PRESENCE, PRIVACY, AND PSEUDONYMITY

Sonja Vivienne
University of Queensland

Tama Leaver
Curtin University

Brady Robards
University of Tasmania

Emily van der Nagel
Swinburne Institute of Technology

This panel seeks to map the intersections and contradictions evident among communities and individuals at the cutting edge of negotiations over digital, networked ‘presence’. Presence has multiple definitions - the fact of existing or being present; a person or thing that exists but is not seen; a group of people exerting an influence in a particular time or place; and finally the impressive manner or appearance of a person. These variations in meaning reveal issues at the heart of digitally mediated life.

Routine and everyday engagements with digital platforms and technologies are catalysing profound cultural shifts in how we understand identity performance in public, and personal privacy. Concepts like networked identity (boyd, 2011) and digital dualisms (Jurgenson, 2012) are breaking down binary oppositions between face to face and digitally mediated experiences. People laugh ironically at the use of ‘IRL’, wondering what this really means. Similarly, a growing awareness that anonymity is an impossibility and that pseudonymity is contingent, are causing us to rethink privacy.

The early days of the internet fostered dreams of democratic self-representation and correlated social change. However, the correlation between online sharing of personal (sometimes private) stories, like those hosted by ‘It Gets Better’ for example, and greater public acceptance or decreased face-to-face persecution, is disputable to say the least. Triumphant testimonials are matched by notorious failures, represented by too many youth suicides. The risks and rewards of online self-disclosure remain complicated, especially for those with limited agency - children, marginalised communities or the socially maligned. Seeking affirmation in supposedly closed groups, using pseudonymity in abusive ways, and the ethics of representing those who cannot
give consent all evoke debate about the ‘contextual integrity’ of privacy (Nissenbaum, 2004).

Our first paper explores current platform politics and everyday practices in pre-birth representations on social media, and canvasses the presumption of agency, forms of intimate surveillance and the ethics of control over mediated representation.

The second paper considers how curating congruent presence might offer an alternative to inadequate pseudonymity. It draws on case studies in which young queer people in Russia seek affirmation in supposedly private groups online, while unintentionally revealing their presence to attackers. Simultaneously, attackers utilise the same social network platform to circulate images of violent encounters and recruit homophobic followers.

The third paper considers new conventions governing physical and online spaces as they emerge among a small population of young Facebook users in Tasmania. It maps sustained disclosure practices, driven by three distinct forces; changes in the way Facebook makes disclosures visible; diversification and mainstreaming of the site’s user-base; and changes in disclosure practices among sub-networks of users.

These papers are all linked by arguments for, or observations of increasing digital literacy, and the final paper plays out against a background in which hacker communities and the geek elite propagate skills and infrastructures that enable ordinary people to engage with the dark net, via distributed servers worldwide. Wikileaks and Anonymous challenge the authority of governments and global corporations to retain highly confidential (secret) information, while journalists continue to correlate pseudonymity with heightened and toxic trolling.

Through the unmasking of Violentacrez this paper maps a disruption to the idea of the anonymous troll, an event that presents social media users with a challenge to their sense of privacy, but also an opportunity to be reminded that the boundaries of public and private on social media are never stable.

Greater awareness of our digital trace, and identity 2.0 (Helmond, 2010) – under construction, never complete, fragmented, partially created by others, persistent and searchable – is effecting our sustained and evolving online engagements. Collectively we map the liminal boundaries and intersections threaded through current thinking and emerging definitions of presence, privacy and pseudonymity, negotiated across space, time and evolving experiences.

References:


While the issue of how presences and interactions online differ from face to face communication has been a core question for internet studies since the field began to cohere, the vast majority of work regarding identity focuses on active users who have agency to either direct, shape or resist the way they portray themselves online, and are portrayed by others. This paper, by contrast, outlines an investigation into the way that the presence of very young people is shaped by parents, guardians and other loved ones from the day they are born. While parental sharing of photos, videos and other material about children is almost always done with the very best intentions, there is nevertheless a seeming disconnection between the way that individuals approach their own privacy online compared to the privacy afforded, or not afforded, to young people.

To address this issue, this paper is broken into three main sections. Firstly, I will offer a brief overview of current conceptualisations of presence and identity online and explicate the role of parents and others in creating the initial presences of children. Secondly, I will situate identity practices in relation to the shifting terrain of surveillance, including the possibilities of surveillance itself as a resistant practice, positing the concept of *intimate surveillance*. The third and final section uses two key examples – pregnancy and baby activity tracking apps such *Sprout*; and the use of the #ultrasound hashtag to share prenatal scan images on Instagram – to explore intimate surveillance as it occurs. The paper concludes not condemning or demonising any particular practices, but highlighting the need for increased digital literacies, especially for parents, to make more informed choices about the way sharing they are shaping a young person’s identity.

**Online Identities**

danah boyd (2010), argues that networked selves can be characterised by persistence (information does not organically decay), replicability (it can be easily copied), scalability (one copy or a million copies are equally straightforward) and searchability (information is organised and presented by third parties, such as search engines). Additionally, and significantly, identity fragments tend to be owned and managed by private corporations (Aufderheide, 2010). Anne Helmond (Helmond, 2010) characterises ‘Identity 2.0’ in a similar manner, adding that identities are always under construction, never completed, and that identity fragments online about one person are often created by other users. Allen (2009) and Leaver (2010) use the concept of web presence and differentiate between footprints – online identity material a user controls – and shadows – material
about them but out of their immediate control. Moreover, they argue that contemporary identity is a collage of online fragments which are reassembled in different ways; a content-generated user. At their core, all of these frameworks explicating online presences presume that users have agency, can control the shape of their identity to some extent, and often posit users gaining more agency as a solution when the management of identities online becomes complicated.

However when children are born they have no agency. Moreover, as Deborah Upton (2013, p. 42) has argued, posting first ultrasound photographs on social media has become a ritualised and everyday part of process of visualising and sharing the unborn. For many young people, their – often publicly shared – digital legacy begins before birth. And this is a legacy which young people will have to, at some point, wrestle with, especially in a digital landscape increasingly driven by 'real names' policies (Zoonen, 2013), where private corporations and governments are discouraging the user of anonymity and pseudonyms online.

**Shifting Surveillance**

In a culture where CCTV cameras, airport body scanners and various forms of government tracking are commonplace, surveillance itself is seemingly near-universal. Even well-intentioned sharing can often be a form of surveillance, however, this does not always have to be an oppressive act. Albrechtslund (2008) for example, characterises “social surveillance” as a form of knowing play, while E.J. Westlake (2008) goes a step further, arguing that because a user’s online performance is being recorded, performances can be entirely misleading. The notion of sousveillance as "inverse surveillance", countering/reversing organisational surveillance with wearable devices and individuals’ surveying society and each other is also increasingly popular (Mann, et al, 2002). However, ‘peer surveillance’ (Andrejevic, 2005) can equally be seen as perpetuating a more complex system which nevertheless exaggerates unequal power relationships. In relation to this field, I propose the concept of intimate surveillance which describes the purposeful (and almost always well-intentioned) surveillance of young people by parents, guardians and friends where the surveyed have little or no agency to resist themselves.

**Negotiating Intimate Surveillance**

While pregnancy-tracking and baby monitoring mobile apps such as Sprout have become increasingly popular, they have also normalised the practice of surveying and analysing offspring. Sprout, for example, can generate graphs and analyses of a baby’s sleeping and eating pattern over days, weeks or months, creating visualisations and recommendations. While useful, this recording and encoding normalises and rewards intimate surveillance, encouraging parents to track and monitor as a sign of love and concern. A more public measure of intimate surveillance can be found in mapping the use of the hashtag #ultrasound on the popular photography-sharing app Instagram. A rudimentary analysis of the hashtag over a month reveals thousands of images (the majority prenatal ultrasounds, although with a variety of other uses also visible), many of which include the metadata visible on an ultrasound, including the mother’s full name, date of the scan, expected due date, and so forth. For many young people these will be
their ‘first photograph’ and where parents are using their real names online, in later years it will take trivial effort to associate these images with the subsequent children.

Conclusions

Intimate surveillance normalises a surveillance culture facilitated by parents, family and friends. Better digital literacies about the uses (and potential abuses) of data shared with apps, platforms and services are needed (informed uses is the key). More transparency is required about how data might be shared and used in all contexts, especially commercial ones. And importantly, social norms need to evolve regarding the sharing (and non-sharing) of data and media generated about young people not just moral panics about data shared by young people.

References


CURATING NETWORKED PRESENCE: BEYOND PSEUDONYMITY

Sonja Vivienne

This paper explores the consequences of unintentional self-exposure by socially maligned identities, and argues that striving for curated pseudonymity - congruence
(rather than coherence) and integrity (rather than authenticity) - offers greater personal safety and possibilities for networked intimate citizenship.

Goffman (1959) argued that we selectively perform different aspects of ourselves for ‘front stage’ and ‘back stage’ audiences. Building on Goffman’s theatrical analogy, Hogan suggests that, online, our multiple representations of self are more like a curated art exhibition (Hogan, 2010) with platforms or apps, like Facebook, Linked In and Grindr, standing in for the gallery and/or exhibition curator. In this explication, we don’t get to choose how the different versions of our selves are hung on the wall because search engine algorithms produce images and text from disparate times and places, originally intended for discrete audiences. Meanwhile Plummer (2003) argues that claiming a space for what may have previously been regarded as backstage, or intimate, private dimensions of self, is integral to engaged citizenship, and the iterative negotiation of social norms. As a means of synthesizing our dueling needs for personal safety and meaningful social connection, I propose ‘networked intimate citizenship’ – the ongoing re-negotiation of presence; simultaneously f2f and online; with networks who are both affirming and antagonistic – as a cautious move beyond fragile pseudonymity, with new found opportunities to curate our own exhibitions of self.

Problems with Pseudonymity

VKontakte (VK) is the second biggest social network service in Europe following Facebook. In Russia, groups like Deti-404, established by 17-year-old Lena Klimova, provide support for young LGBT people who struggle to stay safe in their daily physical environments. The site plays on the ‘error 404 – page not found’ warning and has the motto ‘Children-404. LGBT teens. We exist!’.

While the apparently private space of Deti-404 has no doubt played a pivotal role in offering hope to a socially maligned group, it remains only as safe as its membership and their management of real names or pseudonyms. After 24 year old Olga Bakhaeva, a teacher, commented on a post on a similar ‘Straight Alliance for LGBT equality’ page, she faced months of harassment from another member. It turned out that he was operating under a pseudonym (while she had used her real name) and was actually a leader of another, aggressively homophobic, activist group ‘Parents of Russia’. The harassment escalated when the story was leaked to the press, with threats of violence and phone calls to Olga’s home number. Olga eventually lost her job. (“Russian Teachers Laid Off for Their Sexual Orientation - Альянс гетеросексуалов за равноправие ЛГБТ,” 2013).

While VK hosts support groups it also hosts hundreds of active homophobic groups, like ‘Occupy Pedofilyay’ (Occupy Pedophilia), which has approximately 75,000 followers. Representatives from this loose collective of neo-Nazis and Russian nationalists routinely seek out and join support groups in order to solicit enough identifiable information to physically track down transgressive targets. They use social media strategically, in two ways – firstly, luring gay people (sometimes by posing as prospective dates) into violent physical encounters then, secondly, distributing the resulting documentation (Broderick, 2013). The leader of Occupy Pedophilia regularly
publishes stylised videos of ‘sting operations’ or ‘safaris’ and holds regional seminars to help build their following.

These disastrous examples of networked self-representation are not, however, new. Even ‘before internet’ there was a risk of negative ramifications should the wrong circle of people came into information that was not intended for them. Disparate audiences that converge via digital networks merely increase these risks. Further, if pseudonymity is only as robust as trusting that one’s presence can not be revealed, how can socially marginalised people, with socially maligned identities engage in public and/or online spaces?

Reframing Presence

Theoretical frames drawn from narrative theory, sociology and queer theory offer insight into presence (the fact of existing or being present) and useful distinctions between authenticity and integrity; coherence and congruence. While Giddens argues that self-identity is bound up with consistency, coherence and ‘the capacity to keep a particular narrative going’ (1991, p. 54) narrative theorists counter that ‘the normative mission to find and value coherence marginalizes... non-fitting narrators... and poses ethically questionable pressures upon narrators who have experienced severe political or other trauma. (Hyvärinen, Hyden, Saarenheimo, & Tamboukou, 2010, p. 1)

The improbability of curating a wholly coherent narrative of self is evident among converged publics or, more evocatively, in the hypothetical merging of the average users Facebook and Linked In accounts. Difficulties with coherent identity are also not ‘new’, nor a product of networked technologies. Butler argues persuasively that it is impossible to give an accurate or consistent ‘account of oneself’:

...my story always arrives late. I am always recuperating, reconstructing, even as I produce myself differently in the very act of telling. My account of myself is partial, haunted by that for which I have no definitive story. (Butler, 2005, p. 27)

While the history of post-modern thought reveals many such challenges to the notion of authentic, truthful self-representation, to a large extent this is not reflected in popular understandings of identity.

Conclusion

A cultural shift that replaces ‘authenticity’ with ‘integrity’ might map better onto a global community of people who are always, already online; perhaps more serviceable than the familiar, yet outmoded ‘compare and contrast’ observations of online and f2f interactions, and more accommodating of fluid and non-normative identity (often judged to be incoherent). Curating selective self-representation (including well managed pseudonyms) across space and time; seeking congruence (determined individually) rather than coherence (determined by the spectator) might enable those engaging on VK and Facebook to carefully balance risks and rewards.
While clearly the marginalised of the world would be wise to take into account the mediating influences of platforms that may arbitrarily change the rules, and the possibility of accidental disclosure by breaches of trust and/or surveillance mechanisms, greater understanding of the self-representations that we create, share and own – curated presence - affords agency and ideally, Networked Intimate Citizenship.

References:


MAPPING CHANGES IN DISCLOSURE PRACTICES THROUGH SUSTAINED FACEBOOK USE

Brady Robards

On Facebook, each user’s ‘presence’ is constituted through both synchronous and asynchronous ‘disclosures’ (Stutzman, Gross, Acquisti 2012): IM chat, posting images and status updates, comment threads on posts, likes, and so on. These disclosures are made by users and their Friends, and then filtered through what Hogan (2010: 380) describes as a ‘third party’, Facebook’s servers, that determine ‘who is considered an appropriate audience member for this content and who is not’. In its ten years of operation, how have disclosure practices changed over time, as Facebook’s presentation of these disclosures has also changed?
There is a great wealth of research into the presentation of self on social network sites that has served to establish our understanding of how users are variously ‘present’ in networked publics (boyd 2006, 2007, 2008, 2011a, 2011b; Hewitt & Forte 2006; Menchik & Tian 2008; Tufekci 2008; Pearson 2009; Pinch 2010; Young 2013). Goffman is firmly ensconced in AoIR conference bingo cards. Much of this literature considers how the long and evolving history of conventions that govern physical social spaces are applied to social spaces on the web. This literature has revealed a series of continuities, but also some complications. For example, Mendelson and Papacharissi (2011), in their study of college students’ Facebook photo galleries, note that in personal photography ‘the positive is always recorded over the negative, with moments of celebration emphasized’ (2011: 254). While this finding maps neatly on to Goffman’s (1959) notion of the idealised self, it is also clear that users are not just present themselves online, but also others. One of the participants from the study by Mendelson and Papacharissi found themselves being tagged in photographs uploaded by others that did not align with their idealised self: ‘To another embarrassing photo, the subject commented: “Bad hair!!!! DESTROY! DESTROY!”’ (Participant in Mendelson & Papacharissi 2011: 262).

There are also differences in how people have presented themselves between social network sites. For example, Robards (2012) has argued that the conventions for ‘being’ on MySpace and Facebook were quite. On MySpace, the quantity of Friends one had served as a proxy for social capital (more was better), whereas on Facebook, smaller networks of Friends were framed as ‘more authentic’ or ‘realistic’. While presence on MySpace was constituted largely through the construction and revision of textually rich profiles (including music, images, poems, song lyrics, questionnaires, and so on), Facebook appeared to shift the focus towards specific disclosures that would fade in prominence over time and as new disclosures were made, culminating in the timeline format in place today (Robards 2012).

What is not currently clear is how the social conventions that govern disclosure practices on Facebook have changed over time. All social spaces are dynamic, and the conventions that govern them evolve. On Facebook, this evolution is driven by three forces: first, changes in the way Facebook (as per Hogan’s (2010) ‘third party’) makes disclosures visible to other users, driven by Zuckerberg’s open and transparent ‘theory of privacy’ (Zimmer 2014); second, the diversification and ‘mainstreaming’ of the site’s user base, in terms of age (Madden 2010) and location (Internet World Stats 2012); and third, changes amongst sub-networks or circles of users themselves around disclosure practices. The first two forces shape the third force, but this third force is also distinct and specific to local contexts. In other words, Facebook is not a singular social space but is instead made up by a complex and interrelated network of networks, with each user having slightly different disclosure practices that change over time.

This paper draws on ongoing qualitative research to document and contextualise the changes in disclosure practices of Facebook users in Tasmania, Australia, who have been using the site for more than five years. This project seeks to explore how the ‘digital trace’ (Bowker 2007) of Facebook users manifests through sustained use of the site. The project uses a mixed-methods approach, combining profile observation and one-on-one semi-structured in-depth interviews situated around the participant’s
Facebook timeline as a prompt. Participants are invited to reflect on their timeline as an archive of experiences and mediated memories, describing changes in disclosure practices as they 'scroll down memory lane'.

References


DISRUPTING ANONYMITY ONLINE: THE UNMASKING OF REDDIT’S VIOLENTACREZ

Emily van der Nagel

When blogger Adrian Chen unmasked prominent reddit user Violentacrez in an article describing him as “the biggest troll on the web” (Chen 2012), he disrupted the idea of online anonymity as something that was easy, safe, and permanent. Through a case study of the unmasking, this paper considers the challenges and opportunities present when online anonymity becomes contingent on adhering to the moral codes of other social media users.

On reddit, users post content in themed sections known as ‘subreddits’, which are then awarded up or down votes and commented on by other users, a system that aims to pull quality content towards the top of each page, resulting in a constantly updated list of popular links. Although reddit is famous for question and answer sessions with celebrities, reposted memes, and funny cat pictures, Violentacrez moderated forums such as ‘jailbait’, which featured sexualised photographs of minors, and ‘creepshots’, photos of unaware women in public. Objecting to this content, Chen revealed in his article Violentacrez’ full name and where he worked and lived – as a result, Violentacrez was fired from his job and appeared on CNN ostensibly to apologise for, but in fact to defend, himself and his actions.
The revealing of someone’s identity to shame and punish them has a long history. During the publish offensive, blasphemous, or seditious content anonymously or pseudonymously (Mulsow 2006 p. 220), as speaking out against the ruling class carried severe penalties including jail, disfigurement, or death. Martin Mulsow warns that even without the threat of being injured, the consequences can be dire: “being socially stigmatized should not be taken lightly” (Mulsow 2006 p. 232). He calls the unmasking of authors a form of control that amounts to “symbolic violence” and “literary tyranny” (Mulsow 2006 p. 234).

More recently, a young woman who failed to clean up her dog’s excrement on a train was branded “dog shit girl” and had her picture and name displayed across the internet in South Korea, causing her to drop out of university for receiving so much unwanted attention – which was justified by those that spread the story by claiming that she didn’t deserve privacy because of her actions (Solove 2007). Adrian Chen made a similar justification for his unmasking of Violentacrez; in an interview with The Guardian, he said, “if people use pseudonyms to publish sexualised images of women without their consent, and of underage girls, then there’s not really a legitimate claim to privacy” (Swash 2012).

Chen made the decision to unmask Violentacrez himself, based on his claim that he had done something offensive. Chen is neither a woman whose photograph was posted by Violentacrez, nor is he a law enforcement officer able to prosecute him for breaking any laws. In fact, according to New Zealand’s proposed Harmful Digital Communications Bill (2013), it would be an offence to post content online with the intention to cause harm. Chen has since won a Mirror Award, which “honor reporters[...] who hold a mirror to their own industry for the public’s benefit” (Mirror Awards 2013) for the article, echoing wide approval for his decision, although not everyone agreed that unmasking Violentacrez was the right thing to do. One reddit moderator felt the unmasking put every reddit user at risk, as the site values people being able to “freely express themselves without fear of personal attacks” (TIL_mod 2012).

The disagreement over the unmasking of Violentacrez arose from a clashing of ideals over free speech and privacy. Some applauded the unmasking as they agreed that the content seventeenth century, it was common practice to Violentacrez was posting was unpleasant enough to warrant punishment. Others noted that either people should have the right to say whatever they want, or they should respect the privacy of others – meaning that neither Violentacrez nor Chen were in the wrong, or both were. Helen Nissenbaum (2004) argues that contextual integrity, tying protection of privacy to norms of specific contexts, is essential. As online communication becomes increasingly searchable and permanent, remaining anonymous or pseudonymous is a more important strategy than ever to gain control over social situations, as danah boyd (2012) argues people are doing when they seek to disguise themselves online. For both Violentacrez, who repurposed photographs of women, and Chen, who unmasked Violentacrez as a punishment for doing so, their violations of contextual integrity meant control over personal information was lost.

The implications of the Violentacrez unmasking show that it is difficult to rely on anonymity as a way of gaining privacy when ideas about freedom of speech and
accountability are seen as more valuable. If the privacy of an individual depends on their adherence to the moral codes of others, then it can never be guaranteed. Punishing Violentacrez by unmasking him only echoes the action that he is being punished for, while threatening wider online participation: it highlights how easy it is to reveal an identity that had been hidden to maintain contextual integrity.

When Adrian Chen disrupted the idea that online anonymity could be relied upon, it presented challenges and opportunities to others using anonymity as a strategy. It is challenging to accept that privacy online depends on your behaviour, particularly when danah boyd has pointed out that those who “most heavily rely on pseudonyms[...] are those who are most marginalized by systems of power” (boyd 2011). It is challenging to social media sites such as reddit who wish to ensure their users feel safe in posting and commenting on what they are most interested in, without restraint. And it is challenging to find more secure ways of obscuring an identity. But the unmasking was also an opportunity to be reminded that the boundaries of public and private on social media are never stable or fixed, and those boundaries demand our ongoing attention as we continue to be social online.

References


