

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htmComputer Law
&
Security Review

Privacy trust crisis of personal data in China in the era of Big Data: The survey and countermeasures

Zhong Wang ^{a,*}, Qian Yu ^b^a Beijing Academy of Social Sciences, Beijing, China^b Beijing Normal University, Beijing, China

ABSTRACT

Keywords:

Personal data
Privacy trust
Questionnaires
Interview
Big data

Privacy trust directly affects the personal willingness to share data and thus influences the quality and size of the data, thus affecting the development of big data technology and industry. As China is probably the largest personal data pool and vastest application market of big data, the situation of Chinese privacy trust plays a significant role. Based on the 17 most common data collection scenarios, the following aspects have been observed through 508 questionnaires and interviews of 20 samples. To start with, there is a severe privacy trust crisis in China, both in the field of enterprise services such as online shopping and social networks, etc. and in some public services like medical care and education, etc. Besides, there are also doubts about data collected by the government since individuals refuse to offer personal information or give false information as much as possible. Some people even buy two phone numbers, one is in use, while the other is not carried around or used by them, which is only bought to be offered to data collectors. Secondly, in terms of gender, females have lower trust in enterprises and social associations than males, especially in the fields of social networks and personal consumption. However, there is no obvious difference in fields of government and public services. Females possess stronger awareness but less skilled in precautions than males. Thirdly, people between the ages of 18 and 50 are more suspicious of data collected by enterprises, while age exerts little obvious influence on the credibility of data collected by the government, social associations and public services. Older people are less aware of precautions than people at other ages. In addition, from the perspective of education background, people with higher degrees possess stronger awareness of precautions and thus lower degree of trust. Therefore, it is suggested that more education on privacy consciousness should be given, and relative laws as well as regulations need improving. Besides, innovation in privacy protection technologies should be encouraged. What is more, we need to reinforce the management of the internet industry and strictly regulate personal data collection of the government.

© 2015 Zhong Wang & Qian Yu. Published by Elsevier Ltd. All rights reserved.

* Corresponding author. Beijing Academy of Social Sciences, No. 33, Middle Road, North 4th Ring Road, Chaoyang District, Beijing, China.
E-mail address: wz.0@hotmail.com (Z. Wang).

<http://dx.doi.org/10.1016/j.clsr.2015.08.006>

0267-3649/© 2015 Zhong Wang & Qian Yu. Published by Elsevier Ltd. All rights reserved.

Personal data directly reflects the demand from users,¹ which is at the heart of the current application of big data.² However, the influence of the idea that “Big data is big brother” is increasing.³ The privacy trust crisis leads to the result that individuals are reluctant and may even refuse to share personal data, which will cause a decrease in data quality and quantity and hence cut off the source of big data.⁴ Therefore, it is important to study privacy trust. China as a country with the largest population could be the largest personal data pool and the biggest application market of big data, whose situation of privacy trust will exert a great influence on global big data industry as well as technological development. As a result, it is significant to have an accurate assessment of the basic information regarding the Chinese privacy trust. For this purpose, the authors have undertaken a thorough analysis of the current situation and reasons for the nature of privacy trust among Chinese mainland citizens through questionnaires and in-depth interviews. Countermeasures are proposed at the end of this paper.

1. Literature review

1.1. Personal data/ personal information

According to the laws and the legal standards of various countries and regions, both “personal data” and “personal information” expressions are adopted.⁵ For instance, the European Union mainly uses “personal data”, while in Japan, “personal information” is used most frequently. The same result appears in the research documents.⁶ However, the two terms above are technically different from each other in that “data” places more emphasis on being automatically processed by devices while “information” stresses the transmission of the content.⁷ With the rapid development of information technology, these two become more and more different in semantic meanings. Although the concept of “personal data” is more accurate, the concept of “personal information” is employed in this study for it was used in original laws.

1.2. Privacy

The concept of privacy is developing constantly. Therefore, different countries, nations or even individuals at different

historical phases have different understanding of the term.⁸ Generally speaking, privacy is a concept irrelevant to public and group interest, referring to the information that the clients keep to themselves because they are reluctant to share with others or it is inconvenient for others to know the information, personal affairs that the clients expect no intervention from others or that is not suitable for others to interfere with, and personal domains that the clients does not want others to invade or others are inconvenient to invade.⁹

1.3. Privacy trust

According to Shneiderman, trust is the positive expectation of a person or an organization based on their previous performance and real assurance.¹⁰ Though information technology makes it more convenient in all aspects of life, it provokes people’s attention to personal privacy, resulting in an unprecedented challenge for privacy trust.¹¹ The emergence of big data especially might expose personal privacy to the public, so that privacy protectionists worry about the “Big Data is Big Brother” scenario.¹² The current study on privacy trust focuses on the following aspects: Firstly, factors influencing privacy trust in the network environment. Some scholars state that the key influencing factor of privacy trust is privacy concerns, which means that more concerns about privacy results in lower credibility and higher risks during the process of information sharing.¹³ Secondly, there is privacy trust in e-commerce. Some scholars have done modeling analysis of privacy trust in e-commerce and found that the more the consumers trust a website, the less they will pay attention to their privacy. Therefore, websites can gain trust from their users by establishing a trust system.¹⁴ Thirdly, there is privacy trust in social networks. Dwyer et al. found that the more users trust a website, the more willing they are to share information and develop contacts on social network sites.¹⁵ Most users have not taken

⁸ Hahn, Jim. (2014). Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family. *Library Journal*, 139(10), 124–124.

⁹ Prosser, W. L. (1960). PRIVACY. *California Law Review*, 48(3), 383–423. doi: [10.2307/3478805](https://doi.org/10.2307/3478805).

¹⁰ Shneiderman, Ben. (2000). Designing trust into online experiences. *Communications of the ACM*, 43(12), 57–59.

¹¹ Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1), 153–160. doi: [10.1016/j.chb.2008.08.006](https://doi.org/10.1016/j.chb.2008.08.006).

¹² Carmagnola, Francesca, Osborne, Francesco, & Torre, Ilaria. (2014). Escaping the Big Brother: An empirical study on factors influencing identification and information leakage on the Web.

¹³ Chan, Wendy Wing Lam, & Ma, Will Wai Kit. (2013). Exploring the Influence of Social Ties and Perceived Privacy on Trust in a Social Media Learning Community Hybrid Learning and Continuing Education (pp. 134–144): Springer.

¹⁴ Al-alak, Basheer AM, & Ibrahim, AM. (2010). Mobile Marketing: Examining the Impact of Trust, Privacy Concern and Consumers’ Attitudes on Intention to Purchase. *International Journal of Business & Management*, 5(3), 28–41.

¹⁵ Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 Proceedings*, 339.

¹ Graeff, Timothy R, & Harmon, Susan. (2002). Collecting and using personal data: consumers’ awareness and concerns. *Journal of Consumer Marketing*, 19(4), 302–318.

² Mayer-Schönberger, Viktor, & Cukier, Kenneth. (2013). Big data: A revolution that will transform how we live, work, and think: Houghton Mifflin Harcourt.

³ Marozzi, Matilda. (2013). Big data or big brother. *Voiceworks*, No. 94, Spring 2013: 27–30.

⁴ Chen, Hsinchun, Chiang, Roger HL, & Storey, Veda C. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly*, 36(4), 1165–1188.

⁵ Moon, Jaewan. (2014). A Study on the Concept of Personal Data. *개인정보의 개념에 관한 연구*. *Public Law*, 42(3), 53–77.

⁶ Ter, Kah Leng. (2013). Singapore’s Personal Data Protection legislation: Business perspectives. *Computer Law & Security Review*, 29(3), 264–273. doi: [10.1016/j.clsr.2013.03.007](https://doi.org/10.1016/j.clsr.2013.03.007).

⁷ Cate, Fred H. (2014). Privacy, Big Data, and the Public Good. *Science*, 346(6211), 818–818. doi: [10.1126/science.1261092](https://doi.org/10.1126/science.1261092).

Download English Version:

<https://daneshyari.com/en/article/467632>

Download Persian Version:

<https://daneshyari.com/article/467632>

[Daneshyari.com](https://daneshyari.com)