Social Media & Privacy: A Facebook Case Study

Article · October 2015

CITATIONS
2

READS
60,059

1 author:

Marise Haumann

4 PUBLICATIONS **3** CITATIONS

SEE PROFILE

Social Media & Privacy: A Facebook Case Study

Marise Haumann

Introduction

With the growth of social media websites, such as Facebook, our privacy has become increasingly more vulnerable to surveillance and commodification. As we have uploaded personal information to social networks, we have increasingly allowed others access to our data. Moreover, most social media users remain largely unaware how vulnerable their personal information has become to information-aggregation and reselling activities. This essay contends that our ignorance of privacy settings and policies on social media websites such as Facebook, has exposed us to potential increases in social harassment, state intrusions, corporate surveillance and commodification, and has also reduced our ability to control how others may perceive us. We may only be able to reclaim our ability to control our privacy rights if we are able to control who may access our personal information through opt-in accessibility options, if we have sufficient groups to monitor our rights, and if we have non-commodified social networks to use.

Conceptualising privacy

Privacy can be a complicated concept to define, but a working operational definition of it conceptualises privacy as the right to control access to one's personal information (Guo, 2010; Fuchs, 2011). The right to privacy can thus be defined as the right to control the "appropriate flow of personal information" (Nissenbaum, 2010: 126). That is, one should have the right to reasonably exercise control in how and with whom one's information is shared.

Nevertheless, while access to privacy has positive aspects, it also a right that can have negative consequences. Thus, on the one hand, privacy enables people to be more

independent, more creative, freer, individualistic, and protects people's dignity, and protects people against the violation of their personal information. On the other hand, however, privacy also enables exploitation, entrenches inequalities, secrecy, and non-transparency (Fuchs, 2011; Fuchs, 2012). Thus, although the protection of privacy may strengthen the ability of some to avoid being violated, it also allows others to render their economic activities invisible. That is, it allows the powerful to obscure their economic ventures and thus enables them to enrich themselves, often at the cost of the poor. Consequently, from an empowerment perspective, the right to privacy should be seen as the right to the protection of one's privacy against the capitalist exploitation of the powerful and corporate entities, which usually occurs in the effort to enrich themselves (Fuchs, 2011).

Background: Facebook

Facebook was founded under the leadership of Mark Zuckerberg at Harvard University in early 2004, with the initial intention to create a student directory containing student profiles and pictures (Hodge, 2006; Guo, 2010). Moreover, the website became available for public use in 2006 and by this stage in its development, anyone over the age of 13 could create a profile if they possessed an e-mail address (boyd & Hargittai, 2010; Guo, 2010).

Facebook is characterised as a social media website which "combines features of e-mail, instant messaging, photo-sharing, and blogging programs, as well as a way to monitor one's friends' online activities" (Cohen, 2008: 6). Thus, Facebook functions as one-stop platform that combines various social activities for its users. According to Fuchs (2011), the defining features of Web 2.0 social networking websites, like Facebook and Myspace, are that they allow users to craft their own profiles, link such profiles together in visible social networks, and allow users to communicate with one another. Thus, on social networking websites, users utilise self-created profiles that act as avatars, to interact with one another through interconnected social networks (Solove, 2007; Guo, 2010). In addition, such profiles often contain personal information such as full names, contact

numbers, e-mail addresses, physical addresses, occupations, friendship networks, photos, records of activities, personal preferences, and demographic information (Solove, 2007).

Facebook, however, overtook Myspace's popularity by 2008 and became the most popular social media website in the world (Guo, 2010). By 2015, Facebook was worth at least 245 billion US Dollars (La Monica, 2015). Globally, the website has over 968 million daily users and 1.49 billion monthly users, with nearly 844 million mobile daily users and 3.31 billion mobile monthly users (*See* Figure 1) (Facebook, 2015a).

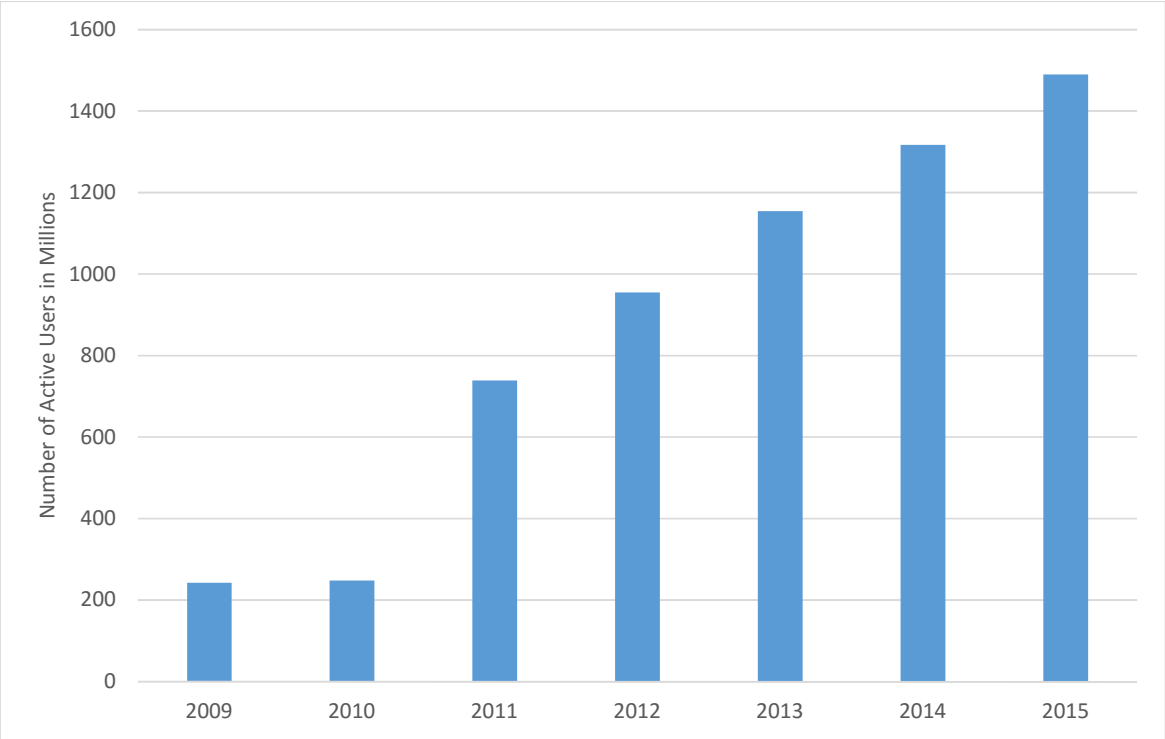

Figure 1: The number of active monthly Facebook users as of mid-2015 (in millions) (Statista, 2015).

Currently, Facebook is the second most popular website globally, with the majority of its users originating from the United States, India, and Brazil (Alexa, 2015). More specifically, approximately 83.1% of Facebook's current users are located outside of North America (Facebook, 2015a). Facebook is currently the most popular social media platform in

South Africa, with 11.8 million active users, of which 8.8 million access it via their mobile phones (*See* Figure 2) (World Wide Worx, 2015).

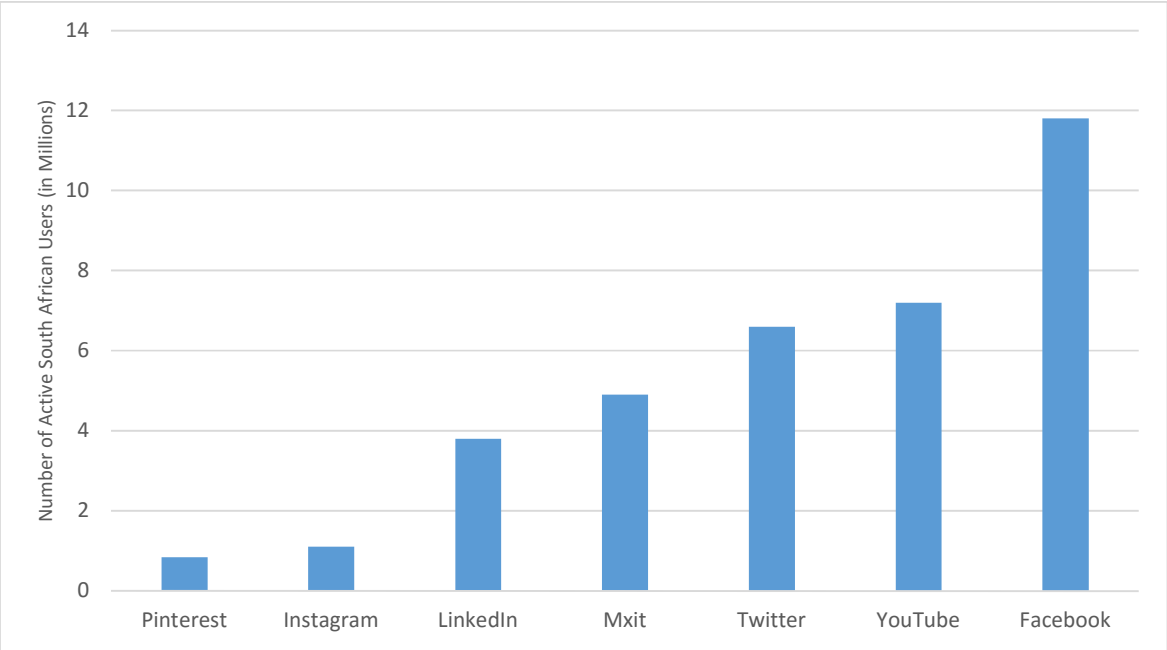

Figure 2: The number of active South African users (in millions) of social media websites (World Wide Worx, 2015).

In addition, Facebook has introduced several different features to its platform since 2004. Its News Feed feature, which was introduced in 2006, allows users to communicate to and view their friends' activities on the website. That is, the previously invisible activities of people on the website became visible to others in their networks with the introduction of the News Feed feature (Guo, 2010). Furthermore, the feature allows advertisers to place advertisements directly on to a user's news feed, thus marketing to the Facebook user directly (Cohen, 2008). By 2007, Facebook introduced the Beacon feature, which collected data on the activities of its users, focusing specifically on their shopping habits. Facebook's users, however, reacted very badly to this feature and Facebook readjusted its surveillance methods. Thus, the corporation began to gather aggregate data through less obtrusive means, so as to re-sell that private information to third-party advertisers (Debatin et al., 2009; Guo, 2010).

Although Facebook's privacy settings were very minimal at its founding, with users' profiles fully visible to all other users on the Harvard University campus, the corporation gradually introduced more sophisticated, yet complicated, settings (boyd & Hargittai, 2010). Facebook's privacy settings seem to allow its users to fine-tune what information is shared with whom. More specifically, one can utilise the settings to determine who sees your profile, what information can be used by third-party advertisers for targeted marketing, and whether one's profile can be used by separate websites for ease of access (Gottsegen, 2015). In other words, through a series of rather complicated steps, one can limit what those in one's network can see of your profile and how deeply Facebook and its advertising partners can mine one's profile for their benefit. Facebook's current data policies indicate that they collect information on the content users upload, information others upload about one another, information on the devices users connect to their accounts, as well as information related to the social networks users connect their profiles to (Facebook, 2015b).

Past research: How people view and use Facebook's privacy settings

Past research has investigated how people tend to view and use Facebook's privacy settings. Acquisti and Gross' (2006) research suggested that Facebook users mainly utilised the website to communicate with one another through crafted public personas, and that although such users were often aware of how publicly visible their profiles were, they were under the impression that they could manage their profiles so as to render them private. Nevertheless, they also discovered that many early Facebook users were unaware of how much their profiles revealed about them online.

In addition, Debatin, Lovejoy, Horn and Hughes' (2009) research suggested that the vast majority of early Facebook users had not read the privacy and data policies related to the website. Although most early Facebook adopters knew they could render their profiles more private, nearly half chose to not utilise privacy features at all (Debatin et al., 2009).

They argued that most Facebook users operated according to the 'third person effect' in relation to the website and privacy concerns. In other words, the majority of users were under the impression that other users were at more risk for privacy violations than they were and, accordingly, the majority did not fine-tune the privacy settings on their personal profiles. More specifically, their research found that Facebook users tended to implement more in-depth privacy measures only if their privacy had personally been invaded on the website. Thus, most users did not respond favourably to warnings that their privacy could be violated on Facebook (Debatin, et al. 2009).

Furthermore, boyd and Hargittai's (2010) study on how the youth utilise privacy settings on Facebook indicated that the majority of such users had at least attempted to adjust such settings to render their profiles less visible. They also discovered that Facebook users from the youth demographic group were more concerned about protecting their privacy against other individuals they already knew than they were about protecting their private information from corporate or state entities (boyd & Hargittai, 2010). While their research showed that there was no gender difference in how people tended to protect their privacy, they found that those who were frequent Facebook users had adjusted their privacy settings the most, while those were less familiar with the platform had spent far less time protecting their profiles (boyd & Hargittai, 2010).

Facebook and personal information: Issues with commodification and privacy

Many social media websites, like Facebook, generate revenue by gathering and selling information related to and produced by their users to third-party advertisers (Cohen & Shade, 2008; Cohen, 2008; Nissenbaum; 2010; Fuchs, 2011; Wang et al., 2011; Fuchs, 2012). Web 2.0 websites, such as Facebook, utilise the free labour performed by its 'prosumers', to mine the data they have produced for advertising revenue sales (Cohen, 2008). Conceptualising the Facebook user as a 'prosumer' frames them as someone who is both a consumer of Facebook's networking capacity, and a producer of its network

content (Fuchs, 2012). Thus, prosumers freely produce the content which constitutes Web 2.0 websites and through this activity, also provide corporations with valuable information on their advertising profiles; which ultimately reward those corporate entities with freely-produced content and readily-accessible advertising markets. Past research has suggested that people actively perform this type of labour, which keeps websites like Facebook running, for free in exchange for the creation and maintenance of their social networks (Cohen, 2008). Thus, the business models of Web 2.0 social media websites rests on the cycle of 'free' consumption, production, and reselling of private information and communication. That is, the true value of a company such as Facebook lies in its capacity to mine for and sell its users aggregated private information – in other words, the commodification of its users' profiles, networks, and private information (Fuchs, 2012).

In addition to this commodification of Facebook-users' private information, the vulnerabilities of Facebook users' privacy on the platform has also had other consequences. Firstly, people have used Facebook to harass on another, by, for example, stalking one another online or releasing embarrassing personal data within each other's social networks (Debatin et al., 2009). Thus, it has been possible to exploit the gaps in Facebook's protection of its users' personal information for social activities. Secondly, in the past, state agencies in the United States have utilised the Patriot Act to collect information on Facebook users' profiles, regardless of the privacy measures users may have implemented to protect their profiles (Debatin et al., 2009). Furthermore, police and government officials have utilised Facebook profiles and histories to crack down on activities ranging from underage drinking to criticisms against ex-President George W. Bush (Hodge, 2006). Consequently, despite reassurances that the company has sought to protect its users' personal information, Facebook has shown that it would expose its user-base to state intrusions. Thirdly, the company earns revenues by selling access to its users' personal profiles to third parties and third party applications (Guo, 2010; Nissenbaum, 2010). This activity has mainly occurred in order to facilitate the production of targeted marketing campaigns, aimed at social media users in online spaces. On the one hand, those in favour of the reselling of aggregated information have argued that it

allows for more targeted communication strategies, thus reducing inefficiency. On the other hand, those critical of the commodification of aggregated personal information have posited that its runs the risk of security challenges and of spreading misinformation through errors (Nissenbaum, 2010). In other words, while targeted marketing may increase efficient marketing and communication activities, it may also expose people's personal information and spread misinformation about people. Finally, an added danger of having an online record of ourselves and our activities on platforms such as Facebook, is that it can constrain us from acting naturally and may restrain us from managing our reputations freely (Solove, 2007). Our reputations are constituted by the collective view others have of who we are, usually based on relevant information, which describes our histories and characters. With the increasingly free flow of information online, both personal and public, which is also increasingly not under the control of any one person, it has become increasingly difficult to manage our personal reputations and, in turn, how others perceive us (Solove, 2007). Consequently, the tendency to put our personal information on social media websites, such as Facebook, has exposed us to increased social harassment, state intrusions, corporate surveillance and commodification, as well as having reduced our ability to control how others may perceive us.

Possible solutions

Fuchs (2012) contends that there are three general solutions to deal with the increasing violations of privacy we face through Web 2.0 platforms. Firstly, he posits that we should have opt-in privacy policies, whereas most websites currently offer opt-out privacy policies. That is, Facebook, for example, currently forces its users to go through a series of steps to opt out of privacy invasions for corporate profit. In contrast, an alternative, more privacy-friendly approach to Web 2.0 policies would offer users the choice to sell their information to third parties. Secondly, he posits that we should create more groups that act as watchdogs against privacy violations. Thirdly, Fuchs (2012) argues that we should develop Web 2.0 social networking websites that are not driven by a profit motive, but rather driven by the aim to promote and maintain online social networks. In other words, if we had social networking websites that were primarily created for social

networking rather than the generation of corporate profits, our private information would not be viewed as virtual commodities.

Thus, we could reduce the risk of privacy violation on social media websites by creating a culture where users have to consent to the commodification of their personal information; by establishing active and effective groups that monitor privacy settings and policies; and by promoting the development and maintenance of non-profit online social networks. In such an environment, people's personal information would be better protected against social, corporate, and state exploitation.

Conclusion

In conclusion, the Facebook case study illustrates how our privacy rights on social media websites have become increasingly vulnerable to exploitation, commodification, and surveillance. Facebook and other social media platforms have become increasingly popular and those who utilise such websites have tended to fill their online profiles with vast amounts of personal information, which in turn, has been mined for re-use and re-sale by various corporate and state entities. These habits have made it increasingly difficult for social media users to manage their reputations, to avoid state intrusions into their private affairs, and to reduce corporate surveillance and exploitation. Nevertheless, it has been argued that although our privacy has become more vulnerable, we can strengthen our privacy protections by establishing opt-in privacy policies, by creating efficient privacy watchdog groups, and by creating social networks that are not driven by a profit motive.

References

Acquisti, A., & Gross, R. 2006. Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Privacy Enhancing Technologies*. Available: http://people.cs.pitt.edu/~chang/265/proj10/zim/imaginedcom.pdf [2015, 3 September].

Alexa. 2015. *Facebook Overview*. Available: http://www.alexa.com/siteinfo/facebook.com [2015, 6 September].

boyd, d. & Hargittai, E. 2010. Facebook privacy settings: Who cares? *First Monday*. 15 (8): 1-23.

Cohen, N. & Shade, L. 2008. Gendering Facebook: Privacy and commodification. *Feminist Media Studies*. 8 (2): 210-214.

Cohen, N. 2008. The valorization of surveillance: Towards a political economy of Facebook. *Democratic Communiqué*. 1: 5-22.

Debatin, B., Lovejoy, J. P., Horn, A. & Hughes, B. N. 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*. 15: 83-108.

Facebook. 2015a. *Company Info: Statistics*. Available: http://newsroom.fb.com/company-info/ [2015, 4 September].

Facebook. 2015b. *Data Policy*. Available: https://www.facebook.com/full_data_use_policy [2015, 3 September].

Fuchs, C. 2011. An alternative view of privacy on Facebook. *Information*. 2: 140-165.

Fuchs, C. 2012. The political economy of Facebook. *Television & New Media*. 13(2): 139-159.

Gottsegen, G. 2015. Here's how to use Facebook's mystifying privacy settings. *Wired*. 11 August. Available: http://www.wired.com/2015/08/how-to-use-facebook-privacy-settings-step-by-step/ [2015, 4 September].

Guo, Y. Y. 2010. The privacy issue on social network sites: Facebook. *Journal of Digital Research and Publishing*. Session 2: 83-90.

Hodge, M. J. 2006. Fourth amendment and privacy issues on the new internet: Facebook.com and myspace.com. *The Southern Illinois University Law Journal*. 31(95): 1-15.

La Monica, P. 2015. Facebook now worth more than Walmart. *CNN*. 23 June. Available: http://money.cnn.com/2015/06/23/investing/facebook-walmart-market-value/ [2015, 6 September].

Nissenbaum, H. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford, CA: Stanford Law Books.

Solove, D. J. 2007. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. London: Yale University Press.

Statista. 2015. *Number of monthly active Facebook users worldwide as of 2nd quarter 2015 (in millions).* Available: http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [2015, 5 September].

Wang, N., Xu, H. & Grossklags, J. 2011. Third-party apps on Facebook: privacy and the illusion of control. In *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology*. Available: http://personal.psu.edu/nzw109/papers/Wang_chimit_2011.pdf [2015, 3 September].

World Wide Worx. 2015. *South African Social Media Landscape 2015*. Available: http://www.worldwideworx.com/wp-content/uploads/2014/11/Exec-Summary-Social-Media-2015.pdf [2015, 3 September].