Humanity & Society

'Putting everything up there': framing how we navigate the intricacies of privacy and security on social media.

Journal:	*Humanity and Society*
Manuscript ID	HAS-19-0014.R1
Manuscript Type:	Original Research Article
Date Submitted by the Author:	n/a
Complete List of Authors:	Spiller, Keith; Birmingham City University, Criminology
Keywords:	Code of the Street, Social Media, Privacy, Security

Abstract:	Posting commentary via social media can have very real consequences and these can drive how users navigate the world of social media. The aim of this paper is to develop a deeper appreciation of how users comprehend their security and privacy within their social media interactions. I turn to Anderson's (2000) work on street-life in attempting to draw upon the decisions made in navigating particular environments – especially those with associated risks. This I argue is similar to how users rationalise their social media behaviour to protect themselves and/or view others. Both are learned behaviours that are at times habituated, reactionary or temporary in the face of heightened threats. Using findings from 27 interviews with UK social media users I present 3 codes that may be useful in framing just how users navigate and comprehend their experiences of social media privacy and security.

Introduction

> *One of the things we talked about with the social workers was the danger of putting stuff online that would make you traceable to the birth parents, who might want to find you.*
>
> *When we were adopting, I'd check the Facebook page of the birth mother, so I was able to check her out that way. She probably put certain things on there that she shouldn't have done, so that made me quite aware of the fact that other people can just go in and read it.*
>
> *(Male, 42, self-employed)*

To search and observe through social media is not unusual; in the above quote, an adoptive father has been told not to post about his daughter online to prevent her identification. Nevertheless, he has searched and viewed the activities of the child's birth mother through the material she has placed on social media. Evident in such calculations is an interesting juxtaposition, where certain information is kept private and secure, but viewing the vested information of others is enticing and immediately available. Similar sentiments could be applied to how employers view the social media activity of employees (Sánchez Abril et al. 2012; McDonald et al 2016). In these instances, the consequence of posting information has the potential to expose employees to the vulnerability of losing their jobs – if they post ill-advisedly. Decisions on what to post or what not to post (or what to view) all have very real consequences and can drive how users navigate the world of social media. The aim of the paper therefore is to develop a deeper appreciation of how users comprehend their security and privacy within their social media interactions. I turn to Anderson's (2000) work on street-life in attempting to draw out the decisions made in navigating particular environments – especially those with associated risks. Life online and life on the streets both engage learned behaviours that are at times habituated, reactionary or temporary, particularly when faced with heightened threats.

Anderson's (2000) 'Code of the Street' reviews the everyday practices of a marginalised community in the USA. He examines a black neighbourhood in Philadelphia and seeks to understand the role of violence in the area. The Code of the Street is largely defensive and Anderson concentrates on the social order and everyday practices that underscore life in the neighbourhood – how people interact,

how people present themselves, the rules of living in this environment. Typical rules of order, policing and the law have been altered due to socio-economic depravation or a sense of lawlessness in the neighbourhood. *Decency* and *violence* frame the Code of the Street - one indicates a hardworking and morally guided way of life, the other a more risk embracing and brutal attitude that often works beyond the law and civil society (see Elias & Jephcott 1978; Keane 2013). By teenage-hood most in Anderson's neighbourhoods have internalised the Code of the Street and are keenly aware of how to operationalise this knowledge to avoid violence (Anderson, 2000:72). Moreover, the etiquette of the street also draws on a performance, one often centred on demonstrations designed to display status, protection, power and popularity. On social media the same logic can apply when traversing between effervescent communications or risky and manufactured behaviours that expose personal or compromising information (Bailey and Steeves 2015; Shin 2010). Users share information to gain 'attention' from networked audiences (Abidin 2016; Díaz Sánchez 2016) and, in parallel, social media presents risks such as bullying, harassment, self-harm and suicide (see Gabriel 2014; Luxton et al. 2012; Wise 2016). Alternatively, concerns have been raised about 'perpetual contact', 'hyper-coordination', not being able to 'switch-off' or grooming (Berriman and Thomson 2015; Hall 2016; Madden et al. 2013; Tennant et al. 2015), as well as having information stolen or identity theft (see Huq 2015; Khan et al 2017). In what follows I want to introduce how some social commentators have considered the dilemma of privacy and security online and I then frame 3 codes that I argue can help in developing our understanding of how social media is appreciated by those who use it. I expand on these codes through my interviews with social media users. Finally, I return to Anderson and echo his sentiments as to how we may be able to extract sociological meaning from the order that is integral to life on the streets and online.

I begin by considering how for contemporary urban ethnographers the physical environment of the street and life online are inextricable entangled; indeed, urban researchers have applied Anderson's Code of the Street to explain how poor, young, black residents use social media to manage exposure

to violence in their neighbourhoods. Stuart (2019), for instance, considers the new rules of gang conflict online that may deescalate gang violence offline. As Stuart highlights gang crime in urban areas has decreased in recent years and he argues social media transforms rather than amplifies offline gang violence. An insult on twitter, for example, may initiate a very different response as opposed to the same insult being delivered face-to-face and on the street. In extending this point, Stuart poses a very pressing methodological question, how do we know social media posts actually cause a violent act to occur? For him, greater attention or a systematic approach is needed to extract or challenge presumptions that social media gang posturing directly contributes to violence. Moreover, Lane (2019) emphasises the beneficial element of social media for the youth of these neighbourhoods, particularly for young women who may share and model positive experiences and thus impress on their audiences an affirmative message. Yet within the urban literature, there is a prominence toward gang members use of social media to instil violence. For Patton et al (2013) 'internet banging' is a form of social media communication used to incite fear or trade insults when street posturing moves online. Patton et al. draw upon the Post-Fordian landscape where industrial masculine identities have become lost and into such a vacuum gang membership and cultural outlets, such as *Hip Hop,* reconfigure identity through rehearsed masculine displays used to establish credibility. The online presentation of the gang members often display references to violence, wealth, drugs or sex with a deliberate and recognisable message for their audiences. Urbanik and Haggerty (2018) extend this further, with some generational considerations, where street criminals of old (or non-digital natives) frown upon new methods of display. Previously, criminal activities were concealed; now such activities are overt and celebrated through social media – all with incriminatory potential. The social media users considered in this paper face limited risk of physical violence, as compared to street life, however their online worlds do expose certain kinds of dangers related to privacy and security and it is how they comprehend and react to these dangers, as we will see, that has comparable rationales to life on the street.

Anderson's work provides a useful framework to enhance understandings of social media; yet, I am not setting up privacy and security as binary notions, instead I am interested in how social media activities are rationalised through lens of security and privacy. Privacy in an online context ensures the appropriate use of data and a regard for private, family and home life (see Council of Europe 2017). In the UK, privacy law is guided by Article 8 of European Convention on Human Rights and abuses might include excessive collection of information, unauthorised exposure of information or other misuses of this information, such as monitoring communications (see ICO 2014). Whereas, online security centres on keeping data safe from theft, hacking or other instances of abuse where data is compromised. For example, passwords stolen to access sensitive information (see CNN 2017). Moreover, the General Data Protection Regulation, which governs UK and European data, is a statutory right protecting the unlawful use of personal data (see European Commission 2018; ICO 2018). What underscores these definitions and how they are considered in the paper are the tensions as to how personal information is understood by social media users (Andrejevic 2006). Social media organisations hold sizeable amounts of users' information (see Ellison and boyd 2013; Uldam 2016); for example, date of birth, password, email address, contact list, communication history, photographs, etc. In addition, fellow users can view the whereabouts, pictures, comments or preferences of others (see Albrechtslund 2008). Furthermore, 'human-data interaction' is a relatively new field of enquiry and forms of 'reflexive self-monitoring' invite others to watch and comment on activities and information shared (Lupton 2016). Such activities include the way in which people interact and make sense of their digital data, as well as 'data materialisation' or how users make their data real, material and visible online.

Nissenbaum (2010) for example considers 'contextual integrity', context is grounded in the system that sets expectation and if these expectations are abridged then anxieties soon follow. Trust and faith is held within the system, for instance, passwords, professionalism, data rights or laws will protect (Nissenbaum 2011). In other contexts, Nissenbaum draws upon how a patient may go to their GP to

discuss a medical problem. The patient enjoys professional confidentiality, but later that night the GP shares with their spouse or dinner guests the nature of the patient's problem. The patient's name is not mentioned but the problem is. Nissenbaum's observations serve to highlight the complex nature of the lived experience of privacy or security. Indeed, Marwick and boyd (2014) build on this notion with 'privacy harms' evident in social media interactions. As they demonstrate, teenagers acclimatise to online harms and rather than relying on the protection of platforms or other users; their sharing online is framed by the assumption all will be viewed (Correa 2016). 'Networked privacy' presumes 'privacy can easily be violated by any individual connected to the user' (Marwick and boyd 2014: 1064). In addition, 'context collapse' may also be a useful concept to explore imagined audiences and their guiding force when actors accentuate their identities in particular ways and quietly hide other identity aspects (Goffman 2002). The collapse is the flattening of multiple audiences into one, for example, audiences that are conceived as separate – work colleagues, family, ex-lovers – are merged (see Davis and Jurgenson, 2014; Marwick and boyd 2010; Vitak 2012).

Other commentators have used the metaphor of the *boundary* to explain the choices made when sharing information (see Petronio 2012). Privacy is mediated through the transfer of individual privacy boundaries to collective privacy boundaries, when for instance information is posted on Facebook and control is held by the network of 'friends' rather than by the user. Disclosure of this sort is also due to the norm of reciprocity - if a friend provides some information to you, then you provide information in return. This lubricates conversations and friendships, but also provides a mutual responsibility as to how the information is managed and the boundary maintained. It builds closeness and trust, and intimacy develops the more information is exchanged (Henderson and Gilding, 2004). Failure to follow boundary rules lead to breaches in friendships and violation of expectations, or termination of relationships. Therefore, there are expectations in the management and control of information, 'friends' enjoy privileges and responsibilities (Acquisti and Gross 2006). Contextual integrity, networked privacy or boundaries offer insight into how privacy and security are negotiated in digital contexts; indeed, they also point toward the tensions inherent in how users value the communication

potential of social media, as well as the problematics of disclosure or exposure (Shin 2010; Tsay-Vogel et al. 2018). Yet, as I want to expand there are also specific codes that ground how such rules are understood, much like those experienced by Anderson's neighbourhood residents.

Social media code

The codes I refer to emerged and developed from my research interviews with social media users (see below) and the codes focus on *presentation*, *protection* and *surveillance*. Firstly, the code of presentation is integral to the Street; an individual should display presentations of being 'streetwise' in order to traverse and navigate the street. The biggest, badest and meanest persona prevails on the street and much of the pantomime is about presenting a 'don't mess with me' air of authority. Equally, grooming, stance and clothing can be used to deter violence or intimidate, and 'is shaped by what he thinks others are thinking of him in relation to his peers' (Anderson 2000: 73). Thus, the presentation on the street formulates uniformity as to how one should present oneself if a particular expectation is required and this can be mirrored in social media interactions (Allmer 2014; Bailey and Steeves 2015). Central to participation on social media is carefully curating an online presence and profile, one that often details users' identity, preferences and past-times (see Quinn and Papacharissi 2014). In addition, gossip, eavesdropping, sharing, and watching are all elements of social media and offer reflections on the self-policing, conformity and self-monitoring practice it may instil (Andrejevic 2009; Tifentale and Manovich 2015). On social media, a homogenising effect is also encouraged and is attentive to the interpretation of others and the formation of identities (see Smith 2016). Becoming part of an online group, for instance, may encourage exaggerated performances that are designed to appeal and conform to the inferred preferences and approval of the group. Smith (2016; 2016a), for instance, draws on the cultural shift to visibility within digital communications; sharing information online provides opportunities for expansive creation and pseudo-individualization, as users are free to promote, reveal and visualise in the ways they see fit – for example creating a stylized identity

(Mascheroni et al., 2015). Indeed, Smith has used the example of the Instagram star Essena O'Neill and her disillusionment with the performative element of posting, posing and positioning herself online. As O'Neill tells us, 'nothing about this is real', rather it is 'contrived perfection made to get attention' (see Guardian 2015a). For her, as a social media 'star', performances are calculated to generate reactions from audiences, endorsements from companies or advance fame. As we will see similar performances and calculations are made by 'non-star' users in how they communicate and in the code of presentation that directs their behaviour.

Secondly, a code of protection on the street can be understood in terms of 'I got yo' back' (Anderson 2000: 88) which refers to friends being vigilant to potential harms or when an individual ensures a degree of personal protection. Equally, the role of protection extends to those with whom the individual associates or perhaps, the individual is from a well-known family in the area and this membership provides deterrence and protection. On social media the need to prevent physical harm may be less pressing (but not exempt, as we will see), however harms such as others using personal data, protection of reputation or popularity and the cost of seeking to protect these and maintain the social capital of the user are comparable (see Tuten and Solomon 2014). However, maintaining an appearance of being up-to-date, being social, being clever, being popular or being 'cool' consigns demands on users – this may not apply to all users, but invariably users do seek to project identities, images and perceptions of themselves and others (Murthy 2012; Smith 2016a). Marwick and boyd (2014a) and Lenhart *et al.* (2011) attest that for 'youth' users maintaining their privacy is routinised and clearly practiced – i.e. keeping their parents 'separate' from the information they post on social media platforms. Evident in the practices of users is an awareness of protection – more specifically, what users should do, much like those on the street hoping to avoid violence or, in the case of social media, compromises to reputation, privilege or status.

Thirdly, a code of surveillance, can take the form of a community watching each other for opportunity, as well as for altruistic or policing intent. For example, if a drug dealer is removed from an area, a rival and observant dealer may profit by filling that space. Equally, surveillance by 'decent' members of the community may deter wrong-doing by their mere presence (Tilley 2014) – knowing there are witnesses can curb criminal intent. On the street, information could be determined by detailing the time an individual leaves their home, who they are likely to meet on a street corner or even what shops they frequent – these details may be advantageous to those who seek to know the movements, likes and preferences of those on the street. Whereas, social media details user's friends, their hobbies, their preferences, their families, their leisure time and so on (Correa 2016), this in turn presents an in-depth timeline of communications, as well as networks of acquaintances (Yang et al. 2012) - which track activity and intent. The State, of course, has the authority to seek this information and smartphone logs, GPS locations, text messages, internet search history or social media posts are all part of this remit. Moreover, a growing body of work has considered how police forces and police officers use social media (Davis et al. 2014; Denef et al. 2013; Trottier and Fuchs 2014). Alternatively, government have sought to target and decrypt WhatsApp conversations in order to prevent terror attacks (Guardian 2017). Other work still, concentrates on the dilemmas of social media, especially when personal and professional participation collide. Pressing here is when police forces communicate through social media inadvisably (Goldsmith 2015); for example, the London Met Police helicopter photographed a well-known comedian crossing a London street and included the image with the tweet, 'Whilst on tasking [sic] in central London this morning we spotted a certain energetic funny man ... Can you guess who?'. There was no suggestion the comedian had done anything wrong and the tweet was supposedly light-hearted; yet questions remain about the protection of the comedian's privacy and security (see Guardian 2015). These are the moments when privacy and security are confronted online.

The Study

The empirical work that informs the paper is taken from a large research project reviewing societal resilience to surveillance, the findings presented here concentrate on internet use and in particular the actions of social media users in select locations in the UK. To be considered a 'user', interviewees where those who had a social media presence and used it on a least a weekly basis. Recruitment began with flyers placed in a shop local to my home. The shop, located in a small UK city, is popular with the local community and has high levels of footfall; staff were also extremely accommodating in helping to promote the research. The flyers had a colourful word-cloud on one side with words such as 'privacy', 'user', 'data' and 'online'. On the reverse, it stated that I was interested in experiences of how surveillance and monitoring touched upon everyday life.

I intended recruitment to grow in a relatively organic manner, as I simply waited for participants to contact me. I had hoped self-selection in this manner would recruit a multifarious and enthusiastic sample. The flyers had two effects; they produced a demographic spread of the local population and after the completion of these initial interviews participants were asked to recommend others whom they felt would be interested in participating. 'Snowball sampling' has in the past proved effective in gaining access to hard-to-reach communities (see Browne 2005; Noy 2008), where the promotion of the research by a known community member acts as a virtual gatekeeper. In this case snowballing encouraged an interactional dynamic, one very much in keeping with the logic of the paper - how users communicate online, participants voluntarily tweeted and posted about the research, which aided recruitment. I set no agenda as to the demographic make-up of those I wished to interview; rather everyone who contacted me was interviewed. Interviews took place within a 6-month period – due to funding constraints. Interviews were semi-structured, conversationally driven and were recorded and transcribed. In total I conducted 27 interviews with a diverse range of users; for instance, participants were aged between 18 and 70, the gender balance was 15 male and 12 female, 26 participants were white and 22 had or were about to receive a university education. Participants' professions included; student, medical doctor, private detective, retired police officer, writer, rights

activist, lawyer, unemployed, academic, archaeologist and shop manager. Interviews typically took place in participants' homes or coffee shops and were on average an hour in duration. In total, I travelled to four UK cities, as well as two regional towns in the south of the UK.

Social Media Privacy and Security

Privacy and security on social media are not exclusive, as both influence, and at times are inter-related: for example, users speak of securing their privacy. Nevertheless it is the tensions felt toward how personal information is communicated via social media that drives, for instance, what users might want to keep offline or for audiences that are privileged, i.e. 'friends', as against the wider viewing public of the internet. In what follows the 3 codes of *presentation, protection* and *surveillance* are used to frame how security and privacy influence thoughts and actions of users. I begin with the code of presentation.

Presentation

The following participant responds to the question, what sort of information do you put up on your Facebook profile?

> *Pretty much everything. I guess, photos, date of birth, where you live, who you're friends with, what school you go to, where you work, so a lot of information…. I'm pretty sensible. If I was taking drugs or something, I wouldn't put that up, but I don't. I probably should censor some things, but I don't. …*
>
> *(Female, 18, student)*

As the participant above suggests, activities that may be illegal or embarrassing are edited from her profile, yet other details are forthcoming, such as her date of birth and home address. She acknowledges she should be more careful with her information; yet the urge to share details with her audience outweigh the potential risks associated with disclosing this personal information (see Sebescen and Vitak 2016; Solove 2015). In similar contexts, users can and do make risqué comment for the benefit of their audience, no matter how unintended their consequences. For example, a UK

politician making a perceived humorous tweet, that had derogatory intent, something she either failed to recognise or sacrificed for dramatic impact (see BBC 2014). Indeed, when participating in social media users at times assign trust to the system, much as Nissambaum's contextual integrity suggests, users may be more willing to express controversial statements due to expected levels of protection, anonymity or being unaware of traceability. As a participant continues,

> *When Thatcher died, the censor barriers just fell down and there was a whole load of blue bloody murder going on. And now I think, oh, shit. Even at the time I thought, this is really stupid because I know that it's not that hard to follow these things up. …. I was the drunk bloke at the bar who was telling everybody the time of day… and my whole point about the Thatcher death is that you say things that are just wrong, and you know they're wrong. It doesn't matter if it's, somebody that you don't know personally. But, actually, when it is somebody you do know … I don't know. … If you had two friends around, you're not going to say something that's going to absolutely fuck one off just because it amuses the other one.*
>
> *(Male, 42, Archaeologist)*

Evident, for this participant, is an awareness of social etiquette which influences his personal interactions, such as not goading friends for amusement, and the dilemma here mirrors Anderson's tensions about making choices and understanding the consequences of those choices. For Anderson decency is a means of distinguishing oneself – i.e. you are not 'street'. Much of what Anderson contemplates is a drive for social capital, 'street' equals hipness or contempt for conventional 'white' lifestyles and for those of a street persuasion doing well in school or speaking standard English are frowned upon. But, the consequences of presenting oneself as 'street' increases the likelihood of becoming embedded in the socio-economic depravation of the neighbourhood and its associated disadvantages. Code-switching, as Anderson calls it, presents an advantageous dexterity to those who can and do traverse between the extremes of violence and decency; 'the decent kid' seeks credibility in both spheres; on the street they exert 'street knowledge' through style of dress or acting 'tough', all designed to ward off danger. At home, or perhaps in school, they are courteous and work hard on their studies, with the aim of enhancing opportunities to further their life (see Anderson 2000: 98-

106). Working code advantageously may also be evident in the following participant's use of social media to gain benefits, such as vouchers or discounts by befriending and following particular accounts.

> *I don't have any friends on Facebook, I just sign up for things that I like and want to get information on… I don't want to engage with people I don't know. Maybe it's not entering into the full spirit of social media, but that is what I do.*
>
> *(Male 44, Journalist)*

Here engagement and presentation is tailored through an account that provides none of the usual personal or social inputs that are expected in social media, instead through a coded participation he receives the promotional incentives that are on offer and retains his detachment.

Protection

The user below uses an assumed name on Twitter and avoids Facebook. This is a precaution because he is an ex-police officer and as he admits there are individuals who may seek retribution,

> *I don't particularly want to have somebody banging on my door, so I'm not on Facebook.*
> *(Male, 62, retired police office)*

Again, there is a presentation evident here, however this presentation is very much rationalised by a fear of physical violence and a desire for protection. Indeed, these measures are advisable in the face of his previous occupation. Much like Anderson's brash presentations of 'street' the above presentation is tailored to the potential of violence. Yet on social media there remains a tenuous balance to posting and sharing information due to its real potential to expose participants to risk. More common however for those I spoke to was having their information violated, invariably an account was hacked or a comment they had posted was misconstrued. These are revelatory moments because their security and privacy had been viscerally challenged. Yet also pressing are the tensions induced as users work to manage their social media privacy and security. The following participant elaborates,

> *I had a really bad experience once where a guy at work, who I'd never met before, he was going to be working with me and he invited me to a meeting, and I walked in and he had a picture of me on his computer and the first thing he said to me was, oh, it was [daughter's name] birthday last week, wasn't it, and you went to the – he was a digital guy – and you went to the zoo, didn't you, with your sister and fed the giraffes. … and I was like, oh my god!*
> *(Female, 43, Publishing Manager)*

The shock felt when information posted on social media is accessed and visualised by a fellow user is plain to see. To some degree her personal and private life was violated within a work context. Yet, despite presenting her information freely on social media (and with no privacy settings), there was little expectation on her part that others (outside of her family and friends) would view her posts. As the participant suggests this was a revelatory moment, details of a family outing were not something she was willing to share with a colleague she did not know. Following the event this user reset her privacy setting and is now 'much more careful'.

Diligence and protecting information is a strenuous activity (Lenhart et al. 2011); the following participant describes a 'security fatigue' toward his protection

> *I'm aware of how vulnerable your own networks are but I suspect, like a lot of people, I suffer from security fatigue. When I set my passwords I'm slightly idle. When I've put a password in and they said moderate security and I've tried various permutations and it's still moderate, I can't be arsed to find one which says high-level. Which is ridiculous, really, because I'd like to think I'm reasonably well-versed in the threats out there. But, again, it's a kind of security fatigue.*
> (Male, 42, shop manager)

Protecting an account and changing passwords or developing new ones is time consuming, as well as taxing on memory - as the participant highlights the 'fatigue' felt outweighs the demands required. Wegner (2010) found when students were given 2 options in creating a password, the first option without any direction on how to create the password and the second option providing guidelines – i.e. word length symbols etc. – 50% of the students chose the first option because it was easier, despite knowing the second option provided better security. Equally, Bada and Sasse (2014) argue 'high

usability = low security' and 'high security = low usability' are preferable to most users. Quite possibly, there is a tipping point where the management of privacy becomes a hindrance to the practicalities and conveniences of using social media – especially when persuading users to perform what are perceived as tedious tasks (Furnell and Thomson 2009). Unlike 'network privacy' where expectations of harm are embedded in how the system is understood and used, here awareness of harm and countering harm are transient and pliable.

The following participant draws on generational observations on the potential dangers of social media and ultimately draws on traditional understandings of protection,

> *I was speaking to my Nan the other day …She's recently found out about Facebook and stuff. She said, don't use that because people have got a bad eye. …. so from a cultural point of view, it's like you're very private about photos … She was like, a bad eye and people don't even know they have it but they can look at the photo and really almost curse it without even realizing it. … I don't know. It's just an Indian thing.*
>
> *(Female, 33, stay-at-home mum)*

In this context, tradition dictates mother and baby stay in-doors and away from bad spirits for a number of days after birth, for the participant's Nan, placing photographs of children online heightens such potential risk. The participant has an awareness of superstition but still places the photographs online. For others certain interactions, as the following participant stresses, should remain within the privacy of the relationship,

> *I've seen, for example, in the last year, a couple, a guy and a girl that I've known for 15 years who were just friends, I've seen them get together and split up on Facebook. It's the most unedifying spectacle the way they've slagged each other off and all this kind of thing and you just like that's not the kind of conversations I want to be having in public.*
>
> *(Male, 45, PhD student)*

During a relationship breakdown emotions are high; however, there is a counter tension of sharing too much and as the participant suggests, it is 'unedifying' to witness the detail and vitriol of a conversation that for him should be conducted away from public audiences and in a private setting. In a similar vein, Anderson (2002) describes *Joe Dickens*, a lone father with unruly children who play on the street 'at all hours', his parenting and the behaviour of his children are frowned upon by his neighbours. Mostly because it disrupts the neighbourhood, but also because it goes against decency and what a family should do. Much like the examples here, there is a tension as to what is acceptable on social media and, more importantly, an acknowledgement of the consequences to posting particular information or behaving in potentially damaging or offensive ways.

Surveillance

The following participant mainly uses Facebook as a source of information,

> *Facebook, for example, very little goes up from me. I use it more to track what people are doing and where my friends are.*
> *(Female, 64, Charity project manager)*

Crawford (2009) describes this type of behaviour as 'lurking' and argues lurkers play an important role, one of the gathered audience, without whom social media has little impact. More accurately, perhaps, this is a form of 'social surveillance', where the masses watch the masses, thus instilling a sense of control on what users do online (Marwick 2012). Unlike more traditional 'top-down' forms of surveillance here self-policing and self-monitoring are peer generated. Yet, fears of being monitored by authorative organisations do prevail. The following participant stresses how his social media input is inhibited and self-censored due to his political allegiances and previous arrest,

> *I've put maybe over time one or two photos from demos up there, because I'm aware that I would have been noticed … I was arrested once on that demo just after the invasion of Iraq, … I would have been noticed before, just by my involvement in [protest] group … I'm not going to put anything politically rated on Facebook.*

(Male, 43, unemployed)

Users are at times aware of the incriminating evidence their posts can reveal, equally there is investigatory potential to social media users and fellow users can observe, monitor and report on illicit or untoward behaviours. The private investigator, below, refers to a commission from an insurance company seeking to verify certain information while processing insurance claims. As the participant states when starting to investigate a person he begins with genealogy websites to establish place of birth, date of birth, parent's names and the person's full name. His second source of information is social media, even when individuals do not have a social media presence:

> *I'll search for one of your brothers or sisters who's got an unusual name. I'll look at their friends' list. I'll find you. And again, even if you haven't got Facebook, one of your family will have. I say to people when they say, oh, you'll never find any photographs of me online. You say, have you been to a family party in the last ten years. And they go, yes. Anybody take your picture? Well, yes, but I haven't got anything online. No. But they have. It's not what you do. It's what everyone else does.*
>
> (Male, 49, Private Investigator)

Social media makes users visible in ways that may not always be immediately clear (Albrechtslund 2008; Trottier 2012; Trottier, 2013; Trottier and Lyon 2012) and audiences such as law enforcement agencies, marketers or fraudsters can easily circumvent privacy and security (boyd 2007). The quotes in this section offer examples of contextual collapse, as the information presented is used by a separate audience to trace and monitor the social media activities of the target person. The audience is one. Yet online representations are often exaggerated or controversial and so the verifying process afforded by social media allows others to view and make decisions on what may be 'real', acceptable or lawful (Anderson 2000: 313). Indeed, what can also be extracted from social media presentations are undeniable truths, such as evidence users were in a certain location when they claim to be elsewhere (as when GPS locators on Instagram positioned a Russian Tank in a prohibited area of Ukraine, see Szoldra 2014). Or, in the case of the private investigator proving someone was skiing when their insurance claim suggested they were having difficulty walking. This is the landscape of

social media where codes are orientated by worlds offline and online – and this may be an additional contextual collapse, where what is said online has repercussions offline. Moreover, controversies such as Cambridge Analytica further demonstrate (see Guardian 2018) - where the details of up to 50 million Facebook users was used without consent - that consent and privacy laws offer limited protections from surveillance of this nature, as social media companies have clearly abused their positions of guardianship toward users' data.

Codes of Privacy and Security

In moving towards a conclusion, I want to revisit the 3 codes highlighted and their relevance to Anderson's (2000) observations. As we have seen social media communications are at times immediate and reactionary, at other times attentive and careful - and this is the crux of privacy and security on social media. Repercussions of posting incendiary comments, or the 'bad eye', or posting about drug-use impact on the reputations, social currency and, in the case of the police officer, physical well-being of users. Codes of *presentation* demonstrate how users mobilise currency such as popularity or social connectivity (Daily, 2014) and are conscious of presentation to specific audiences (Khamis et al. 2017). Anderson would attest equivalent posturing is evident in the Code of the Street where the presentation of personas readily identifiable with violence and decency are forthcoming and used to strategic effect.

Codes of *protection* on social media demand vigilance because presentations may divulge sensitive and offensive messages to their audiences, as users stated, 'I probably should censor some things', 'the censor barriers just fell down'. For others, privacy and security is a tiring process, as alluded to by the 'fatigue' of the shop manager. In a networked privacy context, information is co-constructed (boyd, 2012) and users ensure levels and means of privacy by tailoring what they put online. They also make informed decisions, 'very little from me goes up', much like teenagers sanitizing Facebook comments because they know their parents are on their friend's list (see Marwick and boyd 2014). As

we have seen, things can, and do, go wrong which adds to the tension of social media. Knowing someone went to the zoo or knowing they were arrested on a demo impart detailed, personal and in-depth information. What for Anderson is 'the predatory influence of the street' (2000: 286), in the world of social media, can be seen in pressures to conform, putting information online that represents the image the user wishes to portray . Alternatively, when posting in states of turmoil or inebriation tension abound with ill-judged comment or comment that pays limited regard to a code of protection. Social media may be self-monitoring *extraordinaire*: on the one hand, it is the collection of data by organisations or the authoritative power of governmental agencies; on the other, users monitor their posts or observe the comments of others – as the adoptive father has done. Andrejevic (2009) speaks of 'digital enclosure' where every action generates information, and so nothing goes to waste. Indeed, social media offers much thought to monitoring and surveillance because social media quantifies in very real ways the opinions and thoughts of individuals precisely because the interactions of users become measurable, traceable and visible - and are ultimately never forgotten (Trottier and Lyon 2010). Equally as the private detective states, it is often not about what you do online, rather 'its what others do' that can expose details and indeed the management of your privacy moves beyond personal actions to those of acquaintances and platforms controllers.

Privacy management on social media can also be governed by adverse experiences or tailoring presentations to suit peers, family and/or audiences. This is the code of *surveillance* where users are aware of the expectation of audiences and perhaps remain aware of the damage an ill-conceived commentary can make. Nevertheless, activity is often out-weighted by the drive to communicate or, simply, cautionary intent wanes and fatigues. Anderson speaks of similar transitions when he refers 'Training Again' - when individuals move from the world of violence to the world of decency. For instance, when a one-time drug dealer decides to live a life inside the law and the skills of dealing on the street are redundant in their new interactions with their communities. Inevitably, the gravitas once held is lost as the threat of violence is reduced and the individual has to start again, normally in

low status positions of employment. For the once 'respected' drug dealer the transition is often difficult and the prospect of return to their old ways is high. In a similar way for some users their appreciations of security and privacy may follow trajectories that start with good intentions of being secure but through security fatigue are tempted toward a less protective or surveillance-aware outlook. Users, as we have seen, have experienced trouble online and the space of social media is where participants are exposed to risks, more so, than possibly elsewhere in their offline everyday lives. Being social media smart – i.e. avoiding trouble – is an intuitive or learned sense that has equivalences to 'street' astuteness, all of which highlights how social media users approach and adapt their online privacy and security.

Conclusion

Anderson's (2000) 'Code of the Street' is premised on challenging the notion that street violence is a random act with little or no formal reasoning to it. Instead he argues there is an organisational logic to the street. Anderson's observations are telling in highlighting the informal rules to how life functions in a run-down neighbourhood of Philadelphia and such a code is undoubtedly replicated in many communities. In the vain of Goffman (2002), Becker (2008) or Duneier and Carter (1999) the etiquettes of how 'things are done' presents rich material for the sociologist. Anderson's (2000) observations highlight what the informal code of a specific environment can bring to sociological understandings. This paper in turn has addressed how those who use social media are impacted by codes that guide their behaviours and understandings. These codes mirror Anderson's work in highlighting how specific populations make sense of their environments and learn how to interact within these settings. As we have seen security and privacy are influential to the intentions of social media users; often in ways that are visceral, in ways that change behaviours, or in ways that fatigue users. Nevertheless as the paper has argued these are the codes that help to highlight just how users navigate their security and privacy on social media.

The codes of presentation, protection and surveillance as have been used here demonstrate the associations users hold with privacy and security in their online lives. Additionally they highlight acceptances that if you are using social media then there are risks that you may cause offense, identify yourself to others or create 'unreal' presentations. These risks are off-set by the advancement and enjoyment of information received and relayed and we must not lose sight of the fun and communicative value of social media as this is an important component to its popularity and being. Where the 3 codes are helpful is in framing how these aspects are appreciated by users and in particular how users rationalise their actions and the consequences of these. In this regard, social media use demonstrates the projections of users as they seek to communicate and observe their audiences. While codes of protection are guided by shock or realisations of vulnerabilities to intrusion by audiences. Whereas codes of surveillance presents the underlying monitoring presence of social media and how this is understood and used by users. All of which offer a perspective on the erudition of users in making the choices they do. Key to this paper has been how privacy and security may guide those choices, and much like Anderson's decency and violence, these serve as beacons in the navigation process. Both offer indicators of what may happen and it is for the user or resident to comprehend how the environment functions and accordingly how they act within the codes of these environments.

References:

Abidin, Crystal. 2016. "'Aren't These Just Young, Rich Women Doing Vain Things Online?': Influencer Selfies as Subversive Frivolity". *Social Media+ Society 2*(2): 1-17.

Albrechtslund, Andreas. 2008. "Online social networking as participatory surveillance". *First Monday*, *13*(3).

Allmer, Thomas. 2014. "(Dis)Like Facebook? Dialectical and Critical Perspectives on Social Media". *Javnost - The Public: Journal of the European Institute for Communication and Culture* 21(2): 39-55.

Anderson, Elijah. 2000. *Code of the street: Decency, violence, and the moral life of the inner city*, New York: W Norton & Company

Andrejevic, Marc. 2006. "The discipline of watching: Detection, risk, and lateral surveillance". *Critical Studies in Media Communication* 23(5): 391-407.

Andrejevic, Marc. 2009. *iSpy: Surveillance and power in the interactive era*. Kanas: University of Kansas Press.

Acquisti, Alessandro and Ralph Gross. 2006. "Imagined communities: Awareness, information sharing, and privacy on the Facebook," pp 36-58 in *Privacy enhancing technologies, edited by* Georgr Danezis and Seda Golle, Heidelberg: Springer Berlin

Bada, Maria, Angela M. Sasse, and Jason RC Nurse. 2014. "Cyber security awareness campaigns: Why do they fail to change behaviour?." *arXiv preprint arXiv:1901.02672*.

Bailey, Jane and Val Steeves. 2015. *eGirls, eCitizens: Putting Technology, Theory and Policy into Dialogue with Girls' and Young Women's Voices*. Ottawa: University of Ottawa Press.

BBC. (2014) "Labour's Emily Thornberry quits over 'snobby' twee". Retrieved July 28, 2018 (https://www.bbc.co.uk/news/uk-politics-30139832).

Becker, Howard. 2008. *Outsiders*. New York: Simon and Schuster.

Berriman, Liam and Rachel Thomson. 2015. "Spectacles of intimacy? Mapping the moral landscape of teenage social media". *Journal of Youth Studies 18*(5):583-597.

boyd, dannah. 2007. "Why youth (heart) social network sites: The role of networked publics in teenage social life". *MacArthur foundation series on digital learning–Youth, identity, and digital media:* 119-142.

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

Browne, Kate. 2005. Snowball sampling: using social networks to research non-heterosexual women. *International Journal of Social Research Methodology* 8(1): 47-60.

Correa, Teresa. 2016. "Digital skills and social media use: how Internet skills are related to different types of Facebook use among 'digital natives'". *Information, Communication & Society*, *19*(8): 1095-1107.

Council of Europe. 2017. "European Convention on Human Rights. Article 8". Retrieved July 28, 2018 (http://www.echr.coe.int/Documents/Convention_ENG.pdf)

CNN. (2017). "2016 Presidential Campaign Hacking Fast Facts2. Retrieved January 15 2019 (http://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html)

Crawford, Kate. 2009. "Following you: Disciplines of listening in social media". C*ontinuum: Journal of Media & Cultural Studies 23*(4): 525-535.

Daily, Greg. 2014. "How NOT to Use Social Media Marketing". Retrieved July 28, 2018 (http://www.linkedin.com/today/post/article/20140624212655-92809450-how-not-to-use-social-media-marketing)

Davis, Edward, Alejandro Alves and David Sklansky, D. A. 2014. Social media and police leadership: Lessons from Boston. *Australasian Policing*, *6*(1): 1-24

Davis, Jenny and Nathan Jurgenson. 2014. "Context collapse: theorizing context collusions and collisions." *Information, Communication & Society* 17(4): 476-485

Díaz Sánchez, Laura. 2016. "Tinder and Grindr: a digital sexual revolution. Heterosexual and male homosexual stereotypes in mobile dating apps". Unpublished Masters Thesis: Utrecht University.

Denef, Sebastian, Petra Bayerl and Nico Kaptein NA. 2013. "Social media and the police: tweeting practices of British police forces during the August 2011 riots". In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*: 3471-3480.

Duneier, Mitchell, and Ovie Carter. 1999. *Sidewalk*. New York. Macmillan Press

Elias, Norbert and Edmund Jephcott. 1978. *The civilizing process* (Vol. 1). Oxford, UK: Blackwell.

Furnell, Steven, and Kerry Thomson 2009. "Recognising and addressing 'security fatigue'". *Computer Fraud & Security* 2009(11): 7-11.

Ellison, NB and boyd, dannah. 2013. "Sociality through Social Network Sites". Pp 151-172 in: The Oxford Handbook of Internet Studies, edited by William Dutton. Oxford: Oxford University Press: 151-172.

Gabriel, Fleur. 2014. "Sexting, selfies and self-harm: young people, social media and the performance of self-development". *Media International Australia*, *151*(1): 104-112.

Goldsmith, Andrew. 2015. "Disgracebook policing: social media and the rise of police indiscretion". *Policing and society 25*(3): 249-267.

Goffman, Erving. 2002. *The presentation of self in everyday life*. New York: Garden City.

Guardian. 2015. “Police criticised over spy-cam tweet of comedian Michael McIntyre in street”. Retrieved June 16, 2018 (http://www.theguardian.com/world/2015/jul/15/police-criticised-spy-cam-tweet-comedian-michael-mcintyre)

Guardian. 2015a. “Essena O'Neill quits Instagram claiming social media 'is not real life’”. Retrieved Jue 16, 2018. (https://www.theguardian.com/media/2015/nov/03/instagram-star-essena-oneill-quits-2d-life-to-reveal-true-story-behind-images)

Guardian. 2017. “WhatsApp must be accessible to authorities, says Amber Rudd”. Retrieved June 16, 2018. (https://www.theguardian.com/technology/2017/mar/26/intelligence-services-access-whatsapp-amber-rudd-westminster-attack-encrypted-messaging)

Guardian. 2018. “Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach”. Retrieved January 16, 2019 (https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election)

Hall, Jeffery. 2016. “When is social media use social interaction? Defining mediated social interaction”. *New Media & Society*: 1-18

Henderson, Samantha and Michael Gilding. 2004. “I’ve never clicked this much with anyone in my life: Trust and hyperpersonal communication in online friendships”. *New Media & Society*, 6: 487–506.

Huq, Numaan. 2015. “Follow the data: Dissecting data breaches and debunking myths”. Trend-Micro Research Paper. Retrieved June 16, 2018 (http://www.trendmicro.co.uk/media/wp/dissecting-data-breaches-wp-en.pdf)

ICO. 2014. Conducting privacy impact assessments code of practice. Information Commissioner’s Office. Retrieved June 16, 2018. (https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf)

ICO. 2018. GDPR: the Principles. Retrieved June 16, 2018 (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/)

Keane, John. 2013. *Civil society: Old images, new visions*. London: John Wiley & Sons.

Khan, Zeenath, Salma Rakhman and Aorhi Bangera, A. 2017. "Who Stole Me? Identity Theft on Social Media in the UAE". *Journal of Management and Marketing Review (JMMR)*, *2*(1): 79-86.

Khamis, Susie, Lawerence Ang, and Raymond Welling. 2017. "Self-branding,'micro-celebrity'and the rise of Social Media Influencers". *Celebrity Studies*, *8*(2): 191-208.

Lane, Jeffrey. 2019. The Digital Street. New York: Oxford University Press.

Lenhart, Amanda, Mary Madden, Aaron Smith, Kristen Purcell, Kathryn Zickuhr and Lee Rainie. 2011. "Teens, Kindness and Cruelty on Social Network Sites: How American Teens Navigate the New World of 'Digital Citizenship'". *Pew Internet & American Life Project*. Retrieved June 16, 2018. (http://files.eric.ed.gov/fulltext/ED537516.pdf)

Lupton, Deborah. 2016. *The quantified self*. London: John Wiley & Sons.

Luxton, David, Jennifer June and Jonathon Fairall. 2012. "Social media and suicide: a public health perspective". *American journal of public health*, *102*(S2):195-S200.

Madden, Mary, Amanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, Aaron Smith and Meredith Beaton. 2013. "Teens, social media, and privacy". *Pew Research Center* 21.

Mascheroni, Giovanna, Jane Vincent and Estefanía Jimenez. 2015. "Girls are addicted to likes so they post semi-naked selfies: peer mediation, normativity and the construction of identity online". *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 9 (1): 5.

Marwick, Alice. 2012. "The public domain: Social surveillance in everyday life". *Surveillance & Society*, *9*(4):378- 393

Marwick Alice and donnah boyd. 2010. “I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience”. *New Media & Society* 13(1): 114–133

Marwick, Alice. And donnah boyd. 2014. “Networked privacy: How teenagers negotiate context in social media”. *New Media & Society* 16(7):1051-1067

McDonald, Paula and Paul Thompson. 2016. “Social media (tion) and the reshaping of public/private boundaries in employment relations”. *International Journal of Management Reviews*, *18*(1), 69-84.

Murthy Dhiraj. 2012. “Towards a sociological understanding of social media: Theorizing Twitter”. *Sociology 46*(6): 1059-1073.

Nissenbaum, Helen. 2010. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford: Stanford University Press.

Nissenbaum, Helen. 2011. “A contextual approach to privacy online”. *Daedalus 140* (4): 32-48.

Noy, Chaim. 2008. “Sampling knowledge: The hermeneutics of snowball sampling in qualitative research”. *International Journal of social research methodology 11*(4): 327-344.

Patton, Desmond Upton, Robert D. Eschmann, and Dirk A. Butler. 2013. “Internet Banging: New Trends in Social Media, Gang Violence, Masculinity and Hip Hop.” Computers in Human Behavior 29(5):A54–A59.

Petronio, Sandra. 2012. *Boundaries of privacy: Dialectics of disclosure*. New York: State University of New York Press.

Quinn, Kelly and Papacharissi, Zizi. 2014. “The place where our social networks reside: Social media and sociality”. Pp 189-208 in *Media and social life* edited by Mary Beth Oliver and Arthur A. Raney. London: Routledge.

Sánchez Abril, Patricia, Avner Levin, and Alissa Del Riego. 2012. "Blurred boundaries: Social media privacy and the twenty-first-century employee." *American Business Law Journal* 49 (1): 63-124.

Sebescen, Nina and Jessica Vitak. 2016. "Securing the human: Employee security vulnerability risk in organizational settings". *Journal of the Association for Information Science and Technology* 68 (9): 2237-2247

Shin, Dong-Hee. 2010. "The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption". *Interacting with computers*, *22*(5): 428-438.

Smith, Gavin. 2016. "Companion Surveillance and Surveillant Subjectivities: On the Seduction of Seeing and Been Seen". *Media Fields Journal* 11

Smith, Gavin. 2016a. "Surveillance, Data and Embodiment On the Work of Being Watched". *Body & Society* 22(2): 108-139

Solove, Daniel, 2007. "I've got nothing to hide and other misunderstandings of privacy." *San Diego Law Review* 44 (2007): 745.

Solove, Daniel. 2015. "The meaning and value of privacy". Pp 71-82 in *Social Dimensions of Privacy: Interdisciplinary Perspectives,* editied by B Roessler and D Mokrosinska. Cambridge: Cambridge Uni. Press.

Stuart, Forrest. 2019. "Code of the Tweet: Urban Gang Violence in the Social Media Age". *Social Problems*, https://doi.org/10.1093/socpro/spz010

Szoldra, Paul. 2014. "A Russian Soldier's Instagram Posts May Be The Clearest Indication Of Moscow's Involvement In East Ukraine". *Business Insider*. Retrieved April 29, 2019 (https://www.businessinsider.com/russian-soldier-ukraine-2014-7?r=US&IR=T)

Tennant, Jaclyn, Michelle Demaray, Samantha Coyle and Christine Malecki. 2015. "The dangers of the web: Cybervictimization, depression, and social support in college students". *Computers in Human Behavior*, *50*: 348-357.

Tifentale, Alise and Lev Manovich, L. 2015. "Selfiecity: Exploring photography and self-fashioning in social media". Pp 109-22 in *Postdigital Aesthetics* edited by David Berry and Michael Dieter. London: Palgrave Macmillan.

Tilley, Nick. 2014. *Crime prevention*. London: Routledge

Trottier, Daniel and David Lyon. 2012. Key features of social media surveillance. Pp 109-125 in Internet *and Surveillance*, edited by Christian Fuchs, Kee Boersma, Andreas Albrechtslund, and Manisol Sandoval. London: Routledge.

Trottier, Daniel. 2013. *Social media as surveillance*. Farnham: Ashgate

Trottier, Daniel and Christian Fuchs (2014). *Social media, politics and the state: Protests, revolutions, riots, crime and policing in the age of facebook, twitter and youtube*. London: Routledge.

Tuten, Tracey and Michael Solomon. 2014. *Social media marketing*. London: Sage

Vitak, Jessica. 2012. "The Impact of Context Collapse and Privacy on Social Network Site Disclosures". *Journal of Broadcasting & Electronic Media*, 56:4: 451-470

Wegner, Trevor. 2010. *Applied business statistics: Methods and Excel-based applications*. Cape Town: Juta and Company Ltd.

Wise, Jacqui. 2016. "Anxiety in teenage girls rises sharply in past decade, finds study". *BMJ*, *354*, i4649.

Urbanik, Marta-Marika, and Kevin D. Haggerty. 2018. "'#It's Dangerous': The Online World of Drug Dealers, Rappers and the Street Code." *British Journal of Criminology* 58(6):1343–1360.

Uldam, Julie. 2016. “Corporate management of visibility and the fantasy of the post-political: Social media and surveillance”. *New Media & Society* 18 (2): 201-219

Yang Chao, Robert Harkreader, Jialong Zhang, Seungwon Shin and Geofei Gu. 2012. “Analyzing spammers' social networks for fun and profit: a case study of cyber-criminal ecosystem on twitter”. *Proceedings of the 21st international conference on World Wide Web*: 71-80.