**Putting everything up there: navigating social media privacy and security.**

**Abstract**

In this paper I consider the work of Anderson (2000) and his Code of the Street, and use this to frame how we might begin to draw comparisons between life on the street and life on social media. For Anderson the Code of the Street is used to communicate how to avoid or confront violence; here I want to apply his framework when reviewing the influence of data privacy and security on social media activity. 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 experiences of social media privacy and security.

**Key words:**

Code of the Street, Social Media, Privacy, Security, Tensions,

**Correspondence**: Keith Spiller, Department of Criminology, Curzon Building, Birmingham City University, B4 7BD. Email: [keith.spiller@bcu.ac.uk](mailto:keith.spiller@bcu.ac.uk)

ORCID: 0000-0002-5796-8165

**Acknowledgement:** This work was part of the European Commission FP7 project Increasing Resilience in Surveillance Society (Project ID: [290492](http://cordis.europa.eu/project/rcn/101866_en.html)).

**Introduction**

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). The goal of this paper is to consider security and privacy as an influence on social media users, an influence that often rests between celebrations of its communicative value and the dangers that lurk within. And this is where Anderson’s findings may be informative in establishing how users learn and use this knowledge to navigate the terrain of social media. What I propose in this paper is that we can use Anderson’s framework to enhance understanding of social media. 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.

To date, commentary on social media has emphasised its worth as an enabler of communication and the social consequences of this (Gerbaudo, 2018; Murthy, 2012; Shoemaker and Reese, 2013) – for instance how it was used to propagate the Arab Spring (Khonder, 2011) or the Occupy movement (Juris, 2012). Yet, sociological critique of social media has often centred on the weakening of sociability as social bonds and face-to-face interactions are transferred to online communications (Byron et al., 2013; Murthy, 2012). 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 visualize 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 the social media ‘star’, reactions of audiences, being paid for product placement and fame may entice participation. Users share information to gain ‘attention’ from networked audiences (Abidin, 2016; Díaz Sánchez, 2016) and, in parallel, social media is propelled by a constant hunger for the flow and input of ever-new information. Alternative work has also considered the harms of bullying, harassment, self-harm and suicide provoked through social media use (Gabriel, 2014; Luxton et al., 2012; Wise, 2016) or the dangers of ‘perpetual contact’, ‘hyper-coordination’, not being able to ‘switch-off’, bullying or grooming (Berriman and Thomson, 2015; Hall, 2016; Madden et al. 2013; Tennant et al., 2015). These are not the dangers of the ‘street’, but they do nevertheless reverberate with the loitering menace present in online environs. By teenage-hood most in Anderson’s neighbourhoods have internalized the Code of the Street and are keenly aware of how to operationalise this knowledge to avoid violence (Anderson, 2000, p.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 communication or risky and manufactured behaviours that expose personal or compromising information (Bailey and Steeves, 2015; Shin, 2010). In short, (and as I expand subsequently) there is a code to social media that prescribes how users navigate privacy and security risks.

Privacy and security on social media

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 EC, 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, as Lupton (2016) argues ‘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. 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.

Previous work has considered privacy and security of personal data; 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 example, 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 acclimatize 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, p.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)

New Media commentators such as Petronio (2012) have used the metaphor of the *boundary* to explain the choices made when sharing information. As she proposes 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. And so 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 observations and research interviews with social media users (see below) and the codes focus on *presentation*, *protection* and *surveillance*. Firstly, the code of presentation is an important component to the Code of 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, 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, p.73).Thus, the presentation on the street formulates uniformity as to how one should present oneself if a particular expectation is required (Allmer, 2014; Bailey and Steeves, 2015; Miller, 2011). Central to participation on social media is generating an online presence and profile, one that often details users’ identity, preferences and past-times. In addition, gossip, eavesdropping, sharing, and watching are all elements of social media and do 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. A code of presentation that I would argue directs the behaviour of users.

Secondly, a code of protection on the street can be understood in terms of ‘I got yo’ back’ (Anderson 2000, p. 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. Social media ‘success’ more often than not is viewed through the amount of followers a user has - the premise being the greater number of followers the bigger their appeal and influence (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 routinized 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 and 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 is determined by detailing, for instance, 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) and 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). Or, governmental calls 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 and demonstrate how users navigate their social media.

**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 and 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, but 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. The paper is based on 27 interviews with a diverse range of users; for instance, participants were aged between 18 and 70, and the gender balance was 15 male and 12 female. 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 date of birth and home address. She acknowledges her information should be censored; yet the urge to share intimate 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)*

There are social etiquettes which influence personal interactions, such as not goading friends for amusement, and the dilemma here mirrors Anderson’s tension 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 it associated disadvantages. Therefore knowing how to utilize codes to traverse the worlds of decency and violence can be tactically calibrated for those who Anderson suggest are ‘smart’ and offer presentations that are ultimately acceptable to decent and street audiences (see Anderson 2000, p98). Code-switching, as Anderson calls it, or a dexterity to personal images and behaviours in social media highlights the juxtaposition of offline/online etiquette that can be troublesome for those who offer offensive comment or personal information. In extreme examples vitriolic, violent and offence online comment has resulted in jail time for users (see BBC 2012), however users do maintain the balance between engaging their audience and staying within the realms of acceptable and safe behaviour.

Protection

The user below is careful not to advertise; he uses an assumed name on Twitter and avoids Facebook. This is a precaution against those he may have previously arrested finding him and indeed the threat of physical violence,

*I don’t particularly want to have somebody banging on my door, so I’m not on Facebook.*

*(Male, 62, retired police office)*

This it appears is an underlying tension related to the privacy and security of social media communication or more precisely the effects of how social media information affects how others view a person, as well as the potential physical harms that it may encourage. Common to 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)*

Evident is the shock felt when information posted on social media is accessed and visualised by a fellow user. For this participant, details of a family outing were not something she was willing to share with a colleague she did not know. Following the event the user reset her privacy setting and is now ‘much more careful’.

Being aware of who can view social media communications stimulates awareness in users and also highlights the tensions users may experience. Equally, diligence and protecting information can be strenuous (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)

Account hacking can lead to accessing to private information or posting fraudulently (Harding 2015). 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 is 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 should be sacrosanct and 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. 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 in what is acceptable on social media and more importantly an acknowledgement of the consequences to posting particular information and the challenges brought to their security and privacy or to what is deemed acceptable by other users.

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. However ‘social searching’ or viewing the profiles and posts of those known, or not, can be problematic for those contributing to social media (Heidemann et al*.,* 2012). The following participant stresses how his social media input is inhibited and also 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 and 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). In effect, the code of surveillance includes those in positions of authority, but also those who are audiences on social media. The participant below, is an adoptive parent, and social media allows him to view the activities or opinions of his child’s birth mother. He comments,

*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, CG9)*

To search and observe (within privacy settings and the law) is not unusual; yet in this instance a contradiction of sorts maybe evident. Curiosity was a motive to the search and its results made an impression on the father. Yet, the father was instructed not to make his child visible to the same kind of search which he completed. Here there is a very real example of contextual collapse, the information presented by the birth mum delivers a message that, quite possibly, was for an audience she knew, but also to one she did not recognise, was unaware of or one she did not care about. This is the landscape of social media where the understanding of its codes are orientated by worlds offline and online. The online presents representations of activities that one ‘shouldn’t’ be doing or imagery that is exaggerated or controversial, and so the verifying process afforded by social media allows other to view and make decisions on what may be ‘real’ or acceptable (Anderson 2000, p313). This in turn influences the offline worlds of social workers or insurance claims and their interpretation of the code.

**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 mobilize currency such as popularity or social connectivity (Daily, 2014), like Goffman’s front and backstage (2002), the world of social media is conscious of presentation to specific audiences. While presenting information, images or narrative online can be potentially edited (Smith 20016a; 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, p.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 lacks 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. As we have seen, the privacy management of being online and communicating incites tensions often stemming from adverse experiences. What, however, also remains are the surveillances where users choose to be aware of the openness of social media. Editing of comments, airing grievances, boasting of exploits and many other forms of expression are tailored to suit peers, family and/or audiences and while at times of hyper-awareness the code of *surveillance* is pressing, it also has the potential to wane and to fatigue those who participate. 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 curtailed or made redundant in their new dealings 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. Moreover social media offers a tool to monitor, verify or assess the activities and opinions of other users.

**Conclusion**

I began the paper by highlighting the influence privacy and security may hold on social media use. The 3 codes I have introduced offer an opportunity to examine the consequences and/or the adaptations of using social media in these terms. The current social media literatures contemplate the undoubted benefits of this form of communication, as well as the risks and vulnerabilities it may provoke. Yet what this paper has addressed is how those who use this medium are impacted by codes of social media. These codes as I have emphasised mirror Anderson’s work in highlighting how specific populations make sense of their environments and learn how to interact within these settings. In some instances, aspects of privacy and security have made users think differently about how they interact on social media. Anderson’s 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, residents acquire and learn knowledge that allows them to function on the street. As we have seen security and privacy are influential to the intentions of social media users in ways that are visceral, in ways that change behaviours, or in how users ignore are fatigues by these influences. However as the paper has argued these are the codes that can help to highlight how users navigate their security and privacy on social media.

**References:**

Abidin, C. (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, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3).

Allmer, T. (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, E., (2000). *Code of the street: Decency, violence, and the moral life of the inner city*, New York: W Norton & Company

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

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

Acquisti, A and Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In: Danezis G and Golle P (eds.) *Privacy enhancing technologies*. Heidelberg: Springer Berlin: 36-58.

Bada, M; Sasse, A. (2014). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? Global Cyber Security Capacity Centre, University of Oxford: Oxford. Retrieved from <http://discovery.ucl.ac.uk/1468954/>.

Bailey, J., & Steeves, V. (2015). *eGirls, eCitizens: Putting Technology, Theory and Policy into Dialogue with Girls’ and Young Women’s Voices*. University of Ottawa Press: Ottawa.

BBC. (2012), ‘Fabrice *Muamba: Racist Twitter user jailed for 56 days*’. Retrieved from <http://www.bbc.co.uk/news/uk-wales-17515992>

BBC. (2014) Labour's Emily Thornberry quits over 'snobby' tweet.Retrieved from <https://www.bbc.co.uk/news/uk-politics-30139832>

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

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

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

Byron, P, Albury, K, and Evers, C. (2013). It would be weird to have that on Facebook: young people's use of social media and the risk of sharing sexual health information. *Reproductive health matters* *21*(41): 35-44.

Correa, T. (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 from <http://www.echr.coe.int/Documents/Convention_ENG.pdf>

CNN. (2017). 2016 Presidential Campaign Hacking Fast Facts. Retrieved from <http://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html>

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

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

Daily, G. (2014) How NOT to Use Social Media Marketing. Retrieved from <http://www.linkedin.com/today/post/article/20140624212655-92809450-how-not-to-use-social-media-marketing>

Davis J and Jurgenson N (2014) Context collapse: theorizing context collusions and collisions, Information, Communication & Society, 17:4: 476-485

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

Denef, S, Bayerl, PS and 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.

European Commission. (2018). Data Protection. Retrieved from <https://ec.europa.eu/info/law/law-topic/data-protection_en>

Elias, N., & Jephcott, E. (1978). *The civilizing process* (Vol. 1). Oxford, UK: Blackwell.

Furnell, S., and Thomson, K. L. (2009). Recognising and addressing ‘security fatigue’. *Computer Fraud & Security*, *2009*(11): 7-11.

Ellison, NB and boyd, d. (2013). Sociality through Social Network Sites. In: Dutton, W. H. (Ed.), The Oxford Handbook of Internet Studies. Oxford: Oxford University Press: 151-172.

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

Gerbaudo, P. (2018). *Tweets and the streets: Social media and contemporary activism*. London: Pluto Press.

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

Goffman, E. (2002). The presentation of self in everyday life. *Garden City, New York.*

Guardian. (2015). Police criticised over spy-cam tweet of comedian Michael McIntyre in street. Retrieved from <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 from <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 from <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 from <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

Hall, JA. (2016). When is social media use social interaction? Defining mediated social interaction. *New Media & Society*: 1-18

Harding, K. (2015). How to Protect Your Health Agency or Organization Against Social Media Hacking. In *2015 National Conference on Health Communication, Marketing, and Media: August 11-13*.

Heidemann, J, Klier, M and Probst F. (2012). Online social networks: A survey of a global phenomenon. *Computer Networks* *56*(18): 3866-3878.

Henderson, S and Gilding, M. (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.

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

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

Juris J S. (2012). Reflections on# Occupy Everywhere: Social media, public space, and emerging logics of aggregation. *American Ethnologist* 39(2): 259-279.

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

Khamis, S., Ang, L., & Welling, R. (2017). Self-branding,‘micro-celebrity’and the rise of Social Media Influencers. *Celebrity Studies*, *8*(2): 191-208.

Khonder, HH. (2011). Role of the New Media in the Arab Spring. *Globalizations* Vol 8 (5): 675-679

Lenhart, A, Madden, M, Smith A, Purcell K, Zickuhr, K and Rainie L. (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 from <http://files.eric.ed.gov/fulltext/ED537516.pdf>

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

Luxton, D. D., June, J. D., and Fairall, J. M. (2012). Social media and suicide: a public health perspective. *American journal of public health*, *102*(S2):195-S200.

Madden, M, Lenhart, A, Cortesi, S, Gasser, U, Duggan, M, Smith A and Beaton, M. (2013). Teens, social media, and privacy. *Pew Research Center* 21.

Mascheroni, G, Vincent, J and Jimenez, E. (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, A E. (2012). The public domain: Social surveillance in everyday life. *Surveillance & Society*, *9*(4):378- 393

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

Marwick, A.E. and boyd d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society* 16(7):1051-1067

Miller, D. (2011). *Tales from Facebook*. London: Polity.

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

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

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

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

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

Sebescen, N., and Vitak, J. (2016). Securing the human: Employee security vulnerability risk in organizational settings. *Journal of the Association for Information Science and Technology*. Early view

Shoemaker, P. J., & Reese, S. D. (2013). *Mediating the message in the 21st century: A media sociology perspective*. Routledge.

Shin, D. H. (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, G.(2016). Companion Surveillance and Surveillant Subjectivities: On the Seduction of Seeing and Been Seen. *Media Fields Journal* 11

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

Solove, D. J. (2015). The meaning and value of privacy. In Roessler, B and Mokrosinska, D (eds.) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (pp71-82). Cambridge: Cambridge Uni. Press.

Tennant, J. E., Demaray, M. K., Coyle, S., & Malecki, C. K. (2015). The dangers of the web: Cybervictimization, depression, and social support in college students. *Computers in Human Behavior*, *50*: 348-357.

Tifentale, A., & Manovich, L. (2015). Selfiecity: Exploring photography and self-fashioning in social media. In *Postdigital Aesthetics* (pp. 109-122). Palgrave Macmillan, London.

Tilley, N. (2014). *Crime prevention*. London: Routledge

Trottier, D. and Lyon, D. (2012). Key features of social media surveillance. In Fuchs, C., Boersma, K., Albrechtslund, A., & Sandoval, M. (Eds.) *Internet and Surveillance* (pp. 109-125). London: Routledge.

Trottier, D. (2013). *Social media as surveillance*. Farnham: Ashgate

Trottier, D., & Fuchs, C. (Eds.). (2014). *Social media, politics and the state: Protests, revolutions, riots, crime and policing in the age of facebook, twitter and youtube* (Vol. 16). London: Routledge.

Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New media & Society*, *20*(1): 141-161.

Tuten, T. L., and Solomon, M. R. (2014). *Social media marketing*. London: Sage

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

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

Wise, J. (2016). Anxiety in teenage girls rises sharply in past decade, finds study. *BMJ*, *354*, i4649.

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

Yang C, Harkreader R, Zhang J, Shin S and Gu G. (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.