Taiwanese university students' smartphone use and the privacy paradox

Uso del teléfono inteligente en universitarios taiwaneses y la paradoja de la privacidad

Dr. Yi-Ning Katherine Chen
Full Professor in the College of Communication at National Chengchi University (Taiwan)
(kynchen@nccu.edu.tw) (https://orcid.org/0000-0002-5667-1511)

Chia-Ho Ryan Wen
Research Assistant administering programs and projects from the Ministry of Science
and Technology (Taiwan) (RyanWen@Alumni.LSE.ac.uk)
(https://orcid.org/0000-0003-3477-6248)

Abstract

With the prevalence of smart devices and wireless Internet, privacy has become a pivotal matter in governmental, academic, and technological fields. Our study aims to understand Taiwanese university students' privacy concerns and protective behaviours in relation to online targeting ads and their habitual smartphone usage. Surveying 810 valid subjects, our results first propose that ad relevance has direct bearing on attention to ads. Second, ad relevance inversely correlates with privacy concerns (i.e. descending personal control and surging corporate power) and protective behaviours (self-filtering and ad evasion). Third and finally, neither privacy concerns nor protective behaviours have a negative bearing on habitual smartphone usage. Opposite to previous research, our study concludes that Taiwanese college students exhibit zero privacy paradox, owing to no signs of privacy concern incited by mobile targeting ads, no evidence of significant protective behaviours, and no decreasing habitual smartphone usage out of privacy concern and protection. Our findings indicate Taiwanese university students' shaky awareness of potential risks and crises from exposure to vulnerable online privacy management. To deal with this, we suggest educating youths' understandings of digital jeopardy by experts is urgently needed more so than just technical tutorials of privacy settings.

Resumen

Con la prevalencia de dispositivos inteligentes e Internet inalámbrico, la privacidad se ha convertido en un tema esencial en materias gubernamentales, académicas y tecnológicas. Nuestro estudio se dedica específicamente a entender las preocupaciones de los estudiantes universitarios taiwaneses en privacidad y comportamientos protectores en relación con la publicidad online y el uso habitual de teléfonos inteligen-tes. Con 810 muestras válidas encuestadas, nuestros resultados revelan que: 1) La relevancia de la publi-cidad tiene un efecto directo en su atención; 2) Está asociada inversamente a las preocupaciones de pri-vacidad (por ejemplo, control personal descendiente y poder corporativo ascendiente) y comportamientos protectores (evasión de anuncios y autocensura); 3) La preocupación por ña privacidad ni los comporta-mientos protectores tuvieron efecto negativo en el uso habitual de los smartphones. Nuestro estudio con-cluye que no

hay paradojas de la privacidad halladas en estos jóvenes taiwaneses debido a cambios en su preocupación por la privacidad, generada por la publicidad personalizada en su móvil. Ello evidencia un cambio significativo en los comportamientos protectores. En suma, estos universitarios taiwaneses tienen una débil apreciación de los riesgos potenciales y crisis a los que una vulnerable gestión de la privacidad online les podría exponer. Para abordarlo, una educación que cultive la comprensión de los peligros digita-les para los jóvenes es muy recomendable y requiere urgentemente tutoriales técnicos sobre privacidad.

Keywords / Palabras clave

Privacy strategy, privacy paradox, privacy education, privacy concern, privacy protection, smartphone, targeting advertising, ad avoidance.

Estrategia de privacidad, paradoja de la privacidad, educación de la privacidad, preocupaciones por la privacidad, protección de la privacidad, teléfonos inteligentes, publicidad personalizada, evasión de anuncios.

1. Introduction

Smartphones have become extraordinarily popular in Taiwan, with nearly 85% of Taiwanese people having at least one mobile phone and a 3G/4G user penetration rate of around 120% in 3Q 2017 (National Communications Commission, 2018). Such a high penetration rate has much to do with the rise of social media marketing, as over 90% of Taiwanese have a social media profile (Miniwatts Marketing Group, 2017). With such a powerful social media marketing platform, smartphones are an indispensable tool to reach consumers. Social media are closely connected to smartphones, with almost all personal data synchronised for targeting ads such as contacts, accounts and passcodes, emails, purchase history, user preferences, and privacy settings. Govani and Pashley (2005) find that, even if careful users take full advantage of a platform's privacy settings and upload as little online critical information as possible, their personal details are still traceable through clues leaked by their social media contacts. One main reason for forced privacy leakage is that social media are primarily designed to serve marketing purposes. The default privacy settings on social media and mobile devices are usually very loose, and therefore only the most vigilant users would notice the necessity of tightening their settings, whereas most imprudent users accidentally publicise their data and connect themselves to everyone they know. Social media and mobile device firms are lazy about completing their privacy settings because more thorough privacy settings are adverse to their commercial interests. Target marketing relies upon vigorous personal information sharing to maintain its incredible accuracy. Loose privacy settings concur with their commercial interests. Users exposed to self-relevant ads can efficiently recall their themes and specialty, and the effect endures for weeks. By contrast, conventional advertising is barely memorable.

The advertising effect arises through 'perceived self-relevance'. According to the self-referencing theory, human cognition tends to absorb external environmental cues resonant with personal traits (e.g. race, life experience, education, cultures, class, personality) that people identify with, and hence they actively associate ad contents relevant to their conditions back upon themselves, thus generating power of persuasion (Ahn & Bailenson, 2011). Past studies have substantiated that the self-referencing effect manifests in three facets: first, when personalised ads hit social media users, they hold more friendly attitudes towards not merely the products, but also the brands; second, they are more capable of remembering ad details including scenes, colours, themes, lines, and characters; third, their purchases increase in terms of chance, frequency, and even amount (Curran & al., 2011)

An appropriate amount of ad relevance can indeed aggrandise users' attention, purchase intentions, and memories, yet over a certain limit it just arouses agitation and aversion (Okazaki, Li, & Hirose, 2009). With news reporting that more and more Facebook users are going dormant and fleeing to other social platforms due to overwhelming advertising and surging privacy agitation, Jung (2017) proposes that ad relevance effectively weakens privacy protection like ad avoidance, while conversely it escalates privacy concern that further intensifies privacy protection. However, the

inverse association between ad relevance and ad avoidance is much stronger. High ad relevance would therefore be an ideal advertising strategy to undercut social media users' protective behaviours, albeit stimulating privacy concern.

1.1. Purposes

This research focuses on the following specific objectives: 1) Understanding college students' reasons for smartphone use; 2) Delineating their habitual smartphone use and reaction to social media's targeting advertising; 3) Analysing their privacy management in response to privacy concern over targeting advertising;
4) Identifying suitable pedagogies to improve their privacy awareness and management.

2. Literature review

2.1. Western and Eastern perceptions of privacy

Warren and Brandeis (1890) raise an early idea of privacy defined as the right to enjoy life and be left alone, and form the foundation for a variety of interpretations in the Western world since then. Petronio (2012) likens privacy to interpersonal boundaries by which individuals decide who can access their personal information and how to retain control. Privacy may be perceived disparately in Asia. Kitiyadisai (2005) points out the idea of privacy being extraneous. Asia's hierachicalism and collectivism are considered responsible for thwarting privacy (Cho & al., 2018). While privacy covers interpersonal boundaries in the Western world, in collectivist Asia, nation and family are valued above individuals who are taught and expected to serve both. Moreover, due to the hierarchies of seniority, education, profession, and wealth seen in Asia, it is especially difficult for those with little power to set up boundaries from those with power (Hong, 2018; Dincelli, 2018).

Ozdemir and others (2016) apply Hofstede's multidimensional model of culture for predicting privacy protection and concerns. They compare the scores Singapore, Sweden, and the U.S. got in the dimensions of power distance, individualism/collectivism, masculinity, and uncertainty avoidance (i.e. ambiguity aversion), finding that the U.S. and Singapore are at both ends of the spectrum in the dimensions of power distance, individualism/collectivism, and uncertainty avoidance - that is, the U.S. is the most individualist and uncertainty-avoidant and the least hierarchical, whereas Singapore is the opposite. By entering the scores into the regression analysis as independent variables, with privacy concerns and behaviour as dependent variables, the study indicates privacy protection is triggered by privacy concerns, and that privacy concerns are tempered by a high degree of the power distance index and the collectivism index, while stimulated by a higher degree of the uncertainty avoidance index. In short, different cultures have varying perceptions of privacy (Mathiyalakan & al., 2018; Mohammed & Tejay, 2017).

2.2. Mobile advertising and privacy

Advertising is 'any paid form of non-personal presentation and promotion of ideas, goods or services by an identified sponsor' (Kotler, 2003). With the growth of mobile devices like smartphones, laptops, and tablets, this channel has split off into mobile advertising.

Mobile advertising is now more personalised, owing to the wireless Internet and smart devices. Personalised advertising helps ads perform more in accordance with consumers' needs and at the same time minimise their repellence, by using personal data from their devices in low-key manners. Tucker (2014) examines the effectiveness of personalised mobile advertising, by showing college students 'fabricated' personalised and inclusive ads through Facebook. For instance, ads were designed to personally address readers like 'As an Adele fan like you, we…' or 'As a member of Cambridge University, we…'; celebrity and institution names were changed in order to compare their

effects. The results suggest that participants paid much more attention to personalised ads, on the condition that the celebrity and institution names indeed matched their interests or backgrounds; by contrast, ads not addressing readers with a specific celebrity or institution name received scarce attention. That study's findings also indicate that uniqueness is an influential factor. For example, certain celebrity and institutions were much more valued in one circle than in another. More vitally, the paper notes that as participants gravitated towards and noticed personalised ads, some started checking and intended to adjust their privacy settings.

2.3. The privacy paradox

The privacy paradox is defined as the incongruence between users' worry about privacy infringement and a lack of actual behaviours to protect privacy (Lutz & al., 2018; Ooi & al., 2018). Taddicken (2014) provides causes for the paradox; the incongruence might stem from deficient awareness of privacy risk severity, deficient skills of protection (e.g. adjusting privacy settings, clearing log files, distinguishing fake websites), and deficient knowledge of shared information (e.g. being unconscious of how to check if information is being used for stated purposes) (Beam & al., 2018; Boyd & Hargittai, 2010; Millham & Atkin, 2018).

Lewis, Kaufman, and Christakis (2008) contend that another factor contributing to the incongruence between users' concern about privacy infringement and a lack of behaviours to protect privacy is the peculiar Internet culture, labeling it the dyadic effect. Virtual interaction proceeds on a basis of reciprocal self-disclosure; that is, 'you tell me and I tell you' (McCain & Campbell, 2018; Richey & al., 2018). This reciprocity builds up self-relevance and is how online relationships deepen. Based on the dyadic effect, Taddicken (2014) empirically inspects users' social media smartphone application (app) numbers and finds that people with a privacy concern might be selective of what apps to install, but still become active social media users (van Schaik & al., 2018; Han & al., 2018).

Lee and Rha (2016) prove that the key points as to whether consumers with a privacy concern take protective actions or not are perceived value and self-efficacy. Most participants they surveyed did express anxiety over online privacy insecurity, yet after weighing the pros and cons and ascertaining if the benefits overpower the downsides, they still leaned towards taking risks without any protective measures. Moreover, consumers with little self-efficacy tend to put up with privacy infringement, not because they accept it, but rather their poor skills in detecting problems and learning new computer techniques leave them no choice, but to allow it (Muhammad & al., 2018; Proudfoot & al., 2018).

Young and Quan-Haase (2013) present surveys of 77 subjects and interviews of 21 Canadian college students to see their protective strategies on social media, revealing that most young people are not ignorant of privacy risks; instead, they enjoy the convenience that social media bring to them while carefully managing any possible danger. Strategies commonly favoured include restricting relatives from accessing personal news updates, frequently adjusting content visibility, removing posts when they no longer matter, establishing sub-sets of friend lists corresponding to separate privacy settings, using private one-to-one messaging (e.g. Facebook chat, other instant messaging apps) in lieu of interacting in public via personal pages, removing profile pictures or displaying an uneasily recognizable one, falsifying sensitive personal information, punctiliously scrutinizing friending requests from unfamiliar contacts, and self-untagging (Marwick & Boyd, 2014). These strategies come about due to 'social privacy concerns' so as to decrease the chance of non-essential 'social life dramas' (Dey & al., 2012); conversely, more acute and aggressive institutional privacy concerns (e.g. corporations making unfair privacy agreements, governments allowing cross-departmental access to personal data without authorization, grey areas of secondary usage of purchase history) are given very little thought, implying a jeopardy of unsupervised institutional privacy intrusion (Malgieri & Custers, 2018). Based on this literature above, our first hypothesis goes as follows.

H1: Ad relevance relates positively to (a) attention to ads and (b) privacy concern, yet inversely to (c) privacy protection.

2.4. Habitual smartphone usage

Chin and others (2012) report albeit smartphones have been fairly popularised, direct online shopping via them makes up merely 3% of total shopping revenues, because users feel uncomfortable toward leaving credit card and bank account password info on their phones. Matthews and others (2009) note that users oftentimes start tasks on their smartphones, but intentionally switch to computers to finish them, and that users might install a number of apps but only focus on using a small set of them owing to different amounts of trust they hold over the apps. By and large, consumers perceive smartphones as delicate, portable, convenient, and relatively inexpensive, but also consider them physically fragile and relatively unreliable due to lower data storage security and capability of presenting complicated information (*Wiese & al.,* 2011). Out of all these concerns, consumers are apt to constrain their smartphone usage and turn to other devices for completing certain tasks. We thus present our research questions regarding whether Taiwanese people's habitual smartphone usage reflects their privacy concerns and protective behaviours.

- RQ1: To what degree does privacy concern relate to habitual smartphone usage?
- RQ2: To what degree does privacy protection relate to habitual smartphone usage?

3. Methods

3.1. Procedure

We targeted undergraduates and postgraduates in Taipei City (Taiwan's capital) as our subjects from 6 randomly selected universities: National Taipei University of Technology, National Taipei University of Education, Shih Hsin University, National Taiwan Normal University, Chinese Culture University, and Ming Chuan University. Three classes with 50 or more students registered were randomly picked from each school, of which the majority were general education classes constituted by students of different years. With consent given by the lecturers and students in advance, we handed out the survey from November 17 to December 27, 2017.

3.2. Measurements

Our survey pertains to smartphone usage, motivations for smartphone usage, ad relevance, attention to ads, privacy concerns, and protective behaviours. Seven smartphone habitual usage items have a 5-point Likert scale from 'never' to 'always', where participants were queried about their frequency of using smartphones and social media apps; 3 other items allowed participants to provide the numbers of calls and messages on average that they sent and received every day.
The study had 21 items for participants to express their reasons for smartphone usage, including 'let friends/family know you are concerned about them', 'staying in touch with distant friends/relatives', 'enjoying conversations with people', etc., with a 5-point Likert scale from 'strongly disagree' to 'strongly agree'.
Three ad relevance items come from Jung's social media advertising study (2017), asking participants to evaluate how they felt social media ads met, personalised, and valued their needs, with a 5-point Likert scale from 'strongly disagree' to 'strongly agree'. We revised 3 items from Jung's construct of attention to ads (2017) inclusive of the amounts of interest, attention, and thought usually given to social media ads by users, on a 5-point Likert scale from 'not at all' to 'very much'.
We borrowed 10 items of privacy concerns from Jordaan and Van Heerden's research of Facebook usage and privacy issues (2017). On a 5-point Likert scale from 'strongly disagree' to 'strongly agree', the items enabled participants to assess how they felt in control over their personal data being shared, used, and collected; how much they were annoyed when websites required their personal info, if they tried to be meticulous before submitting personal info, etc.

We finally synthesised items (Jordaan & Van Heerden, 2017; Jung, 2017), developing a construct of protective behaviours comprising 8 items, with a 5-point Likert scale from 'strongly disagree' to 'strongly agree'. The items looked into participants' intention to avert social media ads, unsubscribe from marketing emails, remove cookies and browsing history, restrict undesired people (from contacting them), perform anti-spyware inspections, and act with caution over messages they have received.

We expect each hypothesis, apart from H1c, in the model (Figure 1: https://figshare.com/s/d297025d9803481c8435) to be positive. H1c might be uncertain, since Jung (2017) notes that high ad relevance either wins consumers' appreciation or inflames their repellence; the former scenario weakens their privacy defence, while the latter intensifies it. Table 1 illustrates the major items employed in this study (https://figshare.com/s/94a23ad476ce207be7d9).

4. Results

After coding 829 respondents' feedbacks, we removed 19 unqualified ones, for a total of 810 valid surveys. Unidentifiable answers such as too blurry or not given in the requested formats are coded as missing values.

Of the respondents, 265 are males (32.7%), 529 are females (65.3%); average age is 22 (youngest at 19; oldest at 32); 77 are postgraduates (9.5%); 726 (89.7%) are undergraduates (70 freshmen (8.6%), 310 sophomores (38.3%), 241 juniors (29.8%), 105 seniors (13.0%)); on average they made 1.87 calls (sd=5.17), received 2.77 calls (sd=20.5), sent 14.68 SMS texts (sd=120.2), and received 14.80 SMS texts (sd=72.28) per day; and the average number of years using a cell phone is eight (sd=2.86).

We conducted EFA and reliability tests to extract factors and to verify their validity. In Table 2 (https://figshare.com/s/43406dc8b297e91f5ec6), participants have 5 main reasons for smartphone usage: (1) interacting with family and friends; (2) obtaining new information; (3) relaxing and killing time; (4) discussing and planning activities; (5) staying in touch with distant contacts. We eliminate items 12, 20, and 23 due to insufficient loading values or cross-loading. Other attested factors are (6) smart feature usage (e.g. social media browsing, online messaging); (7) basic feature usage (e.g. SMS texting, telecom network-based calling); (8) ad relevance; (9) attention to ads; (10) self-filtering (of suspicious spyware, social media contacts, and websites); (11) ad avoidance (e.g. ticking off social media ads, unsubscribing from email advertising); (12) concern over ebbing personal control (of private data); (13) concern over growing corporate power. We then slightly revise the initial research model according to EFA and reliability test outcomes, as in Figure 1.

- H1: Ad relevance relates positively to (a) attention to ads and (b) privacy concern, yet inversely to (c) privacy protection.

The regression results denote ad relevance relates directly to attention to ads (β=.51***, adjusted R^2=.26) and negatively to self-filtering (β=-.07*, adjusted R^2=.004), ad avoidance (β=-.24***, adjusted R^2=.06), falling personal control (β=-.17***, adjusted R^2=.03), and growing corporate power (β=-.13***, adjusted R^2=.02). Thus, H1a and H1c are supported, while H1b is refuted.

- RQ1: To what degree does privacy concern relate to habitual smartphone usage? Privacy concern over ebbing personal control positively relates to both basic feature usage (β=.73*, adjusted R^2=.004) and smart feature usage (β=.15***, adjusted R^2=.02) of mobile phones. Concern over growing corporate power positively relates to smart feature usage (β=.11***, adjusted R^2=.01) alone, while its association with basic feature usage is insignificant.

- RQ2: To what degree does privacy protection relate to habitual smartphone usage? Self-filtering relates neither to basic feature usage (p=.75) nor to smart-feature usage (p=.17). Similarly, ad avoidance has no bearing on either basic- (p=.58) or smart-feature usage (p=.66). Thus, there is no significant relationship between privacy protection and habitual smartphone usage.

Dummy codes being set up for gender (with women as the reference group) and grades (with postgraduates as the reference group), the demographic variables are input into the regression

analysis on SPSS 21. Table 3 (https://figshare.com/s/c4505b6e5b948dd90f5d) shows that men have a greater tendency for privacy protection, self-filtering, and a disinclination towards basic smartphone features. Among all subjects, freshmen undergraduates alone are significantly less concerned about falling personal control and growing corporate power over their privacy. On the other hand, years 1-3 undergraduates tend to use smartphones' basic features, with no significance attached to seniors and postgraduates.

5. Discussion and conclusion

Our outcomes corroborate as well as contradict past studies arguing that ad relevance brings more consumer attention to ads, decreases ad evasion, and strengthens privacy concerns (Jung, 2017; Tucker, 2014). We find similar trends whereby higher ad relevance implies more attention to ads and weaker ad evasion. Nevertheless, our research also demonstrates that higher ad relevance coincides significantly with lower privacy anxiety (over both ebbing personal control and rising corporate power) and fewer self-filtering behaviours (e.g. checking spyware, blocking undesired contacts). Although past studies unanimously note that escalating ad relevance disturbs audiences and awakens their misgivings, this hardly explains our paper's heterodox phenomenon.

Cho, Rivera-Sánchez, and Lim (2009) argue that privacy concern is a cultural emotion. Subjects from individualist societies like Australia and the U.S., especially females, exhibit greater anxiety and higher defence upon feeling targeted online, while Koreans acted otherwise. Because Taiwan has similar socio-cultural backgrounds (e.g. collectivism, hierarchicalism, patriarchalism, ageism against the young) to South Korea's, it is likely that Taiwanese users lack an understanding of privacy as clear and firm as that of Western users in which privacy should be guarded and inviolable.

Age may also be a stimulus to weaken privacy concerns. In Table 3 (https://figshare.com/s/c4505b6e5b948dd90f5d), freshmen clearly cared less about privacy issues; yet, there is no sign of older students being more concerned about privacy issues, implying the amount of care Taiwanese college students give to privacy issues does not grow in proportion to age.

We also detect no privacy paradox, which usually appears when conspicuous anxiety over privacy accompanies the absence of protective behaviours, as users calculate benefits and risks, realise the former might overpower the latter, and consequently decide to take risks by curbing defensive reaction. Our findings do indicate low privacy concern and protection, neither of which lead to lower habitual smartphone usage (both smart- and basic-feature). The paucity of both privacy concern and protection discloses Taiwanese college students' incomprehension of the gravity and lurking danger from sensitive personal data being abused by institutions infringing upon their rights. In line with comparative studies, we further confirm that Taiwanese college students do not recognise privacy as inviolable and unequivocal boundaries like Western people do, and that their ignorance stems from scant comprehension of and little caution against institutional power that could be exercised with malignant intentions.

Several studies recommend enhancing privacy awareness via cooperation with social media by rolling out tips or nudges (Wisniewski & al., 2017; Martin & al., 2018; Wisniewski, Knijnenburg, & Lipford, 2016; Chugh & Ruhi, 2018; Haffner & al., 2018), but without accurately identifying causes of poor privacy management, generic tips and education could barely help. Wisniewski and others (2017) categorise Facebook users based on whether they exhibit privacy concerns, concluding that tutorial tips such as how to adjust the visibility of posts, customise friend lists, and restrict chats on Facebook would be useful only when users have privacy concerns, but employ limited corresponding protective measures, because they are likely unaware of how to set them up (Alalwan, 2018; Rauschnabel, He, & Ro, 2018; Ketelaar & van Balen, 2018). Conversely, those who exhibit neither privacy concern nor protection urgently need warning tips on the risks and possible negative consequences of their current settings (Tsay-Vogel & al., 2018; Wang & al., 2014; Gerber & al., 2018). Judging by our findings, we suggest the Taiwanese government push for privacy education

by cultivating an awareness of the risks that reckless online privacy management exposes users to versus just offering privacy setting tutorials.

This paper yields theoretical implications. Because the privacy concerns employed herein are based simultaneously on two major forces that smartphone users must be wary of in the near future - attenuating personal control and expanding corporate power – many studies focus on a relatively narrow spectrum of privacy concerns, thus curtailing the big picture of how individual users weigh the pros and cons and strategise their privacy behaviours. Our paper does not discuss habitual smartphone usage as uniform behaviour, but instead dissects it into basic- and smart-feature usages. Our findings offer no signs of decreasing smartphone usage out of privacy concerns in either of the two dimensions, thus unveiling our other implication: while it is posited in international research on the privacy paradox that privacy concern is a natural emotion inevitably triggered by social media interaction and smart device utilization, our results question this assumption, owing to no clues of ascending privacy concern witnessed by the subjects, not to mention low protective behaviours. Therefore, we recommend future privacy paradox research to approach related issues through cultural and regional aspects and comparative analyses in order to characterise how privacy is perceived in individual societies and practiced in relation to power and boundaries.

Our study does have limitations, with the most crucial one likely being the methodology. Kokolakis (2017) notes that privacy research faces inconclusive debates over methodological effectiveness. In recalling how they normally react to privacy issues, our subjects probably forgot they had set up a certain level of cautionary settings in everyday life. The gap between subjective perceptions and unnoticed subconscious watchful behaviours could generate misleading biases. To tackle this technical difficulty and precisely delineate subjects' actual behaviours and trajectories of attitudinal variation, Dienlin and Trepte (2015) advise to measure the privacy paradox by surveys and observation-oriented experiments at the same time so that the gulf between cognition and subconsciousness can be appropriately captured and analysed.

References

Adhikari, K., & Panda, R.K. (2018). Users' information privacy concerns and privacy protection behaviors in social networks. Journal of Global Marketing, 31(2), 96-110. https://doi.org/10.1080/08911762.2017.1412552

Ahn, S.J., & Bailenson, J.N. (2011). Self-endorsing versus other-endorsing in virtual environments. Journal of Advertising, 40(2), 93-106. https://doi.org/10.2753/joa0091-3367400207

Alalwan, A.A. (2018). Investigating the impact of social media advertising features on customer purchase intention. International Journal of Information Management, 42, 65-77. https://doi.org/10.1016/j.ijinfomgt.2018.06.001

Balasubraman, S., Peterson, R.A., & Jarvenpaa, S.L. (2002). Exploring the implications of m-commerce for markets and marketing. Journal of the Academy of Marketing Science, 30(4), 348-361. https://doi.org/10.1177/009207002236910

Bart, Y., Shankar, V., Sultan, F., & Urban, G.L. (2005). Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. Journal of Marketing, 69(4), 133-152. https://doi.org/10.1509/jmkg.2005.69.4.133

Beam, M.A., Child, J.T., Hutchens, M.J., & Hmielowski, J.D. (2018). Context collapse and privacy management: Diversity in Facebook friends increases online news reading and sharing. New Media & Society, 20(7), 2296-2314. https://doi.org/10.1177/1461444817714790

Chin, E., Felt, A.P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. In Proceedings of the Eighth Symposium on Usable Privacy and Security (pp. 1-6). Washington, D.C: SOUPS. https://doi.org/10.1145/2335356.2335358

Choi, T.R., & Sung, Y. (2018). Instagram versus Snapchat: Self-expression and privacy concern on social media. Telematics and Informatics, 35(8), 2289-2298. https://doi.org/10.1016/j.tele.2018.09.009

Chugh, R., & Ruhi, U. (2018). Social media in higher education: A literature review of Facebook. Education and Information Technologies, 23(2), 605-616. https://doi.org/10.1007/s10639-017-9621-2

Consolvo, S., Smith, I.E., Matthews, T., LaMarca, A., Tabert, J., & Powledge, P. (2005). Location disclosure to social relations: Why, when, & what people want to share. In Proceedings of the SIGCHI conference on human factors in computing systems (pp. 81-90). ACM. https://doi.org/10.1145/1054972.1054985

Curran, K., Graham, S., & Temple, C. (2011). Advertising on Facebook. International Journal of E-Business Development, 1(1), 26-33. http://bit.ly/2FQGJNA

Cho, H., Knijnenburg, B., Kobsa, A., & Li, Y. (2018). Collective privacy management in social media: A cross-cultural validation. ACM Transactions on Computer-Human Interaction (TOCHI), 25(3), 17. https://doi.org/10.1145/3193120

Dey, R., Jelveh, Z., & Ross, K. (2012). Facebook users have become much more private: A large-scale study. In 2012 IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshops 2012 (pp. 346-352). https://doi.org/10.1109/percomw.2012.6197508

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology, 45(3), 285-297. https://doi.org/10.1002/ejsp.2049

Gerber, N., Gerber, P., Drews, H., Kirchner, E., Schlegel, N., Schmidt, T., & Scholz, L. (2018). FoxIT: enhancing mobile users' privacy behavior by increasing knowledge and awareness. In Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust (pp. 53-63). ACM. https://doi.org/10.1145/3167996.3167999

Greene, D., & Shilton, K. (2018). Platform privacies: Governance, collaboration, and the different meanings of 'privacy' in iOS and Android development. New Media & Society, 20(4), 1640-1657. https://doi.org/10.1177/1461444817702397

Haffner, M., Mathews, A.J., Fekete, E., & Finchum, G.A. (2018). Location-based social media behavior and perception: Views of university students. Geographical Review, 108(2), 203-224. https://doi.org/10.1111/gere.12250

Han, K., Jung, H., Jang, J.Y., & Lee, D. (2018). Understanding users' privacy attitudes through subjective and objective assessments: An instagram case study. Computer, 51(6), 18-28. https://doi.org/10.1109/mc.2018.2701648

Hargittai, E. (2010). Facebook privacy settings: Who cares? First Monday, 15(8). https://doi.org/10.5210/fm.v15i8.3086

Jordaan, Y., & Van Heerden, G. (2017). Online privacy-related predictors of Facebook usage intensity. Computers in Human Behavior, 70, 90-96. https://doi.org/10.1016/j.chb.2016.12.048

Jung, A.R. (2017). The influence of perceived ad relevance on social media advertising: An empirical examination of a mediating role of privacy concern. Computers in Human Behavior, 70, 303-309. https://doi.org/10.1016/j.chb.2017.01.008

Ketelaar, P.E., & Van-Balen, M. (2018). The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. Computers in Human Behavior, 78, 174-182. https://doi.org/10.1016/j.chb.2017.09.034

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, 122-134. https://doi.org/10.1016/j.cose.2015.07.002

Kotler, P. (2003). Marketing Management. Upper Saddle River, New Jersey: Pearson Education.

Lee, J.M., & Rha, J.Y. (2016). Personalization–privacy paradox and consumer conflict with the use of location-based mobile commerce. Computers in Human Behavior, 63, 453-462. https://doi.org/10.1016/j.chb.2016.05.056

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. Journal of Computer-Mediated Communication, 14(1), 79-100. https://doi.org/10.1111/j.1083-6101.2008.01432.x

Lutz, C., Hoffmann, C. P., Bucher, E., & Fieseler, C. (2018). The role of privacy concerns in the sharing economy. Information, Communication & Society, 21(10), 1472-1492. https://doi.org/10.1080/1369118x.2017.1339726

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: A power–responsibility equilibrium perspective. Journal of the Academy of Marketing Science, 35(4), 572-585. https://doi.org/10.1007/s11747-006-0003-3

Malgieri, G., & Custers, B. (2018). Pricing privacy – the right to know the value of your personal data. Computer Law & Security Review, 34(2), 289-303. https://doi.org/10.1016/j.clsr.2017.08.006

Martin, F., Wang, C., Petty, T., Wang, W., & Wilkins, P. (2018). Middle school students' social media use. Journal of Educational Technology & Society, 21(1), 213-224. http://bit.ly/2I6TLbx

Marwick, A.E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. New Media & Society, 16(7), 1051-1067. https://doi.org/10.1177/1461444814543995

Mathiyalakan, S., Heilman, G., Ho, K.K., & Law, W. (2018). An examination of the impact of gender and culture on Facebook privacy and trust in Guam. Journal of International Technology and Information management, 27(1), 26-59. http://bit.ly/2JBhVNz

Matthews, T., Pierce, J., & Tang, J. (2009). No smart phone is an island: The impact of places, situations, and other devices on smart phone use. IBM RJ10452, 1-10. https://ibm.co/2COtkUg

McCain, J.L., & Campbell, W.K. (2018). Narcissism and social media use: A meta-analytic review. Psychology of Popular Media Culture, 7(3), 308. https://doi.org/10.1037/ppm0000137

Millham, M.H., & Atkin, D. (2018). Managing the virtual boundaries: Online social networks, disclosure, and privacy behaviors. New Media & Society, 20(1), 50-67. https://doi.org/10.1177/1461444816654465

Milne, G.R., & Culnan, M.J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. Journal of Interactive Marketing, 18(3), 15-29. https://doi.org/10.1002/dir.20009

Miniwatts Marketing Group (Ed.) (2017). Internet usage in Asia: Internet users, Facebook subscribers & population statistics for 35 countries and regions in Asia. https://bit.ly/29kEOQq

Mohammed, Z., & Tejay, G.P. (2017). Examining privacy concerns and ecommerce adoption in developing countries: The impact of culture in shaping individuals' perceptions toward technology. Computers & Security, 67. https://doi.org/10.1016/j.cose.2017.03.001

Muhammad, S.S., Dey, B.L., & Weerakkody, V. (2018). Analysis of factors that influence customers' willingness to leave big data digital footprints on social media: A systematic review of literature. Information Systems Frontiers, 20(3), 559-576. https://doi.org/10.1007/s10796-017-9802-y

National Communications Commission (Ed.) (2018). 2G/3G/4G statistics of mobile communication market in Q3 2017. https://bit.ly/2TRChqI

Okazaki, S., Li, H., & Hirose, M. (2009). Consumer privacy concerns and preference for degree of regulatory control. Journal of Advertising, 38(4), 63-77. https://doi.org/10.2753/joa0091-3367380405

Ooi, K.B., Hew, J.J., & Lin, B. (2018). Unfolding the privacy paradox among mobile social commerce users: a multi-mediation approach. Behaviour & Information Technology, 37(6), 575-595. https://doi.org/10.1080/0144929x.2018.1465997

Ozdemir, Z.D., Benamati, J.H., & Smith, H.J. (2016). A cross-cultural comparison of information privacy concerns in Singapore, Sweden and the united states. In Proceedings of the 18th Annual International Conference on Electronic Commerce: e-Commerce in smart connected world (p. 4). ACM. https://doi.org/10.1145/2971603.2971607

Petronio, S. (2012). Boundaries of privacy: Dialectics of disclosure. Albany, NY: State University of New York Press. https://doi.org/10.5860/choice.40-4304

Phelps, J., D'Souza, G., & Nowak, G. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. Journal of Interactive Marketing, 15(4), 2-17. https://doi.org/10.1002/dir.1019

Proudfoot, J.G., Wilson, D., Valacich, J.S., & Byrd, M.D. (2018). Saving face on Facebook: Privacy concerns, social benefits, and impression management. Behaviour & Information Technology, 37(1), 16-37. https://doi.org/10.1080/0144929x.2017.1389988

Rauschnabel, P.A., He, J., & Ro, Y. K. (2018). Antecedents to the adoption of augmented reality smart glasses: A closer look at privacy risks. Journal of Business Research, 92, 374-384. https://doi.org/10.1016/j.jbusres.2018.08.008

Richey, M., Gonibeed, A., & Ravishankar, M.N. (2018). The perils and promises of self-disclosure on social media. Information Systems Frontiers, 1-13. https://doi.org/10.1007/s10796-017-9806-7

Schoenbachler, D.D., & Gordon, G.L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. Journal of Interactive Marketing, 16(3), 2-16. https://doi.org/10.1002/dir.10033

Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. Journal of Computer-Mediated Communication, 19(2), 248-273. https://doi.org/10.1111/jcc4.12052

Taraszow, T., Aristodemou, E., Shitta, G., Laouris, Y., & Arsoy, A. (2010). Disclosure of personal and contact information by young people in social networking sites: An analysis using Facebook pro files as an example. International Journal of Media & Cultural Politics, 6(1), 81-101. https://doi.org/10.1386/macp.6.1.81/1

Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. New Media & Society, 20(1), 141-161. https://doi.org/10.1177/1461444816660731

Tucker, C.E. (2014). Social networks, personalized advertising, and privacy controls. Journal of Marketing Research, 51(5), 546-562. https://doi.org/10.2139/ssrn.1694319

Van-Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. Computers in Human Behavior, 78, 283-297. https://doi.org/10.1016/j.chb.2017.10.007

Wang, N., Wisniewski, P., Xu, H., & Grossklags, J. (2014). Designing the default privacy settings for Facebook applications. In Proceedings of the companion publication of the 17th ACM conference on Computer supported cooperative work & social computing (pp. 249-252). ACM. https://doi.org/10.1145/2556420.2556495

Wiese, J., Kelley, P.G., Cranor, L.F., Dabbish, L., Hong, J.I., & Zimmerman, J. (2011). Are you close with me? Are you nearby? Investigating social groups, closeness, and willingness to share. UbiComp, 11, 197-206. https://doi.org/10.1145/2030112.2030140

Wisniewski, P.J., Knijnenburg, B.P., & Lipford, H.R. (2017). Making privacy personal: Profiling social network users to inform privacy education and nudging. International Journal of Human-Computer Studies, 98, 95-108. https://doi.org/10.1016/j.ijhcs.2016.09.006

Wisniewski, P.J., Najmul-Islam, A.K., Lipford, H.R., & Wilso, D.C. (2016). Framing and measuring multi-dimensional interpersonal privacy preferences of social networking site users. Communications of the Association for Information Systems, 38(1). https://doi.org/10.17705/1cais.03810

Young, A.L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. Information, Communication & Society, 16(4), 479-500. https://doi.org/10.1080/1369118x.2013.777757