Valuation and Analysis of Relational Privacy in Social Networks Postprint

Authors: Guoquan Zang, Zhou Xiaoqian

Date: 2023-04-01T00:00:00+00:00

Abstract

[Purpose/Significance] With the proliferation of social networks, users extensively download and utilize third-party applications (i.e., social APPs) through social platforms, thereby generating privacy concerns. The scope of these concerns extends beyond personal privacy to encompass users' friends' privacy, referred to as interdependent privacy. By quantifying the value of interdependent privacy, this study substantiates its pervasive existence and provides an empirical foundation for the formulation of interdependent privacy policies in social APPs. [Method/Process] Through empirical investigation and literature review, the widespread existence of interdependent privacy is established, and corresponding research questions and hypotheses are proposed. Employing conjoint analysis, individual preferences are examined via questionnaire surveys to infer the factors influencing users' APP selection decisions and to quantitatively estimate the value of interdependent privacy. [Results/Conclusion] The findings indicate that users do consider friends' privacy when selecting APPs, yet assign relatively low valuation to it. When examining the influence of contextual factors regarding social APPs' collection of user information on interdependent privacy value, two scenarios are introduced: whether the collection of users' friends' information by APPs enhances functional implementation and usage effectiveness. The results demonstrate that significant differences in interdependent privacy valuation emerge only when these two scenarios pertain to friends' complete information. This suggests that protecting friends' basic information is of limited importance to users, whereas unreasonable requests for sensitive information (defined as the portion of complete information remaining after excluding basic information) exert a negative effect on APP evaluations.

Full Text

Value Measurement and Analysis of Linking Privacy in Social Networks

Zang Guoquan[1],[2], **Zhou Xiaoqian**[1] [1]School of Information Management, Zhengzhou University, Zhengzhou 450001 [2]Institute of Data Science, Zhengzhou University, Zhengzhou 450001

Abstract: [Purpose/Significance] With the widespread popularity of social networks, users download and use numerous third-party applications (social APPs) through social platforms, raising privacy concerns that extend beyond personal privacy (direct privacy) to include users' friends' privacy, termed linking privacy. By measuring the value of linking privacy, this study confirms its extensive existence and provides a basis for formulating linking privacy policies in social APPs. [Method/Process] Through empirical investigation and literature review, this paper confirms the pervasive nature of linking privacy and proposes corresponding research questions and hypotheses. Using conjoint analysis, the study examines individual preferences via questionnaires, deduces factors influencing users' APP selection, and quantitatively estimates the value of linking privacy. [Result/Conclusion] The findings reveal that users consider friends'privacy when choosing APPs, but value it relatively low. When examining how the context of social APPs collecting user information affects linking privacy value, the study introduces two scenarios: whether the APP' s collection of users' friends' information enhances APP functionality and usage effectiveness. Results show that only when these two scenarios affect friends' complete information do significant differences in linking privacy emerge, indicating that protecting friends' basic information is not particularly important to users, but unreasonable requests for sensitive information (the portion of complete information excluding basic information) negatively impact APP evaluation.

Keywords: social network; linking privacy; privacy value; privacy measurement **Classification Number:** G251 **DOI:** 10.13266/j.issn.0252-3116.2020.14.009

1 Problem Statement

The popularity of social networks has led to continuous functional expansion, including the integration of third-party programs (social APPs) that users download and use through social platforms to meet various needs. Such APPs have achieved tremendous market success, with global downloads exceeding 204 billion in 2019, of which China' s market accounted for nearly 50%, making it the largest application market [1]. However, alongside their popularity, social APPs generate user privacy concerns relating to both users' own privacy (direct privacy) and users' friends' privacy (linking privacy).

Linking privacy is prevalent in social APPs. On one hand, social APPs can request extensive information about users' friends, including birthdays, photos,

identification documents, addresses, work experience, educational background, and location data. In China, such information collection is typically bundled in APP privacy policies, while abroad it is often presented as a list for user selection. On the other hand, social APPs are frequently installed, and even though some APPs only request specific types of information, the collection of users' friends' information across social APPs as a category is substantial. These APPs often set prerequisites for collecting users' personal information, requiring authorization before use, yet users cannot judge whether collection is excessive, raising concerns about passive inducement to over-authorize and suspicion of information misuse. Simultaneously, these APPs also set thresholds for collecting users'friends'information, requiring user permission but not friends' consent, with friends often unaware of such collection.

Domestically, APPs explicitly collect multiple types of user information, some involving friends' information, such as user contact lists that may contain friends' names, phone numbers, addresses, and email addresses; call records that include both users' and friends' conversation content; and dialed/received calls that record friends' phone numbers. Thus, these APPs implicitly collect users' friends' information, bundled within privacy policies. According to a May 2019 survey by the Cyberspace Administration of China [2] of 100 popular Android APPs, the statistics on major information types collected from users' friends are shown in .

Internationally, during summer 2019, the authors surveyed 1,500 most-downloaded Facebook APPs from 2018, counting each APP' s required permissions to access friends' information. The results, summarized by information type and calculated based on 2018 download frequencies, are shown in .

Based on , although official 2019 Android APP download statistics are unavailable in China, the phenomenon of Android APPs collecting users' friends' information is widespread. shows that internationally, while the proportion of APPs collecting any given information type is not high, these APPs have extremely high download frequencies, making the total volume of collected information substantial. Therefore, linking privacy is a serious issue in social networks both domestically and internationally.

2 Literature Review

2.1 Privacy Value Measurement

Privacy value measurement often employs privacy cost-benefit tradeoff theory, which views privacy as an economic good. When facing information disclosure, users consciously conduct cost-benefit analysis, weighing perceived costs against perceived benefits to make optimal choices while also considering factors such as trust in information recipients. Privacy measurement methods commonly use experimental economics approaches, including direct surveys, BDM experiments, scenario simulation, field experiments, discrete choice experiments, con-

joint analysis, and contingent valuation. For example, S. Schudy et al. [3] used the BDM mechanism to estimate the value of different personal information items by measuring the minimum amount required to share personal information. R. K. Chellappa et al. [4] used scenario simulation to investigate users' value perceptions of personal information in online environments and explore the tradeoff mechanism between personalized services and privacy leakage. S. Spiekermann et al. [5] assessed personal information privacy value by measuring users' willingness to pay to retain their Facebook information. H. Krasnova et al. [6] used discrete choice experiments to study users' concerns about personal information leakage when using Facebook Connect. I. H. Hann et al. [7] employed conjoint analysis to explore the cost-benefit tradeoff of online personal information disclosure and measure its monetary value. V. Bennndorf et al. [8] used contingent valuation to assess the monetary value of personal information contributed to social networks.

Privacy measurement results depend on survey context, as different contexts allow for different experimental methods, and introducing various context-based experiments is a common approach to addressing challenges in measuring personal information value. Generally, consumers are willing to purchase privacy-friendly products, but some contexts exhibit a privacy paradox. For instance, in online shopping, users willingly disclose sensitive information for better personalized services [9]. On average, users' willingness to sell personal information exceeds their willingness to protect it, though some contexts yield different conclusions. Hospital patients highly value protecting sensitive medical data (e.g., infectious disease data), with almost no willingness to sell (e.g., HIV data). Geographic and monetary incentive contexts also affect privacy measurement, such as differences in monetary valuation of location data across EU countries [10], and moderate monetary incentives leading many users to contribute personal information [10]. Privacy policy statements and platform reputation are also important contextual variables, as J. Kim et al. [11] found that privacy statements positively influence willingness to disclose personal information, while E. B. Andrade et al. [12] found that platform reputation negatively correlates with privacy concerns.

2.2 Linking Privacy

In linking privacy emergence research, some studies have summarized its occurrence based on APP download counts in social networks. For example, in 2013, B. Gergely et al. [13] surveyed 27,000 popular Facebook APPs for friends' information collection, while N. Wang et al. [14] examined 9,400 most-used APPs on the platform. The China Consumers Association [15] tested 100 APPs each from the App Store and Android markets, finding that 28% requested access to users' contact lists (friends), with some even requesting call records between users and friends. Analyzing user data also reveals linking privacy issues, as P. Shi et al. [16] analyzed Facebook blog comments to examine linking privacy concerns arising from friends' information leakage due to user behavior, and

H. Krasnova et al. [6] surveyed 199 Facebook users about 38 types of friends' information, finding both "privacy egoism" and concern for friends' information leakage.

Linking privacy theory research remains scarce domestically and limited internationally. M. E. Johnson [17] analyzed privacy concerns from enterprises' information leakage regarding negative impacts on employees, customers, agents, and suppliers. T. L. James et al. [18] treated users and friends aware of their sensitive medical data as original and co-owners, where leakage affects both parties and causes privacy concerns from co-owners, developing a measurement scale. J. Wirth et al. [19] studied concerns from friends aware of individuals' leaked privacy and analyzed factors influencing their motivation to protect the individuals' privacy.

The theoretical foundation for linking privacy is "other-regarding preferences," where decision-making considers both self-interest and others' welfare. In social APP contexts, this means users consider friends' interests and privacy when deciding to download APPs involving friends' information collection. Linking privacy measurement follows context dependency theory, where data request context relevance affects information disclosure behavior and privacy perception. For example, users installing a birthday APP to remind them of friends' birthdays would have different privacy concerns than when APPs collect context-irrelevant information.

3 Research Hypotheses and Experimental Settings

Based on context dependency theory, this study sets up two scenarios, randomly assigning subjects to one without crossover:

S1: The APP' s collection of users' friends' information does not enhance APP functionality or usage effectiveness.

S2: The APP' s collection of users' friends' information enhances APP functionality or usage effectiveness.

Extensive research [20-21] shows that in many decision contexts, individuals deviate from pure self-interest, exhibiting other-regarding preferences that selflessly care about others'welfare and reciprocate goodwill, especially when choices directly determine others' interests. Applied to this study, social APP users are predicted to show other-regarding preferences, caring about friends' privacy. Research also shows [22] that online interpersonal interaction helps individuals develop and maintain online social capital, which refers to non-material resources accumulated through interpersonal relationships that benefit individuals and increase opportunities for diverse thought and positive information. As online community components, social APP users accumulate social capital and must evaluate behaviors that may harm community members, including friends' information leakage. Therefore:

H1: Social APP users positively evaluate friends' information value, exhibiting other-regarding preferences in linking privacy leakage decision contexts.

While users show privacy concerns when disclosing personal information (self-regarding preferences) [22], APP users also value friends' information (other-regarding preferences), though the degree varies by person and context [23]. Whether users' concern for their own privacy exceeds concern for friends' privacy is context-dependent and an empirical question. However, interpersonal connections vary in strength, with strong ties existing between people with mutual trust and overlapping social circles, while online social capital building creates relatively weak coupling [24]. Generally, stronger ties correlate with higher concern. Therefore:

H2: When choosing APPs, social users exhibit higher privacy concern for their own information than for friends' information.

Context dependency means the reasonableness of information collection depends on specific contexts, and when information collection is context-irrelevant, privacy concerns increase [25]. This study defines two contexts: whether APP collection of friends' information enhances functionality and usage effectiveness. Therefore:

H3: Users exhibit higher linking privacy concerns when social APPs collect context-independent friends' information compared to context-dependent information.

4 Research Design

4.1 Conjoint Analysis Design

This study employs conjoint analysis, first proposed by P. E. Green et al. [26] in 1990 for measuring user preferences in cost-benefit tradeoffs and later used to estimate personal privacy concerns' monetary value. This method quantitatively estimates linking privacy value by analyzing users' APP evaluation behavior to deduce influencing factors. Social APPs are viewed as combinations of multiple attributes, where collecting friends' information is one attribute with levels representing different collection types.

4.1.1 Attribute Determination Focus group interviews determined social APP attributes for conjoint analysis through the question: "What factors influence your choice to download and use an APP?" Twenty participants from Zhengzhou University (5 each of faculty, PhD students, master' s students, and undergraduates) were interviewed, half with privacy leakage experience and half without, as this may affect privacy concerns. Major factors are summarized in , showing that the main factors for choosing APPs are four dimensions: price, popularity, user personal privacy concern, and user friends' privacy concern.

4.1.2 Level Determination Semi-structured interviews based on selected attributes obtained users' level perceptions.

(1) APP Price Levels: Statistics from the top 1,000 paid APPs in Apple' s App Store were averaged, combined with respondents'willingness to pay, yielding price levels of "0 yuan" and "15 yuan."

(2) Popularity Levels: Based on respondents' perception of friends' usage percentage, where 70% considered an APP used by one-third of friends as popular, while less than 10% usage was unpopular. Thus, popularity levels are 10% and 30%.

(3) User Personal Information Levels: Based on the national communications industry standard "Telecom and Internet User Personal Information Protection Definitions and Classification" (YD/S2781-2014), the authors' Facebook survey, and mobile APP permission management, three levels were designed: none, basic information (name, ID number, age, gender, workplace, education, address), and complete information (basic plus location, schedule, photos, audio, video, bank accounts).

(4) User Friends' Privacy Levels: Same as personal privacy levels. APP attributes and levels are summarized in .

4.1.3 APP Profile Selection Based on , APP profiles consist of 4 attributes (2 with 2 levels, 2 with 3 levels), yielding 36 possible profiles (2$×2×3×$3). Ranking 36 profiles is impractical, so SPSS 23.0' s orthogonal design selected 9 representative profiles shown in .

4.2 Survey Design

An online questionnaire using between-subjects design was implemented via "Question Star" software.

(1) Questionnaire Testing: Five faculty, PhD students, master' s students, and undergraduates from Zhengzhou University evaluated design rationality and content validity.

(2) Survey Implementation: From September-October 2019, a 10-person research team used snowball sampling among Zhengzhou University faculty and students, who distributed questionnaires to friends. A total of 353 questionnaires were collected. Respondents needed social network accounts and at least 10 installed APPs to ensure quality, receiving 10 yuan compensation for completion.

(3) Survey Process: The survey included: (a) purpose explanation, (b) demographic information (gender, age, education, occupation), (c) ranking 9 APP profiles with attribute explanations (separately for scenarios S1 and S2), and (d) additional questions about social network friend counts for further privacy preference analysis.

5 Data Analysis

5.1 Sample Acquisition

Data collection gathered 353 responses (S1: 175, S2: 178). After cleaning low-quality questionnaires violating common sense (e.g., preferring a paid APP collecting complete personal information over a free APP collecting none when other attributes were equal), 103 valid S1 and 102 valid S2 questionnaires remained.

5.2 Component Utility and Importance Analysis

SPSS conjoint analysis module output utility values () and relative importance (). Utility values reflect preference for attribute levels, while relative importance reflects each attribute' s decision weight. Results show price is the most important factor, with utility decreasing as price increases. Personal privacy ranks second in both scenarios, with higher collection decreasing utility. Friends' privacy ranks third, with higher collection decreasing utility, confirming other-regarding preferences. Personal privacy importance exceeds friends' privacy, confirming self-regarding preferences. Popularity is least important, with utility increasing with popularity.

5.3 Monetary Value Analysis of Level Changes

For each attribute, level change utility differences were calculated, then converted to monetary equivalents reflecting users' economic valuation. Results are in . The "Utility Change" column shows utility differences from attribute level changes. Price changes create the largest utility shifts, indicating strongest user aversion to paid versions. Personal information changes show negative utility, indicating preference for less collection. Friends' information shows similar patterns. Popularity has positive utility correlation.

Monetary conversion algorithm: First, calculate utility change per price unit (S1: $3.73/15 = 0.2487$; S2: $3.82/15 = 0.2547$). Then divide other attributes' utility changes by this value. For example, preventing collection of friends' basic information is valued at 0.44 yuan in S1 and 0.35 yuan in S2. Overall, preventing complete friends' information collection is valued at 6.32 yuan in S1 and 4.47 yuan in S2. One-sample t-tests show all utility changes are significant except "none→basic information" for friends' information, indicating low valuation of basic friends' information but high valuation of complete information. Thus, H1 is partially supported.

5.4 Comparison of Monetary Values for Personal and Friends' Privacy

Extracting monetary values for personal and friends' privacy from yields . Users' valuation of personal privacy significantly exceeds that of friends' privacy, confirming individuals care more about themselves, supporting H2. In social networks, friends' privacy monetary value refers to valuation of all friends' personal

information. For comparability, converting to per-friend value (dividing by friend count) yields very small values. Thus, users are "privacy egoists" with weak coupling to most online friends, caring only about small portions of friends' privacy. This further supports H2.

5.5 Comparison of Privacy Level Monetary Values Across Scenarios

Extracting scenario S1 and S2 monetary values from yields . All S1 monetary value absolute amounts exceed S2, indicating higher privacy concern in S1. However, statistical analysis shows no significant differences for personal privacy changes between scenarios. For friends' privacy changes, three cases exist: (1) "none→basic information" shows no significant difference, indicating low concern for basic information regardless of context. (2) "basic→complete information" shows significantly higher monetary value in S1, indicating greater sensitivity when APPs collect more sensitive information (photos, location). (3) "none→complete information" also shows significant differences, confirming sensitivity to particularly sensitive data. The first case does not support H3, but the latter two support H3, showing that information collection context significantly affects concern for friends' sensitive (not basic) information. Thus, H3 is partially supported.

6 Research Findings

This study proposes a method to quantify linking privacy' s monetary value. Results show friends' privacy ranks third in importance across both scenarios, below personal privacy and price. Comparing monetary values reveals users consider friends' privacy when choosing APPs but value it relatively low. Accounting for friend count, per-friend privacy valuation is far lower than personal privacy valuation. All three cases indicate users exhibit both privacy egoism and privacy altruism when deciding on APP usage, with the former dominating.

The study also analyzes how social APP information collection context affects linking privacy value. S1 shows higher valuations for both personal and friends' privacy than S2, but significant differences only emerge for friends' complete information. This suggests protecting friends' basic information is not particularly important to users, but unreasonable requests for sensitive information (complete minus basic information) negatively impact APP evaluation.

Theoretical Contributions: Linking privacy has received attention abroad but limited domestic research. This phenomenon objectively exists widely in China, where most APPs bundle friends' information collection authorization in privacy policies, often without friends' knowledge. This study defines linking privacy, expands personal privacy scope, and constructs a measurement method.

Practical Contributions: Results inform APP privacy policy development. Users' relatively low valuation of friends' information suggests such sharing should be more strictly limited or require explicit user consent. Privacy policymakers should encourage improved APP privacy statements clearly informing

users about friends' information collection practices and strengthen process management, such as embedding technologies to quickly assess relevance between requested information (especially friends' sensitive data) and APP functionality, enabling transparent decisions. Management and technical interventions can increase awareness for users and their friends about information collection, improving decision transparency.

Limitations: First, actual APP usage lacks privacy emphasis mechanisms, but this study directly asked about privacy as an important attribute, potentially overestimating privacy concerns and monetary values. Future research could measure privacy without explicitly asking about it. Second, this study only considered APP information collection context, not other factors like APP type or specific usage purposes. Future research should incorporate more dimensions. Finally, while confirming linking privacy's existence and value, this study did not examine user factors like personal experience, trust tendencies, and personality traits, which future structural equation modeling could address.

References

[1] AppAnnie: 2020 Mobile Market Report [EB/OL]. [2020-01-18]. http://www.199it.com/archives/998993.htm
[2] Cyberspace Administration of China. Survey of Personal Information Collection and Usage Permissions in 100 Popular Apps [EB/OL]. [2019-08-20]. http://www.cac.gov.cn/2019-05/24/c_{1124538535}.htm. [3] SCHUDY S, UTIKAL V. 'You must not know about me' -On the willingness to share personal data [J]. Journal of economic behavior & organization, 2017, 141(9): 1-13. [4] CHELLAPPA R K, SIN R G. Personalization versus privacy: an empirical examination of the online consumer' s dilemma [J]. Information technology & management, 2005, 6(2/3): 181-202. [5] SPIEKERMANN S, BAUER C, KORUNOVSKAJ. Psychology of ownership and asset defense: why people value their personal information beyond privacy [J]. Social science electronic publishing, 2012, 4(1): 41-47. [6] KRASNOVA H, ELING N, ABRAMOVA O, et al. Dangers of 'facebook login' for mobile apps: is there a price tag for social information? [EB/OL]. [2019-11-25]. https://www.researchgate.net/profile/Hanna_{Krasnova}/publication/277597655_{{{Dangers}}{{of}}}%27
of-Facebook-Login-for-Mobile-Apps-Is-There-a-Price-Tag-for-Social-Information.pdf.
[7] HANN I H, HUI K L, LEE S Y T, et al. Online information privacy: measuring the cost-benefit trade-off [EB/OL]. [2019-11-26]. https://aisel.aisnet.org/icis2002/1/. [8] BENNNDORF V, NORMANN H. The willingness to sell personal data [J]. Dice discussion papers, 2018, 120(4): 1260-1278. [9] SPIEKERMANN S, BERENDT B, GROSSKLAGS J. E-Privacy in 2nd generation E-Commerce: privacy preferences versus actual behavior [EB/OL]. [2019-11-25]. https://papers.ssrn.com/sol3/papers.cfm?abstract_{id}=761107.
[10] CHRISTIN N, EGELMAN S, VIDAS T, et al. It' s all about the money: a preliminary study on incentivizing users to ignore security advice [C]//Financial cryptography and data security-15th international conference. Berlin: Springer, 2011: 16-30. [11] KIM J, NAM C, KIM S. The economic value of personal

information and policy implications [C]//26th European regional IT conference. Madrid: International Telecommunications Society, 2015: 24-27. [12] ANDRADE E B, KALTCHEVA V, WEITZ B. Self-disclosure on the web: the impact of privacy policy, reward, and company reputation [C]//Companion publication of the 17th ACM conference on computer supported cooperative work & social computing. New York: Association for Computing Machinery, 2013: 35-38. [13] GERGELY B, CHIA P H. Interdependent privacy: let me share your data [C]//International conference on financial cryptography and data security. Berlin: Springer, 2013: 338-353. [14] WANG N, GROSSKLAGS J, XU H. An online experiment of privacy authorization dialogues for social applications [C]//Conference on computer supported cooperative work. New York: ACM Press, 2013: 261-272. [15] 100-APP Personal Information Collection and Privacy Policy Evaluation Report [EB/OL]. [2019-08-28]. http://www.ce.cn/xwzx/gnsz/gdxw/201811/28/t20181128_{30892018}.shtml. [16] SHI P, XU H, CHEN Y. Using contextual integrity to examine interpersonal information boundary on social network sites [C]//Sigchi conference on human factors in computing systems. New York: Association for Computing Machinery, 2013: 35-38. [17] JOHNSON M E. Information risk of inadvertent disclosure: analysis of file-sharing risk in the financial supply chain [J]. Journal of management information systems, 2008, 25(2): 97-123. [18] JAMES T L, WALLACE L, WARKENTIN M, et al. Exposing others' information on online social networks (OSNs): perceived shared risk, its determinants, and its influence on OSN privacy control use [J]. Information & management, 2017, 54(7): 851-863. [19] WIRTH J, MAIER C, LAUMER S, et al. Perceived information sensitivity and interdependent privacy protection: a quantitative study [J]. Electronic markets, 2019, 29(3): 359-378. [20] COOPER D, KAGEL J. Other-regarding preferences: a selective survey of experimental results [EB/OL]. [2019-08-25]. https://www.onacademic.com/detail/journal_{{{100003979745010}}_{{ff18}}}.html. [21] STAHL D O, HARUVY E. Other-regarding preferences: egalitarianism, empathy, and group size [J]. Journal of economic behavior & organization, 2006, 61(1): 20-41. [22] SMITH H J, BURKE M S. Information privacy: measuring individuals' concerns about organizational practices [J]. MIS quarterly, 1996, 20(2): 167-196. [23] FEHR E, RIEDL K A. Does fairness prevent market clearing? an experimental investigation [J]. The quarterly journal of economics, 1993, 108(2): 437-459. [24] ITOH H. Moral hazard and other-regarding preferences [J]. Japanese economic review, 2004, 55(1): 18-45. [25] WANG N, WISNIEWSKI P, XU H, et al. Designing the default privacy settings for facebook applications [C]//Proceedings of the companion publication of the 17th ACM conference on computer supported cooperative work & social computing. New York: Association for Computing Machinery, 2014: 249-252. [26] GREEN P E, SRINIVASAN V. Conjoint analysis in marketing: new developments with implications for research and practice [J]. Journal of marketing, 1990, 54(4): 3-19. [27] GUPTA S, MELA C F. What is a free customer worth? armchair calculations of nonpaying customers' value can lead to flawed strategies [J]. Harvard business review, 2008, 86(11): 102-109.

Author Contributions: Zang Guoquan proposed the research idea, designed the study, and revised the paper; Zhou Xiaoqian collected and analyzed data, created figures/tables, and wrote the initial draft.

Note: Figure translations are in progress. See original paper for figures.