An Investigation of Twitter Users Who Gave Likes to Tweets Disclosing Submitters' Personal Information

Yasuhiko Watanabe, Toshiki Nakano, Hiromu Nishimura, and Yoshihiro Okada
Ryukoku University
Seta, Otsu, Shiga, Japan
Email: watanabe@rins.ryukoku.ac.jp, t180450@mail.ryukoku.ac.jp,
t160405@mail.ryukoku.ac.jp, okada@rins.ryukoku.ac.jp

***Abstract*—Nowadays, many people use a Social Networking Service (SNS). Most SNS users are careful in protecting the privacy of personal information: name, age, gender, address, telephone number, birthday, etc. However, some SNS users disclose their personal information that can threaten their privacy and security even if they use unreal name accounts. In this study, we investigated Twitter users who gave likes to tweets disclosing submitters' personal information that potentially threatened submitters' privacy and security. We collected 318 tweets promising to disclose submitters' personal information. Then, we investigated the relations between the submitters of these 318 tweets and users who gave likes to them. The results of our survey showed that the submitters followed most of the users mutually before the users gave likes to tweets promising to disclose submitters' personal information. On the other hand, most of the users did not follow each other although they followed the same submitters and gave likes to their tweets.**

Keywords–personal information; Twitter; SNS; mutual follows; privacy risk; unreal name account user.

I. INTRODUCTION

Nowadays, many people use a Social Networking Service (SNS) to communicate with each other and try to enlarge their circle of friends. SNS users are generally concerned about potential privacy risks [1]. To be specific, they are afraid that unwanted audiences will obtain information about them or their families, such as where they live, work, and play. As a result, SNS users are generally careful in disclosing their personal information. However, some SNS users, especially young users, disclose their personal information on their profiles, for example, real full name, gender, hometown and full date of birth, which can potentially be used to identify details of their real life. In order to discuss the reasons why some SNS users disclose their personal information willingly, it is important to investigate who they want to read their SNS messages disclosing their personal information. However, it is difficult to ask them who they want to read them. To solve this problem, it is important to investigate who gave responses to their SNS messages disclosing their personal information. This is because, if submitters felt unwanted audiences read and gave responses to their SNS messages disclosing their personal information, they would delete them. In order to investigate who gave responses to SNS messages disclosing submitters' personal information, we investigate Twitter users who gave likes to tweets disclosing submitters' personal information. Furthermore, we investigate whether users concerned with a tweet disclosing submitter's personal information followed each other. In other words, we investigate whether

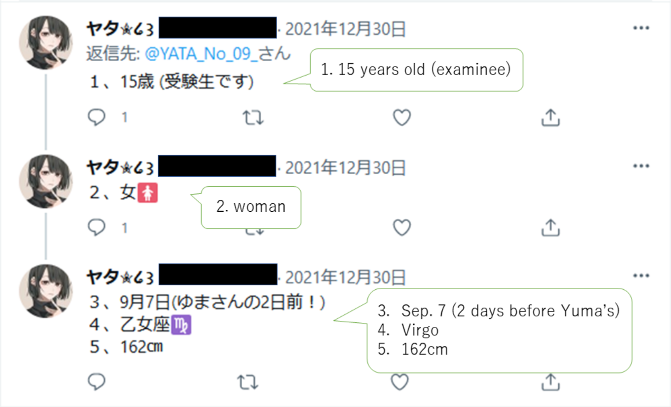
- a submitter followed users who gave likes to his/her tweet disclosing his/her personal information,
- users who gave likes to a tweet disclosing submitter's personal information followed the submitter, and
- each user who gave a like to a tweet disclosing submitter's personal information followed every other user who gave a like to the same tweet.

In this study, we examine these points by checking their Twitter follow relations. The investigation is based on an idea: when an user follow someone on Twitter, he/she is not a stranger to the user. By using the results of the investigation, we discuss the relations of submitters of tweets disclosing their personal information and users who gave likes to the tweets. The results of the investigation might improve social media design elements, such as privacy controls and friend introductions.

The rest of this paper is organized as follows: In Section II, we survey the related works. In Section III, we show how to collect tweets where submitters seemingly disclosed their personal information honestly and detect users who gave likes to them. In Section IV, we examine whether users concerned with a tweet disclosing submitter's personal information followed each other and discuss the relations of them. Finally, in Section V, we present our conclusions.

II. RELATED WORK

Personally identifiable information is defined as information, which can be used to distinguish or trace an individual's identity, such as social security number, biometric records, etc. alone, or when combined with other information that is linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. [2] [3]. Internet users are generally concerned about unwanted audiences obtaining personal information. Fox et al. reported that 86% of Internet users are concerned that unwanted audiences will obtain information about them or their families [1]. However, Internet users, especially young users, tend to disclose personal information on their profiles, for example, real full name, gender, hometown and full date of birth. As a result, many researchers discussed the reasons why young users willingly disclose personal information on their SNS profiles. Acquisti and Gross explained this phenomenon as a disconnection between the users' desire to protect their privacy and their actual behavior [4]. Also, Livingstone pointed out that teenagers' conception of privacy does not match the privacy settings of most SNSs [5]. On the other hand, Barnes argued that Internet users, especially teenagers, are not aware of the nature of the Internet and SNSs [6]. Viseu, Clement, and Aspinall reported that many online



ヤタ☆63 [redacted] · 2021年12月30日
返信先: @YATA_No_09_さん
1、15歳 (受験生です)

1. 15 years old (examinee)

ヤタ☆63 [redacted] · 2021年12月30日
2、女🚺

2. woman

ヤタ☆63 [redacted] · 2021年12月30日
3、9月7日(ゆまさんの2日前！)
4、乙女座♍
5、162㎝

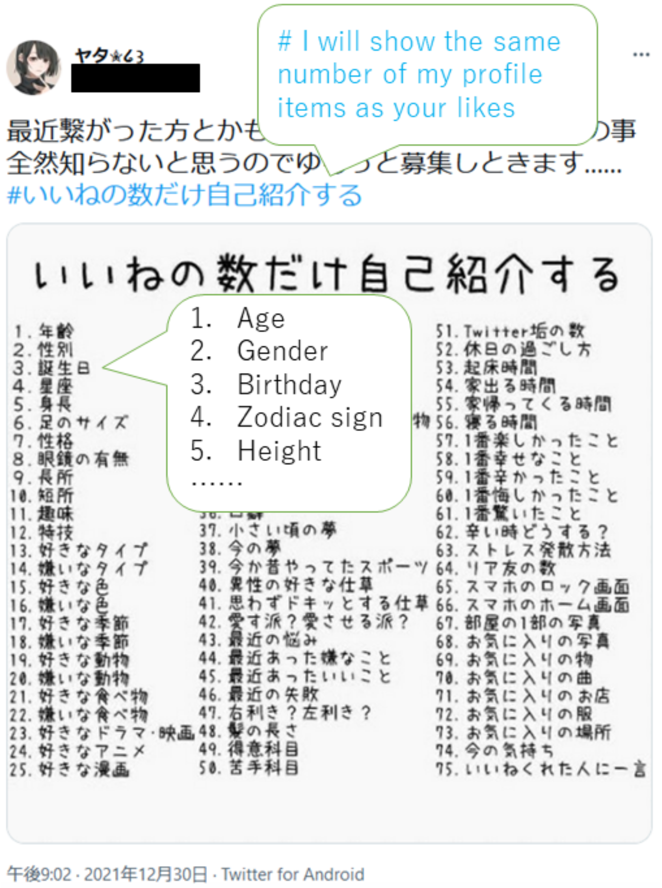
3. Sep. 7 (2 days before Yuma’s)
4. Virgo
5. 162cm

Figure 1. An unreal name account user, *Yata*, disclosed her personal profile items in her tweets.

users believe the benefits of disclosing personal information in order to use an Internet site is greater than the potential privacy risks [7]. The authors think that most SNS users are seriously concerned about their privacy and security. However, they often underestimate the risk of their online messages and submit them. Hirai reported that many users had troubles in SNSs because they never thought that strangers observed their communication with their friends [8]. Watanabe, Nishimura, Chikuki, Nakajima, and Okada reported that some Twitter users submitted tweets disclosing their personal information that can threaten their privacy and security even if they use unreal name accounts [9]. In this study, we investigate what relations existed between users concerned with a tweet disclosing submitter’s personal information. In order to analyze relations in communities, many researchers have adopted tie strength. Granovetter defined tie strength as the strength of a friendship: close friends are strong ties and acquaintances are weak ties [10]. Both strong ties and weak ties are useful because they provide access to different types of resources [11]. For example, strongly tied peers have greater motivation for assistance and provide access to information known by the group [10]. In contrast, weak ties provide diverse perspectives as well as novel information and resources [12]. Panovich, Miller, and Karger investigated the relation of tie strength to answer quality and showed that social network Q&A is more effective when the asker and answerer know each other well [13]. Gilbert and Karahalios proposed a predictive model of tie strength on Facebook using profile characteristics [14]. In this study, we investigate what relations existed between Twitter users concerned with a tweet disclosing submitter’s personal information by checking their Twitter follow relations.

III. A COLLECTION OF TWEETS DISCLOSING SUBMITTERS’ PERSONAL INFORMATION

It is difficult to collect tweets disclosing submitters’ personal information, such as tweets in Figure 1, directly. To solve this problem, we focused on tweets where submitters promised their audiences to disclose the same number of their own personal profile items as likes to their tweets. Figure 2 shows a tweet submitted by *Yata* on December 30, 2021. Both in Figure 1 and Figure 2, her screen name is redacted for privacy. Figure 2 shows that *Yata* promised her audiences to disclose the same number of her personal profile items as likes to her tweet.



ヤタ☆63
[redacted]

I will show the same number of my profile items as your likes

最近繋がった方とかも　　　の事
全然知らないと思うのでゆ　っと募集しときます……
#いいねの数だけ自己紹介する

いいねの数だけ自己紹介する

1. 年齢
2. 性別
3. 誕生日
4. 星座
5. 身長
6. 足のサイズ
7. 性格
8. 眼鏡の有無
9. 長所
10. 短所
11. 趣味
12. 特技
13. 好きなタイプ
14. 嫌いなタイプ
15. 好きな色
16. 嫌いな色
17. 好きな季節
18. 嫌いな季節
19. 好きな動物
20. 嫌いな動物
21. 好きな食べ物
22. 嫌いな食べ物
23. 好きなドラマ·映画
24. 好きなアニメ
25. 好きな漫画

37. 小さい頃の夢
38. 今の夢
39. 今か昔やってたスポーツ
40. 異性の好きな仕草
41. 思わずドキッとする仕草
42. 愛す派？愛させる派？
43. 最近の悩み
44. 最近あった嫌なこと
45. 最近あったいいこと
46. 最近の失敗
47. 右利き？左利き？
48. 髪の長さ
49. 得意科目
50. 苦手科目

51. Twitter垢の数
52. 休日の過ごし方
53. 起床時間
54. 家出る時間
55. 家帰ってくる時間
56. 寝る時間
57. 1番楽しかったこと
58. 1番幸せなこと
59. 1番辛かったこと
60. 1番悔しかったこと
61. 1番驚いたこと
62. 辛い時どうする？
63. ストレス発散方法
64. リア友の数
65. スマホのロック画面
66. スマホのホーム画面
67. 部屋の1部の写真
68. お気に入りの写真
69. お気に入りの物
70. お気に入りの曲
71. お気に入りのお店
72. お気に入りの服
73. お気に入りの場所
74. 今の気持ち
75. いいねくれた人に一言

1. Age
2. Gender
3. Birthday
4. Zodiac sign
5. Height
……

午後9:02 · 2021年12月30日 · Twitter for Android

Figure 2. A tweet promising to disclose the same number of submitter’s personal profile items as likes to it.

Actually, as shown in Figure 1, *Yata* submitted three replies disclosing her five personal profile items to her tweet shown in Figure 2 on December 30, 2021. Watanabe, Nishimura, Chikuki, Nakajima, and Okada reported that Twitter users seemingly disclosed their personal information honestly when they promised to do it, such as *Yata*’s tweet in Figure 2 [9]. As a result, it is easy to collect tweets disclosing submitters’ personal profile items when we collect tweets promising to disclose submitters’ personal profile items. Furthermore, they often used the same sentence in their tweets, like a game password, as shown in Figure 2, *# I will show the same number of my profile items as your likes*. In order to collect tweets promising to disclose submitters’ personal profile items, we used the shared sentence as key to collect them. To be specific, we collected these tweets by using Twitter API v2 [15]. Twitter API v2 helps us to collect tweets where the given sentence is used. Also, Twitter API v2 helps us to collect user accounts who submitted a specific tweet and who gave likes to it. Every 10 PM, we tried to collect user accounts and their tweets

- that contained *# I will show the same number of my profile items as your likes*
- that were submitted in the past 24 hours, and
- that were given one or more likes.

After we obtained the tweets promising to disclose submitters’ personal profile items, we tried to collect user accounts who

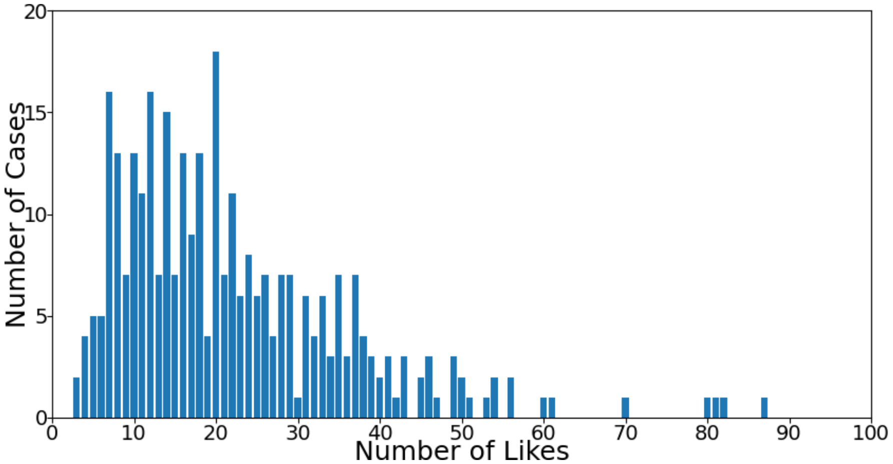


Figure 3. The histogram of the number of likes given to the 318 tweets promising to disclose submitters' personal information.

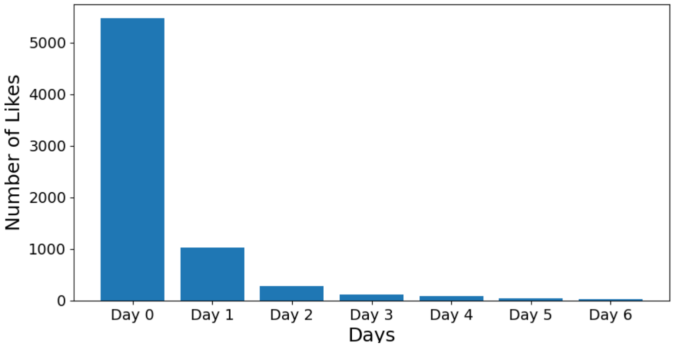


Figure 4. The daily number of likes given to the obtained 318 tweets since the tweets were submitted.

gave likes to the obtained tweets every 10 PM for a week. Finally, we collected 318 Japanese tweets promising to disclose submitters' personal information. These 318 tweets were submitted from December 30, 2021 to January 31, 2022 by 317 users. One out of the 317 users submitted two tweets promising to disclose his personal information on January 12 and 17, 2022. These 318 tweets were given 7060 likes by 6325 users within a week after they were submitted. Figure 3 shows the histogram of the number of likes given to the obtained 318 tweets promising to disclose submitters' personal information. Figure 4 shows the daily number of likes given to the obtained 318 tweets in the investigation period. Day N in Figure 4 means that N days have passed since the obtained tweet was submitted and our investigation started. Day 6 was the last day of the investigation period. Figure 4 shows that 77 % of likes were given on Day 0. 30 tweets out of the 318 tweets were deleted within a week after they were submitted.

IV. An analysis of tweets disclosing submitters' personal information

In this section, we investigate whether users concerned with a tweet disclosing submitter's personal information followed each other. To be specific, we survey

- Twitter users who submitted tweets promising to disclose the same number of their own personal profile items as likes and
- Twitter users who gave likes to these tweets

and investigate

- whether an user who submitted a tweet promising to disclose his/her personal information followed users who gave likes to the tweet,
- whether users who gave likes to a tweet promising to disclose submitter's personal information followed the submitter, and
- whether users who gave likes to a tweet promising to disclose submitter's personal information followed each other.

The investigation is based on an idea: when an user follow someone on Twitter, he/she is not a stranger to the user. We can know whether an user follows someone on Twitter by using Twitter API v2.

After collecting user accounts of submitters and users who gave likes to submitters' tweets, we analyze the relations between them. The relations between a submitter and an user who gave a like to submitter's tweet can be classified into three types:

- mutual follow relation: The submitter and the user mutually followed each other.
- one sided follow relation: The submitter followed the user, however, the user did not. Or, the user followed the submitter, however, the submitter did not.
- no follow relation: The submitter and the user did not follow each other.

Furthermore, we analyze the relations among users who gave likes to submitter's tweet. They can also be classified into three types: mutual follow relation, on sided follow relation, or no follow relation.

Let us consider one example. As shown in Figure 2, a Twitter user, *Yata*, submitted a tweet promising her audiences to disclose the same number of her own personal profile items as likes on December 30, 2021 at 9:02 PM. We detected her tweet on the same day at 10:00 PM, and then, recorded that she received five likes and submitted three replies disclosing her five personal profile items on December 30, 2021. After that, every 10 PM, we tried to check whether someone gave likes to her tweet. On January 5, 2022, we confirmed that five users gave five likes to her tweet on December 30, 2021, as shown in Figure 2, and finished the investigation on her tweet. Then, we analyzed the relations between *Yata* and each of the five users and confirmed that she followed them and each of them followed her. As a result, the relations between *Yata* and each of the five users were mutual follow relations. Furthermore, we analyzed the relations among the five users. There were ten cases to choose two out of the five users. In one case out of the ten, two users followed each other. On the other hand, in nine cases out of the ten, two users did not follow each other. As a result, the relation of one case was a mutual follow relation and the relations of the other nine cases were no follow relations.

A. Follow relations between submitters and users who gave likes to submitters' tweets

At first, we discuss the mutual follow relations between submitters and users who gave likes to submitters' tweets. In order to discuss this problem, we introduce the ratio of mutual follow relations between a submitter and users who gave likes to his/her tweet. Suppose that the number of users who gave likes to tweet t is n and m of them are mutually following the submitter of tweet t. Then, the ratio of mutual follow relations between the submitter of tweet t and the users who gave likes to it, $P_{MF1}(t)$, is defined as follows:

$$P_{MF1}(t) = \frac{m}{n}$$

Figure 5 shows the distribution of the ratio of mutual follow relations between the submitters of the obtained 318 tweets and the users who gave likes to them. Furthermore, Figure 5 (a) and (b) shows the distribution of them investigated on the Day 0 and Day 6, respectively. As shown in Figure 5, it is probable that most of the users have followed the submitters mutually before they gave likes to submitters' tweets promising to disclose their personal information. In other words, the submitters and most of the users were not strangers to each other. The distribution of the mutual relation ratio on Day 6 (Figure 5 (b)) moved to the left than that on Day 0 (Figure 5 (a)). It showed that the number of users who did not follow the submitters and whom the submitters did not follow increased. It is probable that submitters were careful to follow unfamiliar users even if they gave likes to their tweets.

Next, we discuss the no follow relations between submitters and users who gave likes to submitters' tweets. In order to discuss this problem, we introduce the ratio of no follow relations between a submitter and users who gave likes to his/her tweet. Suppose that the number of users who gave likes to tweet t is n and l of them are not following the submitter of tweet t and the submitter is not following them, too. Then, the ratio of no follow relations between the submitter of tweet t and the users who gave likes to it, $P_{NF1}(t)$, is defined as follows:

$$P_{NF1}(t) = \frac{l}{n}$$

Figure 6 shows the distribution of the ratio of no follow relations between the submitters of the obtained 318 tweets and the users who gave likes to them. Figure 6 shows that the number of users who had the no follow relations with the submitters was small on Day 0 and increased after Day 1. It is probable that the delays were caused by the time it took to find tweets disclosing submitters' personal information.

B. Follow relations among users who gave likes to submitters' tweets

At first, we discuss the mutual follow relations among users who gave likes to submitters' tweets. In order to discuss this problem, we introduce the ratio of mutual follow relations among users who gave likes to a tweet. Suppose that the number of users who gave likes to tweet t is n and there are m cases where two users of them are following each other. Then, the ratio of mutual follow relations among the users who gave likes to tweet t, $P_{MF2}(t)$, is defined as follows:

$$P_{MF2}(t) = \frac{m}{n(n-1)/2}$$

Figure 7 shows the distribution of the ratio of mutual follow relations among the users who gave likes to the obtained 318 tweets. Figure 7 shows that it is probable that most of the users did not follow each other mutually. In other words, most of the users were strangers to each other although they followed the same submitters and gave likes to their tweets.

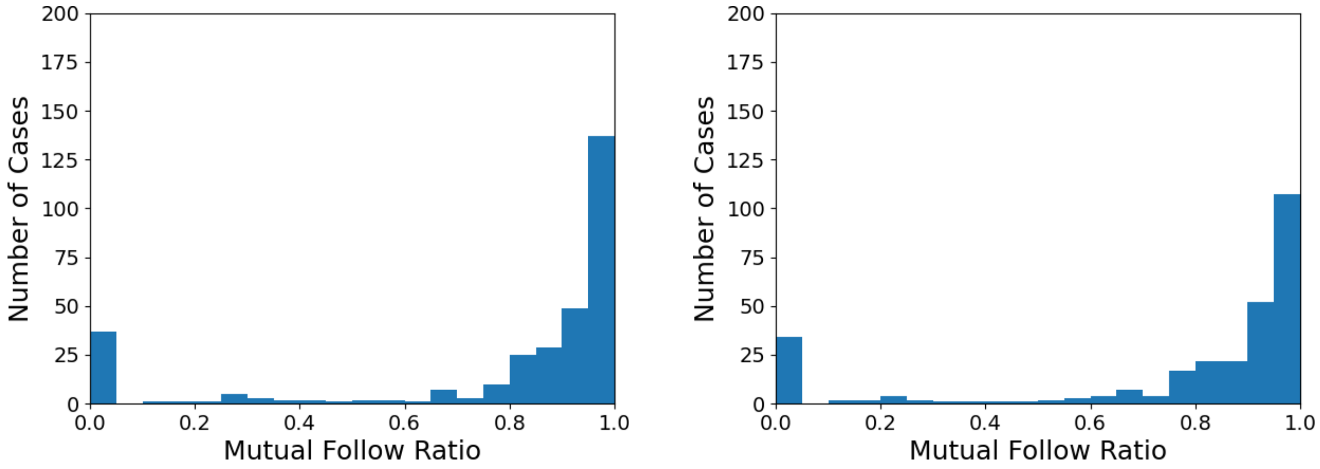
Next, we discuss the no follow relations among users who gave likes to submitters' tweets. In order to discuss this problem, we introduce the ratio of no follow relations among users who gave likes to a tweet. Suppose that the number of users who gave likes to tweet t is n and there are l cases where two users of them are not following each other. Then, the ratio of no follow relations among the users who gave likes to tweet t, $P_{NF2}(t)$, is defined as follows:

$$P_{NF2}(t) = \frac{l}{n(n-1)/2}$$

Figure 8 shows the distribution of the ratio of no follow relations among the users who gave likes to the obtained 318 tweets. The distribution of the no relation ratio on Day 6 (Figure 8 (b)) was similar to that on Day 0 (Figure 8 (a)). It showed that it is probable that not many users started to follow users within a week even if they gave likes to the same tweets. It is probable that users were careful to follow unfamiliar users even if they gave likes to the same tweets.

V. CONCLUSION

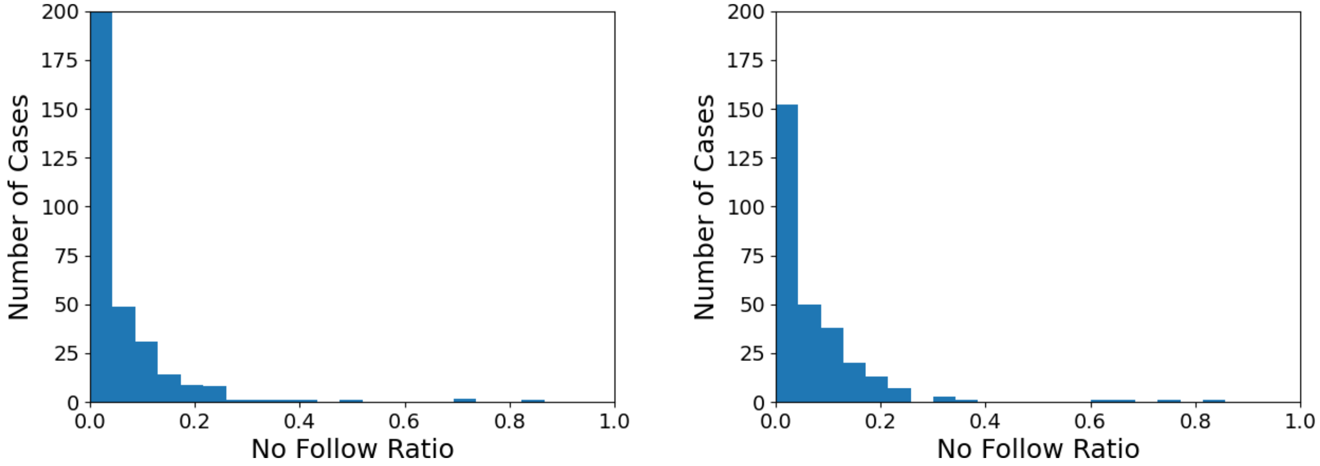
In this paper, we investigated the relations of submitters of tweets promising to disclose their personal information and users who gave likes to the tweets. The results of our investigation show that most of the users had followed the submitters mutually before they gave likes to submitters' tweets promising to disclose their personal information. On the other hand, most of the users did not follow each other although they followed the same submitters and gave likes to their tweets. As time went on, the number of users who gave likes to submitters' tweets but did not follow the submitters and whom the submitters did not follow increased. It is probable that submitters were careful to follow unfamiliar users even if they gave likes to their tweets. Also, users were careful to follow unfamiliar users even if they followed the same submitters and gave likes to the same tweets. The system that understands these relations might carefully treat users who choose not to friend someone with good reasons.



(a) the first day (Day 0)

(b) the last day (Day 6)

Figure 5. The histograms of the ratio of mutual follow relations between the submitters of the obtained 318 tweets and the users who gave likes to them on the first day (Day 0) and the last day (Day 6) of the investigation period.



(a) the first day (Day 0)

(b) the last day (Day 6)

Figure 6. The histograms of the ratio of no follow relations between the submitters of the obtained 318 tweets and the users who gave likes to them on the first day (Day 0) and the last day (Day 6) of our observation.

REFERENCES

[1] S. Fox et al., Trust and Privacy Online: Why Americans Want to Rewrite the Rules, The Pew Internet & American Life Project, 2000. [Online]. Available: http://www.pewinternet.org/2000/08/20/trust-and-privacy-online/ [accessed: 2022-04-08]

[2] C. Johnson III, Safeguarding against and responding to the breach of personally identifiable information, Office of Management and Budget Memorandum, 2007. [Online]. Available: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-16.pdf [accessed: 2022-04-08]

[3] B. Krishnamurthy and C. E. Wills, "On the leakage of personally identifiable information via online social networks," Computer Communication Review, vol. 40, no. 1, 2010, pp. 112–117. [Online]. Available: https://doi.org/10.1145/1672308.1672328 [accessed: 2022-04-08]

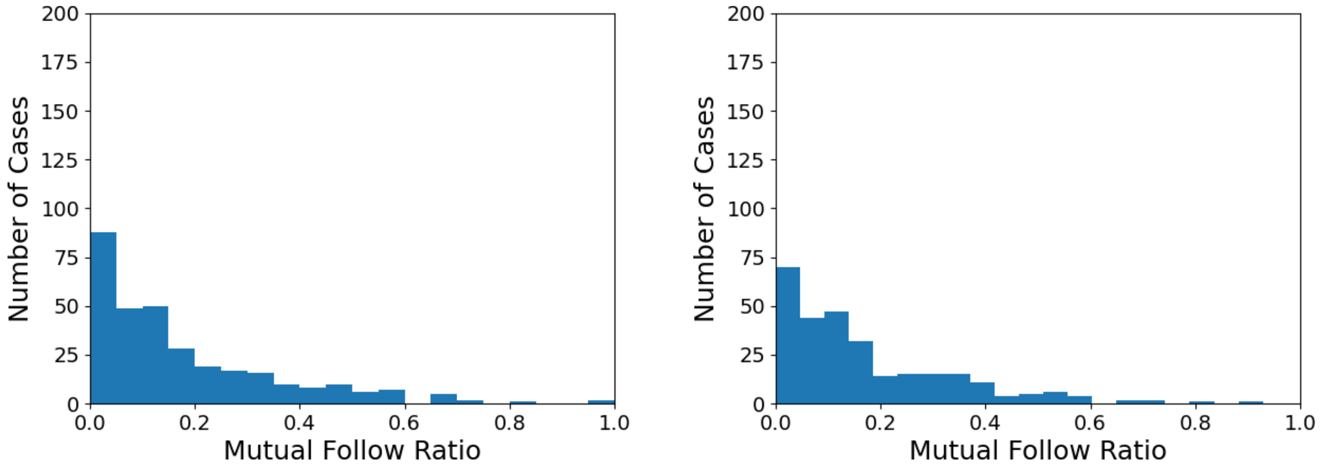
[4] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the facebook," in Proceedings of the 6th International Conference on Privacy Enhancing Technologies, ser. PET'06. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 36–58. [Online]. Available: https://doi.org/10.1007/11957454_3 [accessed: 2022-04-08]

[5] S. Livingstone, "Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression." New Media & Society, vol. 10, no. 3, 2008, pp. 393–411. [Online]. Available: https://journals.sagepub.com/doi/10.1177/1461444808089415 [accessed: 2022-04-08]

[6] S. B. Barnes, "A privacy paradox: Social networking in the United States." First Monday, vol. 11, no. 9, 2006. [Online]. Available: http://firstmonday.org/article/view/1394/1312 [accessed: 2022-04-08]

[7] A. Viseu, A. Clement, and J. Aspinall, "Situating privacy online: Complex perception and everyday practices," Information, Communication & Society, 2004, pp. 92–114. [Online]. Available: https://doi.org/10.1080/1369118042000208924 [accessed: 2022-04-08]

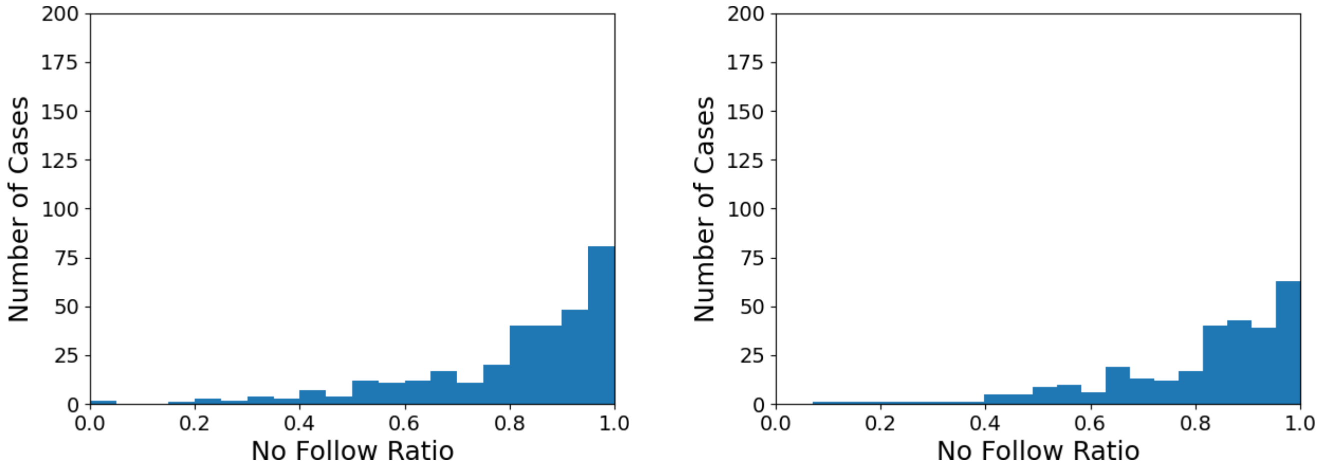
[8] T. Hirai, "Why does "Enjyo" happen on the Web? : An Examination based on Japanese Web Culture," Journal of Information and



(a) the first day (Day 0)

(b) the last day (Day 6)

Figure 7. The histograms of the ratio of mutual follow relations among the users who gave likes to the obtained 318 tweets on the first day (Day 0) and the last day (Day 6) of our observation.



(a) the first day (Day 0)

(b) the last day (Day 6)

Figure 8. The histograms of the ratio of no follow relations among the users who gave likes to the obtained 318 tweets on the first day (Day 0) and the last day (Day 6) of our observation.

Communication Research, vol. 29, no. 4, mar 2012, pp. 61–71. [Online]. Available: http://doi.org/10.11430/jsicr.29.4_61 [accessed: 2022-04-08]

[9] Y. Watanabe, H. Nishimura, Y. Chikuki, K. Nakajima, and Y. Okada, "An Investigation of Twitter Users Who Disclosed Their Personal Profile Items in Their Tweets Honestly," in Proceedings of the Sixth International Conference on Human and Social Analytics (HUSO 2020), Oct 2020, pp. 20–25. [Online]. Available: http://www.thinkmind.org/index.php?view=article&articleid=huso_2020_1_40_80035 [accessed: 2022-04-08]

[10] M. S. Granovetter, "The Strength of Weak Ties," American Journal of Sociology, vol. 78, no. 6, 1973, pp. 1360–1380.

[11] C. Haythornthwaite, "Strong, Weak and Latent Ties and the Impact of New Media," The Information Society, vol. 18, no. 5, October 2002, pp. 385–401. [Online]. Available: https://doi.org/10.1080/01972240290108195 [accessed: 2022-04-08]

[12] N. B. Ellison, J. Vitak, R. Gray, and C. Lampe, "Cultivating Social Resources on Social Network Sites: Facebook Relationship Maintenance Behaviors and Their Role in Social Capital Processes*," Journal of Computer-Mediated Communication, vol. 19, no. 4, 07 2014, pp. 855–870. [Online]. Available: https://doi.org/10.1111/jcc4.12078 [accessed: 2022-04-08]

[13] K. Panovich, R. Miller, and D. Karger, "Tie strength in question & answer on social network sites," in Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work, ser. CSCW '12. New York, NY, USA: Association for Computing Machinery, 2012, p. 10571066. [Online]. Available: https://doi.org/10.1145/2145204.2145361 [accessed: 2022-04-08]

[14] E. Gilbert and K. Karahalios, "Predicting tie strength with social media," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ser. CHI '09. New York, NY, USA: Association for Computing Machinery, 2009, p. 211220. [Online]. Available: https://doi.org/10.1145/1518701.1518736 [accessed: 2022-04-08]

[15] Twitter, Inc. Twitter API. [Online]. Available: https://developer.twitter.com/en/docs/twitter-api [accessed: 2022-04-08]