International Journal of Future Generation Communication and Networking
Vol. 9, No. 3 (2016), pp. 279-288
http://dx.doi.org/10.14257/ijfgcn.2016.9.3.25

The Causality Test of Network Technical Anonymity and Perceptive Anonymity

Xi Chen* and Yujie Li

School Of Business Management and Tourism Management, Yunnan University, chen_xi1231@qq.com

Abstract

In order to discuss different types of network anonymity and the correlations among them, this paper separates network anonymity into two variables on the basis of subject object dichotomy. One is network technical anonymity, referring to the amount of information concealed that lead to difficulties in identifying the subject; the other is perceptive anonymity, which means how anonymous one perceive him/herself has been. Then the author explores how to measure these variables and set up a test model to see if there is any causal relation between them. The data was collected from Sina Weibo, and it is intended for empirical test. This thesis proved that there is an obvious causal relation between the two types of anonymity.

Keywords*: network anonymity, technical anonymity, perceptive anonymity*

1. Introduction

Anonymity refers to the concealment of one's real social identity. In fact, it has two different situations: one is no identity related information presented; the other is difficulties in identifying one's personal social information [1]. It is clear that anonymity is a social state, and it only happens when there is at least one object or audience [2]. Scholars have been very much interested in how people act when they are anonymous. Anonymity refers to the concealment of one's real social identity [3]. Mostly, it happens on the Internet where users using nicknames is a basic character. Therefore, social activities under the online environment would have some extent of anonymity [4]. With the online society intermingling with the real world, concerns about cyber-violence, inappropriate remarks, privacy security is on the rise, and this has something to do with anonymity [5]. Under this circumstance, there have been fierce debates about whether real-name registration system should be applied to the online society [6]. In terms of the implementation of real-name registration system, requiring every user to produce genuine personal information is a must. It is believed that with the real information provided, there won't be any anonymity on the internet [7]. However, this thesis insists that it is never a simple binary logic in regards to the user identity on the internet. There are two arguments we want to make. Firstly, the unique way of interaction online means that though user does provide real information, his/her identity will not be presented to other people in the same app [8]. It needs some extra efforts to find one's real identity too. Secondly, on the opposite, if the user does not provide real information, it is possible to identify them with the limited information too, and that is where human flesh search comes from. Therefore, it is impossible for absolute anonymity to happen on the internet, but anonymity commonly exists in various network environments. For all these time, most of the studies on anonymity see it as a general condition or objective phenomenon. What they lacked is to differentiate technical and perceptive anonymity. Besides, they did not explore the extent of anonymity, though it will affect users' behavior [9].

Based on the understanding of the above question, this study would explore network anonymity in two new perspectives. One is to divide it into technical and perceptive

ISSN: 2233-7857 IJFGCN

anonymity and provide detailed definition; the other is to regards the degree of anonymity as a continuous variable and to discuss how to measure it. By doing these, we will present an empirical test of the causality between these two types of anonymity. This study would provide some basics for future researches on the relations between different network anonymity and human behavior.

2. Formatting the Notion and Measurement of Network Anonymity

The operation of online society is based on virtual identity, which leads to different extent of anonymity of user identity. Compared with no identity, network anonymity should rather be seen as not identifiableness [1], which means that one cannot get accurate personal information of the users such as sex, age, religion and occupation. Therefore, network anonymity is believed to commonly exist in online society. So far, most theoretical models of network behaviors presented online interaction under the circumstances of anonymity [10]. Hayne and Rice claimed that anonymity in social interaction could be categorized into network and social anonymity [11]. With the logic of subject object dichotomy in philosophy, network anonymity is divided into technical and social anonymity, representing respectively objective and subjective anonymity. One can be identified through identifiable information, and technical anonymity means that the information related to one's identity is completely concealed; while social anonymity means that information lacked in certain contexts, that is, perceptive anonymity during social interaction. Thus, network social anonymity could also be divided into two types: technical and perceptive anonymity. The former refers to not identifiable technically, or the difficulties in identifying someone with the information on the internet; the latter refers to how anonymous user feel.

2.1. Establish and Measure Network Technical Anonymity Degree

Network technical anonymity degree can be defined as how difficult to identify the subject with the available information. It has two implications: lack of information related to identity; difficulties in identifying the subject, or the cost one should take to identify. The anonymity degree varies in different network applications. For example, if an application requires user to register their real personal information, it is relatively easy to identify them. In addition, different subjects may provide different amount of identity-related information, even though they are in the same application. What's more, due to the differences in user habits, experiences and knowledge, each subject may also provide different amount of information. As a result, network anonymity degree could at lease serve as an evaluation index to reflect how anonymous the subjects are in three aspects: firstly, how anonymous the network application is; secondly, how anonymous different users in the same app are; thirdly, how anonymous a behavioral agent is on the internet. It is shown as follows:

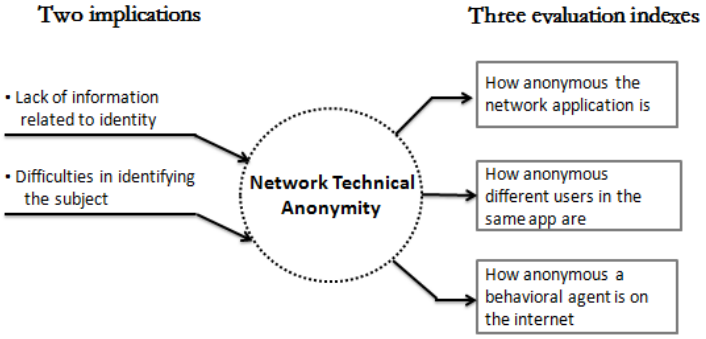

Figure 1. The Implications and Evaluation Indexes of Network Technical Anonymity Degree

The evaluation of network technical anonymity degree could be designed from the following three perspectives:

2.1.1. Comprehensive Evaluation Method

Xichen and Gangli applied analytic hierarchy process and fuzzy comprehensive evaluation, in order to measure the identifiable degree of real identity. They also used several commonly seen network applications in China as case studies [12]. Their definitions of evaluation indexes and weights (represented by vector $\vec{W}$) are as follows:

Table 1. Evaluation Indexes of the Identifiable Degree of Real Identity

No.	Index	Explanation	Weight
1	Legitimate name	The name network subject registered in the household management administration. The subject should be a natural person in the real society, which means he/she has a real identity.	0.529
2	Valid address	The valid address the subject live in the real world	0.141
3	Network alias	The alias the subject uses in the online society, which is also called network ID; one subject could have one or more network aliases.	0.102
4	Network behavior	Messages subjects leave on the internet, such as online remarks, comments and access record	0.056
5	Social attributes	Information related to social attributes such as age, sex, occupation and hobbies provided on the network applications	0.172

TR, the identifiable degree of behavioral agent in the network could be calculated in the following formula:

$$TR = \sum_{i=1}^{5} Y_i W_i \quad (1)$$

In this formula, Y represents the richness and completeness of real identity revealed information. On the internet, technical anonymity refers to the difficulties in identifying the subject, while in social activities, removing identity related information could also conceal their identity.

Anonymous can be defined as the degree of how ignorant we are about the real identity of the behavioral agent. The definition already puts emphasis on the different degree of anonymity, which shows that anonymity could be a continuous variable [13]. It is similar online. The identity of users is not absolutely concealed or revealed, instead, it is partly anonymous [14]. Even though their real name has been concealed, they could always use alias to get some extent of anonymity. Therefore, we believe that the network identity of a subject is not limited to two states: anonymous or revealed. For most net users, there is no such thing as complete anonymous or absolute real name system. The so-called anonymous or real-name system lies on how much it costs to identify users' real social identity. The higher the cost, the higher the anonymity degree; otherwise the higher the real name degree. Therefore, the network technical anonymity degree could be shown in a reverse formula of the identifiable degree.

$$TA = TR^{-1} \quad (2)$$

2.1.2. Indicated Method with Information Quantity

Network technical anonymity could be represented by the richness of information. The information quantity lies on to what extent the information could eliminate the uncertainty of one's identity; the more it eliminates the uncertainty, the larger the information quantity is; and vice versa. The measurement formula of information quantity is as follows:

$$H(x) = -\sum P(X_i) \log_2 P(X_i) \quad (3)$$

In the above formula, $P(X_i)$ is a probability density function for using available information to identify the behavioral agent. The information quantity can be seen as a reflection of network technical anonymity. Under certain network environment, the anonymity relies on how much information is provided during online social activities. It is the objective existence of one's real identity in the network society. Through online tract, text and data analysis, one could get this information.

2.1.3. Subjective Assessment Measurement

When measuring, a simple way is to ask behavioral agent to report on different indexes about their identification. Therefore, as a simple but effective way, network technical anonymity degree could be measured from the following five entries:

Table 2. Measuring Network Technical Anonymity Degree

Entry	Explanation
TA_1	Identification information of real name provided when you use the application (reverse coded)
TA_2	Valid address provided when you use the application (reverse coded)
TA_3	Network nickname shown in the application that may possible reveal your identity (reverse coded)
TA_4	Behavior records shown in the application that may possible reveal your identity (reverse coded)
TA_5	By using this application, you revealed many real social attributes (such as: age, occupation, hobbies) (reverse coded)

During the survey, users could rate the above entries from absolutely disagree to totally agree with the evaluation method of Likert scale.

2.2. Establish Network Perceptive Anonymity

Network perceptive anonymity is a subjective anonymity in nature, representing how anonymous a subject feel when using an application. In other words, it refers to to what extent one feel that others do not know his/her identity. Network anonymity is limited to certain social contexts when the behavioral agent cannot be identified due to a lack of related information. That is to say, even though it is possible to identify the subject, he/she still feels anonymous [15]. Many researches show that people believe that they are anonymous on the internet [16-19]. With IP address tracking and identification technology, technical anonymity commonly exists. However, perceptive anonymity might be the more important factor that influences how users comment and behave online. Compared with objective anonymity, perceptive anonymity could exert stronger influence on human behaviors [14]. Scholars also find that the degree of perceptive anonymity is different from human behaviors [15]. All this time, most related studies regarded network

perceptive anonymity as a variable of the setting. Quantization of perceptive anonymity is significant for researches on the relations between network anonymity and behaviors. As Scott states that what people do on the internet largely depends on how anonymous they feel, which is a continuous variable ranging from complete anonymous to absolute autonym [20]. In cyber society, perceptive anonymity might have greater influence on human behavior than objective anonymity. Dwight probed into how to evaluate and measure network perceptive anonymity, in order to provide an effective and reliable quantization for future research. Serving as a measuring tool, it can be used to explore how perceptive affect human behaviors in different settings [15]. Based on their study, indexes for perceptive anonymity are measured from the following five entries:

Table 3. Measurement of Network Perceptive Anonymity

Entry	Explanation
PA_1	I am confident that others do not know who I am
PA_2	I believe that my personal identity remains unknown to others
PA_3	I am easily identified as an individual by others (reverse coded)
PA_4	Others are likely to know who I am (reverse coded)
PA_5	My personal identity is known to others (reverse coded)

During the survey, users could rate the above entries from absolutely disagree to totally agree with the evaluation method of Likert scale.

2.3. Model to Test Relations between Network Technical and Perceptive Anonymity

Network technical and perceptive anonymity represents a worldview of subject object dichotomy. The former is objective, referring to the possibility to identify the behavioral subject by the information left on the internet; while the latter is how anonymous the behavioral subject feel. In fact, perceptive anonymity relies on how much information user provided during online social activities. Clearly, there is a causal relation between technical anonymity and perceptive one. This study tries to test the causality by applying structural equation model, the equation assumption is as follows:

Based on the research questions and variables, we could build an initial model about technical anonymity (TA) and perceptive anonymity (PA). The mathematics is shown below:

Measurement index for TA: $V_i = \lambda_i TA + \varepsilon_i;\ ,\ i = 1,2,3,4,5;$ (4)

Measurement index for PA: $T_j = \tau_j TA + \varepsilon_k,\ j = 1,2,3,4,5,\ k = 6,7,8,9,10;$ (5)

Structural equation: $PA = \gamma TA + Z;$ (6)

Based on the coefficient matrix analysis in the equation, we can test the causality between measurable variable and latent variable, or between two latent variables.

3. Causality Test between Two Indexes

This study collected related data of users in Sina Weibo via network platform, and used for an empirical test of causality between technical anonymity and perceptive anonymity. We sent group e-mails to Sina Weibo users, in which they were invited to fill a questionnaire. Then according to the below screening rules, we chose valid questionnaire.

The following are invalid questionnaire: (1) the answering time is less than 5 minutes; (2) most of the answers are quite the same, which seems very casual; (3) answers of different questions are paradox; (4) incomplete questionnaire. It took 2 days to collect the data, with a total of 426 valid questionnaires. The sample targeted young person under 34 years old and conforms to the age distribution of Weibo user. Most of the respondents received higher education, with more than five years of using the Internet. 3.74% of the respondents started using Weibo within a year, while a majority of them regularly checked Weibo for over two years. It shows that most of the respondents are quite familiar with Weibo. In general, respondents are common users of Weibo. Those who claimed they seldom log on Weibo only accounts for 5%.

3.1. Data Analysis and Model Test

This study adopts software Amos20 and Spss16 to test the validity of sample, for confirmatory factor analysis and the setup of structural equation model. Kurtosis and Skewness test method to test the normal distribution of the sample. As a result, the skew and kurtosis is close to zero, so we could say that the data is in accordance with univariate norm distribution. It also show that the data is proper for further statistical treatment and analysis.

3.1.1. Validity and Reliability Analysis

Coefficient of internal consistency Cronbach.a value is commonly adopted in academy to test the reliability of data. Cronbach states that $a<0.35$ represents low reliability, $0.35<a<0.7$ medium, $a>0.7$ high. It is confirmed that the Cronbach.a of all factors are over 0.7, which means the data and scale is highly reliable. Meanwhile, the model and assumption is on the basis of previous studies. Therefore, we could start testing with the structural equation.

Table 4. Coefficient Value of Variable Validity and Reliability Test

Latent variables	Observational variables	Standardized load	Index reliability R^2	Cronbach a coefficient	AVE	Composite reliability CR
Network technical anonymity (TA)	TA_1	0.756	0.571	0.755	0.487	0.824
	TA_2	0.692	0.479			
	TA_3	0.602	0.374			
	TA_4	0.697	0.486			
	TA_5	0.728	0.524			
Network perceptive anonymity (PA)	PA_1	0.832	0.692	0.848	0.654	0.850
	PA_2	0.865	0.748			
	PA_3	0.723	0.522			
	PA_4	0.790	0.577			
	PA_5	0.806	0.649			

From the above table, we could see the standardized load and AVE, CR value of each latent variable. Since all the CR value is greater than 0.7, which prove the high reliability of scales. The AVE value of TA is 0.486, which is acceptable; the average variance of perceptive anonymity is 0.654, which implies high convergence of data and scale. The

correlation coefficient of TA and PA is 0.481, AVE value under which implicates the scale is valid.

The KMO value of Bartlett.s Test of Sphericity is 0.841, and it is obvious on the P<0.001 level, so the data is proper for factor analysis. Since data has been collected through questionnaire, we still need to test the common method bias. This study adopted Hannan's single factor test. We put all the questions of the survey together for factor analysis and to judge whether the first principal component preceding rotation explain most of the variance. If the single factor explains more than 50% of variance, it is believed that there is common method bias. According to the below figure, it can be see that four common factors with eigenvalue greater than 1, the largest one can explain 31.654% of variance, which is within an acceptable range. Therefore, we could say that there is no common method bias.

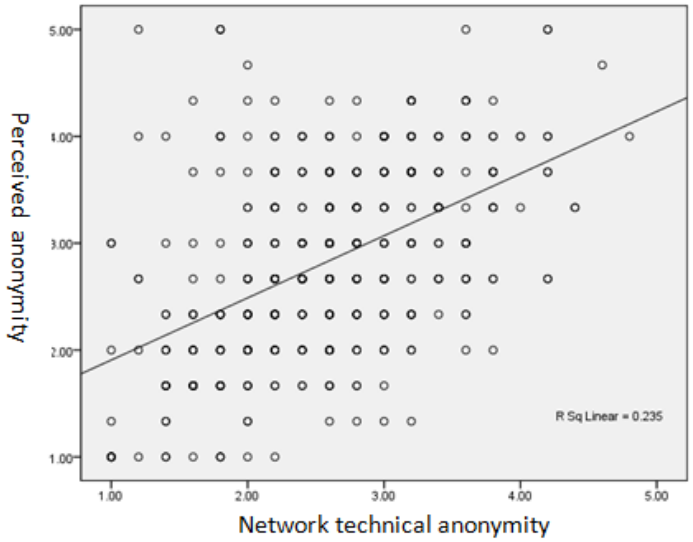

Figure 2. TA And PA Scatter Diagram

The correlation coefficient of TA and PA is 0.485, p<0.01

Table 5. Matrix of Relation of Measured Items

	TA_1	TA_2	TA_3	TA_4	TA_5	PA_1	PA_2	PA_3	PA_4	PA_5
TA_1	1	.618**	.159**	.444**	.420**	.428**	.387**	.430**	.306**	.410**
TA_2	.618**	1	.185**	.406**	.477**	.301**	.288**	.319**	.182**	.279**
TA_3	.159**	.185**	1	.302**	.214**	.147**	.124*	.128**	.135**	.146**
TA_4	.444**	.406**	.302**	1	.515**	.482**	.432**	.432**	.402**	.464**
TA_5	.420**	.477**	.214**	.515**	1	.345**	.301**	.334**	.270**	.336**
PA_1	.428**	.301**	.147**	.482**	.345**	1	.885**	.893**	.849**	.968**
PA_2	.387**	.288**	.124*	.432**	.301**	.885**	1	.717**	.612**	.739**
PA_3	.430**	.319**	.128**	.432**	.334**	.893**	.717**	1	.621**	.904**
PA_4	.306**	.182**	.135**	.402**	.270**	.849**	.612**	.621**	1	.896**
PA_5	.410**	.279**	.146**	.464**	.336**	.968**	.739**	.904**	.896**	1

3.1.2 Model Test

Use AMOS20 software to test the model, and the results are shown below:

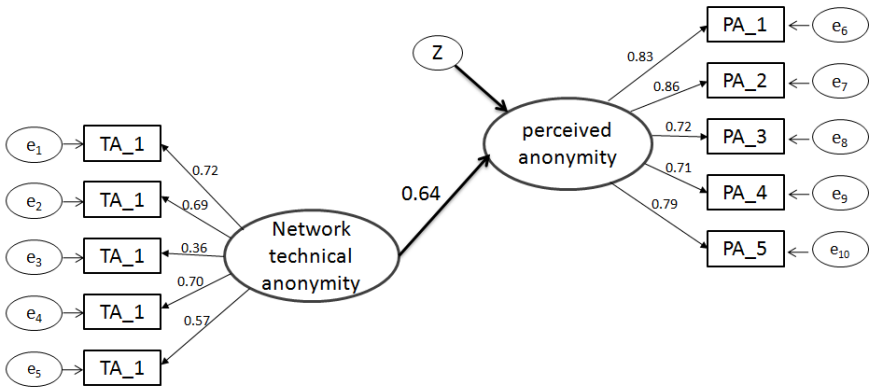

Figure 3. Structural Equation Model Test

The goodness of fit of the model is:

Table 6. The Goodness of Fit of the Structural Equation Model

Index	Chi-square value	DOF	P value	GFI	CFI	NFI	NNFI	RMSEA
Numerical value	207.046	96	0.000	0.942	0.961	0.931	0.952	0.052

The goodness of fit is RMSEA<0. 08, and NFI, NNFI, CFI, GFI are greater than 0.90. T values of each variable are all obvious. As is shown that standardized path coefficient is obvious. The goodness of fit is relatively proper and the model can be applied. The assumption is proved to be right: there is causality between TA and PA.

4. Conclusion

This study divided network anonymity into TA and PA with the logic of subject-object dichotomy. TA refers to objective anonymity of one's real identity, while PA refers to how anonymous the behavioral subject feels. This paper discusses evaluation methods of two network anonymity, and provides a test model for the causality between TA and PA. Data was collected from Sina Weibo. After an empirical test of the model, we proved that the obvious causality exists. In cyber society, the identifiableness and perceptive anonymity could coexist. The study verified that these two is independent, and have causality between them. The authors further verified the validity and reliability of TA and PA indexes. However, the AVE value of TA is merely acceptable and has not reached a satisfactory level. In addition, three measured entries of TA indexes have standardized loads of less than 0.7. The implications are pointing to future research on TA indexes. So far there is highly valid and reliable evaluation tool for PA. Future studies could thoroughly explore the evaluation of TA base on this research.

On the basis of this study, further research will be conducted on the relations of network anonymous with the human behaviors in many aspects, such as the purchasing behaviors in E-commerce, network social activities, and organizational behaviors.

Acknowledgments

Support for this work was provided by National Social Science Fund Project 15CSH017.

References

[1] N. Lapidot-Lefler and A. Barak, "Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition", Computers in human behavior, vol. 28, no. 2, **(2012)**, pp. 434-443.
[2] H. Qian and C.R. Scott, "Anonymity and Self-Disclosure on Weblogs", Journal of Computer-Mediated Communication, no. 12, **(2007)**, pp. 1428-1451.
[3] L. Lingchen, "Calm Thinking on the Generalization of Real-name System", Journal of Gansu Political Science and Law Institute, no. 5, **(2008)**150-154.
[4] L. Pin and A.-Y. Hsieh, "Speech or silence: The effect of user anonymity and member familiarity on the willingness to express opinions in virtual communities", Online Information Review, vol. 38, no. 7, **(2014)**, pp. 881-895.
[5] R. Gao, "Reflections on the Abolishment of Real-name System in Korea", Contemporary Communications, no. 1, **(2013)**, p. 47.
[6] Z. Wang and D. Li, "Real-name System and Right for Anonymous Comments", Contemporary Communications, no. 4, **(2013)**, pp. 75-78.
[7] G. Wenmiao, "On Real-name System from a Legal Perspective", Journal of Lanzhou, no. 03, **(2012)**, pp. 167-170.
[8] H. Tian and G. Meng, "On Problems and Countermeasures of Real-name System in China", Journal of Modern Information, no. 9, **(2013)**, pp. 68-76.
[9] S.P. Robbins and T.A. Judge, "Organizational Behavior", New Jersey: Prentice Hall, **(2011)**.
[10] J. Adamson, "Cyber Behavioral Psychology: Virtual World and Real World", Beijing: The Commercial Press, **(2010)**.
[11] S. Hayne and R. Rice, "Attribution Accuracy When Using Anonymity In Group Support Systems", International Journal of Human Computer Studies, no. 3, **(1997)**, pp. 429-450.
[12] X. Chen and G. Li, "Evaluation Indicators and Model of Network Technical Anonymity", International Journal of Future Generation Communication and Networking, vol. 6, no. 4, **(2013)**, pp. 181-192.
[13] R. King, "Assessing Anonymous Communication on Internet: policy Deliberations", AAAS, **(2001)**.
[14] S.A. Rains and C.R. Scott, "To identify or not to identify: A theoretical model of receiver responses to anonymous communication", Communication Theory, vol. 17, no. 1, **(2007)**, pp. 61-91.
[15] M.H. Dwight, V. Troy and R. Adrian, "Measuring Perceived Anonymity: The Development of a Context Independent Instrument", Journal of Methods and Measurement in the Social Sciences, vol. 5, no. 1, **(2014)**, pp. 22-39.
[16] A. Ben-Ze'ev, "Privacy, emotional closeness, and openness in cyberspace", Computers in Human Behavior, vol. 19, **(2003)**, pp. 451-467.
[17] A. Carvalheira and F.A. Gomes, "Cybersex in Portuguese chatrooms: A study of sexual behaviors related to online sex", Journal of Sex & Marital Therapy, vol. 29, **(2003)**, pp. 345-360.
[18] K.Y.A. McKenna and J.A. Bargh, "Plan 9 from cyberspace: The implications of the internet for personality and social psychology", Personality & Social Psychology Review, vol. 4, **(2000)**, pp. 57-75.
[19] J. Suler, "The online disinhibition effect", CyberPsychology & Behavior, vol. 7, **(2004)**, pp. 321-326.
[20] C.R. Scott, "Reveal or not to reveal: A theoretical model of anonymous communication", Communication Theory, vol. 8, **(1998)**, pp. 381-407.

