Naivety, Privacy and Life Online

Dr. Brad Warren
School of Communication and Creative Arts,
Deakin University, Melbourne.

Abstract

The paper addresses contemporary usage of online environments, particularly social networking websites such as Facebook. It is concerned with issues of privacy and security, and the extent to which many Internet users are unaware of the full extent of potential problems. In exploring this topic, the paper engages with Friedman’s The Lexus and the Olive Tree (1999), as well as with a range of more recent literature, and with documentary footage from both television and YouTube. Firsthand qualitative material from these sources serves to highlight the conflicting and sometimes contradictory opinions that today’s ‘digital natives’ hold vis-a-vis their online safety. The paper also examines the Internet and social networking in the light of Foucault’s theoretical engagement with Bentham’s Panopticon (drawing on Discipline and Punish (1977) and Power / Knowledge (1980)). Foucault uses the Panopticon as a metaphor for contemporary society, with regard to how (at least the possibility of) constant surveillance serves to regulate behaviour. It is argued that the Panopticon still retains some validity as an explanatory device for online contexts, but not without some qualifications concerning the roles of those involved in surveillance, and their agendas.

Keywords: Facebook, Foucault, Online, Panopticon, Privacy, Security

‘Facebook is life’ (Chalkley et. al., forthcoming 2011, Chapter 13).

A succinct beginning. While perhaps an overstatement, it is nonetheless a fairly accurate indication of the extent to which the day-to-day interactions of Generation Y (the first
generation of truly ‘digital natives’) are mediated in and through online environments, including but not limited to social media websites such as Facebook. Increasingly, people are putting themselves ‘out there’, publishing (at least aspects of their lives) online. The primary contention of this paper concerns the dangers inherent in that practice, and the extent to which many are unaware of the potential ramifications. This issue will be explored utilising Friedman’s commentary on new technology and globalisation, Foucault’s reflections on Bentham’s panopticon, as well as firsthand qualitative research.

The ‘virus of overconnectedness is spreading daily and has no known cure’ (Friedman, 1999: 403). At the risk of scaremongering, it is not an exaggeration to state that every personal detail, every picture, every blog entry posted online, not only has the potential to be subverted and used in ways that outstrip the intentions of the original author but, once ‘published’, is (again, potentially) in cyberspace forever, even if the original posting or picture is removed. Over the last decade, there has been no shortage of concern over online privacy / security, as reflected in the abundance of literature available on the topic. Friedman was among the earlier writers to engage with the issue:

... a national [U.S.] poll in the summer of 1998 found that “81 percent of people believe their personal information, including credit ratings, medical histories and ... financial records, is insecure”. (1999: 409)

However, what people might believe isn’t necessarily a reflection of what is (or isn’t) true. Nonetheless, it is a reasonable assumption that such fear / concern (paranoia?) comes from somewhere, as is borne out by the following:

The report added that states such as Texas are already putting their state criminal histories online. The Texas criminal-record database is searchable for $3.15 per name ... An offshore company called PublicData, based in Anguilla, British West Indies, buys public records in bulk and puts them online in a database searchable for as little as 3 cents per search (Friedman, 1999: 409).

Today, more than a decade later, ‘PublicData’ is not the only player in this particular field; data-mining is a multi-million dollar industry. More recent publications express similar sentiments:

... [in an] interactive network, not only do users often voluntarily give up their right to control their own information by providing personal information without fully considering future consequences, but ... individual users’ identities become
more and more exposed, while [those conducting] … surveillance … become less and less identifiable. (Woo and Lee, 2006: 16 – 17)

Gross and Acquisti enumerate several risks that users subject themselves to as a result [of participation in social networking sites], including embarrassment, blackmailing, stalking, and even identify theft. (Gross and Acquisti, 2005, cited in Lewis et. al., 2008: 80)

In 1999, Scott McNealy, CEO of Sun Microsystems said “you have no privacy … get over it” (Sprenger, 1999). And popular notions suggest that the new millennial generation is perhaps the most cavalier about their expectations of privacy and what they are willing to disclose, particularly in online contexts. (Kisselburgh, 2009: 30 – 31)

Social media websites are fertile soil for the combing of personal details by sexual predators, burglars and others. Have you published where you work on your Facebook page?; Whether or not you’re employed full-time?; Who you live with?; What you do for a living? If so, you’ve declared to the world at large when your house is empty...

All of which may cause you to raise an eyebrow, to admit that, indeed, you hadn’t thought through the full implications of Life Online … but then again it might not. In the interests of fair treatment of existent literature, it must also be said that there are an abundance of claims by Internet users that they are fully cognizant of the associated risks:

There has only been one major study of the threat of sexual predators online. Funded by the Department of Justice, the study confirmed what many kids have been saying all along, that most of them know to ignore unwanted solicitations they receive on the internet. (Cutting Edge, 2008)

In a similar vein (and post-dating the study just mentioned), Cho et. al. examine awareness of, and engagement with, privacy issues in online contexts across a number of different demographics. Their findings reflect Cutting Edge’s assertion that today’s Internet-natives are very security conscious and, further, they ‘identified three underlying dimensions of privacy protection behaviour – avoidance, opt-out and proactive protection’ (2009: 395).

Qualifying her assertion about the dangers of Life Online (above), Kisselburgh also grants consideration to both sides of this issue:

Young adults, who use technology daily for both utility and social (reasons), are concerned about privacy. While they recognize and take for granted the public
nature of social technologies, they expect and desire a level of control (autonomy) in their visibility in such venues. (2009: 31).

The comfort and (at least perceived sense of) security with which Gen Y digital natives navigate online environments is best conveyed through their own testimonies. Consider the following:

[Student One:] ‘My parents, like, they don’t understand that I’ve spent since, like, second grade online, and that I know what to avoid and I know, pretty much, like, what can happen, and I think sometimes they forget that ‘cos they didn’t have, like, they didn’t grow up online.’

[Student Two:] ‘[If someone] … IM’s [instant-messages] you and says, like, “Hey, where do you live? I wanna meet you.” [laughs] It’s pretty obvious, like, this person might be a predator [laughs sarcastically].’

[Student Three:] ‘If someone asks me, like, “Where do you live?”’, I’ll delete them as a friend, like, why do you want to know where I live at? Like, I don’t tell people where I live at.’

(Cutting Edge, 2008)

To say that young people participating online are perhaps not ideally equipped to make claims about their security / privacy is rather a moot point, since the case cannot be adequately proven either way. Nonetheless, the processes by which personal details are gleaned (harvested?) in such environments generally take place without the knowledge of those from whom they are taken. In itself, this is sufficient justification to at least air the possibility that social network users are not as secure as they might feel or believe.

However, to revisit the last passage cited, what is more interesting about Student Three’s assertion that she would ‘delete … as a friend’ anyone who asked her personal or inappropriate questions, is that it begs the question of how such an unsavoury individual got to be her friend in the first place?! The answer to this will be readily apparent to anyone who has spent more than a few moments perusing sites such as Facebook: the vast majority of users have far more ‘Facebook-friends’ than they could possibly maintain relationships with in the real (offline) world. According to the Facebook website itself, the average user has 130 friends (Facebook, 2010), but even this figure might be misleadingly low. The following interview extracts are taken from a YouTube clip in which a variety of students are asked about their usage of social networking sites:
“How many close friends and family do you have, that you talk to often?”

‘... like, ten close people, probably’

‘... and, I probably have, about ten, like, really close friends’

‘oh, about ten or twelve’

‘And how many friends do you have on Facebook and MySpace?’

‘Oh, about three hundred, four hundred’

‘Oh, probably like eight hundred, or something [laughs]’

‘Oh, like, five or six hundred, or something ridiculous’

There are several routes via which social network users might come to have such a glut of online acquaintances. These include informal competitions between (offline) friends to see how many ‘Facebook-friends’ one can accumulate, a tendency to click ‘accept’ to anyone who sends a friend request (a particularly risky practice, since it opens the door to online predators), as well as blurred distinctions between Facebook-for-socialising and Facebook-for-business-promotion. However, regardless of how such unwieldy friend-lists come about, what must be emphasised is that there comes a point at which privacy settings are unimportant. It doesn’t matter how strongly you police the boundaries between ‘friends’ and ‘others’ if you don’t know who all your friends are!

And still we haven’t exhausted the potential problems of having ‘too many friends’ on social networking sites. Sometimes, if the friend-list is large enough – and even if we at least know who all our ‘Facebook-friends’ are – difficulties can arise if we forget exactly who’s there. Consider the following, a personal email from a student to a lecturer, requesting an assignment extension:

Kate (not her real name): Dear Professor, I am writing to request an extension for the assignment due next Monday ... I have been unwell and today (Friday) I am worse than ever and want to spend the weekend in bed and recover properly, screw up the writing I have done while I was sick and start again. As a result, would it be possible to get a week’s extension, sorry I have been too sick to go to the Dr. Thanx, Kate. (Chalkley et. al., forthcoming 2011, Chapter 16).

The lecturer addressed in this email teaches media, and Facebook is a regular topic of discussion. As a result, many students request that he become their ‘Facebook-friend’. Kate was one such student, and here the problems arise:
STATUS UPDATE [on Facebook the following Sunday]:

Kate: MINE WAS THE BEST 18th EVER!!! Thanx guys for coming, awesome fotos posted soon. Still pissed from sat ;-) After party at ##### this arvo!”

(Chalkley et. al., forthcoming 2011, Chapter 16).

Clearly, ‘Kate’ did not intend for her lecturer to see this message; she has inadvertently compromised her own privacy as a result of an injudicious posting and / or maintenance of her Friend-list. But this raises thorny issues for her teacher: How should he respond? Should he feel outraged, because real friends shouldn’t lie to one another? Or should he penalise the essay? Deny the extension? Confront Kate about her deceit? The correct response hinges upon exactly what the relationship between Kate and her lecturer is – friend or not-friend – but the answer to this remains unclear. It seems that ‘offline’ solutions to such moral / ethical dilemmas might not hold in cyberspace – or, at very least, they are complicated or confounded by the new social situations that can arise online.

This, in turn, suggests a more general question about the nature of the Internet, and about social networking sites in particular, vis-à-vis the extent to which constant surveillance serves to regulate behaviour. One is reminded of Foucault’s reflections on Bentham’s Panopticon, ‘an architectural plan for a prison system relatively simple in design, but socially and psychologically complex in effect’ (Campbell and Carlson, 2002: 589). In short, the Panopticon consisted of:

... an annular building ... at the periphery ... ; at the centre, a tower; this tower is pierced with wide windows that open onto the inner side of the ring; [and] the peripheric building is divided into cells … All that is needed, then, is to place a supervisor in a central tower and to shut up in each cell a madman, a patient, a condemned man, a worker or a schoolboy’ (Foucault, 1977: 200).

The reference here to ‘workers’ and ‘schoolboys’ is Foucault underlining that his use of the Panopticon was as a metaphor for the disciplinary power he held to operate in contemporary society more generally. The exercise of such power is, he maintains, is ‘one of the great inventions of bourgeois society. It has been a fundamental instrument in the constitution of industrial capitalism and of the type of society that is its accompaniment’ (1980: 105).

Expanding on the Panopticon’s nature, Foucault argues that its ‘major effect ... [is] to induce in the inmate a state of conscious and permanent visibility that assures the automatic
functioning of power. So to arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its actions; that the perfection of power should tend to render its actual exercise unnecessary’ (1977: 201). Or, to rephrase, it is the possibility of constant surveillance, even if such surveillance is not actually present at any given moment, that causes the Panopticon’s prisoners / society to self-regulate, to impose disciplinary order upon themselves for fear of the reprisals that might otherwise ensue.

Given the dangers inherent in Life Online, it must be asked whether or not the Panopticon functions effectively in cyberspace? That is to say, if online contexts self-regulate, how is it that the worst consequences of breached privacy / security (such as identity-theft, stalking and other predatory behaviours) even exist? It is clear that most Internet users do self-regulate, that they bring to their online interactions their own ‘ideals or codes of restraint on human behaviour’ (Friedman, 1999: 449). If this were not so, the Internet would not merely be potentially dangerous, it would be unresolvable chaos.

However, there are at least two points at which Foucault’s metaphor seems not to hold in contemporary online contexts. Firstly, inside the Panopticon, if transgression was observed, punishment was guaranteed. This notion is of fundamental importance to regulating behaviour. It is an entirely different thing to say that (as per today’s cyberspace environments), if transgression is seen, punishment may or may not follow. To illustrate this point by example, if someone commits online fraud, perhaps they will be noticed. So far, this is in line with the Panopticon metaphor. However, in the Panopticon, responses to the following two questions:

   Observed by whom?
   With what consequences?

... were known quantities, with the answers being ‘the prison guards’ and ‘some form of punishment’, respectively. In cyberspace, the identity / role of the potential observer(s), and whether or not they care about an instance of online fraud either way, are in no sense guaranteed. These additional variables serve to weaken the effectiveness of a society to self-regulate, as they decrease the likelihood that transgressions will be detected.

Secondly, part of the successful functioning of the Panopticon lies in the fact that the guard’s tower is always visible to the prison population, serving as a constant reminder that conformity to imposed regulation is the best course of action. Although somewhat of an indictment on human nature, the absence of such reminders lessens the likelihood of the
desired behaviour. Campbell and Carlson point out that there are no such reminders in the
contemporary milieu, that ‘the agent of surveillance is not as apparent in cyberspace – neither
the guard nor the central tower can be seen even though they can be assumed to be
omnipresent’ (2002: 603). In summary, then, Foucault’s Panopticon is a very small, very
closed system, and hence perhaps not a completely adequate analogy for our complicated and
multifaceted online existences.

One question that the preceding discussion has not adequately addressed is What can be done
about all this? That is, short of unplugging everything and hiding under the bed, how might
the big questions of online privacy and security be addressed? Unfortunately, final answers
are beyond the scope of this paper (and even were the space available, I suspect they would
still remain elusive). The best that can be done, for now, is to end on a cautionary note: It
might once have been true that What happens in Vegas stays in Vegas. A more appropriate
turn of phrase for the current cyber-environment(s) could be that ‘What happens in Vegas
stays on YouTube’ (Qualman, 2009: 33). By all means, live your Lives Online, but do so in
the knowledge that being ‘out there’ potentially means being ‘out there’ for anyone /
everyone, and being ‘out there’ forever.

References
commodification of privacy’, Journal of Broadcasting & Electronic Media, 46(4),
Cutting Edge (01/04/2008) ‘Growing Up Online’. SBS.
[accessed 29/07/2010].


Global Consumer Culture (2000 – 01) ‘Globalisation and Social Media’ [YouTube clip]

http://www.youtube.com/watch?v=lUy8YivYjFg [accessed 28/07/10].


---

The statement, ‘Facebook is life’, is attributable to a Gen Y friend of this author (an unrepentant Gen X), in response to my apology for delivering a birthday invitation in an online chat, because I felt that a phone call would have been more personal, and therefore more appropriate. For many, apparently, such is not the case.