# IMAT3429 - Privacy and Data Protection

## Privacy on Social Media Platforms

Michael Bull

$1^{st}$ February 2015

## 1 Abstract

As the online world increasingly adapts and exposes itself to the evergrowing platform that is social media, consumers are becoming increasingly self aware of their online presence and general privacy on the Internet. This paper aims to discuss what it means to be private on the Internet, explore how consumers control their online presence, debate the ideology of privacy as a human right, and discuss misconceptions involved with how consumers approach online privacy. The paper's focus will be on the two most popular social media sites in the world: Facebook and Twitter. With 890 million daily active users on Facebook (Facebook 2014), and users creating 500 million tweets per day (Twitter 2015), these platforms are the industry leaders in the social media world and provide the standard that new industry entrants will follow. For this reason, it is imperative that these organisations be aware of consumer concerns regarding privacy, as their initial adoption of increased privacy awareness techniques will encourage competitors to follow.

## 2 Introduction

As consumers continually post sensitive information in the form of photographs, videos, locations, and relationships; the privacy threats they are exposed to are ever increasing. Threats such as identity theft and cyber bullying rely on personal information that users have published online, a resultant effect that the typical consumer is not aware of when adopting the rich functionality that these platforms offer. For many consumers, it takes being directly affected from these threats to become concerned about them, as most dismiss these threats as non-issues. It is for this reason that the responsibility of caring for users privacy is not solely in the consumer's hands, but also falls to the operators of the social media platforms.

# 3 Exploring Privacy

To understand how privacy is affected by the adoption of social media platforms, it is important to explore what fundamentally defines privacy. In 2002, Stein and Sinha defined privacy as "the rights of individuals to enjoy autonomy, to be left alone, and to determine whether and how information about one's self is revealed to others". The latter part of this definition often contradicts the approach that many social media platforms have with regards to privacy, as they rarely provide the user with enough control to determine whether and how their information is distributed. An example of this is Twitter, a platform on which users "tweet about any topic within the 140-character limit and follow others to receive their tweets" (Kwak et al. 2010). The 'tweet' system that Twitter has implemented does not allow an author to specify who can view a specific tweet on a user-by-user basis. In this case, Facebook shows a greater concern for privacy as their system, known as sharing a 'status', allows the user to define a subset of specific individuals that have the ability to view the shared status. The lack of functionality to determine who can view a tweet can be construed as ignorance on behalf of the developers at Twitter, as in 2002 Chung and Paynter outlined that "consumers are really interested in the safeguard of their privacy".

A potential retort from the operators of Twitter regarding this subject may include the claim that sharing private information with a third party, such as a social media platform, is essentially giving up the 'right' to privacy that Stein and Sinha discussed in their definition. However, this claim raises many ethical issues regarding the sacrificing of our personal information; as the platforms are designed to enrich the user experience as further private and sensitive information is collected. This lack of transparency by social media platforms regarding how information is stored and used to increase the user experience, for example being used to provide targeted advertisements, heavily violates the definition that Stein and Sinha provided over a decade ago. One could argue that the definition provided by Stein and Sinha is now outdated, however with the definition being provided before these platforms even existed, it is clear that there was an active avoidance in following the definition during their creation by their respective development teams.

After scrutinising the lack of adherence by the social media platforms regarding the definition of privacy, it is important to identify where the organisations are succeeding to follow preferred privacy techniques. Both Facebook and Twitter provide a well designed blocking feature that allows a user to block all interactions that another user on that platform may have with them. This functionality greatly follows the "right to be left alone" that Stein and Sinha discussed, as a user may choose at any point to block another user, and in extreme cases may even deactivate their account completely in order to be left alone by everybody on the platform. This helps users deal with the previously mentioned privacy threat of cyber bullying, as blocking interaction completely with a user can be seen as the best way of dealing with such a situation, as opposed to engaging with the bully.

# 4 Analysing The Threat

As the Internet is generally a free and open place for information to travel without restriction, there is an initially high threat level for privacy invasion to those who use it. The rise of social media platforms towards the end of the previous decade can be seen as only increasing the threat, as few have actively pursued techniques to reduce privacy invasion threats below the level that they were at before the introduction of such platforms. Analysing how privacy was perceived before the introduction of social media platforms, Clarke in 1999 regards privacy as a "moral or legal right" (Clarke 1999). With this in mind, Facebook and Twitter have attempted to morally abide by the concept of privacy with the implementation of privacy control settings, however, lack of substantial legislation that is up-to-date with the introduction of these platforms can be identified as a reason that the developers of these platforms are not as concerned in improving such functionality as they could be. This is due to outdated legislation in countries such as the United Kingdom, whose most recent privacy laws include the Data Protection Act of 1998. Looking at the year of publication, this legislation was created far before the concept of social media platforms ever existed, and for this reason cannot adhere to the privacy concerns that have arisen with such platforms.

Pursuit in updated legislation may force developers of social media platforms to follow the guidelines for successful online privacy concerns, as outlined by Cranor in 1999: "they must be accompanied by tools and procedures to provide strong security" (Cranor 1999). As previously discussed, these tools are implemented in current social media platforms, however as previously identified in this paper their inability to provide 'strong security' is palpable. Over a decade after Clarke and Cranor's papers were published, studies were performed to assess the usefulness of the implemented privacy settings, which resulted in the conclusion that "the current approach to privacy settings is fundamentally flawed and cannot be fixed" (Madejski et al. 2011).

With the requirement of further developed privacy settings from the operators of social media platforms, it is important that the developers provide an easy-to-use group of settings that does not confuse the user. In 2009, Garfinkel and Cox described the current state of privacy settings on social media platforms as "notoriously difficult to audit because they are complex and generally not apparent with today's user interfaces". The concern regarding the navigability of privacy settings has therefore been identified for many years, and as such the lack of innovation in the area puts users at a clear disadvantage in protecting their online identity. As well as requiring a certain level of self research, users may feel the need for further education in order to fully grasp the levels of control that they are truly offered by the platforms. This clear need for further development in both functionality and usability aspects is strengthened by a claim from Fuchs et al. who states that "the traditional privacy concept is challenged, and new protective measures must be developed" (Fuchs et al. 2013).

# 5 Educating Users

As identified in the previous section, the need for formal education regarding the subject of online privacy is imperative to decrease privacy concerns for future users of social media platforms. With the responsibility lying with both the developers of social media platforms, as well as traditional education institutes, it is important that both understand that "existing policy-configuration tools are difficult for average users to understand and use" (Fang and LeFevre 2010). Statistics further strengthen the claim regarding lack of education, as far before such platforms became too popular for developers to manage privacy concerns, there was a clear issue with the exposure that users were giving their online presence; as in 2009, Debatin et al. observed that "13 per cent of Facebook profiles at Michigan state University were restricted to 'friends only'" (Debatin et al. 2009). This shockingly low statistic, provided by a consensus performed at an average American university, suggests that the average age group of Facebook users, 18-25 year olds (Ken Burbary 2011), are seemingly unaware of, ignorant of, or actively participating in the potential privacy risks that such online transparency entails. The risks identified with the broadcasting of such a private profile can often go unnoticed by users, as identified in 2006 by Krishnamurthy and Wills who highlighted that "most users do not have an idea if any of the various bits of private information that add up to their identity is disseminated to parties other than the sites directly visited" (Krishnamurthy and Wills 2006). This again is a clear identification regarding lack of education on the subject of online privacy threats.

This push for education regarding online privacy was also supported by Debatin et al. in 2009, who recommended "better privacy protection, higher transparency of who is visiting one's page, and more education about the risk of posting personal information to reduce risky behaviour" (Debatin et al. 2009). The transparency on who is visiting one's page is yet another privacy concern that both Facebook and Twitter neglect, as neither of these platforms have any implementation to view a history of page viewers. Similarly, neither of these platforms provide a detailed level of education regarding the risks of sharing personal information, as it is in their best interest to collect and encourage the distribution of private information from their users. The introduction of this subject in to formal education, such as secondary school in the UK, would greatly help to introduce the concept of online privacy to future users of such platforms, as well as potentially inspire future developers who may, in future, work on or create similar platforms; thus being provided with the required level of education to be adequately concerned about privacy threats.

# 6 Encouraging Developers

As discussed towards the end of the previous section, education regarding the subject of online privacy can help to inspire and encourage future developers of social media platforms and similar products. This inspiration would help offset the lack of legal and moral pressure that the operators of such platforms currently face, as the monopolies they impose on the industry provide them with the ability to be ignorant and lazy in the pursuit of further privacy innovations. This concern was raised by Hoadley et al. in 2010 who, whilst also discussing Facebook, claimed that "it appears the notions of privacy as perceived control and easier information access have not yet been taken up by online social network promoters or designers" (Hoadley et al. 2010).

The research conducted during this paper provides many suggestions and guidelines by academics, outlining the fundamental principles of online privacy as well as the required functionality that a truly privacy concerned platform should implement. These include "transparency on who is visiting one's page" (Debatin et al. 2009), navigable and clear user interfaces, details of third parties that personal information is distributed to, as well as further "tools and procedures to provide strong security" (Cranor 1999).

# 7 Conclusion

Throughout this paper there has been a clear theme regarding the need for innovation and education of online privacy threats that have been elevated throughout the past decade with the introduction of social media platforms. The current approach that such platforms apply to privacy is inherently flawed and requires severe improvement that, with the help of academic research and advice, can ultimately provide the user with a much safer experience that is more likely to keep them engaged with such products. The legal and moral requirements for online privacy have helped to shape the current state of privacy concerns, however, with the distinct lack of updates to the legislation and general moral ignorance of privacy threats, industry leaders are becoming less concerned for the safety of their users and are instead looking to enrich the experience their platforms offer with further sacrifices of private information. As users further embrace the technology age, it is important that new users are exposed to an adequate amount of education on the subject of online privacy; allowing new generations to be concerned when using such platforms and encouraging new developers to also understand the concerns that users may have. This message will help new developers to clearly understand that the functionality that their platform offers should not be a direct result of privacy sacrifices, as stated by Schwartz, who outlined that "the Internet's technical qualities also have a negative consequence: they make possible an intense surveillance of activities in cyberspace" (Schwartz 1999).

# References


Facebook (2014). *Company Info | Facebook Newsroom*. URL: http://newsroom.fb.com/company-info/.

Twitter (2015). *Twitter Usage Statistics - Internet Live Stats*. URL: http://www.internetlivestats.com/twitter-statistics/.

Stein, Laura and Nikhil Sinha (2002). "New global media and communication policy: the role of the state in the twenty-first century". In: *Handbook of new media: Social shaping and consequences of ICTs*, pp. 410–31.

Chung, Winnie and John Paynter (2002). "Privacy issues on the Internet". In: *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*. IEEE, 9–pp.

Kwak, Haewoon et al. (2010). "What is Twitter, a social network or a news media?" In: *Proceedings of the 19th international conference on World wide web*. ACM, pp. 591–600.

Clarke, Roger (1999). "Internet privacy concerns confirm the case for intervention". In: *Communications of the ACM* 42.2, pp. 60–67.

Cranor, Lorrie Faith (1999). "Internet privacy". In: *Communications of the ACM* 42.2, pp. 28–38.

Madejski, Michelle, Maritza Lupe Johnson, and Steven Michael Bellovin (2011). "The failure of online social network privacy settings". In:

Garfinkel, Simson and David Cox (2009). *Finding and archiving the internet footprint*. Tech. rep. DTIC Document.

Fuchs, Christian et al. (2013). *Internet and surveillance: The challenges of Web 2.0 and social media*. Vol. 16. Routledge.

Fang, Lujun and Kristen LeFevre (2010). "Privacy wizards for social networking sites". In: *Proceedings of the 19th international conference on World wide web*. ACM, pp. 351–360.

Debatin, Bernhard et al. (2009). "Facebook and online privacy: Attitudes, behaviors, and unintended consequences". In: *Journal of Computer-Mediated Communication* 15.1, pp. 83–108.

Ken Burbary (2011). *Facebook Demographics Revisited - 2011 Statistics*. URL: http://www.kenburbary.com/2011/03/facebook-demographics-revisited-2011-statistics-2/.

Krishnamurthy, Balachander and Craig E Wills (2006). "Generating a privacy footprint on the Internet". In: *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*. ACM, pp. 65–70.

Hoadley, Christopher M et al. (2010). "Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry". In: *Electronic commerce research and applications* 9.1, pp. 50–60.

Schwartz, Paul M (1999). "Privacy and democracy in cyberspace". In: *Vand. L. Rev.* 52, p. 1607.