eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

What's in a (pseudo)name? Ethical conundrums for the principles of anonymisation in social media research

Ysabel Gerrard (iD)
Department of Sociological Studies, University of Sheffield, UK

Abstract

Scholars from wide-ranging disciplines are turning to social media platforms as research sites, and as platforms expand their communicative possibilities, they create more spaces for users to enact a multitude of identities. Most platforms allow users to have 'pseudonymous' identities; that is, they can engage in practices intended to facilitate nonidentifiable content. But pseudonymity presents a series of unique challenges to the principles of anonymisation in qualitative research. This article explores the slippery nature of dealing with pseudonymous social media users' personally identifiable data during research, framed around my responses to four questions I was asked when I applied for ethical approval to conduct research with pseudonymous fan communities on social media. The four questions concern: (Q1) changing notions of 'public' and 'private' forms of data; (Q2) identifying underage and therefore vulnerable participants online; (Q3) changes to the processes of obtaining informed consent from social media users; and (Q4) the risks social media research might bring to those conducting it. This article concludes by calling for qualitative researchers and Ethics Review Boards (ERBs) to engage with institutional ethics review across the duration of a project, or at the very least to advocate for ongoing consent as research progresses, especially for (but certainly not limited to) research involving pseudonymous social media users. The article aims to be useful to other researchers facing similar dilemmas. Indeed, given the popularity of pseudonymity on social media and the growing penetration of platforms across global demographics, a need for ethical discussions of this kind is surely set to increase.

Corresponding author:

Ysabel Gerrard, Department of Sociological Studies, Elmfield Building, Northumberland Road, Sheffield, South Yorkshire, S10 2TU.
Email: y.gerrard@sheffield.ac.uk

Introduction: what's in a (pseudo)name?

Scholars from wide-ranging disciplines are turning to social media platforms as research sites, and as platforms expand their communicative possibilities, they create more spaces for users to enact a multitude of identities. Most platforms allow users to have *pseudonymous* identities; that is, they can engage in practices intended to 'facilitate nonidentifiable content' (Hogan, 2015: 293). Internet identities exist on a spectrum, ranging from the 'totally anonymous to the thoroughly named' (Donath, 1999: 51). But true anonymity – 'a state implying the absence of personally identifying qualities' (Hogan, 2015: 293) – is actually very rare online (van der Nagel, 2017). Instead, social media users frequently embrace pseudonymity, a practice ranging from simply changing your Instagram username to something that resembles but differs from your 'real' (i.e. legal) name to adopting a television character's identity through a role-playing Facebook fan Page.[1] Where you sit on the spectrum of pseudonymity also depends on a given social media platform's norms and rules around identity. Some founders, like Facebook's Mark Zuckerberg, feel that pseudonyms are a form of deception and have enforced 'real name' policies to combat identity play (Zimmer, 2010b). Whereas others, like 4chan's Chris Poole, actively encourage their users to post pseudonymously (Richmond, 2011). Most platforms' naming policies fall somewhere in-between, neither encouraging nor banning the use of pseudonyms. But increasingly complex identity practices across a growing number of social media platforms make for increasingly complex ethical decisions, and researching pseudonymous social media users presents unique and under-discussed practical challenges to established ethical principles in qualitative research, particularly the *anonymisation* of research participants and sites.

People use pseudonyms for a range of reasons: some do it to protect their safety, like domestic abuse survivors or victims of stalking (Lingel and Gillespie, 2014), while others choose pseudonyms for arguably more mundane reasons, like personal branding. Indeed, the idea that people tailor their social performances according to different situations – what Goffman called 'impression management' in 1959 – forms a core part of how we live our everyday lives. But sometimes people use pseudonyms to be deceptive or cruel, like catfishing (adopting a fake persona to trick someone) or trolling (deliberately upsetting and provoking someone) (Phillips and Milner, 2017). Many people use pseudonyms because their identities or practices are marginalised, like transgender people (Haimson and Hoffmann, 2016), queer youth in rural towns (Gray, 2003), drag queens (Lingel, 2017), nude selfie-takers (Tiidenberg, 2018; van der Nagel and Frith, 2015), amongst many others, and this paper explores the pseudonymous practices of a group of people who feel their identities are stigmatised: adult fans of teen drama television shows (see Gerrard, 2017). The majority of my adult participants use pseudonyms on social media to avoid scorn from those who might deem their behaviour 'unacceptable', both within and outside of fan communities. In what follows, I map the ethical challenges of research with pseudonymous teen drama fans on to four questions I was asked when I sought approval from an Ethics Review Board (ERB) in the United Kingdom to observe and interview my participants:

Q1.   Are you collecting data that is available in the public domain?
Q2.   Will any of the research participants be under the age of 16?

Q3.   Will informed consent be obtained from the research participants?

Q4.   Does the research involve any risks to the researchers themselves?

It was difficult to answer these questions *before* the research began because, simply put, I did not have clear answers about who my participants would be and how they felt their personal data should be treated (see Schrag, 2011; Whelan, 2018): an issue long faced by researchers using other qualitative methods, like ethnography. But being 'ethically sound' of course involves far more than simply passing ethics review, and the ethical issues denoted in these four questions arose at every stage of the research, from its initial design and implementation to its dissemination.

To be clear, this paper does not make an argument *for* or *against* anonymisation but instead explains how and why this process is less straightforward for pseudonymous social media users. This is partly because researchers must deal with so many aspects of an already-pseudonymous participant's identity, creating significant practical challenges and increasing the risk that the participant may become unintentionally de-anonymised through research outputs.

I begin this article by examining current challenges to the principles of anonymisation in qualitative research, before turning to an exploration of my answers to the ERB questions listed above and the ethical strategies I used in my research. Here, I discuss the tensions between 'public' and 'private' social media data before exploring the dilemmas of identifying underage research participants, given the ease with which social media users can falsify their dates of birth. Next, I consider how pseudonymous social media users challenge traditional ways of obtaining informed consent. I then turn to a discussion of the risks researchers face when they communicate with respondents using their own social media accounts, weighing up the extent to which we should anonymise our own data for safeguarding purposes. Finally, I conclude with a call for qualitative researchers and ERBs to engage with institutional ethics review across the duration of a project, or at the very least to advocate for ongoing consent as research progresses, especially for (but certainly not limited to) research involving pseudonymous social media users.

The changing principles of anonymisation in qualitative research

Many of the challenges I faced over the life course of my research were linked to the extent to which I should (or should not) anonymise my participants' personally identifiable information, and the practical issues in doing so. Anonymisation is a guiding principle of qualitative research and refers to 'removing or obscuring the names of participants or research sites, and not including information that might lead participants or research sites to be identified' (Tilley and Woodthorpe, 2011: 198). According to Moore, the principle of anonymisation in qualitative research was born from the assumption that 'naming is dangerous' (2012: 333) and was motivated by the desire to protect research participants from harm if they were to be re-identified. This principle has been 'normalised through well-established ethical codes of practice' and is 'mentioned only briefly, and usually unproblematically, in accounts of the research process' (Tilley and

Woodthorpe, 2011: 198). As Saunders et al. note, 'Many official ethics guidelines recommend disguising the personal identities of research participants as a *default* position' (2015: 617). Qualitative researchers therefore generally 'only use real names when respondents are public officials' (Guenther, 2009: 411) and often go to great lengths to disguise respondents' identities.

There are often very clear reasons why a researcher would anonymise the identities of research participants and sites. For example, Tilley and Woodthorpe (2011) cite research with children and certain highly sensitive topics as two of the many scenarios in which participant anonymisation is likely appropriate. But plenty of qualitative researchers dispute the need to always anonymise research data. For example, Wiles et al. discuss the tensions between, on the one hand, researchers' need to safeguard participants, and on the other, participants' desire to be '*seen* as well as heard', particularly in visual research (2012: 41, emphasis in original). But the decision to non-anonymise may also be subjected to 'pressure from peers, publishers, regulatory bodies and research stakeholders' who may fight to 'uphold the principle of anonymisation' (Wiles et al., 2012: 42). *To anonymise or non-anonymise* becomes an equally complicated question when researching pseudonymous social media users: which aspect(s) of their identity should a researcher anonymise, if any? How should researchers anonymise their participants' data? At what stage should anonymisation happen? And how should researchers manage ethical regulation (i.e. from ERBs or funding bodies)?

As Warfield et al. (2019) note, these questions must often be answered *before* research takes place, as ERBs typically ask that all research involving human subjects and/or personal data undergo ethical review before data gathering commences. ERBs emerged in the 1970s and have traditionally been charged with three main tasks: (1) ensuring adequate consent is obtained from research participants, (2) minimising the occurrence of undue harm to research participants and anticipating risks as far in advance as possible and (3) maintaining research participants' anonymity (Buchanan, 2011: 87; Vainio, 2012: 685–686). Before data gathering commences, researchers should generally tell participants how their data will be used, and participants should be given sufficient time to ask questions about the research and the use of their data. But it is difficult for researchers to know how to deal with pseudonymous social media users' personally identifiable information in advance because of the complex reasons why people use pseudonyms. This is something researchers often learn throughout the life course of the project, once again highlighting the need for ongoing ethics review and/or ongoing consent.

Social media researchers face an extra set of requirements from the platform(s) they obtain data from. Popular microblogging platform Twitter, for example, has its own rules about data representation. In its Developer Terms, Twitter explains that those wishing to display Tweets must: 'Display real, unmodified Tweets from real accounts' and must not 'Modify Tweet text' (Twitter, 2020). Researchers who might be inclined to, for example, exclude Twitter usernames from academic publications for ethical reasons are now not permitted to do so, meaning Twitter's Terms pose a direct challenge to the principles of anonymisation in qualitative research. Indeed, the attitude *against* anonymisation seems relatively unique to internet research.

Awareness of the ethical challenges facing internet research has grown exponentially in the last decade: The Association of Internet Researchers (AoIR) has released three

ethical decision-making blueprints – 2002, 2012 and 2019 – and the United Kingdom's British Psychological Association (BPA, 2017), Economic and Social Research Council (ESRC, 2015) and British Sociological Association (BSA, 2017) have issued similar guidelines. As Warfield et al. explain, these guidelines generally reject 'ethical universalism' and instead advocate for 'attention to nuance, situated narratives, and granular ethical complexities' (2019: 2071). Across these documents there is a clear emphasis on social media users' *expectations* of privacy, and a call to arms for researchers to avoid directly quoting from social media data simply because it is publicly available. But none of the guidelines mentioned above address *pseudonymity* as a unique ethical consideration, which is often implicitly framed as an ethical challenge through case studies of internet and social media research but not discussed in its own right. While I agree with Warfield et al. that institutions' ethics guidelines are wise to reject 'ethical universalism' (2019: 2071), the complexity of social media identities perhaps ought to be better addressed by bodies like the AoIR, partly because where a user sits on this spectrum of pseudonymity might tell us how to treat them ethically. To highlight this point, I now turn to a discussion of the ethical decisions I made during my research with teen drama fans.

Pseudonyms in social media research: four ethical conundrums

The arguments presented in this article are based on four years of qualitative research with 22 adult fans of three television series predominantly aimed at teenagers: *Pretty Little Liars* (2010–2017), *Revenge* (2011–2015) and *The Vampire Diaries* (2009–2017). The research was motivated by a longstanding devaluation of young women's popular cultures (amongst others, see Radway, 1984) and explored adult fans' efforts to enact pseudonymous identities on social media to avoid scorn from people in their lives and within the fan community. The main question underpinning this research was: 'how does the relationship between derision, guilt and pleasure emerge through teen drama fans' articulations and negotiations, and how are social media platforms integrated into and conceptualised within these dynamics?' The research combined two qualitative methods: 22 semi-structured interviews held via Skype audio/video or email, and an observation of 17 participants' fan accounts across several social media platforms. I did not scrape or even screenshot any social media data to avoid collecting data from those who had not consented to be researched and instead took hand-written and typed field notes.

Social media is a core tool and site for qualitative research and the issues I discuss herein extend far beyond this specific case study. I structure this section around four questions my ERB asked me and that pertain to the practical issues of anonymising already-pseudonymous social media users' data, but this framing is neither intended to suggest that all researchers have uniform experiences with ERBs, nor is it necessarily intended to criticise the ERB in question. Instead, the aim is to explore how social media researchers might deal with the slippery nature of personally identifiable information while situated in (and out) of the field with already-pseudonymised participants, and to be useful to other researchers facing similar dilemmas. Given the popularity of pseudonymity on social media, coupled with the growing penetration of

platforms across global demographics, a need for ethical discussions of this kind is surely set to increase.

Q1: Are you collecting data that is available in the public domain?

The question above could be answered simply, as 'public' social media data might be taken to include content unprotected by users' privacy settings and accessible to anyone with (and sometimes without) an account registered to a certain platform. For example, Instagram and Twitter users can set their accounts to 'public' instead of 'private', meaning anyone can see their posts instead of an approved list of 'followers'. Some platforms' rules against pseudonymity might also contribute to the handling of their users' data. Facebook, for example, has adopted a 'real name' model wherein users are required to provide their real (i.e. legal) identity markers when they create an account (Lingel and Gillespie, 2014). Facebook's prediction is that people will behave better online if they are tied to their real names: what Matias (2017) calls the 'real name fallacy'. But if tech industry workers like Mark Zuckerberg continue to propel the myth that 'privacy is no longer a social norm' (Barnett, 2010: n.p.), is there a greater likelihood that users' data will be regarded as 'public' and potentially de-anonymised? This is one of many examples of the tensions between platforms' policies and longer-standing ethical principles of anonymisation within qualitative research.

I amongst many others would argue that how researchers understand the 'public' domain should largely, if not entirely, rest on participants' expectations. But it is difficult to know how pseudonymous social media users feel about their privacy until researchers establish rapport with them, which typically happens once they are in the field. Pseudonymous social media users take careful steps to obscure parts of their identities, sometimes enacting new ones, indicating an awareness that their online content is searchable. Even if their data does not at first seem to be sensitive, a users' drive to conceal parts of their identity might be read as a sign that they require a greater level of protection. On the surface, teen drama fandom has comparatively low stakes to other pseudonymous social media users and communities, but the allure of secrecy drew my participants to certain platforms and they each referred to their fandom as their 'secret' (Oscar), 'anonymous' (Emily, Gioia and Taylor), 'hidden' (Kat), 'private' (Reesa) or similar acts. I should note here that these names are pseudonyms chosen by already-pseudonymous social media users, and they are neither the fans' legal names, nor are they the names they use in fan communities. My decision to anonymise pseudonyms was not without consequence, partly because valuable contextual details resided in the original pseudonyms. Although I lost some important contextual details, this decision also meant I fabricated (Markham, 2012) fewer details in publications and other outputs, as the fans told me a lot about their 'offline' identities during our interviews. I often found myself *fabricating fabrications* during the dissemination phrase of this research to ensure my participants' compartmentalised (van der Nagel, 2018) identities could not be linked together. For example, in addition to excluding usernames, I also felt it unethical to directly quote from my participants' online fan accounts, even if they were public in the technical sense. As Roberts notes:

> In some cases, pseudonyms of pseudonyms and settings may be used. However, this alone is unlikely to be enough to protect the identification of the individual or the setting. When providing direct quotes, even without attribution, the pseudonym and community may be locatable through search engines, log files and user profiles. (2015: 319).

Instead of using direct quotes from pseudonymised social media accounts, Markham proposes fabrication – a method borrowing from remix culture to provide a non-identical account of research data – as a 'sensible and ethically grounded solution for protecting privacy in arenas of shifting public/private context' (2012: 342). Despite critics of this method who, as Markham (2012) explains, deem it *un*ethical, fabrication is often one of the only harm-minimising way of ensuring the inclusion of particular voices in the research agenda.

If I had not been asked to make decisions about anonymising usernames and other forms of social media data *before* the research began, I might have opted to identify some of the participants in written materials. I learned that some fans work very hard on their accounts, referring to their fandom as a 'part-time job' (Nina; Felix), 'full-time job' (Emily) and 'work' (Elena; Kat), and ongoing consent around anonymisation would have offered greater respect for my research participants' wishes, resonating with the experiences of other qualitative researchers. I now turn to a discussion of a further ethical conundrum: ascertaining pseudonymous social media users' ages.

Q2: Will any of the research participants be under the age of 16?

Pseudonymous social media users deliberately falsify some of their identity markers, or might not reveal them at all. But this makes it difficult for researchers to know if users are underage, which has profound implications not only on the decisions researchers make around anonymisation but also how – and whether – to ethically involve certain participants in the research. As Livingstone et al. note, 'on the Internet no one knows who is an adult and who is a child, and SNSs rely heavily on users' professed ages or dates of birth' (2013: 305). But not all platforms require users to display their dates of birth and these details are also easily fabricated. At the time of writing, the three most popular platforms among my participants – Facebook Pages, Instagram and Twitter – did not require users to publish their dates of birth on their Profiles, yet the focus of my research (*teen* drama series) implied an underage demographic, and so I assumed some of my research participants would be underage.

Social media platforms also have their own rules about their users' ages. For example, American platforms like Facebook, Instagram and Twitter are governed by the Children's Online Privacy Protection Act 1998 (COPPA) and require users to be 13 to create an account (Lilley and Ball, 2013). But individual nation states can impose higher age limits, like the European General Data Protection Regulation (GDPR), which 'prevent[s] those under 16 from using social media and other online platforms unless the social media site or platform obtains parental consent' (Livingstone, 2016: n.p.). But unless social media users truthfully self-identify their ages on all platforms, researchers often neither know how old they are, nor can they take participation on platforms as a

signal of parental consent, which is still understood as a requirement for research involving children by some internet researchers (amongst others, Townsend and Wallace, 2016) and ERBs.

In my research, I offered potential participants the option of either typing their responses to a set of structured interview questions or answering some semi-structured questions through Skype audio or video. Of the participants who disclosed their age or age range, none were under the age of 16. Some, particularly those who conducted typed online interviews, did not identify their ages at all. Given my participants' desire to maintain secrecy and in consultation with my ERB, I decided not to ask them to provide their legal name, age, gender, sexual orientation, ethnicity, marital status, education history, country of residence, or similar details and instead allowed them to emerge through our discussions. Based on their responses, I then made decisions about the extent to which I would anonymise this personally identifiable information, which may or may not have been truthful and accurate to begin with. The consent form stipulated that I would exclude participants' legal names and pseudonyms from the research but they knew I might use other identity markers to paint a fuller picture of their fandom. I chose to exclude details that might make them traceable, especially those participants who had a particularly rare or popular online presence (for a similar argument, see Roberts, 2015). The consent form also stipulated that if a participant was under the age of 16, they should show their parents the information sheet. I cannot say for certain if any underage participants did this. Indeed, some fans said that they would not provide me with identifying information if I asked for it, and one fan sent an angry reply to a Facebook Message questioning my credentials and telling me that their fandom was none of my business.

I had to make a decision between: (1) requiring participants to provide their age (which might not have been entirely reliable) and obtaining parental consent to safeguard underage participants, and (2) respecting their desire to be pseudonymous online. My ERB approved the latter choice. The main question driving this research was to understand how people experience their socially devalued teen drama fandom, and the very reason they might not have revealed their ages to me or other people is because of this stigmatisation. For example, one of my participants, Amanda – a fortysomething and heterosexual woman who lives in North America – enacted the identity of her teenage child on her *Pretty Little Liars* Facebook fan Page. She talked about events happening in her child's life to construct this identity, like applying for colleges and attending summer camp, and yet she was a mother-of-two with a Master's in Business Administration (MBA) degree who worked part-time as an events manager. Her child was aware that she adopted their identity but other people in her life – friends, work colleagues and other family members – did not know about her fandom. Amanda used her child's identity because she was bullied for being an adult fan of a teen show when she participated in the show's official Facebook Page using her Facebook Profile, which disclosed her 'real' identity. Although Amanda revealed these intimate details to me, she did not agree to a Skype video interview and we spoke using only audio. Anonymising Amanda's personally identifiable information proved to be incredibly complex.

Spriggs argues that 'parental consent in addition to young people's consent is not always ethically required because adolescence is a time for young people to establish 'independence', and so they may choose to 'keep parts of their lives private' (2009: 9;8)

from their parents or guardians. Similarly, in Gray's ethnography of North America's rural queer youth, she convinced her ERB to waive parental consent because 'without such a waiver, youth from families hostile to queer identities who sought permission to participate would be put at greater risk' (2003: 19). As teen drama fandom is often enacted in secret, my research participants could have faced greater harm if I had required their parents' consent for them to participate. This is precisely why I argue that pseudonymous social media users present different challenges to ethical decision-making, particularly the practicalities of anonymisation, to those who use their legal names and ages. Indeed, a person's online pseudonym and their engagement in complex identity work might be taken as a signal that they require *greater* ethical protection. The following section discusses a further ethical practicality challenged by pseudonymity: obtaining informed consent.

Q3: Will informed consent be obtained from the research participants?

One of the foundational ethical principles of qualitative research is to obtain informed consent from participants. As Tiidenberg explains, informed consent means that researchers 'commit to giving detailed information on the purpose, duration, methods, risks and benefits of the study to participants, while participants have an absolute right to withdraw at any time' (2018: 470). Most ethics boards require researchers to obtain informed consent when researching human subjects unless they have very good reasons for not doing so (Livingstone and Locatelli, 2014). But informed consent is not always obtained for internet research, partly because the definition of 'human subjects' gets fuzzier when data cannot be easily tied to an identifiable individual (e.g. in 'Big' datasets), and because the growing volume of social media data makes it difficult for researchers to obtain informed consent from all users. This ethical discrepancy is also linked to the identity politics of different platforms. For example, in this article's introduction, I explain that 4chan and Facebook's founders have opposing rules and norms around their users' identities, meaning it might seem more acceptable to not seek consent from 4chan users than those using Facebook. While I did not view my participants' social media content as freely available to de-anonymise and use for research purposes, their desire for pseudonymity challenged some of the more traditional ways of obtaining their consent.

For example, qualitative research participants have traditionally hand-signed consent forms in offline settings. But as Livingstone and Locatelli ask, 'how can researchers gain hand-signed informed consent from participants known only by their online chat names?' (2014: 68). Like Tiidenberg (2018), I allowed participants to sign the consent form using their social media handle, given my ethical commitment to not asking for any identifying details. This gave participants an extra layer of anonymisation. Pseudonymous social media users face a further set of complications to those who go by their real names as they often do not want their falsified identities to be linked with any others, and I had to make subjective decisions about what counts as personally identifiable information (PII). As Zimmer explains, in the United States, PII is defined as an 'individual's name or other personally identifiable elements such as a social security number, a driver's license number, or a credit card number', whereas in the European Union the definition of PII is much broader, and includes subjects' 'physical, physiological, mental, economic,

cultural or social identity' (2010a: 319). As decisions about what counts as PII in a social media dataset are often subjective and unaided by the vague definitions cited above, social media data presents a further practical issue for anonymisation.

For example, two of my research participants, Felix and Oscar, identified as male and heterosexual fans of *Pretty Little Liars*. They ran a popular series of social media accounts for the show through which they selectively disclosed PII because they did not want anyone they worked with to know they were fans of a show aimed at teenage girls. Although Felix and Oscar told me where they worked, lived and what their legal names and ages were during our interview, I felt an ethical responsibility to replicate only the PII they included on their social media fans accounts when I presented my research findings. To an extent, pseudonymous social media users like Felix and Oscar helped me to make ethical decisions about anonymisation by limiting their own disclosure of PII.

Pretty Little Liars fan Reesa similarly told me that she did not include hyperlinks to any of her fan accounts on her personal Facebook Profile (which I did not observe). She perceived details like her legal name to be threats to her privacy and so she adopted a fan identity that she felt was PII-free. *Revenge* fan Emily controlled her online identities in a similar way: she did not reveal her legal name or geographical location to other fans and instead operated as her social media handle when she engaged in online fandom. Emily also told fans that she was Canadian even though she is not: 'every now and then I'll drop in– like I'm celebrating Canadian Thanksgiving, or little things here and there'. Although Emily had multiple accounts on the same social media platform (two Facebook Pages and a Profile), she imagined her privacy differently according the account's purpose. This was because, due to Facebook's real-name policy, Emily provided her legal identity information on her Facebook Profile and used an image of herself as her Profile picture, but on her Pages she 'role-played' as two *Revenge* characters. Although Facebook users must have a Profile in order to create a Page, the connection between a user's Profile and Page(s) are visible only to them, enabling people to create 'secret' Pages. Ethical decisions must thus be made at both an *inter-platform* level (by accounting for the differences between platforms) and at an *intra-platform* level (by accounting for the myriad communicative dynamics that exist within one platform). These technological specificities create further challenges for anonymisation in qualitative research outputs because, while the researcher might be aware of the connections between a person's social media identities and accounts, they must carefully avoid connecting the deliberately disparate dots. Social media researchers must weigh up the benefits and risks of including certain descriptive details in their work, especially if participants do not include them in their online presence but discuss them elsewhere (for example, in an interview).

In offline qualitative research, scholars often engage in 'extensive masking by, for example, altering identifying characteristics about people (e.g., changing a person's gender or occupation) and places (e.g., altering historical events or census data), omitting primary source references, and/or creating composite character' (Murphy and Jerolmack, 2016: 14). Although the same masking techniques can be applied to social media research – see Markham (2012) on 'fabrication' – respondents' online data is arguably more 'searchable' than those studied offline. Murphy and Jerolmack feel that researchers should ask people if they want to be anonymised in research outputs (see also Guenther, 2009; Moore, 2012), but this question is more difficult to ask of a pseudonymised social

media research participant. For example, if a participant wanted their pseudonym to be published in research outputs, they might not be aware that it is fairly easy to build a fuller picture of their identity using search engines. As Roberts notes, pseudonyms also develop reputations 'over time' (2015: 319), meaning there might be risks of non-anonymisation in the 'longer'-term, of which neither the participant nor the researcher could foresee (Wiles et al., 2012: 42). The final question I discuss in this paper concerns a different set of risks: 'friending' your research participants and anonymising your own social media data.

Q4: Does the research involve any risks to the researchers themselves?

One of the main differences between the AoIR's Internet Research Ethics 2.0 and 3.0 guidelines is that the latter version, published in 2019 (see franzke et al., 2019), includes a section on safeguarding researchers. Academics across disciplines are harnessing social media for their personal and professional lives, creating their own online presence and information trails. Using social media to engage with respondents and maintain professional and other relationships (if the two can be neatly separated) exposes researchers to 'the full array of hate speech, threats, and acts that are now routinely directed at them – especially if they are women researching predominantly male hate behaviors (e.g., Massanari, 2016)' (Ess, 2017: xiv). For example, games studies scholars Chess and Shaw organised a fishbowl at an academic conference to discuss identity and diversity in video games studies. Participants contributed to a Google Doc which was shared on Twitter and found by a group of users who were not at the conference. They:

> began researching Shaw, collecting her publications, and reviewing her Twitter account. She was accused of having imposter syndrome which was intended to be a point of attack; 'call them frauds, that's a week [sic] point' (Burgers and Fries, 2014). (Chess and Shaw, 2015: 212)

Chess and Shaw are not alone. Shortly after the 2016 U.S. presidential election, social scientist Cuevas (2018) participated in a Twitter conversation about the merits of the Electoral College system versus the popular vote. He was later targeted by members of the far-right. They called him 'n*****' and a 'f*****', told him he must 'go back' (i.e. be deported) because he is Hispanic and was accused of anti-Semitism (Cuevas, 2018, n.p.).[2]

These are two of the many instances of online harassment against academics, typically those who are female and/or have marginalised identities. Although Ess (2017) argues that the risks facing researchers are central issues for IRE 3.0, the question 'does the research involve any risks to the researchers themselves, or people not directly involved in the research?' was one of the last on the ERB I completed. The de-prioritisation of risks to researchers by this particular ERB might discourage internet researchers from taking this issue seriously. I found it difficult to answer this question before the research took place, meaning my response was based largely on my assumption that the subject matter – teen television series – would be more or less risk-free. But my response unintentionally reproduced stereotypes of young and

female-centric fandoms by framing them as trivial. And yet, despite my assumptions, I faced a number of difficult scenarios.

For example, one participant asked me to mail some women's fashion magazines to her, like *Teen Vogue* and *Cosmopolitan*, as her father would not permit her to have them. She wanted me to do this in exchange for her help and I felt this was a fair request. She had, after all, given up 2 hours of her time to talk about her fandom, allowed me to observe her social media account and introduced me to other members of the fan community. But I decided to respect her father's wishes and not mail her the magazines. I had the opposite relationship with some research participants. Many added me as a friend or 'followed' me on my personal social media accounts, and while these friendships were an unexpected and mostly positive outcome of the research, they forced me to make ethical judgements far beyond what I wrote or even thought about in the ERB. Robards (2013) shares a similar experience of 'friending' his research participants on Facebook and MySpace. Robards changed his research design part-way through the project by deciding not to friend his 15–17-year-old research participants to avoid 'invasiveness' (2013: 227) in the young people's social media spaces.

Incidents like these opened my eyes to the risks of recruiting participants through social media, but creating new accounts without years' worth of content to ascertain your credibility might be unwise. I used three online avenues to contact potential participants: my University email address, my Twitter account and my Facebook Profile. Although Twitter is a non-academic social networking platform (unlike academia.edu or similar), I consider my account to be for 'professional' purposes as I identify with my job title and use the account to interact with fellow scholars. I did not create a separate academic account on Facebook to recruit participants. I used my personal Profile, through which I interact with friends from both within and outside of academia. McKee and Porter note that a key issue facing qualitative internet researchers is that the methods to establish their identity differ from face-to-face interactions, through which participants can make assumptions about the researcher based on their 'embodiment (presence of a physical body)' (2009: 99). I used my Facebook Profile to establish my credibility as a researcher, given that it features various identity markers (e.g. a profile picture, gender, current city, and work and education information). Given my decision to use snowball sampling as a recruitment method, the majority of my research participants were entirely unknown to me, and as was I to them, increasing my desire to be as transparent as possible about my identity and intentions. McKee and Porter argue that transparency of this kind is 'critical to maintaining both personal and research credibility when studying online communities' (2009: 102).

There are of course consequences to this decision. I took strategic measures to protect the privacy of my own Facebook friends by, for example, restricting the visibility of my friends list to 'only me', limiting the audience of past posts, removing or hiding profile and cover images featuring other people, and hiding content from Facebook users who had not requested to be my friend. Ethical decisions like the ones I made in my research are of increasing importance given the growing uptake of social media use amongst academics. While the focus of this article has been on the conundrums of anonymising already-pseudonymous participants' research data,

researchers also need to consider the anonymisation of their own online presence. But it was very difficult, perhaps even impossible, to anticipate these risks ahead of time, so perhaps ERBs could ask internet researchers what safeguarding measures they have in place, especially if they are researching pseudonymous social media users, given the near-certainty that they will use online avenues to recruit and interact with their respondents.

Conclusions

This article has not claimed to offer the 'right' answers to the questions discussed above, and nor has it argued *for* or *against* the principles of anonymisation. Instead, it has addressed some of the challenges pseudonymous social media identities present to the ethical principles of anonymisation in qualitative research. Its main intention is to assist researchers facing similar ethical conundrums, given the popularity of pseudonymity on social media and the growing penetration of platforms across global demographics. By exploring my own ethical decision-making processes, the article has addressed some of the challenges pseudonymity presents to the processes and principles of anonymisation. Many of the challenges I faced over the life course of my research were linked to the extent to which I should (or should not) anonymise my participants' personally identifiable information, and the practical issues of doing so. These ethical conundrums include: shifting notions of 'pubic' and 'private' forms of research data, the parameters of which are often rigidly defined by social media platforms; safeguarding underage and therefore vulnerable research participants, and the uncertainties of ascertaining a social media user's age; ways of obtaining informed consent that can differ from the approaches used in traditional, offline qualitative research; and questioning the extent to which researchers should anonymise their own data for personal safeguarding purposes. The ethical quandaries discussed in this paper have several implications for the conduct of social media research and the workings of ethics reviews committees, two of which are discussed below.

First, this paper joins other qualitative researchers to make the case for ethics review to be *ongoing* over the life course of research instead of only at the beginning, especially when research involves pseudonymous social media users. Along with researchers like Warfield et al. (2019), I also advocate for ongoing consent procedures across the duration of a project. Pseudonymous social media users engage in often-elaborate identity cloaking mechanisms, which inevitably evolve over time as platforms change in scope and scale. This means both researchers *and* already-pseudonymised research participants might not be aware of the benefits or harms of anonymisation until they are already in the field, and which might not be fully realised until an even later stage. Core stages in the qualitative research process where ethics procedures might need to be revised include, but are certainly not limited to: research design; participant recruitment; data gathering (revised at multiple points for mixed-methods approaches); data storage and analysis; and data representation(s). A shift towards ongoing ethics review is already being embraced by some institutions: for example, the ESRC's Framework for Research Ethics notes that, in participatory social science research:

> Highly formalised or bureaucratic ways of securing consent should be avoided in favour of fostering relationships in which ongoing ethics regard for participants is to be sustained, even after the study itself has been completed. Review mechanisms will need to enable this where appropriate. (2015: 31)

As Saunders et al. note, 'anonymising is very much an evolving exercise that continues to throw up challenges and surprises' (2015: 630), and my hope is that the ESRC's ethos is embraced across other funding bodies and institutions.

Second, I advise ethical decision-making blueprints for social media research to more directly address the challenges pseudonymous social media identities create for the treatment of personally identifiable information. Pseudonymity is highly likely to remain popular with social media users and qualitative researchers for many years to come, and online identity politics are becoming increasingly complex as platforms grow. Qualitative internet researchers must therefore deal with many aspects of an already-pseudonymised participant's identity, creating significant practical challenges and increasing the risk that the participant may become unintentionally de-anonymised through research outputs. While there are lots of reasons why people use pseudonyms on social media, might their efforts to do so be read as a sign that they require *greater* ethical protections? Questions like this ought to be more frequently explored in ethical blueprints.

Qualitative researchers are already engaged in debates about the nature of anonymisation and are calling for an overhaul of some of its processes. My article adds to this body of work by exploring how pseudonymous social media users raise unique and challenging questions for the *if, how, when* and *why* of participant anonymisation.

ORCID iD

Ysabel Gerrard https://orcid.org/0000-0003-1298-9365

Notes

1. When I capitalise 'Pages' I am referring to Facebook's Pages function as a distinct communicative space from Profiles.
2. I have censored the two words in this sentence to avoid distressing readers, but it should be noted that the abusers used the full words.

References

Barnett E (2010, 11 January) Facebook's Mark Zuckerberg says privacy is no longer a 'social norm'. *The Telegraph*. Available at: https://www.telegraph.co.uk/technology/facebook/6966628/Facebooks-Mark-Zuckerberg-says-privacy-is-no-longer-a-social-norm.html (accessed 29 August 2018).

British Psychological Association (2007) Ethics Guidelines for Internet-Mediated Research. Available at: https://www.bps.org.uk/news-and-policy/ethics-guidelines-internet-mediated-research-2017 (accessed 12 May 2020).

British Sociological Association (2017) Ethics Guidelines and Collated Resources for Digital Research: Statement of Ethical Practice Annexe. Available at: https://www.britsoc.co.uk/media/24309/bsa_statement_of_ethical_practice_annexe.pdf (accessed 12 May 2020).

Buchanan E (2011) Internet research ethics: past, present, and future. In: Consalvo M and Ess C (eds) *The Handbook of Internet Studies*. Malden, MA: Wiley-Blackwell, 83–108.

Burgers and Fries (2014) IRC chat log on 'The Zoe Quinnspiracy'. Available at: http://gamergate.giz.moe/wp-content/uploads/2014/09/burgersandfries-IRC-Chat-Log.txt (accessed 12 May 2020).

Chess S and Shaw A (2015) A conspiracy of fishes, or, how we learned to stop worrying about #GamerGate and embrace hegemonic masculinity. *Journal of Broadcasting and Electronic Media* 59(1): 208–220.

Cuevas JA (2018) A new reality? The far right's use of cyberharassment against academics. American Association of University Professors. Available at: https://www.aaup.org/article/new-reality-far-rights-use-cyberharassment-against-academics#.W4lPFi2ZMy4 (accessed 31 August 2018).

Donath J (1999) Identity and deception in the virtual community. In: Kollock P (ed) *Communities in Cyberspace*. London; New York: Routledge, 29–59.

Economic and Social Research Council (ESRC) (2015) ESRC framework for research ethics. Available at: https://esrc.ukri.org/files/funding/guidance-for-applicants/esrc-framework-for-research-ethics-2015/ (accessed 5 February 2020).

Ess C (2017) Foreword: grounding internet research ethics 3.0: a view from (the) AoIR. In: Zimmer M and Kinder-Kurlanda K (eds) *Internet Research Ethics for the Social Age*. New York: Peter Lang, ix–xv.

franzke AS, Bechmann A, Zimmer M, et al. (2019) Internet research: ethical guidelines 3.0. Available at: https://aoir.org/reports/ethics3.pdf (accessed 13 February 2020).

Gerrard Y (2017) 'It's a secret thing': digital disembedding through online teen drama fandom. *First Monday* 22(8). Available at: https://doi.org/10.5210/fm.v22i8.7877 (accessed 12 May 2020).

Gray ML (2003) The plasticity of vulnerability: research with a stigmatized community. *Anthropology News* 44(8): 19.

Guenther KM (2009) The politics of names: rethinking the methodological and ethical significance of naming people, organizations, and places. *Qualitative Research* 9(4): 411–421.

Haimson OL and Hoffman AL (2016) Constructing and enforcing 'authentic' identity online: Facebook, real names, and non-normative identities. *First Monday* 21(6). Available at: https://journals.uic.edu/ojs/index.php/fm/article/view/6791 (accessed 29 January 2018).

Hogan B (2015) Pseudonyms and the rise of the real-name Web. In: Hartley J, Burgess J and Bruns A (eds) *A Companion to New Media Dynamics*. Chichester: Wiley-Blackwell, 290–310.

Lilley C and Ball C (2013) Younger children and social networking sites: a blind spot. National Society for the Prevention of Cruelty to Children (NSPCC). Available at: https://www.nspcc.org.uk/globalassets/documents/research-reports/younger-children-social-networking-sites-report.pdf (accessed 21 January 2018).

Lingel J (2017) *Digital Counter-Cultures and the Struggle for Community*. Cambridge, MA: MIT Press.

Lingel J and Gillespie T (2014, October 2) One name to rule them all: Facebook's identity problem. *The Atlantic*. Available at: https://www.theatlantic.com/technology/archive/2014/10/one-name-to-rule-them-all-facebook-still-insists-on-a-single-identity/381039/ (accessed 4 February 2020).

Livingstone S (2016, 17 October) To be 13 or 16, that is the question: the implications for UK teenagers of the European General Data Protection Regulation. LSE Media Policy Project Blog. Available at: http://blogs.lse.ac.uk/mediapolicyproject/2016/10/17/to-be-13-or-16-that-is-the-question-the-implications-for-uk-teenagers-of-the-european-data-protection-regulation/ (accessed 8 February 2018).

Livingstone S and Locatelli E (2014) Ethical dilemmas in qualitative research with youth on/offline. *International Journal of Learning and Media* 4(2): 67–75.

Livingstone S, Ólafsson K and Staksrud E (2013) Risky social networking practices among 'underage' users: lessons for evidence-based policy. *Journal of Computer-Mediated Communication* 18(3): 303–320.

Markham A (2012) Fabrication as ethical practice: qualitative inquiry in ambiguous internet contexts. *Information, Communication and Society* 15(3): 334–353.

Massanari A (2016) The changing nature of research in the age of #Gamergate. In: *Association of Internet Researchers annual Internet Research conference*, Panel presentation, Berlin, 6 October 2016.

Matias JN (2017, 3 January) The real name fallacy. *The Coral Project*. Available at: https://coralproject.net/blog/the-real-name-fallacy/ (accessed 21 August 2018).

McKee HA and Porter JE (2009) *The Ethics of Internet Research: A Rhetorical, Case-Based Process*. New York; Oxford: Peter Lang.

Moore N (2012) The politics and ethics of naming: questioning anonymisation in (archival) research. *International Journal of Social Research Methodology* 15(4): 331–340.

Murphy A and Jerolmack C (2016) Ethnographic masking in an era of data transparency. *Contexts* 5(2): 10–19.

Phillips W and Milner R (2017) *The Ambivalent Internet: Mischief, Oddity and Antagonism Online*. Cambridge, UK; Malden, MA: Polity.

Radway J (1984) *Reading the Romance: Women, Patriarchy, and Popular Literature*. Chapel Hill, CA: University of North Carolina Press.

Richmond S (2011, 14 March) Facebook wrong about anonymity, says 4chan founder. *The Telegraph*. Available at: https://www.telegraph.co.uk/technology/sxsw/8379895/Facebook-wrong-about-anonymity-says-4chan-founder.html (accessed 22 August 2018).

Robards B (2013) Friending participants: managing the researcher-participant relationship on social network sites. *Young* 21(3): 217–235.

Roberts LD (2015) Ethical issues in conducting qualitative research in online communities. *Qualitative Research in Psychology* 12(3): 314–325.

Saunders B, Kitzinger J and Kitzinger C (2015) Anonymizing interview data: challenges and compromise in practice. *Qualitative Research* 15(5): 616–632.

Schrag ZM (2011) The case against ethics review in the social sciences. *Research Ethics* 7(4): 120–131.

Spriggs M (2009) Consent in cyberspace: internet-based research involving young people. *Monash Bioethics Review* 28(4): 1–15.

Tiidenberg K (2018) Ethics in digital research. In: Flick U (ed) *The SAGE Handbook of Qualitative Data Collection*. London: SAGE, 466–481.

Tilley L and Woodthorpe K (2011) Is this the end for anonymity as we know it? A critical examination of the ethical principle of anonymity in the context of 21st century demands on the qualitative researcher. *Qualitative Research* 11(2): 197–212.

Townsend L and Wallace C (2016) Social media research: a guide to ethics. Available at: https://www.gla.ac.uk/media/media_487729_en.pdf (accessed 27 January 2018).

Twitter (2020) Display requirements: tweets. developer terms. Available at: https://developer.twitter.com/en/developer-terms/display-requirements (accessed 4 February 2020).

Vainio A (2012) Beyond research ethics: anonymity as 'ontology', 'analysis' and 'independence'. *Qualitative Research* 13(6): 685–698.

Van der Nagel E (2017) *Social media pseudonymity: affordances, practices, disruptions*. PhD Thesis, Swinburne University. Available at: https://researchbank.swinburne.edu.au/items/25cfcac7-82ea-4d9e-8681-d9965e6247d1/1/ (accessed 15 August 2018).

Van der Nagel E (2018) Alts and automediality: compartmentalising the self through multiple social media profiles. *M/C Journal: A Journal of Media and Culture* 21(2). Available at: http://journal.media-culture.org.au/index.php/mcjournal/article/view/1379 (accessed 7 February 2020).

Van der Nagel E and Frith J (2015) Anonymity, pseudonymity, and the agency of online identity: examining the social practices of r/Gonewild. *First Monday* 20(3). Available at: https://firstmonday.org/article/view/5615/4346 (accessed 20 January 2018).

Warfield K, Hoholuk J, Vincent B, et al. (2019) Pics, dicks, tits, and tats: negotiating ethics working with images of bodies in social media research. *New Media and Society* 21(9): 2068–2086.

Whelan A (2018) Ethics are admin: Australian human research ethics review forms as (un)ethical actors. *Social Media + Society* 4(2): 1–9.

Wiles R, Coffey A, Robinson J, et al. (2012) Anonymisation and visual images: issues of respect, 'voice' and protection. *International Journal of Social Research Methodology* 15(1): 41–53.

Zimmer M (2010a) 'But the data is already public': on the ethics of research in Facebook. *Ethics and Information Technology* 12(4): 313–325.

Zimmer M (2010b) Facebook's Zuckerberg: 'Having two identities for yourself is an example of a lack of integrity'. [Blog]. Available at: http://www.michaelzimmer.org/2010/05/14/facebooks-zuckerberg-having-two-identities-for-yourself-is-an-example-of-a-lack-of-integrity/ (accessed 3 February 2018).

Author biography

Ysabel Gerrard is a lecturer in Digital Media and Society at the University of Sheffield, UK. She is interested in the relationship between social media and identity and researches, amongst other things, social media content moderation, secret-telling apps, and mental health communities. Gerrard is the current Vice Chair of ECREA's Digital Culture and Communication section, the Book Reviews Editor for *Convergence: The International Journal of Research into New Media Technologies*, and a former Microsoft Research New England intern. Her writing and research have been featured in academic publications like *New Media and Society* and *First Monday*, and her popular writing and policy contributions have included in venues like *BBC News, The Guardian* and *WIRED*.