Effects of Social Media on Internet Privacy

Michael Bull

January 15, 2013

1 Abstract

One of the biggest threats in the technology age is online privacy. With the recent mass exposure to social media online, users are increasingly leaving themselves open to privacy threats. This paper will explore what it means to be private on the Internet, the threat that social media brings to our online privacy, the fundamental right to privacy, as well as expose some of the more common misconceptions with online privacy. The paper will mainly focus on one of the largest social networks in the world: Facebook. With one billion monthly active users (Facebook 2012) spending "more than 700 billion minutes per month on Facebook" (Porterfield, Khare, and Vahl 2011), it is one of the most popular sites in the world and a platform nearly everyone in a developed country is aware of. With many controversies arising from executive decisions at Facebook, it is a prime example when analysing online privacy with regards to both its strengths and weaknesses.

2 Introduction

With the issue of privacy becoming ever more relevant in our daily lives as we continue to publicise our actions on many online platforms, it comes as no surprise that the measures in place to protect privacy are being actively worked on by developers. With many of us publicising our lives to our friends through social media, many new threats arise such as identity theft and personal attacks, however for many it takes directly dealing with these threats for them to be concerned about such issues. With research suggesting that most users actively choose to display their information publicly, the expectation for privacy protection turns to the developers of the popular social media sites, and the responsibility of adding adequate privacy control tools as well as educating the users on configuring the controls lays in their hands.

3 Understanding Privacy

In order to adequately assess the impacts on privacy from social media, we must first understand what it means to be truly private, both online and offline. H.F. Nissenbaum argued in 2010 that there is "great ambiguity in the way personal information is used" as a common term and that "it can mean sensitive or intimate information, any information about a person, or only personally identifying information" (Nissenbaum 2009). 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' (Stein and Sinha 2002). Whether this definition of privacy is relevant given the advancements in the last decade is debatable, however it is easily adaptable to the concept of online privacy in its current form. The definition claims that privacy is a 'right' of an individual; however it can be argued that using a third party such as a social media site is essentially giving up this right, regardless of the ethical issues that such a claim raises. The definition also raises the point of being able to determine what information is revealed about a user, and controlling that information. Social networks generally adhere to this section of the definition, but albeit in a poor manner as more often than not the privacy settings of your profile are limited to what the site developers deem necessary in privacy control, as opposed to being able to fully control how accessible your online identity is. Systems such as the privacy control options allow users to choose who is able to see what content; however the full ability to control it on a 'user by user' basis is lacking on many popular social networks.

Twitter is one of the most popular social networks in the 21st century, with over 200 million active users creating 340 million 'tweets' per day (Twitter 2012a). Users on Twitter "tweet about any topic within the 140-character limit and follow others to receive their tweets" (Kwak et al. 2010). On Twitter there is no way to allow a specific 'tweet' to be viewable by a specific follower that you have (Twitter 2012b). The lack of this functionality can be surprising to many considering that in a quote from over a decade ago the general consensus was that "consumers are really interested in the safeguard of their privacy" (Chung and Paynter 2002). Finally, the definition states that individuals have the right to be "left alone". Most social networks easily integrate a blocking mechanism into their system, allowing a user to either block a specific person who is harassing them, or block themselves off from new people entirely. After analysing this somewhat outdated definition of privacy, it is clear that social networks have difficulty adhering to the definition of privacy that is already ten years old and had enough time to become widely accepted.

4 Elevating The Threat

With the Internet being a generally open place for the freedom of information, the threat of privacy online is initially high. The introduction of social media has only increased this threat and shown no attempt to decrease it further than its original state. As privacy is often thought of as a moral or a legal right (Clarke 1999), social networks have taken it upon themselves to attempt to lower the threat of a privacy breach with various settings and tools such as the profile privacy settings on Facebook. These do indeed allow a user to limit the availability of their profile online (and thus decrease the exposure to a privacy breach), however the systems provided are not adequate and do not give the user enough customisable options to fully protect the individual. The lack of ability to completely customise the privacy options contradict what is defined as success for online privacy initiatives by L.F. Cranor: they must be accompanied by tools and procedures to provide strong security (Cranor 1999). The social media sites do indeed accompany their systems with tools and procedures to provide security, but the ability to do this with great strength is doubted by many in light of previous privacy breach cases, which lead a recent research paper to conclude that "the current approach to privacy settings is fundamentally flawed and cannot be fixed" (Madejski, Johnson, and Bellovin 2011).

Aside from the ability to fully restrict an account on a social media site, another caveat is the ability to easily navigate and control what restricted privacy options are available. Many users may struggle to use the privacy settings included with social networks, mainly because such options are hidden away from easy access and are generally hard to operate once found. This was highlighted by S. Garfinkel and D. Cox in 2009, who stated it is "notoriously difficult to audit security settings because they are complex and generally not apparent with today's user interfaces" (Garfinkel and Cox 2009). The concern with the ease of the use of privacy settings only puts users at a disadvantage, but it can be remedied with an in-depth education on the subject and correct teaching of how to conduct one's self whilst online, which is covered in the next section of this paper. This point is strengthened by C. Fuchs et al who recently claimed that "the traditional privacy concept is challenged, and new protective measures must be developed" (Fuchs et al. 2013).

5 Educating The Masses

In a paper over seven years old by H. Jones and J.H. Soltren, statistics show that with regards to demographic data and interests: "over 70willing to disclose both categories of information, making the Facebook a valuable trove of demographic data for marketers" (Jones and Soltren 2005). With these statistics in mind, arguably the best way of remedying the lack of usability and general awareness of online privacy is to formally educate people on the subject. Whether this is the responsibility of the social networks themselves or the responsibility of the state is questionable, but regardless of either the education itself is becoming a necessity. In 2010 L. Fang and K. LeFevre summed up the lack of education by stating that "While these sites are growing rapidly in popularity, existing policy-configuration tools are difficult for average users to understand and use" (Fang and LeFevre 2010). An example of the arguably lack of education on the subject is

shown by Ellison, Steinfield & Lampe (2007), who discovered that only 13 per cent of Facebook profiles at Michigan state University were restricted to "friends only" (Debatin et al. 2009). This example of a census, within an average university, suggests that the majority of the most common age user group on Facebook of 18-25 year olds (Twitter 2012a) is either unaware or actively choosing to put themselves at risk of a privacy breach by allowing their account to be viewed by anyone online.

The lack of education regarding the matter of online privacy was highlighted more than half a decade ago by B. Krishnamurthy and C.E. Willis in 2006, claiming 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 early reaction to online privacy shows the lack of awareness from both the people signed up to these sites and the operators of the sites themselves. Educating people on the severity of the issue would help people to protect themselves and enlighten the operators of the sites on just how important the issue is.

The idea of education on the subject itself is not a relatively new idea. In 2009, B. Debatin cited a paper from Dwyer et al (2007), writing that: "the authors recommend 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". With this statement in mind, it is clear that the notion of educating people about online privacy risks is a widely accepted practice, but only by those observing the sites. Currently, neither Facebook nor Twitter allow the user to effectively see who has been browsing their online profile (which would then allow the user to see who is accessing their private information) and neither of them adequately inform the user of potential privacy issues that may arise from use of their sites. One way to combat this situation would be to introduce a lesson in primary or elementary schools worldwide, which would help teach pupils that are growing up in the information age about the threats of such technology. Many users of social networks are children and teenagers, completely unaware and uneducated about the dangers of the Internet as it is not covered in any conventional computer associated lessons. Introduction of a standalone lesson or integration into an existing lesson would help reinforce these privacy lessons into the coming generations and may help to inspire those who go on to work for such social networks in their future.

6 Encouraging Social Networks

Following on from educating the users of the sites, the users themselves should be demanding/encouraging social networks to aid them in their quest for full online privacy. Currently, with social networks being of such a huge size, they have little to no pressure on them to adhere to any individual's needs. This lack of pressure on the company leads to laziness and an overall poor experience for the end user (similar to the effect of a monopoly in any other business environment). Without users explicitly demonstrating need for online privacy, the sites are never likely to implement such features, however with the lack of ability to be heard by such corporate giants, such a task can be quite unrealistic. Three years ago, C.M. Hoadley et al raised this very concern in a paper, claiming 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 such as the operators of Facebook (Hoadley et al. 2010). With this concern being raised over three years ago, it can be seen as a shock to many that Facebook have not yet rectified the issue.

Encouraging the sites themselves can be a very hard task; however below is a list of various improvements that have been suggested by academics in the field and discussed time and time again with regards to this subject.

- Transparency on who is visiting one's page (Dwyer et al, 2007).
- Less complex and more apparent user interfaces.
- Transparency on what data is provided to third parties.
- Inclusion of tools and procedures to provide strong security. (Cranor 1999)

7 Common Misconceptions

Novice users of the Internet are often subject to common misconceptions when using and participating in any internet related activity. These misconceptions can be incredibly damaging to a user when dealing with their personal information, especially on social network sites which rely on the user giving up nearly all of their personal information. D. Rosenblum strengthened this point in 2007 by stating that "this artificial sense of the anonymity of Net communications leads people to actually lower their inhibitions, and to feel protected from the consequences of their speech" (Rosenblum 2007).

Probably the biggest misconception with any social network is presuming that your information is, by default, safe and secure. On nearly every popular social network, your personal information is set to be publicly accessible, and only after visiting the privacy settings is this able to be changed. This common misconception often leaves users vulnerable and it takes an attempted privacy breach for the user to come to the realization that their information is not safe.

Along with misconceptions based on social networks themselves, many make assumptions about browsing elsewhere online and assume that it is completely unrelated to their social networking experience. However, with social media integration getting more complex, it is entirely possible for other webpages to interact with your social media account, even when you are not logged into the social media site. This opens the user up to a whole new world of potential unwanted harm to their online privacy, purely by visiting sites that are not considered legitimate. This is also relatable to the points made by A. Acquisti and J. Grossklags in 2005: similar misconceptions were found related to the ability to browse anonymously by deleting browser cookies (Acquisti and Grossklags 2005). Here we see that users often think that deleting the browser history and session items such as cookies and cache will guarantee anonymity when browsing the web from that point forward, however this is not the case and such misconceptions can potentially lead to large security breaches on a user's system and private information.

8 Conclusion

The current state of concerns for privacy online requires reassessing in order to correctly protect innocent and unaware users from privacy breaches when using social media sites. The lack of support for specific requirements of users, such as the ability to monitor, track, and stop certain other users from accessing your information is cause for concern. Academic research in the field helps to reinforce the points made with regards to social networks respecting the right to privacy for users on a legal and moral level, as well as giving viable alternatives and improvements to the systems that are in place together with teaching valuable lessons to those new and upcoming social networks. Education for the topic of online privacy should become a de facto standard within our current education system worldwide. As we move further into the technology age, we must embrace these new concepts and be able to teach new generations about the use of such technology and how to protect yourself when using it. This message is best summed up by P.M. Schwartz who claims that despite the positive effect that the Internet has had on our society, "the Internet's technical qualities also have a negative consequence: they make possible an intense surveillance of activities in cyberspace" (Schwartz 1999).

References

Facebook (2012). *Key Facts - Facebook Newsroom*. URL: `http://newsroom.fb.com/Key-Facts`.

Porterfield, Amy, Phyllis Khare, and Andrea Vahl (2011). *Facebook marketing all-in-one for dummies*. John Wiley & Sons.

Nissenbaum, Helen (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

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.

Twitter (2012a). *What is Twitter? · Twitter for Business*. URL: `https://business.twitter.com/basics/what-is-twitter/`.

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.

Twitter (2012b). *Twitter Settings*. URL: `https://twitter.com/settings/account`.

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.

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.

Jones, Harvey and José Hiram Soltren (2005). "Facebook: Threats to privacy". In: *Project MAC: MIT Project on Mathematics and Computing* 1.

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.

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.

Rosenblum, David (2007). "What anyone can know: The privacy risks of social networking sites". In: *IEEE Security and Privacy* 5.3, pp. 40–49.

Acquisti, Alessandro and Jens Grossklags (2005). "Privacy and rationality in individual decision making". In: *IEEE Security & Privacy* 2, pp. 24–30.

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