Conference Proceedings of

A*i*CE 2012

Melbourne, 13 February, 2012.

Sixth AUSTRALIAN INSTITUTE OF COMPUTER ETHICS CONFERENCE

Edited by:
Shona Leitch and Matthew Warren
ISBN 978-0-9872298-1-6

Proceedings of

A*i*CE 2012

Edited by
Shona Leitch and Matthew Warren
ISBN 978-0-9872298-1-6

Organised By
Information Security, Privacy & Ethics (iSPER) Group, School of Information Systems, Faculty of Business and Law, Deakin University.

Published by the School of Information Systems, Deakin University, Burwood, Victoria, 3125, Australia.

All papers published in the conference proceedings have been blind refereed by at least two of the A*i*CE 2012 **Organising and Review** committee.

Welcome

The A*i*CE 2012 conference follows on from the highly successful initial A*I*CE 99 conference and the A*i*CE 2000, A*i*CE 2002, A*i*CE 2005 and A*i*CE 2008 conferences. This conference looks at the continued development of Computer Ethics within Australia, taking into account the current issues that impact Australia such as social media.

Members of the conference organising committee accepted each paper in the proceedings after a careful review; this took the form of a **blind review** by at least **two** members of the conference organising committee. The papers were subsequently reviewed and developed where appropriate; taking into accounts the comments of the reviewers. The aim of this conference is to further the work already achieved within Australia and bring together researchers in the field to discuss the latest issues and their implications upon Australia.

We commend the authors for their hard work and sharing their results, and the reviewers of the conference for producing an excellent program.

A*i*CE 2012 Organising Committee

John Barlow, Australian Catholic University.
Mike Bowern, Australian National University.
Oliver Burmeister, Charles Sturt University.
Shona Leitch, Deakin University.
John Lenarcic, Royal Melbourne Institute of Technology.
Richard Lucas, University of Canberra.
Donald McDermid, Edith Cowan University.
Craig McDonald, University of Canberra.
Matthew Warren, Deakin University. (Conference Chair).
John Weckert, Charles Sturt University.

Contents

You are what you type: Privacy in online social networks

R Kanha Sar[1], Y Al-Saggaf[2] and T Zia[3]

School of computing and mathematics, Charles Sturt University, Australia
[1] rsar@csu.edu.au,
[2] yalsaggaf@csu.edu.au
[3] tzia@csu.edu.au

ABSTRACT: *The increasing popularity of social network system (SNS) sites such as Facebook, Twitter and LinkedIn, has raised concerns about privacy particularly the risk of private information leakages and the secondary use of those information. Users' information is being shared/leaked in a number of ways including the use of tracking technologies (such as HTTP cookies). This paper will provide an analysis of the privacy issues related to OSNs and using a hypothetical scenario it will argue for the SNS users' right to privacy. It is hoped that the analysis will raise awareness about the threats to privacy from the current practice to information leakages and the future possibilities of information leakage.*

Keywords: Privacy, Ethics, Social Network System, Online Social Networks.

INTRODUCTION

Over the past few years, social network sites (SNS) such as Facebook, Twitter, and LinkedIn, have become increasingly popular since they provide new means of communication. Users of these systems are typically required to fill out their online profile with minimum personal information such as name, date of birth, email address and/or profile picture. Then they can share their thoughts, ideas and creativities, form online social communities and keep in touch with people they know from both online and offline.

It is reported by the Digital Criminal (as cited in Irvine, 2009) that nearly two fifths of polled 2,000 social network users posted details of their holiday plans and 41% of them reveal private information (such as date of birth, and workplace) to public or complete strangers. A study of Twitter content has shown that users do write about themselves, their activities and where they are (Humphreys, Gill, & Krishnamurthy, 2010). By having different pieces of identifiable and/or personal information diffused online, and having no clue of who has access to those information, the users expose themselves to various risks ranging from the risk of privacy loss and the associated risks such as harassment, identity theft, and digital dossier.

An example of this would be the story of an Australian Olympic swimmer Stephanie Rice was dumped by sponsor Jaguar over her a Twitter message she wrote and was forced to apologize to those offended by her Tweet when she claimed the South African rugby team were homosexuals (Bymes, 2010). Her gay friend, Matthew Mitchum, defended her saying she meant no harm but nevertheless her message was offensive and thoughtless. A number of conclusions can be drawn from this situation: (a) Rice has no idea of who (in the world) have access to her Tweets, (b) Rice treated Twitter as a private space, and/or (c) Such an incidence would never happen if she said exactly the same thing with her close friend, in a private space (e.g. her home).

Privacy might not be valued to the same degree among users from different countries and cultures, but the users should at least have knowledge about or control over what type of information about them is being collected. Privacy issue in SNS become a concern because large amount of personal information are voluntarily shared and they can be harvested so rapidly and stored for an unknown time period.

In this paper, we discuss different possible information leakages caused by SNS and non-SNS in a number of ways such as the tracking technologies (e.g. cookies). We also present a scenario to illustrate how different bits and pieces of user's information diffused online may be used to build a detailed picture of a person's life - which may affect his/her future job opportunities and/or health insurance –

without that person's knowledge: that is when the privacy issue arises.

SOCIAL NETWORK SITE OVERVIEW

For the purpose of this paper, social network site (SNS) is defined as “web-based services that allow individuals to (a) construct a public or semi-public profile within a bounded system, (b) articulate a list of other users with whom they share a connection, and (c) view and traverse their list of connections and those made by others within the systems” (Boyd & Ellison, 2007).

The first recognizable SNS was launched in 1997. sixdegrees.com allowed users to create and populate their profiles, list their friends and surf the friend lists in 1998. Despite the fact that it attracted million of users, it lasted for only 3 years (Boyd & Ellison, 2007). From 1997 to 2011, a number of SNS like Ryze (www.ryze.com) was launched to help people leverage their business works. While Ryze failed to acquire mass popularity, LinkedIn becomes a very powerful network attracting professional users. Remarkably, Facebook, which was launched in 2004, becomes very popular and successful. It attracted 500 million users in mid 2010 (Zuckerberg, 2010) and continues to grow to more than 800 million in 2011 (Facebook, 2011).

SNS can be grouped into different categories such as business, common interest, dating, face-to-face facilitation, friends, pets, and photo (Social Software Weblog, as cited in (Gross & Acquisti, 2005). Some sites are designed for specific ethnic, political, religious, or sexual orientation categories. With the popularity of smart phones with the Internet access, mobile specific social network site like Foursquare (www.foursquare.com) emerged, and some web-based SNSs like Facebook (Slee, 2007) and LinkedIn (Nash, 2009) also provide mobile access to the sites. The number of users access Facebook from mobile increases from 100 million (Palihapitiya, 2010) in early 2010 to 350 million in 2011 (Facebook, 2011).

PRIVACY

Given the ease of access and the popularity of the SNS, privacy issues have emerged which becomes a major concern among SNS users.

There is no rigid definition of privacy. Different ways of life in different societies give different forms of privacy. Privacy is not about all or nothing; we need to give up our privacy to some extent to live in a society, but we cannot experience a total loss of privacy. Ruth Gavison (1980, as cited in Gibbs, 2008) defines privacy as the limitation of other's access to an individual, and that limitation of access has three key elements: control of information about oneself (Secrecy), freedom from other's attention (Anonymity) and freedom from surveillance and observation (Solitude). Meanwhile, privacy is classified into four distinct types: Physical/Accessibility (involving one's physical space), Decisional (noninterference involving one's choices), Psychological/Mental (non-intrusion/ noninterference involving one's thoughts and one's personal identity), and Informational Privacy (Having control over/limiting access to one's personal information) (Tavani, 2007).

Al-Saggaf and Weckert (2011) point out that our inner thoughts and feelings, our personal relationships, our personal information (particularly about our lives as our health and finance), our own space (e.g. our house, desk, room), and our state of being unobserved should be treated as an individual's business and should be private matters, at least in a sense that those involved want to be able to choose what details they intend to share to which third parties. People might not mind others knowing various things about them, but the control over access to the knowledge is crucial.

Information being shared among SNS and non-SNS sites

Concerns involving technologies that threaten information privacy is not new. However, what makes the difference is \the type of information "being voluntarily shared by the SNS users and being leaked from the SNS to the third party sites without the user's knowledge. In order to join an SNS, the users are typically required to fill in their profile pages with basic and/or personal information such as full name, email address, location, gender and date of birth. Later, they also provide extra information to enrich their profile pages. Those information can be classified into five groups (Krishnamurthy & Wills, 2008) known as: (1) Thumbnail (A brief profile contains at least full name and image), (2) Greater profile (Additional information including interests and relationship status), (3) List of friends, (4) User generated content (e.g. pictures, video, links and comments), and (5) Comments (Status updates, testimonial and tags). There are at least three ways the user's information are leaked/ become available to the third party organization: privacy setting, tracking technologies and the use of application programming interface (API).

SNS provide privacy setting that allows users to set different privacy levels to whom they decide to share the information to. By default, the user's profile page is publicly available and searchable in the search engines. Some users do not care about changing their privacy setting (Boyd & Hargittai, 2010) while others change the privacy setting for their profile to be viewed by people they know only (Young, 2009). There are two main reasons why the users do not change the default setting online; either they may be uninformed that they can change the default setting or they might not have technological knowledge to change it (Shah, and Kesan, 2003, as cited in Humphreys et al., 2010). By exposing and sharing personal and sensitive information, the users might expose themselves to various real-life and cyber risks such as phishing attack, identity theft and digital dossier.

Another contribution to the information leakage is the tracking technologies such as HTTP cookies, flash cookies and web beacons or web bugs (Angwin, 2010). HTTP cookie is a small piece of information transferred back and forth between servers and clients. It is used by the web-based application to maintain the state in the stateless HTTP protocol (Kristol, 2001). Meanwhile, Flash Cookies were originally used to remember user's preferences such as volume for online videos (Brinkmann, 2007) but they can also be used to re-install regular cookies that a user has deleted, and cannot be controlled through the cookies privacy control in the browser (Schneier, 2009). Web Beacon or Web bugs and Pixels, on the other hand, are pieces of code run on a web page, which can track the user's movement on the page including what is being typed or where the mouse is moving (Angwin, 2010). Different pieces of information (including SNS ID) are being leaked to the third parties from SNS (Krishnamurthy &Wills, 2010a) and non-SNS (Krishnamurthy & Wills, 2009) from the desktop as well as mobile devices (Krishnamurthy & Wills, 2010b) via the use of cookies; which mean a user's online behavior combined with his/her SNS unique ID, and/or mobile phone unique ID, can reveal so much about a person's life. This information sharing or leakages keep increasing without the user's knowledge (Krishnamurthy &Wills, 2009).

The users' information is also being shared via the use of Application Programming Interface (API) among SNS (Ko, Cheek, & Shehab, 2010). The API services allow the third party sites develop social applications without having to build their own social networks. These applications provide interesting contents to users' existing profiles. Through the use of API, SNS allow limited access to the users' information to the third parties. For example, by installing the third party music application called iLike (www.iLike.com), Facebook users can share music with their Facebook friends, and in order to install iLike, users have to give up some certain information to iLike in exchange for the service.

As a result, the user digital dossier can be built at ease with the combination of the user's partial PII, the location information, the mobile device unique identifier and the available large amount of personal data from the API.

DISCUSSION AND ANALYSIS

Let us consider a scenario of a girl named Emilie:
Emilie is a nice and helpful girl. She has just finished her undergraduate degree from a university in Paris. She is updating her profile in LinkedIn and looking for a job. She is also learning English and using Dictionary.com (The site with the most tracking files in a case study by the Wall Street Journal (Angwin, 2010)) as reference for English vocabulary. She is also on Facebook keeping in touch with her friends and relatives. Her activities on Facebook include posting pictures, comments and statuses, using check-in service to reveal her location to her friends, and playing third party game like Farmville (by Zynga). Sadly, she has a friend who is HIV-positive and depressed, and is having problem with drugs and alcohol. In order to provide mental support to her friend, Emilie spends some time searching for information to understand her friend's condition. Meanwhile, she helps her pregnant cousin order the books and vitamin supplements for pregnancy from online stores. Her Internet access is done via both her desktop computer and her mobile phone.

By being part of SNS and non-SNS, Emilie's minimal information being diffused on the internet include: her online activities, personal information, SNS unique identifier, mobile phone unique identifier, location, interests and preferences. This information is being tracked and recorded by SNS and non-SNS like Dictionary.com.

To find out how privacy concerns are generated by SNS and non-SNS, we analyze Emilie's story based on two ethical theories: utilitarianism and deontology. From a utilitarianism view point, the expected outcome or consequences of an act is very important to determine whether or not that act is morally acceptable while the role of duty and respect for persons are the key to what is morally permissible for a deontologist (Tavani, 2011). Two outcomes can be drawn from the Emilie's story.

Thanks to Facebook default setting which makes users' profile pages publicly available and searchable, Emilie's childhood friends are able to find and reconnect with her based on Emilie's basic personal information including pictures, her hometown and high school. The tracking technologies help to provide the tailored advertisements, and Emilie is able to get the book and vitamin supplements for pregnancy at discounted prices from online stores. Facebook Connect, meanwhile, allows Zynga to provide more interactive and social online games like Marfia wars and Farmville - which allow users to engage more in online games with their existing Facebook friends. The act of sharing and gathering SNS users' information in order to enhance their online experience (e.g. friendship reconnection, relevant ads, and interactive games) appears to be consistent with both Kant's principles of treating people as ends in themselves and the principles of utilitarianism which promote the greatest good for the greatest number.

On the other hand, different pieces of Emilie's information, her interests and preferences are being harvested and tracked without her consent. This information can later be exchanged, transferred, traded, and/or combined. The combination of her online activities, her SNS profiles and her psychological profiles may reveal too much about her, which could be embarrassing or damaging to her future job opportunity. Her job or health insurance applications may be rejected simply because she may be pregnant and she might be involved with HIV, drugs, and alcohol. Almost half of European recruiters seek information on candidates based on their online reputation in various SNS (EurActiv, 2010). What is worse is that not all the information is 100% accurate about Emilie's life. She is neither pregnant, nor HIV-positive, but the cookies are not aware that she did the search for her friend and cousin (YOU ARE WHAT YOU TYPE!). From a deontologist viewpoint, SNS users are not respected as persons and they are treated as means to some ends (the means being users' information while the ends being the income generated from the sales of those information). Their informational privacy is violated since the ability to control what type of information about them is being collected, by whom and for what purpose the information will be used is not given to them. This also results in negativity for online image/reputation and job opportunity for the majority of SNS users - which is not morally permissible according to utilitarianism.

CONCLUSION AND FUTURE RESEARCH

Social network sites (SNSs) offer exciting new opportunities and benefits for interaction and communication, but also raise privacy concerns. SNS default setting, tracking technologies (e.g. traditional cookies, flash cookies and web beacons), and the use of Application Programming Interface (API) among SNSs contribute to the leakages of user's personal information from those SNS to the third party sites, without the user's knowledge. There is no definite answer to who has access to and control over users' information. Large amount of users' personal information are voluntarily shared among SNS or non-SNS. They can be harvested so rapidly and stored for an unknown time period without the user's knowledge. In the event of SNS ownership changes, through merges or bankruptcy, it is not clear what will happen to that information. Different bits of user's information diffused online can be accumulated over time. Through the secondary use of personal information (e.g. data mining technique) from SNS and non-SNS, the user's identity could be combined and revealed.

The users might have different tolerance toward their privacy and/or they might be aware of the collection of bits and pieces of their information, but they may not be aware that the combination of their information can be used to build a detailed profile of their lives. Emilie may voluntarily give her personal and professional information, online game behavior, shopping preferences, and browsing interests to SNS, online game company, online stores and search engine respectively; however, she may not authorize any third party organization to make the secondary use of her information. While analyzing Emilie's story by using ethical theories reveals both positive and negative impacts brought by cyber-technology, particularly, among SNS and non-SNS. However, to maximize the positive impact, the users should at least have control over the amount and type of information being gathered, how and whether or not it is necessary, and by whom.

Despite the fact that we did not provide concrete solution to the threats to privacy in SNSs, by pointing out the potentials for violating the users' privacy, we hope that this article will raise users' awareness alerting them that they are what they type.

In the future work, we intend to look at the impacts of SNS on privacy from three different angles: technical, social and philosophical. The technical angle will employ a qualitative approach using a case study method of an SNS user to investigate the types of information being leaked/shared among SNS and non-SNS in the HTTP headers and HTTP cookies, and the consequences of the leakages within that case. The social angle will use ethnography method to study the importance of privacy from the perspective of online users, particularly the users of SNS. The finding of these two studies will then be analyzed by using different philosophical theories. The research will shed light on what types of information leakages posing threats to privacy, why privacy is important from social and philosophical viewpoint. It will also provide recommendations to improve the current situation.

REFERENCES

Al-Saggaf, Y., & Weckert, J. (2011). Privacy from a Saudi Arabian perspective. *Journal of Information Ethics*, 20 (1), 34-53.

Angwin, J. (2010, July). The web's new gold mine: Your secrets. *The Wall Street Journal*. Available from: http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html

Boyd, D., & Ellison, N. B. (2007, November). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13 (1-2). Available from http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

Boyd, D., & Hargittai, E. (2010, August 2). Facebook privacy settings: Who cares? *First Monday, 15* (8). Available from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086

Brinkmann, M. (2007, May). *Flash cookies explained*. ghacks.net. Available from http://www.ghacks.net/2007/05/04/flash-cookies-explained/

Bymes, H. (2010, September). *Shattered Stephanie rice says sorry over homophobic tweet*. Available from http://www.dailytelegraph.com.au/news/shattered-stephanie-rice-says-sorry-over-homophobic-tweet/story-e6freuy9-1225915930831

EurActiv. (2010, February). *Social networks put careers at risk, survey finds*. EurActiv. Available from http://www.euractiv.com/en/Social-networks-careers-risk

Facebook. (2011, October). *Facebook statistics*. Available from http://www.facebook.com/press/info.php?statistics

Gibbs, M. (2008). Privacy. In D. McDermid (Ed.), *Ethics in ICT: An Australian perspective* (p. 89-123). Malaysia: Pearson Education Australia.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *In Proceedings of the 2005 ACM workshop on privacy in the electronic society* (pp. 71{80). New York, NY, USA: ACM. Available from http://doi.acm.org/10.1145/1102199.1102214

Humphreys, L., Gill, P., & Krishnamurthy, B. (2010, June). *How much is too much? privacy issues on twitter*. Available from http://www.cs.utoronto.ca/~phillipa/papers/ica10.pdf

Irvine, C. (2009, August). *Facebook and twitter users could be targeted by burglars*. The Telegraph. Available from http://www.telegraph.co.uk/technology/twitter/6096677/Facebook-and-Twitter-users-could-be-targeted-by-burglars.html

Ko, M. N., Cheek, G. P., & Shehab, M. (2010, August). Social networks connect services. *Computer: Innovative Technology for Computer Professionals*, 43 (8), 37-43. (IEEE Computer Society)

Krishnamurthy, B., & Wills, C. (2009). Privacy diffusion on the web: a longitudinal perspective. *In Proceedings of the 18th international conference on world wide web* (pp. 541{550). New York, NY, USA: ACM. Available from http://doi.acm.org/10.1145/1526709.1526782

Krishnamurthy, B., & Wills, C. E. (2008). Characterizing privacy in online social networks. *In Proceedings of the first workshop on online social networks* (pp. 37{42). New York, NY, USA: ACM. Available from http://doi.acm.org/10.1145/1397735.1397744

Krishnamurthy, B., & Wills, C. E. (2010a, January). On the leakage of personally identifiable information via online social networks. *SIGCOMM Comput. Commun. Rev.*, 40, 112{117. Available from http://doi.acm.org/10.1145/1672308.1672328

Krishnamurthy, B., & Wills, C. E. (2010b). Privacy leakage in mobile online social networks. *In*

Proceedings of the 3rd conference on online social networks (pp. 4{4). Berkeley, CA, USA: USENIX Association. Available from http://portal.acm.org/citation.cfm?id=1863190.1863194

Kristol, D. M. (2001, November). HTTP cookies: Standards, privacy, and politics. *ACM Trans. Internet Technol.* , 1 , 151{198. Available from http://doi.acm.org/10.1145/502152.502153

Nash, A. (2009, December 28). *Linkedin for iphone 3.0: Let's get this party started.* LinkedIn Blog. Available from http://blog.linkedin.com/2009/12/28/linkedin-for-iphone-3-0-lets-get-this-party-started/

Palihapitiya, C. (2010, February 11). *Facebook mobile: 100 million and growing.* Facebook Blog. Available from http://www.facebook.com/blog.php?post=297879717130

Schneier, B. (2009, August). *Flash cookies.* Schneier on Security. Available from http://www.schneier.com/blog/archives/2009/08/flash\ cookies.html

Slee, M. (2007, January 10). *Facebook your phone.* Facebook Blog. Available from http://ja-jp.facebook.com/blog.php?post=2228532130

Tavani, H. T. (2007). *Ethics and technology: Ethical issues in an age of information and communication technology* (2nd ed.). United States of America: Bruce Spatz.

Tavani, H. T. (2011). *Ethics and technology: controversies, questions, and strategies for ethical computing* (3rd ed.). United States of America: Wiley.

Young, K. (2009). Online social networking: An Australian perspective. *International Journal of Emerging Technologies and Society,* 7 (1), 39-57.

Zuckerberg, M. (2010, July 22). *500 million stories.* Facebook Blog. Available from http://www.facebook.com/blog.php?post=409753352130