have removed parts of conversations that were not relevant to the main point, for brevity (indicated by a … between lines). We denote extracts by their session number and beginning line number from the transcript.

Previous research has noted that it is difficult to determine whether people's behaviour or talk is caused by privacy threats, as privacy behaviours are often covert, subtle, or encoded (boyd, 2012; boyd & Marwick, 2011; Ellis et al., 2013a; Marx, 2003). Our discursive approach helps to identify when privacy is articulated or implicit. We follow the lead of Ellis, Tucker and Harper (2013a), who found that individuals do not fully articulate their discomfort with surveillance, but

rather they hesitate or there can be disruption or disfluency in their speech. One can also look for instances when privacy discourses shift within a conversation.

Analysis

The first point we make is that these participants often assume the presence of surveillance in their everyday lives. Under this assumption, different discursive and identity resources are employed to shape and often justify their ongoing participation in, or acceptance of, surveillance-capable technologies. There are instances where participants raise objections to surveillance – we illustrate when these discourses connect to either the (in)visibility of surveillance technology, and normative assumptions that they should be allowed to choose how they (or what aspects of themselves) are seen. Lastly, we will show that one way of absolving the concern about being seen by surveillance is to argue that one can manage their privacy by separating aspects of their lives, or their digital and physical self.

The Assumed Ubiquity of Surveillance

We start the analysis by illustrating a pervasive notion, conveyed in these focus groups, that surveillance technology is becoming increasingly ubiquitous in their society and that therefore one can assume that they are always under some surveillance (what we are calling the "assumed ubiquity of surveillance"). What is striking about this assumption is that rather than it being characterised by an increasing fear of surveillance (as one might expect), it more often led to the formulation of justifications for further surveillance.

In the following conversation the participants were discussing whether their university needs to gain consent to use location-tracking tools on its students. While some of them expressed objections to the proposal, the 'counterpoint' that one person raises is that they are always being "spied on".

M1 yeah just the idea of monitoring people it- it sounds- it's a bit like irritating, not because you- I- I think it's it's it is a bit-
F1 sounds like you're being spied on
M1 exactly. Yeah

F2 but I guess that's how- we- we are always being spied on technically, with security cameras we just don't- it's because (unclear) really affect us we don't think about it
Mmm
F2 say if it was maybe if I didn't know about it I wouldn't, I don't- like if I wouldn't be bothered but if I found out maybe I'd be like
F3 oh yeah
(Session 2, line 521)

There is an assumption in this conversation that they already live in a surveillance society – or rather, this is used by F2 to argue against M1 and F1s initial objections. F2 uses the ubiquity of surveillance argument as a way of dismissing further surveillance as a threat. The "technically" part that follows this statement is telling: the technicality of being spied on by security cameras is legitimised because it ostensibly does not affect them. F2 furnishes her argument with what resembles an "ignorance is bliss" argument – surveillance goes on without her knowledge and she is not bothered by it.

This extract shows the definition of privacy being negotiated amongst the participants in relation to whether the (technical) ubiquity of surveillance is problematic or not. M1 says that the idea of monitoring is a "bit irritating". This is notably not a strong objection (the articulation of privacy threat is rarely overt or a thoroughly argued position, Ellis et al., 2013a), until F1 interrupts by labelling it as spying. M1 and F1 define the presence of surveillance as a privacy invasion, but for F2 the (lack of) consequences are more pertinent. We see based on F2's response, that objections to surveillance can be discounted on the basis of the current level of surveillance that we are "always" under. F2's contribution to the discussion also serves to turn the conversation away from a question of whether the surveillance should exist, to instead discuss whether they are aware of any intrusion on their lives or not.

This type of justification occurred in several other discussions as well. One group said that if the "University wanted to improve the services, and everyone was doing it [location-tracking]. You might not mind too much"; because the university is constituted as a "credible institution" (session 4, 706). That is, the notion that "everyone" is conducting or participating in surveillance is used as an argument for surveillance (by way of being 'normal'). In another example a similar argument is used

to justify further surveillance by using a security-privacy trade-off argument (Solove, 2011). They were discussing whether someone needs to police online content that violates other people's privacy – such as videos that film down women's shirts. When one person objected that social networks are supposed to be free from policing, a participant replied that, "there's always gonna be a monitor, I'm sure there's someone who monitors Twitter or someone else who monitors- people monitor YouTube or Snapchat with the 2-second videos there's gotta be someone behind working the…working all the cogs and stuff" (session 1, 709). This discursive assumption that they are always being watched or monitored – which does not indicate unequivocal support of surveillance – does appear to lead the discussions away from finalising or producing a clear position of resistance to surveillance, and sets up a basis upon which people can argue that more surveillance is needed.

Surveillance as Excessive

The clearest example of when the focus group discussants rejected surveillance was when the surveillance could be situated as pointless, excessive, or futile in relation to its proposed purpose. Highlighting the disproportional excessiveness of surveillance might seem like a good avenue for setting up the expectation that surveillance technology needs to prove necessary or provide additional value in order to be socially acceptable. However, this discourse also led to a rhetorical trajectory that, while (or perhaps *because*) it is excessive, it is also harmless. We demonstrate two ways in which this played out in talk. In the first example, the proposed use of location tracking to monitor students' use of campus facilities was described as unnecessary because there could be other ways of obtaining that data (i.e. from their timetables). Yet, at the same time, it was described as inconsequential.

> F If they wanted to know where I was at twelve o'clock on Wednesday they can just look at my timetable and see if I have got a lecture. I don't live that much of an exciting life where between lectures I am going to the Physics Building to snort cocaine off the back of the toilets. My life isn't that exciting.
> M It doesn't matter when you are on campus because you are just walking about doing like normal things, there is no like consequence of them knowing where you are really, I think.
> *(Session 6, 425)*

The participants in this extract are illustrating a 'nothing to hide' argument, which is furnished with a somewhat humorous extreme case formulation (Pomerantz, 1986) where she says she is not snorting cocaine in the Physics building. As students, they attend to knowledge that their relationship with the university is characterised by many of their activities being monitored, and they do not identify any behaviour the university could observe them doing that would be outside of the university's remit, and reflects this normalizing effect of the assumed ubiquity of surveillance. Thus, in this case location tracking is constructed as unnecessary and potentially escapable, but also inconsequential.

The following extract illustrates how location-tracking could be constructed from a similar starting point – the university can already know where she is, and therefore location tracking is constructed as unnecessary.

> F but I think something like that they could just ask us I mean it's not one of those things that's really hard to find out- literally that they could just email me and I'll just tell them what sort of times I'll be around
> F whereas I don't think they need to follow me or whatever

Again she does not dispute the notion that such information should be accessible in the first place, but rather that the university does not 'need' to follow her to gain access. It is a form of resistance to surveillance, based on the identification of alternative forms of data collection. However, continuing on in this discussion, the same participant later talks about Google tailoring its advertisements to users based on the key words scanned from their emails. Here, the rejection of surveillance on the same grounds (i.e. that it is not needed) is no longer tenable.

> F [Google] scanning key words, maybe if it was the subject line that would have been ok but it's really weird and I don't like them doing that but that's not the issue
> **But you still use it anyway?**
> F mhmm- it's Google
> [laughs]
> F I don't- I do probably do that with everything. Yes. I sort of said that I don't wanna do the big adverts and I sort of tried to do as much as I could to stop them recording but that means they sort of just guess using my emails, I don't think there's any way that I can stop them looking at my emails 'cause I suppose really I am using their servers and everything and I am using their services so I guess they get to read my stuff. That seems payment *(Session1, 928)*

Thus, like Ellis et al (2013a) we note that participant's discussions of surveillance technology shift as their reference points in conversation shift. In this latter extract she also raises an objection to surveillance, but when the moderator asks her why she continues to use Google, she defends her participation by arguing that she has done all that she can, but she cannot stop them (unlike in the previous university location tracking scenario). The simple statement "it's Google" shows assumedly shared knowledge that Google is not optional. She then rationalises her ongoing use of Google by falling back on the social contractual exchange or bargaining argument between service and user (Pallitto, 2013). Thus, she alters her constitution of privacy - it can be exchanged as a form of payment. This discourse also serves the role of creating a position of trust in the surveiller. Other research has shown that trust can be compensatory in times of risk (Joinson et al., 2010). Thus as an invested consumer of internet technology, the inescapable and assumed ubiquity of surveillance rhetorically leads to two conclusions: to trust surveillers and to allow privacy to be exchanged for a service.

The Threat of Future Surveillance Technology

In the following example we demonstrate how more subtle privacy discourse can become more explicit when talking about new technology – in particular here, the wearable Google Glass.

> M1 I think the fact that would be so easy to, people wouldn't be able to tell you were taking photos, that could be quite bad in quite a few situations but it's quite easy to take photos with like Smartphones and things without most people realising so it's a step on, it's harder to tell with Google Glass but it's not a massive step forward like a lot of people seem to be saying it is.
> F1 Especially if you have to actually say like 'take a picture' it's kind of slightly obvious [laughter].
> **Yeah but I mean if there was just like a little tap or.**
> F1 Like it looks a lot more stupid wearing Google Glass.
> M1 It just looks creepy.
> F1 It looks weird.
> *(Session 5, 394)*

In this conversation we see that participants are discussing whether surveillance-capable technology is a threat based on its perceptibility or visibility - in this case not being able to see if someone is taking your picture is implied to be the reason for concern (unlike in previous 'ignorance

is bliss' arguments). But M1 then discounts a normative argument that Google Glass is a "massive" step forward ("like a lot of people seem to be saying it is"). F1's continuance of the conversation indicates a shared assumption that the "obviousness" of Google Glass is what allows it to be dismissed as a privacy threat (and is often argued to be the reason it will not be a successful product, e.g. Fitzpatrick, 2014). Moreover, the subsequent alternating descriptions of Google Glass as "stupid", "creepy", and "weird" are examples of a rhetorical 'dance' of defining privacy concerns. As the conversation continues their construction of how Google Glass threatens privacy became more apparent – revolving around the prospect of Google Glass becoming normative in the future.

> M2 Well I think it's just for now like in a few years' time everybody will be wearing them so it's not that stupid.
> M1 That's the thing like in 20 or 30 years' time like Google Glass and what was the other thing you were talking about?
> **Life logging cameras.**
> M1 The life logging thing it will all become normal and I think, I hope not, I mean that's what I'm really worried about, exactly the same thoughts as you.
> **Why does that concern you then?**
> M1 I don't know. I mean like people 20 or 30 years' ago would have probably thought it was really weird that people have Facebook and people have Twitter I mean like my grandparents and other elderly people I know they just can't understand Facebook, some people that I know. For me I can't understand like these new things like Google Glass, I'm sure I will but it will take some time but it just feels really weird that your whole life could be documented on a video or a picture, I think life's a bit more than that, if that makes sense.
> **Yeah so there's still a difference between seeing it as kind of pointless and being concerned that it's going to become more popular, do you see what I mean. Like you might think it's pointless but it also somehow worries you. Can you articulate why?**
> M3 It's just quite intrusive, like so many moments of your life could be documented by people you don't know about, like there could be so many pictures of like where you are in the background doing things and you'd never know about any of them. It just feels like a bit, it's like the cy-world is stalking you in a way.
> M4 Yeah cos we all get sketched up enough about like CCTV cameras and like they're in fixed positions and this is like people walking around with like glasses that are recording everything you know it's like 20 times worse. It all gets a bit I Robot-y to me so that's why I don't really like it.
> M5 It's all big brother.
> M4 A bit big brothery.
> *(Session 5, 405)*

What we see above is a slowly emerging and co-constructed formulation of what is threatening about Google Glass. M1, responding to M2, says that he has "exactly the same thoughts", although then says he doesn't know why it bothers him, and dismisses himself as being of

the wrong generation. M3 picks up the discussion by framing the issue as a form of stalking, to which M4 extends by stating Google Glass is worse than CCTV because it is not in a fixed location. What emerges from this discussion is a definition of privacy in rather implicit terms: not knowing that you are being documented (notions of your "whole life", and that "life's a bit more than that"), and that the "cy-world" is constituted as a whole entity that is capable of stalking you.

Thus surveillance technology is initially constructed as creepy and weird if it is socially obnoxious and obtrusive, but also if it is (or will be) everywhere or if it's harder to detect. There is a shared construction of this future as concerning, and what underpins this is an implied notion that it is wrong to capture a whole or complete picture of people's lives. It is essentially an argument for the right to privacy, but they do not explicitly state it as such.

In relation to the assumed ubiquity of surveillance that we presented earlier, here the increasing presence of surveillance is discussed as a problem and does actually provoke (subtle illusions) to privacy concern. What is different about this discourse then, and is a point we will draw together in the discussion, appears to be a concern - not that one is documented or watched - but that such documentation of the self can be woven together to form a more complete picture of you.

When Surveillance Notices "Me"

We turn now to what we suggest is the nexus of where arguments for privacy become most apparent: when the technology is said to restrict one's ability to withhold aspects of their life, or when undesirable self-consequences can be identified. We analyse several variations of what we are referring to as this "surveillance-identity threat". In the first example below a participant tells an account of having her gender on Facebook accidentally changed, and how this resulted in a shift in the targeted advertisements that she receives:

> F Yeh it's like my Facebook profile got reset to male for some reason. I think like Facebook–
> M Someone Frape you?
> F No I think Facebook had done it just randomly. But then I started getting adverts for gays all around [location]...and I was like no thanks I am really not interested in that. And it was really weird, quite scary that Facebook follows close, I was in a relationship with a guy so Facebook saw it. I was like ah!

M Gay!
F Adverts suitable and just like it's really creepy that they follow your profile that closely.
(Session 4, 456)

The narrowing down of the wide surveillance lens onto her, and the designation of Facebook as an entity ("they") imputes the idea that such surveillance is intentional, intelligent (see Tucker et al., 2012) and thus it becomes creepy. But we note that she calls it creepy specifically because the shift in advertising was mismatched with her gender identity and sexual orientation (see boyd, 2012, for similar examples). In the next example the participant says that when she has not "chosen" what information about her is used in advertisements she feels "a bit spooked".

F But you also get lots of different things you've recently been searching when you're on Facebook; the adverts are tailored to you, aren't they? That's really not cool.
How does that make you feel, though, when that happens?
F Just a bit spooked, I dunno.
M Yeah.
F Yeah, 'cause I suppose you haven't chosen to share that information with anyone. So they just kind of know. It's a bit like, hmmm.
(Session 7, 203).

While Facebook might classify their tailoring of advertisements as entirely consensual based on users' acceptance of terms and conditions, she places a different meaning on what she has ostensibly "chosen" to share. She says that her online searches (assumedly through an internet search engine) were not "chosen" to be shared with Facebook. This example share similarities to the earlier extract about Google scanning emails (p. 13). While both scenarios produce a lack of alternative positions (e.g. ceasing to be a user of the service), this participant does not fall back on a service exchange argument. What might distinguish this example based on prior research is that people place importance on the separation of contexts (i.e. internet platforms) (Nissenbaum, 2004).

Similarly in the following example the participant's rhetorical question "it's private isn't it?" assumes a shared understanding that the articles she reads online are private from Facebook.

M …But I am also aware now people can also see certain things I am reading and political things I follow. And I don't always want people knowing my politics.
F Yeh, I worry if I am reading articles online that it might link to Facebook because obviously you know at the bottom it always says do you want to share this on Facebook.

> What happens if I accidentally click it? I don't want people knowing what I am reading on, whatever. You know what I mean, like, it's private isn't it?
> **Yeh.**
> M Hmm.
> F Hmm and it's like with Amazon every time you buy something it's come on, do you want to share this on Facebook? I went no.
> *(Session 4, 433)*

The distinction between choosing to post (e.g. to Facebook) and linking to browsing or purchasing behaviours elsewhere is that they convey an expected difference between active self-presentation and more passive behavioural monitoring that might occur across different sites. As articulated further on in the conversation the distinction they make is that "it's not just people knowing what you've posted, it's people knowing what you're doing."*(Session 4, 1020).* They are conveying an expectation that they should have an ability to conceal their identities. Indeed, this reflects a traditional definition of privacy – personal control that enables autonomy (Margulis, 1977). In other words, being able to keep some things to oneself, as a way of presenting ourselves in the way that we want to be seen (Goffman, 1959).

Another way in which self-presentation relates to privacy, from the literature on social network sites, is in terms of not knowing how wide your audience reach is (see Acquisti & Gross, 2006; Marwick & boyd, 2011; Tufekci, 2008). In the following example, the participant talks about how she likes sharing her family holiday pictures, despite her sister's request not to:

> F I am the sort of person put them on Facebook, I want everyone to see our nice pictures on holiday. My sister sort of messaged me, "why did you feel the need to put them on Facebook it was our holiday, we don't need everyone to see them". And I was kind of like, "well they're my photos as well and I, you know, want my friends to see our holiday".
> *(Session 4, 206)*

Prior research would examine this extract in relation to how privacy boundaries are negotiated by co-owners (Petronio, 2002, 2010), however using a discursive lens what stands out here is her investment in being "the sort of person" who posts photos on Facebook for her friends. What is interesting about this conversation is that later the group are talking about how some

people have large numbers of Facebook friends and the participant realises that her imagined audience is incorrect:

> F Yeh I just thought it was ridiculous the other day. I messaged my sister about this; I was just like looking at my brother's profile. He has a thousand five hundred friends. Well no he doesn't because when I clicked mutual friends he basically just added all my friends for example. In his mind it's obviously to cool to have loads of friends. But it's not because everything he posts about him is being seen by a thousand five hundred people plus probably all their friends or whatever. And it just gets to the point of ridiculous really. I mean that's quite extreme. But it just proves how many people can see your information.
> F Actually photos I am tagged in with him, I just realised, will be posted to all this thousand five hundred friends which actually I would not be that happy about, which again comes down to me posting our holiday photos and tagging him in them. It suddenly means that me, you know, I'm going to be seen by that many people. I didn't think about that, but yeh.
> *(Session 4, 900)*

Thus her justification for her behaviour earlier is undone by telling the story about her brother's alternative sort of person (where "it's cool to have loads of friends"). Other research has demonstrated that privacy breaches occur when people inaccurately picture their imagined communities (Acquisti & Gross, 2006), and in this case the noticeable contradiction of their different ways of presenting themselves led to a change in her expectation of what constitutes a Facebook "friend". It is in being seen in an unexpected way, or by an unexpected audience, that the normalising effect of assumed everyday surveillance may come undone.

Restoration of Privacy through Separation

Finally, we demonstrate some examples of people's assumptions about the separation of their digital and physical self, and how surveillance of the digital self can be constructed as non-privacy threatening because it is not really "you". In the following example, when discussing the university location tracking scenario, they construct the idea that "me" can be separated from their digitally recorded movements.

> M2 they could- they could follow us but without knowing it's us
> F2 yeah
> F1 yeah
> F3 yeah

M2 so I'm ok if they follow me if they don't know it's me but the fact is yeah if I'm like taking the day off on Xbox and they ask "yeah why why why weren't you" (unclear) and they say and I would say "I'm sick" I mean. It's not.
F4 I think it's (unclear) really
So if they're using it to say "why didn't you hand in your assignment?"
F4 it would like almost a totalitarian state like
F1 yeah
F4 (unclear) what's what's the next thing after that it's just
F1 yeah if you support something like this then you'd just be giving into something which was not it's not desirable by university students they want to be independent they don't want to be constantly followed if they wanted that they would have stayed at home so yeah
(Session 1, 884)

"I'm ok if they follow me if they don't know it's me" conveys an idea that your identity can be detached from digital data accumulated about your movements. Such a separation serves to de-link their accountability for their behaviour (i.e. as long as they do not have to explain why they are taking the day off). It is only when the suggestion is made that they can be identifiable, and their behaviour punishable, that they identify a link between a threat to their (independent) selves and that data.

In the next example participants respond to the question of how they deal with other people posting information about them:

…when other people put you in a post and– do you ever feel like "I don't want to be a part of that?"
F I think you can always un-tag yourself. If you don't want to be involved you can just un-tag it, and then you don't get any more notifications and stuff.
M It's that separation; it means other people don't associate with you, other people don't associate that photo with you. Someone that doesn't know you very well going onto your profile, looking at all your photos. If that photo's un-tagged then they have to do a lot of work to find it again. It disconnects it from the central hub that is your online life.
(Session 6, 119)

In an earlier example (p. 16, the "cy-world" is stalking you), what they objected to was the idea that your life can be documented and pieced together without your knowledge. In this example they did not object to the photograph being posted or remaining online, because they say the photo can be separated from "you", or from a "central hub". That is, a position is available to them where they say they could choose to "un-tag" themselves. They assume that a "central hub" or "cy-world" exists but can be electively opted out from, and as a result the separation of selves is talked about as

an acceptable and satisfactory method for restoring privacy. Therefore, like in previous examples (p. 14), in the above two examples it is not the idea of surveillance itself that leads them to object – instead the tension posed by the ubiquity of surveillance is resolved by creating a separation between the digital and physical self.

Discussion

This paper makes contributions to understanding when privacy becomes relevant in conversations about surveillance, in the context of the ubiquity of surveillance and social network technology. In particular we connect our research on surveillance to other work on privacy that emphasises the role that contextual or relationship boundary breach has in provoking privacy threat (e.g. Houghton, Joinson, Caldwell, & Marder, 2013; Nissenbaum, 2004; Petronio, 2010; Petronio & Reierson, 2009), and on impression management strategies that people use to maintain contextual integrity (Marwick & boyd, 2011).

Discourses of Privacy under Surveillance

Our focus groups discussions revealed assumptions of the ubiquity of surveillance in their lives, yet this did not always produce a corresponding anxiety about privacy (as other research might suggest, Westin, 2003). The discursive resources they drew on to arrive at positions of concern, but not necessarily alarm, included utilising the normalisation of surveillance to leverage an argument for even more monitoring (by a trusted source). They also rehearsed the economic trope that it is acceptable to exchange privacy for a service. Furthermore, when some of them identify an ostensible 'excessiveness' of some surveillance methods, such a concern was able to be absolved by drawing on the knowledge that they are in a form of pre-existing consenting relationship with the entity or institution doing the surveillance. The role of trust in privacy is established in previous research (e.g. Westin, 1967), but this paper shows how trust is bound up with the ideological and identity related discursive resources that people can draw on to continue to produce a position of non-resistance to surveillance.

When people did say they were surprised by a privacy breach, it was talked about in terms of unexpected exposure or misrepresentation, or through making allusions to having one's life 'woven together'. They resolved these dilemmas of knowing they were under surveillance by discussing how one can (re)separate aspects of their online lives. This seems to indicate that the assumption of ubiquitous surveillance may not include the notion that this surveillance feeds information across different contexts or to different institutions or platforms (i.e. the notion proposed by Haggerty and Ericson (2000) that surveillance forms an "assemblage"). As a consequence, they neutralise the threat of surveillance by arguing that one can still achieve privacy by ensuring a separation of selves.

Our paper also makes contributions to understanding how people connect the (in)visibility of surveillance technology to its relevance to their privacy. The notion of the often invisible presence of surveillance in their lives produced two seemingly contradictory arguments. On one hand, the notion that subtle surveillance technology can make it harder to tell if someone is capturing you was said to violate an expectation of privacy, in other cases the ostensible imperceptibility of surveillance led to nothing to hide/ignorance is bliss arguments. Rather than viewing these as the contradictory opinions of different individuals, a discursive approach illustrates what people are defending against or how they are supporting their identity investments. For example, when you examine the trajectory of these arguments, dismissing surveillance could occur when queried about a technology that they are already using (e.g. with Google Mail), but rhetorical resistance occurred when a surveiller was identified as engaging in an overreach in their usual level of surveillance and if surveillance is obtrusive in a way that restricts identity. The notable presence of surveillance can make identity constructions more difficult, and understanding these restrictions may be one way to explain the privacy paradox (or so called lack of action around privacy) – that is, there are only some situations in which identities are threatened under surveillance.

Implications for the Study of Identity and Privacy

In addition to demonstrating the discursive constructions of privacy under surveillance, we now also highlight how this research may be relevant to non-discursive approaches, in particular to studying identity threat and misrecognition – as these were particularly prominent findings in this paper. Some of the ideas we present as potential privacy awareness raising approaches have been attempted by privacy advocates, but not in systematic psychological research. Social psychologists could engage in similar exercises, as Kende et al (2015) argue, to "pressure test" existing theory in online social media.

Misrepresentation. Examples of a concern about misrepresentation in this paper included noticing incorrectly tailored advertising that renders the surveillance visible, or having to explain that you had a legitimate reason for not attending classes because the surveillance data might indicate non-attendance. This can be interpreted as a desire for authenticity (see Goffman, 1959; Marwick & boyd, 2011), but there also might be particularly negative consequences resulting from misrepresentation, for example the frustration caused by misrecognition and targeting by surveillance in airports (Blackwood, Hopkins, & Reicher, 2013). Misrecognition can provoke *psychological reactance* (Brehm, 1966) that may cause people to protect their privacy, and may be a useable counter to the "nothing to hide" argument - *you have nothing to hide, but what if the surveillance is wrong?* We do however caution that for psychological reactance to be useable as a trigger for surveillance resistance, people need the freedom to point out that assessments about them are wrong (Miron & Brehm, 2006).

Expressive privacy. A second type of identity threat that could be seen in this paper refers to a core personal privacy definition often referred to as "expressive privacy" - the expected privacy of one's inner thoughts and behaviours (Burgoon et al., 1989) and in turn the ability to engage in (chosen) self-presentations (Tucker et al., 2012, presented a similar example). Light (2010) argues that digital technology now turns people 'inside out'- exposing us to privacy violations that we might never have faced before (e.g. digitally tracing the news articles you read, where you focus your

attention on a screen, or even your heart rate). Agency or choice is again important to account for (Tucker et al., 2012), and increasingly some technologies do not provide an opt-out. This means that it may be the case that the lack of opt-out for such technologies could cause people to shift their basic constitutions of privacy.

Maintaining separation of context/identity. The third type of identity threat that we identified can be connected to Nissenbaum's theory of privacy as contextual integrity (Nissenbaum, 2004, 2011). Contextual integrity is a normative notion that social contexts should remain separate (colloquially, "what happens in Vegas, stays in Vegas"). In this paper, examples of such were represented when talking about wanting to "disconnect the central hub" of your online life, and when talking about Facebook learning about your activity elsewhere online. While social psychological research has examined how people experience conflict when they possess multiple identities, it has paid relatively less attention to why people might expect that contexts (or identities) should be kept apart or how people achieve this (although see Roccas & Brewer, 2002; Vignoles, Regalia, Manzi, Golledge, & Scabini, 2006, for concepts of identity compartmentalisation and continuity). This could be studied across technologies that vary in how restrictive they are of people's ability to engage in contextual separation (as privacy) practices – for example some online platforms encourage users to present a unified chronological self to a collapsed audience (e.g. Facebook), whereas others allow for some multiplicity or separation (e.g. Snapchat).

An additional component of the contextual integrity concept that arose in these discussions is the idea of achieving separation of the digital and physical "you"– reflecting the digital dualism fallacy (Jurgenson, 2011, 2012; Rey & Boesel, 2014) that allows for surveillance of the "digital you" to be constructed as inconsequential. A potential for future research is to connect this to Haggerty and Ericson's (2000) theorisation of "data doubles" - where your digital presence can be pieced together and targeted by surveillance. Interventions could be developed that demonstrate that the "data double" is identifiable, and that de-anonymization of ostensibly anonymous data is possible (e.g. Narayanan & Shmatikov, 2008).

Limitations

There are barriers that prevent psychologists from studying technology use in situ, which is one of the reasons why analysing discourse about technology and online behaviour is useful. There are also some limitations to our approach – talk about online behaviour does not reflect actual behaviour, and studying how people do behave under different surveillance conditions is important. We also cannot comment concretely here, but suspect there would be different ways that people present themselves in social networks, than they do in focus groups. What our analysis contributes instead is an understanding of the ideological assumptions that underpin the legitimation of surveillance, and how people bring into being positions of either resistance or acceptance when they are asked to explain their participation in surveillance capable technologies.

In addition our sample population is quite homogenous, although being young adults they are big consumers of social media and a relevant target group, it does means that different privacy discourses would arise under different conditions. For example it would be important to talk to people who have more at stake for being under surveillance, such as stigmatised minorities where the "nothing to hide" argument would not be tenable. The particular scenarios we chose also framed the type of surveillance that was being debated. While in some respects the focus group format is thought to allow for a relatively more naturalistic conversation than an interview, others have critiqued the way that moderators direct for particular types of responses and discount conversations between participants (Puchta & Potter, 2002). The benefit of producing collective meaning making about privacy in a group conversation is somewhat undermined by the reduced ability to allow contrary arguments from others in the group. The positive re-interpretation of this criticism of focus groups is to look at the practices that people are discussing – in the case of privacy for example – as a matter of co-regulation (Petronio, 2002), where the meaning of the subject is not fixed, but created and changed in talk.

Conclusion

We write this in the context of perceptions that the general public are unconcerned about their privacy. In some respects this could be seen in this study - participants rarely went past saying that surveillance was “weird” or “creepy” to talk about actions they could take in resistance to surveillance. Tucker et al (2012) claim that thinking “surveillantly” becomes a part of everyday life and that this results in wariness but not outright action (an example in our study is the participant who said she has taken steps to prevent Google tracking her, but continues to use Google, p. 14). Thus in social relations and surveillance there is always a bargaining process, where people actively allow forms of regulation that work with them for some mutual benefit, rather than being enforced upon them (Pallitto, 2013; Spears & Lea, 1994), and the trust relationship with the surveiller is central to understanding participation in surveillance technology and why people self-disclose online (Joinson & Paine, 2007; Joinson et al., 2010; McKnight & Chervany, 2001). Moreover, sometimes it is only because we are not really free to escape such an arrangement that we might place greater trust in surveillers. However what is peculiar about surveillance technologies is the impersonal and abstract nature of them, and the imperceptibility of the data that are collected about us. Indeed, the unobtrusiveness and invisibility of technology is often a key feature of its commercial success (Hjelm, 2005). Thus the facilitation of the relationship between surveillers and surveilled is not direct. Ellis et al (2013b), drawing on Giddens (1990) notion of access points, argue that surveillance resistance might be created by giving “faces” to surveillance systems. In line with this one suggestion we make to social psychologists is to develop surveillance resistance interventions by drawing on the social psychology of leadership and identity. For example, how leaders behaviours are legitimised when they are seen as in line with the group, or how this relationship can be undermined if it contradicts a shared identity (see Haslam, Reicher, & Platow, 2011; Haslam & Reicher, 2012; O'Donnell et al., 2010a; Subašić et al., 2011).

There is little prior discursive research on privacy and surveillance, other than the work by Ellis et al (2013a). While they focussed on detecting people’s implicit and emotional awareness of

surveillance (e.g. the feeling 'deep down' of being watched), in our paper we focussed on identity, context, and impression management. Despite taking different starting points, we also found that the presence of surveillance appears to produce a normalising argument, and that explicit articulations of the right to privacy were not well formulated. Together this set of work demonstrates that a discursive approach to privacy can help us understand how assumptions about privacy and surveillance are shared and co-constructed.

Our research aimed to demonstrate the relevance of online social networks and surveillance technologies for the advancement of social psychology theory and application. Privacy, while treated as a concerning social issue, is not typically viewed as being of interest to the development of psychological theory (Margulis, 2003) – yet privacy is an important part of identity processes, group behaviour, and social interaction. Without privacy, people cannot freely express themselves or freely engage in their communities, and surveillance technologies are increasingly making privacy more difficult to retain.

Finally, the key point to be made from this research is that privacy awareness might be better raised by highlighting the identity consequences of surveillance, rather than constructing surveillance as a generalised privacy threat. While the notion that surveillance is spreading across all aspects of our lives sounds ominous to some and is theorised to increased people's concern for privacy as technologies evolve (Junglas, Johnson, & Spitzmüller, 2008; Westin, 2003), what prior research has struggled to account for is the apparent lack of action against surveillance, and this may be because surveillance has a normalising effect. We have demonstrated here that what 'creeps' people out is the creeping ability to piece together their lives rather than the creep of surveillance into further domains. For those concerned with creating an informed debate about the implications for privacy in the digital age, the difference is subtle but important.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514. doi:10.1126/science.aaa1465

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on Facebook. *PET*, 1-22.

Altman, I. (1974). Privacy: A conceptual analysis. In D. H. Carson (Ed.), *Man-environment interactions: Evaluations and applications*. Washington, D.C.: Environmental Design Research Association.

Altman, I., Vinsel, A., & Brown, B. B. (1981). Dialectic conceptions in social psychology: An application to social penetration and privacy regulation. *Advances in Experimental Social Psychology* (Vol. 14, pp. 107-160): livAcademic Press, Inc.

Antaki, C., Barnes, R., & Leudar, I. (2005). Self-disclosure as a situated interactional practice. *British Journal of Social Psychology, 44*(2), 181-199.

Barreto, M., & Ellemers, N. (2003). The effects of being categorised: The interplay between internal and external social identities. *European Review of Social Psychology, 14*, 139-170. doi:10.1080/10463280340000045

Blackwood, L., Hopkins, N., & Reicher, S. (2013). Turning the analytic gaze on 'us': The role of authorities in the alienation of minorities. *European Psychologist, 18*(4), 245-252. doi:10.1027/1016-9040/a000151

boyd, d. (2012). Networked privacy. *Surveillance & Society, 10*(3/4), 348-350.

boyd, d., & Marwick, A. E. (2011). *Social privacy in networked publics: Teens' attitudes, practices, and strategies*. Paper presented at the "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society", Oxford Institute. http://ssrn.com/abstract=1925128

Brehm, J. W. (1966). *A theory of psychological reactance*. New York: Academic Press.

Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. *Journal of Social and Personal Relationships, 6*, 131-158.

Chambers, C. (2014). Facebook fiasco: was Cornell's study of 'emotional contagion' an ethics breach? *The Guardian.*

Cranor, L. F., Reagle, J., & Ackerman, M. S. (2000). Beyond concern: Understanding net users' attitudes about online privacy. In I. Vogelsang. & B. M. Compaine. (Eds.), *The internet upheaval: Raising questions, seeking answers in communications*. Cambridge, MA: MIT Press.

Davis, J. L., & Jurgenson, N. (2014). Context collapse: theorizing context collusions and collisions. *Information, Communication & Society, 17*(4), 476-485. doi:10.1080/1369118X.2014.888458

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285-297. doi:10.1002/ejsp.2049

Edley, N., & Wetherell, M. (2001). Jekyll and Hyde: Men's constructions of feminism and feminists. *Feminism & Psychology, 11*(4), 439-457.

Edwards, D., & Potter, J. (1992). *Discursive psychology*. London: Sage.

Ellemers, N., & Barreto, M. (2006). Categorization in everyday life: The effects of positive and negative categorizations on emotions and self-views. *European Journal of Social Psychology, 36*, 931-942.

Ellis, D., Harper, D., & Tucker, I. (2013a). The affective atmospheres of surveillance. *Theory & Psychology, 23*(6), 716-731. doi:10.1177/0959354313496604

Ellis, D., Harper, D., & Tucker, I. (2013b). The dynamics of impersonal trust and distrust in surveillance systems. *Sociological Research Online, 18*(3), 8.

Farfade, S. S., Saberian, M., & Li, L.-J. (2015). Multi-view face detection using deep convolutional neural networks. *arXiv preprint arXiv:1502.02766*.

Fitzpatrick, A. (2014). Why Google Glass isn't the future. *Time Magazine.* Retrieved from http://time.com/3588143/google-glass/

Foucault, M. (1977). *Discipline and punish: The birth of the prison.*: Vintage.

Gergen, K. J. (1991). *The saturated self: Dilemmas of identity in contemporary life*. USA: Basic Books.

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

Goffman, E. (1959). *The presentation of self in everyday life*. New York: Anchor Books.

Goffman, E. (1961). *Asylums: Essays on the social situation of mental patients and other inmates.*: Penguin Books.

Goffman, E. (1972). *Relations in public*. Harmondsworth: Penguin.

Greenwald, G. (2013). NSA collecting phone records of millions of Verizon customers daily. *The Guardian.* Retrieved from www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order/

Haggerty, K. D. (2011). Tear down the walls: On demolishing the panopticon. In D. Lyon (Ed.), *Theorizing surveillance*. New York: Routledge.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology, 51*(4), 605-622. doi:10.1080/00071310020015280

Haslam, S. A., Reicher, S., & Platow, M. J. (2011). *The new psychology of leadership: Identity, influence and power*. Hove and New York: Psychology Press.

Haslam, S. A., & Reicher, S. D. (2012). When prisoners take over the prison: A social psychology of resistance. *Personality and Social Psychology Review, 16*, 154-179. doi:10.1177/1088868311419864

Hirsh, J. B., & Kang, S. K. (in press). Mechanisms of identity conflict: Uncertainty, anxiety, and the behavioral inhibition system. *Personality and Social Psychology Review*, 1-22. doi:10.1177/1088868315589475

Hjelm, S. I. (2005). Visualising the vague: Invisible computers in contemporary design. *Design Issues, 21*(2), 71-78.

Houghton, D., Joinson, A. N., Caldwell, N., & Marder, B. (2013). *Tagger's Delight? Disclosure and liking behaviour in Facebook: the effects of sharing photographs amongst multiple known social circles*. University of Birmingham.

Jeni, L. A., Lőrincz, A., Nagy, T., Palotai, Z., Sebők, J., Szabó, Z., & Takács, D. (2012). 3D shape estimation in video sequences provides high precision evaluation of facial expressions. *Image and Vision Computing, 30*(10), 785-795.

Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the internet. In A. Joinson. (Ed.), *Oxford handbook of internet psychology* (Vol. III). Oxford: Oxford University Press.

Joinson, A. N., Reips, U.-D., Buchanan, T., & Paine Scholfield, C. B. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction, 25*(1), 1-24. doi:10.1080/07370020903586662

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems, 17*(4), 387-402.

Jurgenson, N. (2011). Digital dualism versus augmented reality. *Cyborgology.* Retrieved from https://thesocietypages.org/cyborgology/2011/02/24/digital-dualism-versus-augmented-reality/

Jurgenson, N. (2012). When atoms meet bits: Social media, the mobile web and augmented revolution. *Future Internet, 4*(1), 83-91.

Kende, A., Ujhelyi, A., Joinson, A., & Greitemeyer, T. (2015). Putting the social (psychology) into social media. *European Journal of Social Psychology, 45*(3), 277-278. doi:10.1002/ejsp.2097

Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences, 111*(24), 8788-8790. doi:10.1073/pnas.1320040111

Levine, M. (2000). SIDE and Closed Circuit Television (CCTV): Exploring surveillance in public space. In T. Postmes, R. Spears, M. Lea, & S. Reicher (Eds.), *SIDE issues centre-stage: Recent*

developments in studies of de-individuation in groups. Amsterdam: Royal Netherlands Academy of Arts and Sciences.

Light, A. (2010). The Panopticon reaches within: how digital technology turns us inside out. *IDIS, 3*, 583-598. doi:10.1007/s12394-010-0066-7

Livingstone, S. (2006). Children's privacy online: experimenting with boundaries within and beyond the family. In R. Kraut, M. Brynin, & S. Kiesler (Eds.), *Computers, phones, and the internet: Domesticating information technology. Human technology interaction series.* (pp. 145-167). New York, USA: Oxford University Press.

Margulis, S. T. (1977). Conceptions of privacy: current status and next steps. *Journal of Social Issues, 33*(3), 5-21.

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues, 59*(2), 243-261.

Martin, A. K., van Brakel, R. E., & Bernhard, D. J. (2009). Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society, 6*(3), 213-232.

Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society, 13*, 114-133. doi:10.1177/1461444810365313

Marx, G. T. (2003). A tack in the shoe: Neutralizing and resisting the new surveillance. *Journal of Social Issues, 59*(2), 369-390. doi:10.1111/1540-4560.00069

McKnight, D. H., & Chervany, N. L. (2001). Trust and distrust definitions: One bite at a time *Trust in Cyber-societies* (pp. 27-54): Springer.

McMahon, C., & Aiken, M. (2014). Privacy as identity territoriality: Re-conceptualising behaviour in cyberspace. *Social Science Research Network*. doi:10.2139/ssrn.2390934

Microsoft. (2015). How-Old.net. Retrieved from http://how-old.net/#

Miron, A. M., & Brehm, J. W. (2006). Reactance theory-40 years later. *Zeitschrift für Sozialpsychologie, 37*(1), 9-18.

Narayanan, A., & Shmatikov, V. (2008). *Robust de-anonymization of large sparse datasets.* Paper presented at the Security and Privacy, 2008. SP 2008. IEEE Symposium on.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus, 140*(4), 32-48.

Norberg, P. A., & Horne, D. R. (2007). Privacy attitudes and privacy-related behavior. *Psychology and Marketing, 24*(10), 829-847. doi:10.1002/mar.20186

O'Donnell, A. T., Jetten, J., & Ryan, M. K. (2010a). Watching over your own: How surveillance moderates the impact of shared identity on perceptions of leaders and follower behaviour. *European Journal of Social Psychology, 40*, 1046-1061. doi:10.1002/ejsp.701

O'Donnell, A. T., Jetten, J., & Ryan, M. K. (2010b). Who is watching over you? The role of shared identity in perceptions of surveillance. *European Journal of Social Psychology, 40*(1), 135-147. doi:10.1002/ejsp.615

Oliver, J. (Producer). (2015). Government surveillance. *Last Week Tonight with John Oliver*.

Pallitto, R. M. (2013). Bargaining with the machine: A framework for describing encounters with surveillance technologies. *Surveillance & Society, 11*(1), 4-17.

Petronio, S. (2002). *Boundaries of privacy: Dialetics of disclosure*. USA: State University of New York Press.

Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation? *Journal of Family Theory and Review, 2*, 175-196. doi:10.1111/j.1756-2589.2010.00052.x

Petronio, S., & Reierson, J. (2009). Regulating the privacy of confidentiality. In A. T. Afifi & W. A. Afifi. (Eds.), *Uncertainty, information management, and disclosure decisions: Theories and applications* (pp. 365-383). NY: Routledge.

Pomerantz, A. (1986). Extreme case formulation: A way of legitimizing claims. *Human Studies, 9*(2-3), 219-229.

Puchta, C., & Potter, J. (2002). Manufacturing individual opinions: market research focus groups and the discursive psychology of evaluation. *British Journal of Social Psychology, 41*(3), 345-363. doi:10.1348/014466602760344250

Rey, P., & Boesel, W. E. (2014). *The web, digital prostheses, and augmented subjectivity*. New York: Routledge.

Roccas, S., & Brewer, M. B. (2002). Social identity complexity. *Personality and Social Psychology Review, 6*(2), 88-106. doi:10.1207/S15327957PSPR0602_01

Rudder, C. (2014). We experiment on human beings! *OkCupid.* Retrieved from http://blog.okcupid.com/index.php/we-experiment-on-human-beings/

Schwartz, B. (1968). The social psychology of privacy. *American Journal of Sociology, 73*(6), 741-752.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Q., 35*(4), 989-1016.

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review, 90*(4), 1087-1156.

Solove, D. J. (2007). 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego L. Rev., 44*, 745.

Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*: Yale University Press.

Spears, R., & Lea, M. (1994). Panacea or Panopticon?: The hidden power in computer-mediated communication. *Communication Research, 21*(4), 427-459. doi:10.1177/009365094021004001

Subašić, E., Reynolds, K. J., Turner, J. C., Veenstra, K. E., & Haslam, S. A. (2011). Leadership, power and the use of surveillance: Implications of shared social identity for leaders' capacity to influence. *The Leadership Quarterly, 22*(1), 170-181. doi:http://dx.doi.org/10.1016/j.leaqua.2010.12.014

Tucker, I., Ellis, D., & Harper, D. (2012). Transformative processes of agency: Information technologies and the production of digitally mediated selves. *Culture and Society: Journal of Social Research, 3*(1), 9-24.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28*, 20-36. doi:10.1177/0270467607311484

Turner, J. C., Hogg, M. A., Oakes, P. J., Reicher, S. D., & Wetherell, M. S. (1987). *Rediscovering the social group: A self-categorization theory*. Oxford: Blackwell.

Vignoles, V. L., Regalia, C., Manzi, C., Golledge, J., & Scabini, E. (2006). Beyond self-esteem: Influence of multiple motives on identity construction. *Journal of Personality and Social Psychology, 90*, 308-333. doi:10.1037/0022-3514.90.2.308

Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues, 59*(2), 431-453. doi:10.1111/1540-4560.00072

Wetherell, M. S. (1998). Positioning and interpretative repertoires: conversation analysis and post-structuralism in dialogue. *Discourse & Society, 9*(3), 387-412.

Wetherell, M. S. (2007). A step too far: Discursive psychology, linguistic ethnography and questions of identity. *Journal of Sociolinguistics, 11*(5), 661-681.

Wilkinson, S. (1999). Focus groups: A feminist method. *Psychology of Women Quarterly, 23*, 221-244.