ISSN 2614-0047

Concerns for digital privacy in business and management: an overview and future discourses recommendation

Jaya Addin Linando [a,1,*], Guntur Budi Herwanto [b,2]

[a] Management Department, Universitas Islam Indonesia, Yogyakarta, Indonesia
[b] Computer Science Department, Universitas Gadjah Mada, Yogyakarta, Indonesia
[1] addin.linando@uii.ac.id ; [2] gunturbudi@ugm.ac.id
* corresponding author

ARTICLE INFO

Article history
Received October 30, 2022
Revised November 21, 2022
Accepted December 3, 2022

Keywords
Digital privacy
Data privacy
Consumer privacy
Business
Management

ABSTRACT

This paper aims to highlight the developing awareness of concern for digital privacy from a business and management viewpoint. The authors compile data privacy literature in the management field and visualize the literature into four main clusters of concerns. The four central concerns in data privacy discourse in management are the internet; roles-trust-security; locations; and consumer privacy. This paper contributes to developing research and discourse in the data privacy and management domain. Besides delivering an overview of the digital privacy concerns in business and management fields, the paper also places suggestions for future researchers.

1. Introduction

As the advancement of technology has impacted all aspects of human lives and shaping the future, the discourse of technology-related matters from business and management viewpoint emerges as a pertinent current issue. While on the one hand technology eases a lot of human activities, on the other hand technology also bears many concerns and questions. Hence, the saying that technology is a double-edged sword apparently be plausible. This paper aims to focus on the 'dark' side of technology, in particular from business and management perspective. By no means to disparage another important issues on technology and business (i.e., monopoly practices in digital platform; digital literacy challenges), for the sake of argumentations depth the authors limit the paper's scope on privacy issue.

Privacy grows as one of the biggest concerns in digital era [1], [2]. Data is an incredibly important asset, where collecting and sharing data transform into big businesses in today's digital economy [3]. As companies collect more information about their customers, customers are beginning to recognize the potential drawbacks of data collection [4]. In order to safely and successfully use the data they collected, companies should ensure that the data is strictly private and that consumers are not exposed to unsolicited surveillance [5]. The Cambridge Analytica and Facebook scandals have raised questions about how consumers' personal data can be protected. As privacy escalates to be an integral part of human rights, governments are expected to ensure their citizens' privacy are safe [6]. The upsurge of concern for privacy promotes new laws and regulations like the European Union's General Data Protection Regulation (GDPR) that requires businesses and organizations to adhere to specific privacy and data protection rules. From company's perspective, privacy has evolved into a critical component of a company's image. These highlights of the growing importance of privacy in business and management field triggers the authors to write this piece of note.

2. Method

While there are various arguments on definitions of 'privacy', the relationship of 'privacy' with other associated terms, and the debate of the 'privacy boundaries (see the discussion further on Reference [7], the discourses of privacy in business and management context are relatively convergent. Mainly the business and organizational cases of privacy focus on customers and employees (e.g., Reference [8]; Reference [9]) hence makes human resources management (HRM) and marketing as the two most related management branches to privacy issues. Data protection issues affect most human resources activities, including recruitment [10], monitoring [11] and the management of their data [12]. The main question on HR field regarding data protection is whether employers should be allowed to monitor online activities of their employees. Supposedly employees deem the employers violate their data privacy, the Electronic Communications Privacy Act (ECPA) can enact to help protect employees' fundamental right to privacy in their electronic communications [13].

On the marketing side, marketers are increasingly reliant on customer data for market segmenting and targeting purposes. Marketers are the custodians of their company's brand image, hence ignoring consumer's privacy out of choice or necessity could bear negative impacts on the overall company's image. Marketing field also sees Online personalized advertising (OPA) among one of the most advanced tool to utilize personal data for marketing research. Consumers may view OPA as a beneficial tool, but at the same time may also concern about their personal information being profiled by the company. This is known as the paradox of personal advertising, which is relevant for the current and future marketing discourse and still lacks exploration to date [14].

The authors compile data privacy in HRM and marketing articles through 'title words' and 'keywords' search combinations on Publish or Perish (PoP) software and run the result's visualization using VOSviewer as can be seen in Fig. 1. The visualization was obtained through title field analysis, complete counting method, and minimum 10 occurrences threshold. In total, 464 articles were obtained with a wide-ranging timespan of publication. For instance, a paper discussing the privacy dilemma of intimacy versus intrusion in marketers-customers' relationship management [15]. From Human Resource Management perspective, there is a paper discussing the reciprocal rights and responsibilities between employees and institutions [16]. From the article list, the most cited article is about consumers' privacy concerns and willingness to share their personal information, with more than a thousand citation to date [17].

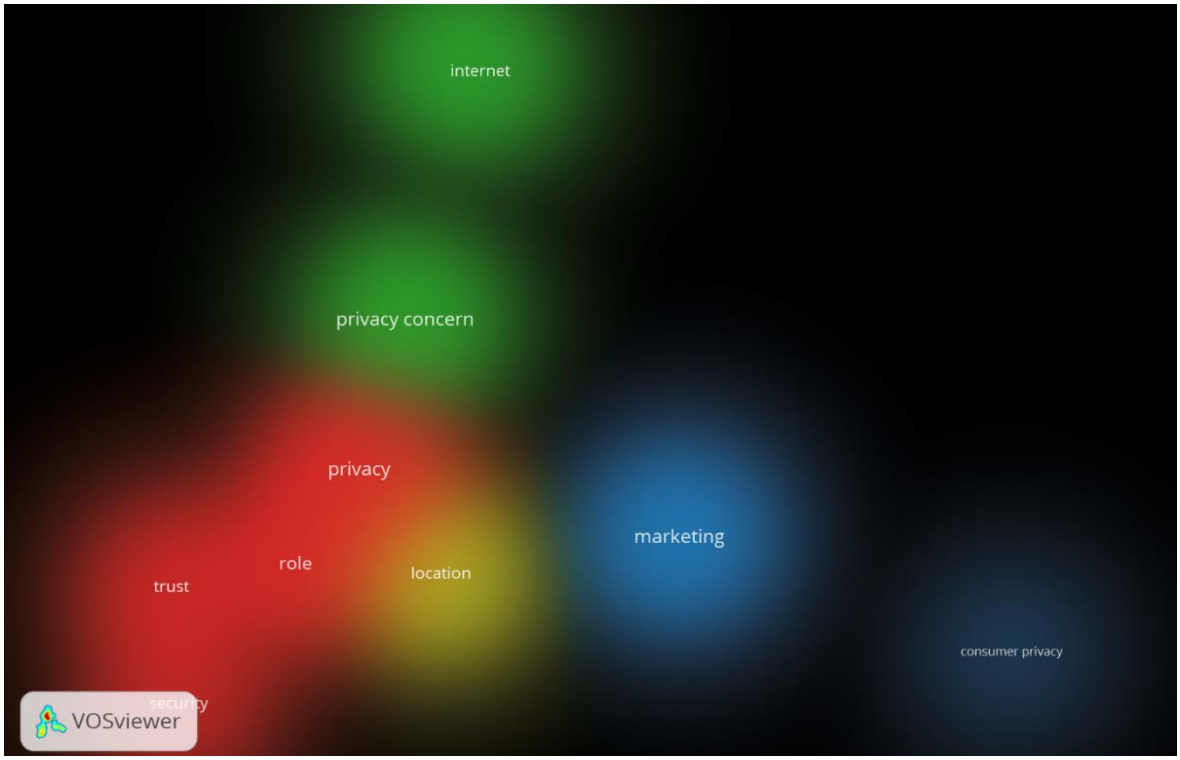

Fig. 1. Concerns for Privacy Themes on Business-Management Fields

3. Results and Discussion

3.1. Results

The visualization was obtained through title field analysis, full counting method, and minimum 10 occurrences threshold. The result shows 4 clusters of concerns which are:

- Internet

  As the leading platform of digital era, internet as a cluster provides general overview of the privacy-related matters happening around the business world. The contents vary from fairness matter on the internet, e-business model, Internet of Things (IoT) to internet users' characteristics.

- Roles-Trust-Security

  This is arguably the most wide-ranging cluster as it concerns the privacy-related interconnected components like the role of digital marketing in political campaigns, the role of user privacy concerns in platforms competition, the role of governmental organization to regulate data privacy and the role of information types that shape privacy issue. The trust variable deals with the conviction on platforms and institutions such as business websites, employee learning tools, hospitals, and cyber games. Finally, the cluster ends on security issues like identity security, organization security compliance, and potential business frauds.

- Locations

  It concerns two main subjects: location-based marketing apps and service and the advertisement location of digital marketing.

- Consumer Privacy

  This marketing subject develops as a particular concern following the number of articles placing consumer privacy as their primary emphasis [18]. Among the discourses on this cluster are related to the perception of privacy from two point of views (consumers and sellers/marketers), business privacy policy to protect the customers, consumer's privacy awareness and different country's regulations of consumer privacy.

3.2. Recomendation

Following this short overview of the growing privacy themes in business and management fields, the authors offer several further discussion topics for the researcher interested on data privacy and business management intersection. The topics are arranged on three (macro-meso-micro) levels to cover the broad research interests.

- Macro Level – Countries/Social

  Future researchers may consider to examine different country's approaches on managing privacy. There are some websites provide country comparison data privacy laws (i.e., www.dlapiperdataprotection.com) that might be helpful to construct the argumentations. It is also possible to evaluate the privacy management effectiveness of particular government policy or institution.

- Meso Level – Organization

  Among the main questions will be how the organization can ensure its consumers and employees that the business and management practices is in compliance to data privacy protection. It is also possible to further discuss the ethical, responsibility, benefit and competition aspects of privacy policy and management within organization.

- Micro Level – Individual

  Mainly concerns individual privacy awareness, consent, the fair exchange of personal information (further elaboration on this matter, see Reference [19]; Reference [20], and the consequences (mental, emotional, or even physical) for individuals upon the case of the privacy breach and misuse.

4. Conclusion

Bearing in mind the loud echoes of digital era for current and future generations, the discourse of digital privacy in business-management field stands as an ever-growing subject. Individuals are more likely to do businesses with organizations that are sensible of data protection matters. The way companies respond to concerns about data privacy will be crucial. In the coming years, it will be a challenge for organizations to show that data privacy and personalization can go hand in hand. By emphasizing their commitment to protecting their stakeholders' privacy, ensuring transparency in the use of data and offering more privacy options, businesses can build a good credential. The authors argue that the future central discourse will revolve in the quest for win-win solution, both for companies and their stakeholders. Where businesses can utilize personal data for their interest and at the same hand, their stakeholders (like consumers and employees) feel safe and respected.

References

[1] E. Santanen, "The value of protecting privacy," *Bus. Horiz.*, vol. 62, no. 1, pp. 5–14, Jan. 2019, doi: 10.1016/j.bushor.2018.04.004.

[2] Z. Allam and Z. A. Dhunny, "On big data, artificial intelligence and smart cities," *Cities*, vol. 89, pp. 80–91, Jun. 2019, doi: 10.1016/j.cities.2019.01.032.

[3] V. S. Litvinenko, "Digital Economy as a Factor in the Technological Development of the Mineral Sector," *Nat. Resour. Res.*, vol. 29, no. 3, pp. 1521–1541, Jun. 2020, doi: 10.1007/s11053-019-09568-4.

[4] Y. Wang, L. Kung, and T. A. Byrd, "Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations," *Technol. Forecast. Soc. Change*, vol. 126, pp. 3–13, Jan. 2018, doi: 10.1016/j.techfore.2015.12.019.

[5] C. Yang, Q. Huang, Z. Li, K. Liu, and F. Hu, "Big Data and cloud computing: innovation opportunities and challenges," *Int. J. Digit. Earth*, vol. 10, no. 1, pp. 13–53, Jan. 2017, doi: 10.1080/17538947.2016.1239771.

[6] L. Yang, N. Elisa, and N. Eliot, "Privacy and Security Aspects of E-Government in Smart Cities," in *Smart Cities Cybersecurity and Privacy*, Elsevier, 2019, pp. 89–102, doi: 10.1016/B978-0-12-815032-0.00007-X.

[7] J. R. Saura, D. Ribeiro-Soriano, and D. Palacios-Marqués, "Evaluating security and privacy issues of social networks based information systems in Industry 4.0," *Enterp. Inf. Syst.*, vol. 16, no. 10–11, pp. 1694–1710, Oct. 2022, doi: 10.1080/17517575.2021.1913765.

[8] K. D. Martin and P. E. Murphy, "The role of data privacy in marketing," *J. Acad. Mark. Sci.*, vol. 45, no. 2, pp. 135–155, Mar. 2017, doi: 10.1007/s11747-016-0495-4.

[9] X. Zhang, Y. Zhu, and N. Hua, "Privacy Parallel Algorithm for Mining Association Rules and its Application in HRM," in *2009 Second International Symposium on Computational Intelligence and Design*, 2009, vol. 2, pp. 296–299, doi: 10.1109/ISCID.2009.220.

[10] P. Swartz, A. Da Veiga, and N. Martins, "Validating an information privacy governance questionnaire to measure the perception of employees," *Inf. Comput. Secur.*, vol. 29, no. 5, pp. 761–786, Nov. 2021, doi: 10.1108/ICS-08-2020-0135.

[11] S. A. Smith and S. R. Brunner, "To Reveal or Conceal: Using Communication Privacy Management Theory to Understand Disclosures in the Workplace," *Manag. Commun. Q.*, vol. 31, no. 3, pp. 429–446, Aug. 2017, doi: 10.1177/0893318917692896.

[12] D. Carpenter, A. McLeod, C. Hicks, and M. Maasberg, "Privacy and biometrics: An empirical examination of employee concerns," *Inf. Syst. Front.*, vol. 20, no. 1, pp. 91–110, Feb. 2018, doi: 10.1007/s10796-016-9667-5.

[13] D. Anthony, C. Campos-Castillo, and C. Horne, "Toward a Sociology of Privacy," *Annu. Rev. Sociol.*, vol. 43, no. 1, pp. 249–269, Jul. 2017, doi: 10.1146/annurev-soc-060116-053643.

[14] Q. Chen, Y. Feng, L. Liu, and X. Tian, "Understanding consumers' reactance of online personalized

advertising: A new scheme of rational choice from a perspective of negative effects," *Int. J. Inf. Manage.*, vol. 44, pp. 53–64, Feb. 2019, doi: 10.1016/j.ijinfomgt.2018.09.001.

[15] L. O'Malley, M. Patterson, and M. Evans, "Intimacy or intrusion? The privacy dilemma for relationship marketing in consumer markets," *J. Mark. Manag.*, vol. 13, no. 6, pp. 541–559, Aug. 1997, doi: 10.1080/0267257X.1997.9964492.

[16] F. A. Mael, "Privacy and personnel selection: Reciprocal rights and responsibilities," *Empl. Responsib. Rights J.*, vol. 11, no. 3, pp. 187–214, 1998, doi: 10.1023/A:1027307400954.

[17] A. Bleier, A. Goldfarb, and C. Tucker, "Consumer privacy and the future of data-based innovation and marketing," *Int. J. Res. Mark.*, vol. 37, no. 3, pp. 466–480, Sep. 2020, doi: 10.1016/j.ijresmar.2020.03.006.

[18] J. A. Obar and A. Oeldorf-Hirsch, "The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services," *Information, Commun. Soc.*, vol. 23, no. 1, pp. 128–147, Jan. 2020, doi: 10.1080/1369118X.2018.1486870.

[19] M. A. Katell, S. R. Mishra, and L. Scaff, "A Fair Exchange: Exploring How Online Privacy is Valued," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Jan. 2016, vol. 2016-March, pp. 1881–1890, doi: 10.1109/HICSS.2016.239.

[20] C. Prince, N. Omrani, A. Maalaoui, M. Dabic, and S. Kraus, "Are We Living in Surveillance Societies and Is Privacy an Illusion? An Empirical Study on Privacy Literacy and Privacy Concerns," *IEEE Trans. Eng. Manag.*, pp. 1–18, 2022, doi: 10.1109/TEM.2021.3092702.