NOVA

University of Newcastle Research Online

nova.newcastle.edu.au

Fulton, Janet M.; Kibby, Marjorie D.; "Millennials and the normalization of surveillance on Facebook". Published in *Continuum: Journal of Media and Cultural Studies* Vol. 31, Issue 1, p. 189-199 (2017)

Available from: <http://dx.doi.org/10.1080/10304312.2016.1265094>

This is an Accepted Manuscript of an article published by Taylor & Francis in *Continuum: Journal of Media and Cultural Studies* on 7/12/16, available online:

<http://www.tandfonline.com/10.1080/10304312.2016.1265094>

Accessed from: <http://hdl.handle.net/1959.13/1353608>

Millennials and the Normalisation of Surveillance on Facebook

While surveillance is usually understood as the purposeful monitoring of individuals by those in authority (Lyon 2007), Albrechtslund (2013) describes a type of surveillance where people willingly keep watch on each other through social media, calling it 'participatory surveillance'. An anonymous focus group and online survey of 81 Australians categorised as part of the Millennial Generation investigated their experience of both authority and participatory surveillance on Facebook, that is, their awareness of the level of surveillance they themselves are under and their surveillance of others. The results reveal that this group are generally concerned about privacy and security for their personal information, though not always sure what they should do to ensure it, and that they are willing to access and distribute the personal information of others. They generally feel that protecting their information from individuals and from the government is a greater concern than ensuring privacy from commercial entities. However this group believe that a reduction in privacy, on and off line, is part of contemporary life, and giving up some information is necessary to participate in the online environment. Social media's participatory surveillance appears to be preparing young people for a lifetime of being watched, by helping to re-define understandings of privacy.

Keywords: Facebook; Millennials; privacy; security; social media; surveillance

Introduction

Social media use is dependent on users' self-disclosure of personal information. Facebook facilitates the sharing of ideas and experiences for an amorphous audience by encouraging 'posts' or updates, enabling a visibility of personal details that goes beyond that which would typically be available to acquaintances (Trottier 2012). 'Status updates' imply constancy in posting and 'life events' normalise the sharing of milestones. Even if there has been no change in status or any life events, Facebook encourages the sharing of 'photos/videos' and these suggestions for posts combine to encourage a flow of personal information. Responses to posts rarely become a two-way

exchange. In using Facebook as a vehicle for staying in touch with personal networks, relationships become more like surveillance as users watch and comment on the activities of others rather than directly communicating with one another (Trottier 2012).

Surveillance practices go beyond facilitating online social networking to actually constitute it, as users continue to return to the site to update their own profiles, or to stay current on others' activities. Self-disclosure is at the core of Facebook interaction, as users present themselves through the release of information about their preferences, histories, activities and opinions. Facebook is synonymous with surveillance; information is currency in the digital age, and governments are not the only ones interested in harvesting it. A number of organisations and services collect and use the information in Facebook (Lee and Cook, 2014), often without the knowledge of the users, even if they have inadvertently consented to its harvesting. Institutions and agencies watch over targeted populations as social media enable law enforcement to focus on suspects rather than activities. Commercial interests watch over their markets, finding Facebook an effective tool for connecting with consumers and identifying market trends. And individuals watch over each other.

Individuals watching each other constitute a variation on traditional surveillance patterns of top-down monitoring of citizens by the state. The peer-to-peer surveillance of partners, friends and relatives is a social surveillance and individuals' online visibility, and their concurrent watching of others, has a social function (Marwick 2012), strengthening connections rather than overtly influencing behaviour. Foucault (1977) used Bentham's panopticon as a metaphor for an assumed surveillance that led subjects to internalise power relations and modify their behaviour to conform. Contemporary surveillance practices complicate this metaphor. While the level of surveillance in society has undoubtedly increased, some forms such as peer surveillance

do not appear to have a regulatory function. Everybody is encouraged to watch and be watched, leading to a series of 'Little Brothers' (Chalkley 2012). In Chalkley's words, 'the modern panopticon is dispersed' (2012, 206) and he uses the term 'omnopticon' to suggest we live in a state of constant mutual surveillance. Social media such as Facebook has introduced a new dynamic into watching others. Rather than the few watching the many, the panopticon model, or the many watching the few, the synopticon model of broadcast media, social media is an omnopticon where the many watch the many (Siapera 2012).

Engaging with social media such as Facebook involves negotiating the benefits and risks of information sharing. While there may be a level of sensitivity towards the loss of privacy, this loss is a necessary component of status seeking through sharing personal information. Users maintain a trade-off between protecting their privacy and performing their identity in posting personal information online (boyd and Hargittai 2010). The risk of misinformation or adverse information being circulated is balanced by the ability to receive immediate updates of changed circumstances, to be the first with the latest social news. Immediacy has become a major component of the Internet experience for the Millennial Generation (Lee and Cook 2014, 1), defined as those born between 1982 and 2000 (Howe and Strauss 2009), and privacy seems to be willingly traded for immediacy. The leaking of information from one context to another may create a risk of embarrassment, or worse, but it gives access to a breadth of personal information on others, information that is usually not available in discrete offline contexts. The cross contextual exchange of information becomes a condition that users manage, rather than a threat of public exposure (Trottier 2011).

The term 'privacy' is an umbrella term, referring to a wide and disparate group of related concepts dependent on culture and context (Solove 2008). In Australia, as in

other societies based on an individualist cultural model, the concept of privacy refers to a person's ability to control access to information about them and to have exemption from, or limitations on, scrutiny, surveillance, or interference (Margulis 2003).

Solove's (2006) taxonomy of privacy lists the same components: information collection, information processing, information dissemination, and invasion, which Sandra Petronio (2012) collectively defines in describing privacy as a feeling that one has the right to own personal information. Petronio's communication privacy management theory maps the ways that people navigate privacy, showing how privacy boundaries guard information that individuals have but others don't know, and the ways that these boundaries are either protected or relaxed. While privacy supports ontological security, information disclosure can strengthen relationships and build social capital, so privacy boundary negotiation and maintenance is a continual process.

The use of online social networks involves a complexity of understanding and maintaining privacy, as it involves the sharing of personal information in a public forum while maintaining control of that information. In Facebook, 'privacy is not about being anonymous' (Albrechtslund 2013, 317). In fact, Facebook requires users to provide the name they use in real life. Users want to share information on their personal lives, but protect their privacy by having their information reach only the intended audience. The issue of privacy, therefore, is more about monitoring who sees a personal profile and how much information they see (Tufekci 2008) rather than inhibiting disclosure of information. Users who want to share personal information online face a dilemma between potential privacy risks and the gratifications that come from sharing this information. Practices to protect privacy in social networks are paradoxical, as content-sharing behaviour conflicts with attempts to reduce the negative consequences of disclosure. This conflict results in boundary turbulence, to use Petronio's (2012) term,

as the boundary between public and private becomes permeable, and individuals rework their personal privacy rules. Most users reconcile a loss of conventional privacy with the benefits of participating in online social networks and rationalise any privacy violations as a normal part of social media visibility (Trottier 2012).

This study of Australian students aged 18-34 (Millennials) asked them about their use of Facebook to uncover the extent to which that use constituted a 'normalization of social media visibility' (Trottier 2012, 321). Howe and Strauss (2009) are widely credited with naming the millennial generation, identifying them as those born between 1982 and 2000. Millennials are the first generation that has not known life without digital media and their lives have been profoundly affected by the online space. They are highly active, in both work and play, on social media platforms and contribute, share, search and consume content on those platforms (Bolton et al. 2013). They also constitute the demographic with the highest presence on Facebook. While Facebook's users have expanded from the original teens and university students, and there is evidence that young people are moving from Facebook to other social media applications, the 16 to 24-year-old and 25 to 34-year-old demographics are still the major users of Facebook internationally (Statista 2015) and in Australia (Sensis 2015). While the number of older users is increasing, young people log on more frequently and have larger friend networks than older users.

There is a significant body of research on university students' social media use, however much of it is focused on the United States (**see for example, Alt 2015; Bolton, et al. 2013; Paradise 2012; Park & Lee 2014; Sheldon 2008; Tandoc, Ferrucci & Duffy 2015; Wang et al. 2015**) with very little exploring usage in regions such as Australia, and there are indications that Australian use patterns cannot be assumed to parallel those in the US (Nicol 2014; Winkels 2014). While there are no

published comparisons, the differences in technological infrastructure, service provision, and youth culture make it difficult to align Australian practices with American research. Analysis of the data, gathered via an online survey and online focus group, identified four key themes around surveillance and privacy: these students are generally concerned about privacy and security for their personal information, though not always sure what they should do to protect it; they take obvious steps to protect their privacy, but are not aware of all the situations that pose a threat; the students feel that privacy from individuals (latent axe murderers and vengeful exes) and from the government (Tax Office, ASIO, and the police) is a greater concern than privacy from commercial entities (Facebook, eBay); and the students believe that giving up some information is necessary to use social media, applications, and games, and a reduction in privacy is part of contemporary life.

Methodology

Following on from an analysis of how students at the University of Newcastle in Australia developed a sense of belonging through peer surveillance on Facebook (Kibby and Fulton 2014), this project examines the broader impact of peer surveillance on attitudes and practices. The researchers used connective ethnography (Hine 2007) and employed a mixed method approach with an analytical framework derived from Petronio's (2012) theories of boundary management in the protection of privacy, and Foucault's (1977) notion of the surveillant gaze as a relationship that is entered into. An online survey used a Likert scale to collect nominal data on the likelihood of participants engaging in a range of surveillance practices on Facebook and on their attitudes to personal surveillance in both online and offline spaces. An asynchronous online discussion forum was used to conduct an unstructured focus group where participants were able to raise their own opinions and experiences of surveillance and

respond to the ideas of others. The survey and focus group forum were made available to participants for the month of October in 2014. Participants in both were recruited from the same pool of students from two courses that teach digital communication and social media. The cohort included students from a broad range of study programs including communication studies, cultural studies, visual communication, arts, teaching, business, law, information technology, engineering, social work, and the sciences. The participants were drawn from first year through to final year students and ranged in age from 18 to 34-years-old.

Online data collection has a number of disadvantages. Among these is the tendency for mode effects where the method has an impact on who responds and how they respond, with net-savvy participants more likely to take part, and to engage more fully (Jackman 2005). Self-selected respondents to an online survey can introduce bias. In addition, there are limitations on the ability to determine whether respondents belong to the target population, and online methods often have low response rates. Identifying university students as the target population for this study reduced some of the disadvantages: as participation was limited to a specific group, all those invited to participate had similar web skills, they could be contacted as a group to encourage involvement, and with more people participating in the survey, the bias would be smaller. The population selection was legitimised by the fact that college students remain the dominant demographic amongst Facebook users (Paradise 2012) and over 90% of college students have a Facebook profile (Sheldon 2008). Participants were further restricted to the so-called Millennials, a group that is seen to rely on social media to communicate and build community (Rainie, Horrigan, Wellman and Boase 2006). While this non-probability convenience sampling cannot be used for statistical inference about a broader population, the results can be seen as indicative of the

attitudes and behaviours of Australian Millennial Generation university students and provides a base for further research in the area.

Eighty-one students completed the online survey. Of those 81, one respondent was excluded as being over the age limit. Respondents were asked to give their nationality to test whether those from the University's international campus or who were exchange students had different perceptions. However, only three students described themselves as other than Australian, so their responses were excluded. This left 77 valid responses to include in the dataset. The survey URL was advertised to 300 students, which gave a response rate to the survey of 25.7%. Fowler states that '[t]here is no agreed-upon standard for a minimum acceptable response rate' (2009, 51) and points out that '[n]ot every effort to gather information requires a strict probability sample survey' (2009, 14). The aim of this study was to gain a sense of contemporary students' attitudes towards surveillance, and an indication of the types of practices they engage in to keep track of their peers and control their own privacy. The goal was not to generate statistics on the impact of Facebook on the normalisation of surveillance, but to illustrate the actions and opinions of the participants, and not to quantify the impact of social media on the perceptions of surveillance.

Likert scale survey questions covered several areas: how do the respondents use social media; how do they manage their own presence online; how do they interact with others online (including family, friends and strangers); and what do they think about the way their data is used by other individuals and agencies. The survey was managed through Survey Monkey and responses were analysed using SPSS software. Survey Monkey software allowed the researchers to embed the survey into course management software for student ease of access as well as to ensure anonymity.

While the online survey had general advantages in terms of cost and convenience, using the online environment for focus group discussions provided specific advantages over face-to-face discussions. While anonymity meant that it was difficult to identify if the same students participated in the forum and completed the survey, the anonymity of the online environment mitigated pressure to conform to group opinions and any influence from inadvertent feedback from the moderator. The online forum also meant participants were able to contribute well-thought-out written responses, and the time frame for participation allowed for reflection and subsequent comment. To ensure anonymity, personal identifiers including Internet Protocol (IP) addresses were never recorded for either the online survey or focus group, with consent acknowledged by simple click-through to the survey and discussion via course management software.

The online forum used the university course management software, Blackboard. Having explored other alternatives such as Yahoo Groups and Google Hangouts, Blackboard discussion forums were selected as participants could use an existing account, they are familiar with this format for online discussion, and it is the only forum that allows complete anonymity. The researchers posted a discussion starter and participants posted on their experiences and opinions, with no intervention from the researchers. The focus group forum allowed contributors to begin a thread on any aspect of surveillance via social media and respond to the posts of others. Sixty-four students participated in the forum and these comments were analysed for common themes. Students' responses in the forum have not been edited and spelling, punctuation and grammar are quoted as originally posted.

Results and Discussion

Concern about Security

Survey respondents' views differed on how their own social media data is used by various stakeholders, including employers, the Australian government, law enforcement agencies, and Facebook and other commercial users, depending on the source of the surveillance. Social network sites are seen as a perfect convergence between 'personal communications and mutual surveillance, public relations and workplace surveillance, criminality and opportunistic surveillance, data-mining and state surveillance, social movements and activist surveillance' (Athique 2013, 225). So social media involves a range of agencies involved in a continuum of personal monitoring from generally benign information collection to a controlling surveillance. A high percentage of the participants showed concern with how these surveillance agencies collect and use available social media data, however the level of concern depended on the agency collecting it with stakeholders such as telecommunication companies (telcos) and employers causing a relatively high level of concern while commercial entities such as Facebook, and governmental agencies such as the police, are less of a worry.

Participants are concerned or extremely concerned if potential or current employers ask to access their social media profiles although the level of concern differed (potential employers: 80.5%; current employers: 75.3%). It seems that these respondents are not as apprehensive about potential employers accessing their Facebook profile: only 10% of respondents are extremely concerned if a potential employer asks for access while almost 20% are extremely concerned if their current employer asked for access. These figures suggest, perhaps, that potential employers are seen to have a more legitimate reason to collect information via social media. **The level of concern, though, may also be a result of the different power/knowledge relationships**

involved, and the relative importance of the connections with current employers and potential employers.

Respondents are less concerned with Facebook providing details of demographic categories, life events, hobbies and interests to consumer data firms with almost a quarter (23.4%) not concerned at all. McChesney (2013) calls this the commercialisation of friendship and the online forum contains several comments that show acceptance of Facebook on-selling personal details while displaying a concern at the amount of information collected:

People act like it is a massive abuse that the service providers are selling our info - info that we freely give. Google/Facebook aren't altruistic companies, and they need to make the money somehow. Of course they are going to try and get as much information as possible.

All of the sites I use like Facebook and twitter, it does hunt you down to the exact street you are standing on which is crazy to me. Even though I feel uncomfortable about it, I still use the sites anyways regardless of being tracked down.

Almost 90% of survey respondents are concerned or extremely concerned that telcos would be asked to retain data, including phone and online records such as Facebook, for the use of law enforcement agencies and government. While the respondents are wary of law enforcement access to their data, there is a lower percentage that worries about the Government accessing Facebook accounts with almost a fifth (18.2%) not at all concerned. A reason for this difference in levels of concern could be the public debate on increased surveillance through data retention on behalf of law enforcement agencies, proposed to assist in combating terrorist threats. This debate was happening at the time with a high amount of media attention, which means that students could have been more aware of the issue of data retention.

While survey respondents were concerned that telcos would collect their personal information they were less concerned that government or commercial organisations would do so. The boundary turbulence (Petronio 2012) around telcos may be a result of a limited understanding of why this information is being collected, and the scope of its processing and dissemination, and an underlying fear that it could result in a level of interference in their online activities. There were, however, comments in the focus group forum that revealed a concern about government collection and use of data:

... companies that I use for free using my data to remain profitable, no real problem so long as they aren't selling to the mafia. Government access to this data, big no no. Main difference in my mind is that the government has executive power. They 100% have the ability to make you disappear for lack of better phrasing ... Too bigbrother like.

... the real issue to me is who has the data and why. Companies making a dollar are no problem. A government who doesn't want to bother with warrants - hell no.

The comments reveal a distrust of government and the power that access to data gives the Government. This may be a reflection of the composition of the group, however, in response to the survey, 32% said they would be extremely concerned to know that the Australian government had requested access to hundreds of users' Facebook accounts, slightly less than those extremely concerned about telcos (39%).

While telco and government agencies received a relatively high level of concern, for most participants a commercial entity such as Facebook is seen as having, if not a legitimate reason for collecting and on-selling their information, then at least an understandable reason for doing so, and a logical motivation for the type of information collected. With government and telco surveillance, there seems to be less knowledge and understanding of what information is being harvested, and why. As one participant says:

How is recording updates on the bands I've seen going to prevent terrorism?

While there is a sense of general concern about government and official surveillance, the widespread use of social media to distribute personal information 'demonstrates a remarkable degree of faith in the integrity and security of SNS platforms' (Athique 2013, 223), although there is a level of wariness:

I don't trust Facebook or Twitter to do the right thing and delete the data like location services when they are finished with them.

While this wariness exists, the overall level of trust in the platform, and the acceptance of a degree of surveillance from commercial entities and government agencies as a consequence of participation, suggests a normalisation of surveillance practices for online Millennials. The participants in the study continue to use Facebook regardless of their concerns, however, they do employ techniques to manage their exposure.

Managing Exposure

As could be predicted, based on the age of the group, a high percentage of the participants in the survey use Facebook to communicate with family and close friends (83.4% often or almost always). A smaller number use Facebook to establish new contacts with classmates, friends of friends or work colleagues (56.4% often or almost always) and maintain contact with past friends, acquaintances or friends of friends (67.6% often or almost always). With this high level of online interaction, the participants use different approaches to managing their exposure online including privacy settings, secret accounts, selective information sharing, and coded messages.

There are three students whose Facebook page is fully open to the public but more than half the participants (51.9%) have their Facebook privacy settings set to 'Friends' with the next highest level (31.2%) using 'Customized' settings, indicating

that with these participants, at least, there is a deliberate decision made on who they share their lives with on social media. Providing further evidence to support this statement, only 20.8% say they often or very often share information or images on Facebook that could be considered personal, with 53.2% stating sometimes but 26% saying rarely or never. While there may be a lack of agreement on what is considered to be personal, these results are in contrast to the typical, often popular, understanding of this age group's habit of oversharing (Carvajal 2014, 81; boyd 2014, 55-56).

Most users of social media, while posting information in public fora, regard that information as private (Athique 2013), owned and to be controlled by them. Social media, including Facebook, is specifically designed to record and disseminate users' information, however the distancing effect of computer-mediated communication creates an impression of privacy. While users may be under each others' surveillant gaze (Foucault 1977), this surveillance is not always obvious. Posters may be aware of co-present others (such as a grandmother, or an employer) and modify their posts accordingly, but are less aware of how they have lost control of information shared with 'friends only', and that this sharing can amount to a very wide distribution (Athique 2013, 223). Some of those contributing to the focus group discussion do have strategies in place for managing the amount of personal information they made available:

I guess this is the reason behind why so many people have different, or secret, accounts for their social media use, one for personal and one for public. But even then, how well you are able to keep the two separated is another issue.

I am particularly careful about my social media activity and censor myself very carefully, and also because I am living in ignorant bliss.

While over 80% of the group responded that they undertake some steps to protect their personal information, many expressed a lack of knowledge about what they should, or

could, do to limit the distribution of their personal information:

It still seems highly intrusive and unethical, even if on most occasions it is our own fault for not reading the T&C [Terms and Conditions].

I pay no attention to terms and conditions or any other such fineprint, and am clueless as to what my profile data may be used for.

Participants also expressed a concern at the lack of awareness displayed by others in regards to who could access their information and how that information could be used:

I remember a Facebook craze going around not long ago that people where 'chain lettering' around, one of those '20 Things About Me' notes where the person had to list information like the street they grew up in and their mother's maiden name; as you all recognised, information that is commonly either used as passwords or answers to security questions! Amazing the people who were happy to provide the info.

I have been able to determine an individual's exact location through a Facebook message I have received from them, and status updates and Instagram posts can do the exact same. It is worrying that people don't seem to be concerned by such a thing.

The proliferation of fine print, the deliberately difficult to read collection of terms, conditions, warnings and advice that accompany online services, makes it difficult for individuals to understand and, therefore, manage the consequences of their use of the service. Establishing privacy boundaries becomes a matter of take-it-or-leave-it when it comes to social media and accepting the surveillant gaze has come to be a normal part of social media use.

Perceptions of Privacy

The discussion in the focus group suggests that while participants share concerns

regarding commercial and government monitoring of their data, a perceived need to maintain privacy from real or imagined threatening individuals is a greater motivation in limiting and restricting disclosure:

I start to freak out a bit when apps and services want my location because I'm one of those paranoid people that think when someone sees my location they will stalk and kill me. I know that the likelihood of this happening is very slim but it still completely freaks me out.

I remember having a creepy stalker guy when my page was on private who sent a message saying how pretty [place name deleted] was, it threw me at first, I didn't know this person, until I realised that my employment was still public.

Nine out of ten of the respondents in the survey stated they are concerned or extremely concerned that videos or photographs of them, taken in public places, could be published without their knowledge. However, despite their concerns regarding their own personal information and fears of how it might be used by others, the majority of respondents admit to using Facebook to collect data on others, or to publish others' information, suggesting that surveillance on social media sites is becoming, or has become, normalised. A high percentage of respondents have checked the Facebook profiles of people they have met casually such as in class (87%), or people they don't know but are personally interested in (81.8%), or celebrities (87%). Before an interview or another important meeting, 62.4% of this group would check the profile of the person(s) they were to meet. This reflects the discussion on their concern about security, but shows a double standard in that while these participants are comfortable checking an interviewer's profile, four out of five participants are concerned or extremely concerned that potential employers would ask for access to their own social media profile.

However, Millennials have an expectation that others' personal data is not only available to them but that they have rights to disseminate it: more than three in four

(76.3%) have either posted videos or photographs of family and friends on Facebook without their permission or would consider doing it, and a similar number (79.2%) has tagged family or friends on Facebook without their permission. Seven out of ten have checked an ex-partner's or former friend's profile to keep track of what they are doing. These figures suggest that there is a high acceptance, and expectation, among this group of users that they will be able to surveille others while attempting to maintain control over their own social media exposure. The surveillant gaze is being normalised by their use of monitoring techniques on their friends and acquaintances.

Acceptance of the Surveillant Gaze

For the participants in this study, there is the perception that surveillance is a normal part of taking part in a digital society - they accept that surveillance is going to occur, but they also accept that they have the right to watch others. This may be a condition of networked society that there is a general consensus that surveillance is the norm (Senft, 2013). Some of those commenting in the online forum saw an increased permeability of their own privacy boundaries (Petronio 2012) as a consequence of easier access to others' personal information:

I think that if we expect to be given the tools and accesibility to look into other peoples lives, often complete strangers, than we should come to expect our own privacy to be compromised. It's like you can't take one without the other. As much as I would like my life to be a bit more private, it's just not realistic with todays society and our knowledge regarding technology.

I think individuals are often concerned about their data being viewed by people they do not know, but when it comes to accessing the data of others, we are happy to become voyeurs. Whilst the idea of voyeurism conjures up a lot of negative connotations, perhaps this should no longer be the case 'in an age where privacy is flouted just as much as it is protected'.

The responses to the survey and the comments in the forum both suggest that these students accept an increasing normalisation of surveillance and recognise that the norms around surveillance and personal privacy are changing. There is a realisation that contemporary lives are experienced within a framework of different types of monitoring, from benign information gathering to controlling surveillance, and that previous conceptions of privacy may no longer be relevant:

We are unconsciously modifying our behaviour as a result of the information about individuals and events we have been previously exposed to on social media. I think we are subconsciously aware of surveillance from other people, the platform, and government.

Maybe privacy should not be the exact thing that we worry about, as the term seems a little outdated as we move forward with such technologies.

Participant comments reveal that they are aware that Facebook is an omnopticon (Jensen 2007) where the many view the many, and that this gaze (Foucault 1977) is a system of control that imposes a form of self-regulation in response to the surveillance. As Facebook users they employ a range of techniques in navigating the boundaries between privacy and sharing of information. On personal Facebook pages, surveillance is a component of relationship maintenance through the sharing of information. The students in this study perceive a number of advantages to surveilling and being surveilled online that for many outweigh their concerns over dissolving privacy barriers. Some of the advantages reported include the personalising of advertisements and news reports, the ability to connect with others, the utility and convenience of the communication tools, and the feeling of belonging:

With google, I know what it is they are collecting and roughly how it will be used. They will sell some of it, customise some ads (I love the trend of getting ads for the

things I have just looked at and determined I can't afford), plus the bit used for actual service providing.

It shows how easily we are manipulated into giving powerful sites our information just so we can simply use the site to update what we are doing with our lives.

Conclusion

Surveillance is now universal. It is a part of everyday life, particularly for Millennials with their smartphones, loyalty cards, urban transit passes, online commercial transactions and social interactions. Social media, as a combination of communication and computing, not only facilitates the collection and distribution of huge amounts of data on ordinary people, but also normalises this gathering and dissemination of information by individuals, commercial entities, and government organisations.

Online surveillance is a complex process that involves the acquisition of information from multiple interconnected sources, only some of which users are aware of, and few of which have been knowingly authorised. The results from this group of research participants suggest that additional research needs to be done on the increasingly nuanced ways that privacy is managed in this age group. The students who participated in this study have broad concerns about their control over privacy boundaries online, and report self-censoring and access management, but they admitted to being generally unaware of the level of surveillance that sharing in Facebook enables, or the specific strategies that could be employed to limit exposure. While many feel uncomfortable with the idea that government and law enforcement agencies could access their data, and that employers could also see their personal information, the majority feel that accepting a reduction in privacy is part of contemporary life, and necessary to participate in the online environment. Most of them depend on the ability to be able to use surveillance of others, from staying in touch with a relative's status or

gathering information on an acquaintance, to covertly watching the activities of a former partner.

The invisible audiences on social media facilitate unauthorised surveillance and create an omnopticon, an environment where mutual surveillance is an everyday practice. It becomes something that everyone is subjected to without a serious level of threat, and something that everyone can and should do to stay informed for their own pleasure and protection. Facebook users routinely monitor others and are aware that they in turn are being monitored, and the awareness of the gaze of others leads to modifications in behaviour that are designed to manage privacy boundaries. People-watching has always occurred at one level or another. People have always watched those around them because it both strengthens connections to the community and gives individuals a strategic power over others (Locke 2010). However, social media has expanded the act of watching to people and activities that would have been impossible or even taboo not so long ago. Everyday benign surveillance on Facebook has led these students to hold increasingly relaxed perceptions of privacy boundaries, though the relaxations have initially been where others' privacy is concerned. While the students are apprehensive about unauthorised breaches of their own privacy boundaries, they seem to have an expectation that others' personal information would be available to them to collect and disseminate should interest or exigencies require it. Social media, by encouraging the surveillance of others, **is contributing to changes in the conceptions of privacy, and helping to prepare young people** for a lifetime of being watched and monitored, online and offline.

Privacy has traditionally been seen in terms of 'rights' in connection with security, safety, personal space, and personal information. Older generations may still see privacy as equivalent to secrecy and keeping the personal hidden from public view,

however the millennials in this study tended to see privacy as a commodity, something that could be exchanged with online friends for social capital, and traded with organisations for services and benefits. As a commodity, privacy is seen as something to be managed rather than protected, and systematic surveillance is accepted as a routine and inescapable part of everyday life.

References

- Albrechtslund, Anders. 2013. "New Media and Changing Perceptions of Surveillance." In *Blackwell Companion to New Media Dynamics*, edited by John Hartley, Jean Burgess and Axel Bruns, 311–321. Chichester: Wiley-Blackwell.
- Alt, D. 2015. "College students' academic motivation, media engagement and fear of missing out." *Computers in Human Behavior* 49: 111-119.
- Athique, Adrian. 2013. *Digital Media and Society: An Introduction*. Cambridge: Polity.
- Bolton, Ruth N., Parasuraman, A., Hoefnagels, Ankie, Migchels, Nanne, Kabadayi, Sertan, Gruber, Thorsten, Loureiro, Yuliya Komarova, Solnet, David. 2013. "Understanding Generation Y and Their Use of Social Media: A Review and Research Agenda." *Journal of Service Management* 24 (3): 245-267.
- boyd, danah. 2014. *It's Complicated: The Social Lives of Networked Teens*. New Haven: Yale University Press.
- boyd, danah. and Hargittai, Eszter. 2010. Facebook Privacy Settings: Who Cares? *First Monday* 15 (8), August 2: n.p.
<http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589>.
- Carvajal, Adrian. 2014. "Social Transformations Facilitated By Facebook On the Filipino Generation Y." *International Journal of Education and Research* 2 (10): 77-90.
- Chalkley, Tony. 2012. "Surveillance: Why Is Everybody Staring?" In *Communication, new media and everyday life*, edited by Tony Chalkley, Adam Brown, Toija Cinque, Brad Warren, Mitchell Hobbs and Mark Finn, 201-214. South Melbourne: Oxford University Press.
- Fowler, Floyd J. 2009. *Survey research methods*. 4th ed. Thousand Oaks: Sage Publications.

- Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison*, trans. Alan Sheridan. New York: Vintage.
- Hine, C., 2007. Connective Ethnography for the Exploration of eScience. *Journal of Computer-Mediated Communication* , 12(2): 618-634.
- Howe, Neil and Strauss, William. 2009. *Millennials Rising: The Next Great Generation*. New York: Vintage.
- Jackman, Simon. 2005. "Pooling the Polls Over an Election Campaign." *Australian Journal of Political Science* 40 (4): 499-517.
- Jensen, J. L. 2007. "The Internet Omnopticon: Surveillance or Counter-Insurgency." In H. Bang, & A. Esmark (Eds.), *New Publics with/out Democracy*. Frederiksberg: Samfundslitteratur Press: 351-380.
- Kibby, M.D. and Fulton, J.M. 2014. "Mutual Surveillance and a Sense of Belonging: Facebook at Uni." In M. Kent & T. Leaver (eds.), *An Education in Facebook? Higher Education and the World's Largest Social Network*, New York: Routledge, 111-120.
- Lee, Ashlin and Peta S. Cook. 2014. "The Conditions of Exposure and Immediacy: Internet Surveillance and Generation Y." *Journal of Sociology*. Advance online publication. DOI 1440783314522870.
- Locke, John L. 2010 *Eavesdropping: An Intimate History*. Oxford: Oxford University Press.
- Lyon, David. 2007 *Surveillance Studies: An Overview*. Cambridge: Polity Press.
- McChesney, Robert W. 2013. *Digital Disconnect: How Capitalism is Turning the Internet Against Democracy*. New York: The New Press.
- Margulis, Stephen T. 2003. "Privacy as a Social Issue and Behavioral Concept." *Journal of Social Issues* 59 (2): 243-261.
- Marwick, Alice. 2012. "The public domain: Surveillance in everyday life." *Surveillance & Society* 9 (4): 378-393.
- Nicol, D. 2014. *The Datification Project*. <http://datafication4.twsydney.com/>.
- Paradise, Angela. 2012. "Picture Perfect? College Students' Experiences and Attitudes Regarding Their Photo-Related Behaviors on Facebook." In *Misbehavior Online in Higher Education (Cutting-edge Technologies in Higher Education, Volume 5)*, edited by Laura A. Wankel and Charles Wankel, 261-292. Bingley: Emerald Group Publishing.

- Park, N., & Lee, S. (2014). "College students' motivations for Facebook use and psychological outcomes." *Journal of Broadcasting & Electronic Media* 58 (4): 601-620.
- Petronio, Sandra. 2012. *Boundaries of Privacy: Dialectics of Disclosure*. New York: SUNY Press.
- Rainie, Lee, John B. Horrigan, Barry Wellman and Jeffrey Boase. 2006. "The Strength of Internet Ties." *Pew Internet*, January 25.
<http://www.pewinternet.org/2006/01/25/the-strength-of-internet-ties/>.
- Senft, Theresa M. 2013. "Microcelebrity and the Branded Self." In *Blackwell Companion to New Media Dynamics*, edited by John Hartley, Jean Burgess and Axel Bruns, 346-354. Chichester: Wiley-Blackwell.
- Sensis. 2015. *Sensis Social Media Report May 2015: How Australian People and Businesses Are Using Social Media*. Accessed July 26 2015.
https://www.sensis.com.au/content/dam/sas/PDFdirectory/Sensis_Social_Media_Report_2015.pdf.
- Sheldon, Pavica. 2008. "The Relationship Between Unwillingness-To-Communicate and Students' Facebook use." *Journal of Media Psychology* 20 (2): 67-75.
- Siapera, Eugenia. 2012. *Understanding New Media*. London: Sage Publications.
- Solove, Daniel J. 2006. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154 (3): 477-564.
- Solove, Daniel J. 2008. *Understanding Privacy*. Cambridge, MA: Harvard University Press.
- Statista. 2015. *Distribution of Active Facebook users Worldwide as of 4th Quarter 2014, By Age*. Accessed July 26 2015.
<http://www.statista.com/statistics/376128/facebook-global-user-age-distribution>.
- Tandoc, E. C., Ferrucci, P., & Duffy, M. 2015. "Facebook use, envy, and depression among college students: Is facebooking depressing?" *Computers in Human Behavior* 43: 139-146.
- Trottier, Daniel. 2011. "A Research Agenda For Social Media Surveillance." *Fast Capitalism* 8 (1), October: n.p.
http://www.uta.edu/huma/agger/fastcapitalism/8_1/trottier8_1.html.
- Trottier, Daniel. 2012. "Interpersonal Surveillance on Social Media." *Canadian Journal of Communication* 37 (2): 319-332.

- Tufekci, Zeynep. 2008. "Can You See Me Now? Audience Disclosure Regulation in Online Social Network Sites." *Bulletin of Science and Technology* 28 (1): 20-36.
- Wang, Y., Niiya, M., Mark, G., Reich, S. M., & Warschauer, M. 2015. "Coming of age (digitally): An ecological view of social media use among college students." In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, March 14-18, Vancouver, BC, Canada: 571-582.
- Winkels, Mitchel. 2014. *The global social network landscape, a country-by country guide to social network usage*. Report published by Emarketer, <https://icgstrategicteam.wikispaces.com/file/view/eMarketer>.