Using Manufactured Identities in Online Social Media

By

Roseann Markham – Curtin University, OUA

Abstract

The use of pseudonyms and personas when creating profiles within online social media serves to provide many vulnerable people with a way to safely have an online presence without the fear of harassment or real world threats. The rise in the number of hacking incidents involving identity theft combined with a growing number of reports of fake online identities being used for malicious and criminal intent, has led to companies such as Facebook implementing security measures such as the real name policy, where all Facebook profile names must be consistent with real world identity protocols. While the argument in favour of the real name policy may appear sincere, some scholars and recent media reports suggest that the motivation for such actions may be commercially driven. While there should be a place within online social media communities for members to utilise pseudonyms and personas, the rise of complacency regarding attention to protecting personal information and the wilful disclosure of private data make it difficult for companies and regulators to ensure the protection of online users' identities. The argument presented here is not for a blanket approach to anonymity online, rather it is for the right to ensure one's privacy protection when using the largest online social network, Facebook, through the use of pseudonyms and personas. It is the intention of this paper to present how, when used for genuine purposes; there are still valid reasons why pseudonyms and personas should remain a part of a user's online presence.

Key Words

Online communities, identity, social networks, pseudonyms, personas, privacy, anonymity, Facebook

Introduction

The issues of user privacy and identity theft have been key elements of discussion on internet security since the rise of the World Wide Web. The advice of software suppliers and internet security companies to regularly change user passwords and to be cautious when sharing personal information, has been the norm for over 25 years with many obedient online users creating pseudonyms and personas as part of their use of different online services including customised email addresses, social media names and website account details. These self-protection measures are now becoming more difficult to sustain, as several of the large and dominant internet companies such as Facebook, Google, LinkedIn and other similar online services press for a global real name policy for all of their users (Hogan, 2013, p. 2). At the same time, the increase in hacking incidents and the subsequent data thefts has escalated concerns regarding the safety of people's personal information being held within the databases of many internet companies. The use of pseudonyms and personas provides a solution for those concerned about risks to their privacy and safety, to access and use online social networks such as Facebook without compromising their real world identities or personal data. The argument presented here should not be misinterpreted as being for a blanket approach to anonymity online, rather it is for the right to ensure one's privacy protection when using the largest online social network, Facebook, through the use of pseudonyms and personas. Strong arguments have been expressed by academics and security experts both in support of the online real name policy and firmly against the measure. Likewise, there are differing views and opinions regarding the use of pseudonyms and personas online, ranging from protecting the vulnerable to facilitating online abuse. By analysing these varying beliefs and establishing a more balanced perspective, it is the intention of this paper to present how, when used for genuine purposes; there are still valid reasons why pseudonyms and personas should remain a part of a user's online presence.

Discussion

Online social networks such as Facebook provide users with a platform for developing and becoming members of online communities. For most people these virtual communities often reflect similar characteristics to offline communities such as "…sociability, meaningful connection to others, conviviality, perhaps even empathy and support" (Parks, 2010, p. 106). Furthermore, due to familiarity with other members within these online communities, users often feel a sense of loyalty, compassion, belonging and confidence in the maintenance of privacy between friends and family (Bauman, 2001). These feelings may fuel an increased level of complacency and a degree of overconfidence in the security of their information that is being shared within the online community.

The trust that users have in other members of their online community often automatically extends to the social network being used by that community, leading to an increase in the quantity and types of personal information being shared, including the location of users of mobile devices, which poses further risks to the protection of their data (Fire, Goldschmidt, Elovici, 2014, p. 1). While some users may try to implement some degree of security in the way that they liaise with others on social media, such as restricting direct communications to private messaging, not posting photos and activating strong privacy and security settings, there is no guarantee that their friends are following the same practices, possibly increasing their level of exposure to breaches of privacy. With the ongoing sharing of personal information comes the elevated likelihood of that data becoming "…more identifiable and potentially vulnerable to cross-site record linkage" (Zhu, Zhang, Singh, Yang, Sherr, 2016, p. 1). The current push by large online platforms such as Facebook for real names to be applied to the profiles of all users goes against many of the original principles promoted by the social network's founder, those being the protection of the vulnerable, eliminating offensive targeted conduct and facilitating a safe environment for freedom of expression (Hogan, 2013, p. 2). While claiming that the need for all users to operate under real names "…helps to create a more just society" (Hogan, 2013, p. 2). It could also be viewed as a measure to satisfy the business needs of

Facebook, increasing the legitimacy and, therefore, the value of personal data being sold to third parties.

The use and misuse of people’s private online data is regularly the topic of front page news, ranging from the revelation of Cambridge Analytica harvesting the personal profiles of 50 million U.S. based Facebook users “…in order to target them with personalised political advertisements” (Cadwalladr and Graham-Harrison, 2018) to the U.S. State Department recommending that many future U.S. immigration visa applicants be required to provide all details of any social media accounts that they have used within five years of their applications (O’Brien, 2018). While these reports may heighten the concerns of some Facebook holders regarding the safety of their personal data and reduce their trust in Facebook’s security measures, this may not be alarming enough to prompt many account holders into any form of pro-active enhancement of their levels of security. One example of security complacency is where many online users appear to be content with the default security settings within Facebook, not realising that these are set at a minimal security level, where information viewed by friends can also be gathered by those friends and shared to others without the knowledge of the original account holder (Saeri, Ogilvie, and La Macchia, 2013, p. 3). The willingness of many Facebook users to accept friend requests from strangers, whose mutual connection may be either a common friend or similar interest, raises further concerns about whether their personal information is simply being kept within close circles or being accessed by external operators who might target specific online users due to more specific and possibly dangerous identifiers including how old they may be, their wealth and their sexual preferences (Fire, Goldschmidt, Elovici, 2014, p1). The damage that can be caused through complacency and ignorance further supports the need for users to be more actively diligent in heightening their online security awareness and acting on that knowledge to protect their personal data.

The bonds that are established between friends within an online community are not subject to the real world credibility of the name that appears on the screen, but is based upon a set of personal commonalities such as cultural ties, artistic taste, shared opinions and beliefs and emotional support that is developed and strengthened over time (Parks, 2010, p. 108-109). While a user’s friends may be comfortable identifying them by a pseudonym, the social media platform hosting their virtual community does not find any value in their artificial identity as only real names are a true commodity, providing companies with real world data on a wide range of subjects, ranging from spending habits, tastes in entertainment, leisure, foods, clothing, travel, political preferences, religion and ethnicity, unfortunately the preferences of Rosey Colordspecs, from Frog's Hollow, Whereami, will not be of as much use to the companies hoping to utilise this type of data (Boyd, 2011). Boyd (2011) notes that pseudonyms and personas have been used as part of many users' Facebook profiles for years without causing any negative effect, highlighting the fact that a significant part of the online community could be adversely affected by the forced disclosure of their real names, such as "…abuse survivors, activists, LGBT people, women, and young people" (Boyd, 2011). More recently, Haimson & Hoffmann (2016) also observed some of the problems that the real name policy was creating, in that some groups in society have names that don't fit within the strict criteria set by Facebook, as their names may be either singular or multi-faceted, this in addition to the many people needing to protect themselves from real world danger, including "…transgender and gender variant users, drag queens, Native Americans, abuse survivors, and others" (Haimson & Hoffmann, 2016, p. 3). This suggests that while these are not people with a desire for trolling or cyberbullying, many feel that they are treated by Facebook in the same manner as those who create fake accounts for malicious intent.

While there are alternatives to Facebook, such as 4chan and 2channel that support the use of anonymity on their platforms, providing subject-related forums and discussion channels for users to share opinions, pictures and comments, their scope, features and functions are very limited in comparison to the opportunity to experience a more holistic online presence offered by Facebook, where the user can manage attendance at events, play games, monitor news reports, follow fandoms and keep in touch with family and friends within the one channel and at the same time maintain a pseudonym or persona that protects their privacy from the broader online community (Knuttila, 2011) (Matsumura, Shibanai, Ohsawa, & Nishida, 2005, p. 2). Different online social networks, academics, internet experts and even politicians appear to hold distinctly opposing views towards the use of an artificial online identity, many classifying them as fake identities and tending to label all who use names other than their own as having malicious or harmful goals and being "…cyber criminals including sexual predators, online fraudsters, advertising campaigners, catfishes, and social bots…" (Wani & Jabin, 2017, p. 1). Interestingly, it was these same scholars, who observed that it is the files of users with real names that are more vulnerable to attacks from those interested in identity theft, reporting that due to their being regularly targeted by cyber criminals "…compromised real profiles spread more malicious content than other types of fake profiles…"and that "…more than 97% (of) profiles are compromised rather than fake" (Wani & Jabin, 2017, p. 3). It appears that those arguing against the use of pseudonyms and artificial personas seem to automatically assume that the person with the created online identity intends to either use it to facilitate malicious purposes or that a manufactured identity will help to better facilitate a means for expressing themselves on social media and other platforms and not fearing personal reprisals for their actions. However, their positions seem to forget about those who are not so much interested in using their artificial personas for standing on an online soapbox as they are about merely having an online presence through different social media platforms, that will allow for the liaising with real world friends, following their interests, staying informed and benefitting from the growing range of platforms and services that exist online.

With over 83 million Facebook current active profiles classified as not real, there is further confusion between those online identities that are for legitimate purposes and others that have been designed to impersonate real users as a means for criminal or harmful intent (Smith, Smith & Blazka, 2017, p. 33). The combination of adverse headlines and confusing attitudes towards the use of pseudonyms and personas on Facebook, also adds to the frustration and paranoia of those users who have utilised the ability to create a manufactured profile to present themselves "…in a less gender stereotypical way online…" (Oberst, Renau, Chamarro & Carbonell, 2016, p. 559) providing them with an environment that had previously been viewed as safe to freely build online identities that they considered were truer reflections of their real selves, without the restrictions of social expectations (Oberst, Renau, Chamarro & Carbonell, 2016, p. 559). By Facebook setting its own rules regarding what classifies as a real name, the organisation has taken to imposing its own values upon the hundreds of millions of users, including those whose real world names or identities may not comply with the rigid name conditions required, being forced to reveal private records to support their claims to their names or having to modify "…their "authentic self" to fit the demands of Facebook's real name policies and restrictions," an action which may involve having to "...lie or distort information about themselves to meet Facebook's standards of authenticity, or refrain from using the site at all" (Haimson & Hoffman, 2016, p. 3). While not officially admitted, there may already be exclusions to the real name policy that facilitates certain occupations and individuals of public profile such as celebrities, law enforcement officers, military personnel, and security operatives. The possibility of this provision suggests that mechanisms may already be in place at Facebook to accommodate those that need the safety of an online pseudonym or persona and exclude them from the strict real name rules.

While Facebook may be publicly declaring that it is enforcing its real name policy and claiming the social network to be proof of its success, there are many account holders who are still using pseudonyms as their Facebook names, cleverly crafting two words into a structure that will fool Facebook's algorithm and appear as a general English name, in addition to the "…countless teens who signed up to Facebook late into the game (and) chose to use pseudonyms or nicknames" (Boyd, 2011). Another argument against the use of real names for online social network profiles relates to the potential for a crossing over of personal data and opinions that would ordinarily be kept within close circles of friends and family within the user's limited online community, spreading into their real world lives, being observed by work mates and associates that should not be privy to very private information such as medical information, personal crisis, emotional or sexual details leading to "…context collapse" (Hogan, 2013, p. 11). Interestingly, while Facebook has regularly been mentioned in the news headlines over concerns regarding user security, it seems that there may be a significant difference between the perceived concerns by young online users of Facebook regarding the safety of their identities and personal data, and the measures that they are prepared to and are actively undertaking, to ensure that the appropriate levels of protection have been met to keep their private information safe (Hargittai & Marwick, 2016, p. 3739). Hargittai and Marwick (2016) further revealed that during a recent survey, American students declared that "…48% posted their sexual orientation, 21% posted their partner's name, and 47% posted their political orientation" (Hargittai & Marwick, 2016, p.

3738). These degrees of ignorance and apathy are particularly dangerous in view of recent revelations regarding data harvesting and the involvement of third party operators handling very sensitive personal data. It is becoming much clearer that the “I don’t have anything to hide” and the “I don’t care what others think of my opinions and actions” attitudes may be very careless and lead to possibly unwanted repercussions.

Internet service providers, regulators and governments are struggling to find a balance between the need to ensure accountability by anonymous persons using their artificial identities for the wrong reasons and the need to respect the privacy of those online users who require an artificial identity for legitimate purposes, a right that has been acknowledged in America’s “… 2011 National Strategy for Trusted Identities in Cyberspace…” which supports the need for online privacy by ruling out the idea of demanding real world documents to prove identity and dismissing the concept of “…a single, centralized authority for authentication of real-world identities” (Wolff, 2012, p. 17). Wolff (2012) further explains that the companies running online social networks have an obligation to regularly review and update their security and privacy regulations and procedures of enforcement and that many of these platforms are operated by large privately owned corporations that seem to be applying their own agenda driven sets of rules, rather than those recommended by supporters of the right to personal privacy and freedom of speech (Wolff, 2012, p. 29). While these companies may have to comply with national and international regulations regarding security, privacy and conduct, it seems that some organisations have already chosen to demonstrate their vigilance by implementing their own security measures, such as Facebook’s real-name policy. However, sceptics might suggest that this policy may have been more about the validating the credibility of the data that has been collected on Facebook users for commercial purposes, rather than out of concern for the security of its users, a view being further fuelled by recent reports regarding the practices of Cambridge Analytica. In response to the dilemma surrounding the use of pseudonyms online and the need to ensure the safety of members and their personal data within online communities on social networks, Hogan (2013) suggested “we may live in a global village but our huts still need curtains” (Hogan, 2013, p. 14).

Conclusion

While the expressions of serious concern by Facebook and other online social media operators over the protection of their users' private information may be claimed as being for genuinely righteous reasons, there is also the possibility that the measures being implemented to alleviate these concerns, such as the real name policy, may be more fuelled by commercial needs rather than caring for the welfare of the users and their identities. While many members of online communities feel comfortable and safe using their real world names within the digital world, there is also a large number of online users that have legitimate reasons to support their need to withhold their real identities from being disclosed online, whose intents are not of a malicious nature, but are based upon the rights of all citizens within the global online community to be allowed to have a safe online presence without the fear of harassment, embarrassment, or unwanted intrusion. Being allowed to use pseudonyms and personas within their online communities is a simple, yet safe solution to this issue.

REFERENCES

Bauman, Z. (2001). *Community: seeking safety in an insecure world*. Cambridge, England: Polity.

Boyd, D. (2011). 'Real Names' Policies Are an Abuse of Power. *Danah Boyd, Apophenia.* Retrieved from: http://www.zephoria.org/thoughts/archives/2011/08/04/real-names.html

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian.* Retrieved from: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: threats and solutions. IEEE Communications Surveys & Tutorials, Vol. 16, Issue: 4, pp: 2019-2036. Retrieved from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6809839

Haimson, O. L., & Hoffmann, A. L. (2016). Constructing and enforcing "authentic" identity online: Facebook, real names, and non-normative identities. *First Monday*, 21(6). Retrieved from: http://www.firstmonday.dk/ojs/index.php/fm/article/view/6791/5521

Hargittai, E., & Marwick, A. (2016). “What can I really do?” Explaining the Privacy Paradox with Online Apathy. International Journal of Communication, Vol.10, Issue: 21, pp: 3737–3757. Retrieved from: http://ijoc.org/index.php/ijoc/article/viewFile/4655/1738

Hogan, B. (2013). Pseudonyms and the Rise of the Real-Name Web, A Companion to New Media Dynamics . Malden, MA: Wiley-Blackwell, pp. 290–308. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2229365

Knuttila, L. (2011). User Unknown: 4chan, Anonymity and Contingency. *First Monday*, 16(10). Retrieved from: http://www.ojphi.org/ojs/index.php/fm/article/view/3665/3055

Matsumura, N., Miura, A., Shibanai, Y., Ohsawa, Y., & Nishida, T. (2005). The Dynamism of 2channel. AI & SOCIETY, Vol. 19, Issue: 1, pp: 84-92. Retrieved from: https://www.researchgate.net/profile/Yukio_Ohsawa2/publication/225177752_The_dynamism_of_2channel/links/00b7d52db355758eb4000000.pdf

O’Brien, B. (2018). U.S. visa applicants to be asked for social media history: State Department. *Reuters World News.* Retrieved from: https://www.reuters.com/article/us-usa-immigration-visa/u-s-visa-applicants-to-be-asked-for-social-media-history-state-department-idUSKBN1H611P?il=0

Oberst, U., Renau, V., Chamarro, A., & Carbonell, X. (2016). Gender Stereotypes in Facebook Profiles: Are women more female online?. Computers in Human Behavior, Vol. 60, pp: 559-564. Retrieved from: https://pdfs.semanticscholar.org/1616/0f740594c74e0936c260177546a157a4a262.pdf

Papacharissi, Z. (2018). A Networked Self: Identity, Community, and Culture on Social Network Sites (1st ed., pp. 105-123). New York, NY: Routledge. Retrieved from: http://viralmedia.pbworks.com/w/file/fetch/45052678/A%20Networked%20Self-Identity,%20Community%20and%20Culture%20on%20Social%20Network%20Sites%20%5B2011%5D.pdf

Saeri, A., Ogilvie, C., La Macchia, S., Smith, J., & Louis, W. (2014). Predicting Facebook Users' Online Privacy Protection: Risk, Trust, Norm Focus Theory, and the Theory of Planned Behavior. The Journal of Social Psychology, Vol. 154, Issue: 4, pp: 352-369, Retrieved from: https://ore.exeter.ac.uk/repository/bitstream/handle/10871/18706/saeri%20et%20al%20jsp.pdf?sequence=1

Smith, L., Smith, K., & Blazka, M. (2017). Follow Me, What's the Harm? Considerations of Catfishing and Utilizing Fake Online Personas on Social Media. Journal of Legal Aspects of Sport, Vol. 27, Issue: 1, pp: 32-45. Retrieved from: https://journals.iupui.edu/index.php/jlas/article/view/22240/21380

Wani, M., Jabin, S., & Ahmad, N. (2017). A Sneak into the Devil's Colony-Fake Profiles in Online Social Networks. arXiv preprint arXiv:1705.09929. Retrieved from: https://arxiv.org/ftp/arxiv/papers/1705/1705.09929.pdf

Wolff, J. C. P. (2012). *Unraveling Internet Identities: accountability & anonymity at the application layer*. Doctoral dissertation, Massachusetts Institute of Technology. Retrieved from: https://dspace.mit.edu/handle/1721.1/72901

Zhu, J., Zhang, S., Singh, L., Yang, G. H., & Sherr, M. (2016, August). Generating Risk Reduction Recommendations to Decrease Vulnerability of Public Online Profiles. 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), pp. 411-416. Retrieved from: https://pdfs.semanticscholar.org/678f/9e3d3378ec0b23b39d7e7067be16664fed33.pdf