Burning Up Privacy on Tinder

Cali Stenson
Wellesley College
21 Wellesley College Rd
Wellesley, MA 02481
cstenson@wellesley.edu

Ana Balcells
Wellesley College
21 Wellesley College Rd
Wellesley, MA 02481
abalcell@wellesley.edu

Megan Chen
Wellesley College
21 Wellesley College Rd
Wellesley, MA 02481
mchen4@wellesley.edu

1. INTRODUCTION

Our research investigates the ease of finding more information about Tinder users than they want to share. We use common web search methods to look for additional information about 30 Tinder users and surveyed 111 Wellesley College students to gauge how they use Tinder and their awareness of Tinder privacy risks.

Tinder allows you to create a profile with your first name, 0-7 pictures of yourself and a short bio. Then, the Tinder app finds the profiles of local users for you to evaluate and swipe - right for like and left for dislike. As you swipe through people's profiles, you can see the pictures they've posted, read their bios, and see common Facebook likes and friends. Tinder users can only access others' profiles temporarily in the swipe feed. If two people "match" (they both swiped right), Tinder allows the two to chat and to access each other's profiles indefinitely.

Like most social media, Tinder introduces privacy concerns for its users. Tinder connects directly to users' Facebook profiles and divulges information about mutual friends to people in users' swipe feeds. This information makes it easy to hop from a mutual friend's profile to a stranger's profile and learn privacy-compromising information. We examined 30 random Tinder user profiles and attempted to link them to social media platforms like Facebook, Twitter, Instagram, LinkedIn, and Tumblr. Further, we Google-searched their images and bio information to find out more about the users. We also evaluated how much Tinder users value their privacy. We surveyed Wellesley College students to see what dating sites and apps people use (if any), why they use them (or choose not to), and what they think about privacy. Our goal was to determine students' notions of privacy, students' use of dating apps and sites, and whether there's any correlation between the two.

2. RE-IDENTIFICATION PROCESS

2.1 Methodology

We re-identified Tinder profiles using Google's reverse image search engine. To do this, we chose a random sample of 30 Tinder matches and took screenshots of their profile pictures and descriptions. We attempted to connect their images with other online accounts using Google reverse image search. If a reverse image search failed to yield results, information was also gathered by searching information using keywords given in their Tinder profile descriptions, such as searching a combination of a user's first name and school/field of study/location. Our methodology makes the following findings particularly interesting since reverse image search software can be utilized by anyone with Internet access; no coding knowledge is necessary in order to re-identify these users.

2.2 Results

Our methods of re-identification led to varied amounts of success in each of the 30 sample cases. We were able to determine the last names of 13 of the individuals (43% of the sample). When we consider successful cases of linkage, where one or more other social media accounts belonging to the user were found, then we were successful in 17 out of the 30 cases (57% of the sample). Of these 17 successfully linked individuals, Facebook was the profile most likely to be discovered, followed by Instagram, Twitter, YouTube, LinkedIn, Vine, and Tumblr accounts (Figure 1).

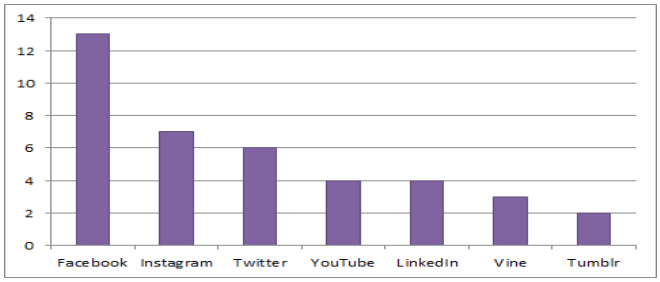

Figure 1 - Social Media Links. Each bar represents the number of users successfully associated with each given account type.

3. SURVEY OF TINDER USERS

3.1 Motivations

We were curious to find out whether or not privacy is a factor that affects whether or not young people use Tinder. We wanted to get a sense of how important privacy is to Wellesley College students. Further, we wanted to gauge how the students' level of regard for privacy correlates with their desire to use dating applications such as Tinder.

3.2 Hypothesis

People who use Tinder don't care about their privacy or are not aware of the risks of how Tinder profiles can be connected to other information online.

3.3 Methodology

To evaluate our hypothesis, we created a survey that contains questions about respondents' dating site/application use and their general regard for online privacy using Google Forms. We surveyed only Wellesley students and limited each wellesley.edu email address to one response so that individuals could not deliberately skew the data. We did not record respondents' usernames to maintain a level of privacy. Our sample population is a very specific niche of dating site users; respondents are primarily female, fall between the ages of 18-24, and are on track to attain a higher level of education than the average American. Even though our data is not generalizable to all dating site/app users, we identified certain trends in Wellesley College students' responses that potentially parallel real-world attitudes about privacy and about dating application use. In total, the survey yielded 111 responses. After the survey closed, we downloaded the survey response data as a CSV file and examined the data using the R statistical software. For questions with qualitative answers, categories representing the different types of responses were created after reading through the data.

3.4 Results and Discussion

A total of 44% percent of respondents use dating sites or applications. To evaluate the respondents' motivations, we examined the qualitative responses dating site/app users gave to the question, "Why do you use dating applications?" Responses to this question fell into seven categories (Figure 2). Most users aim to meet people with romantic and non-romantic intentions. No one cited a privacy-friendly feature in a dating app/site for the reason they use it. Further, no one expressed a desire for such privacy features to exist.

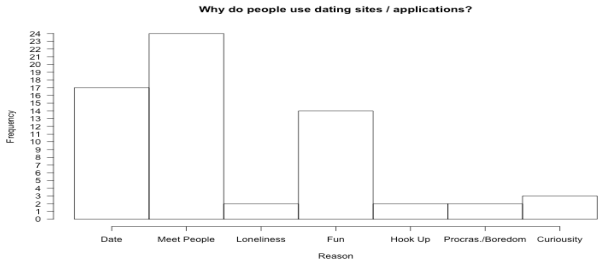

Figure 2 - This histogram shows the distribution of responses to the question "Why do you use dating applications?" Based on the responses, most people use Tinder to find romantic relationships (17), meet platonic friends (24), or for entertainment (14).

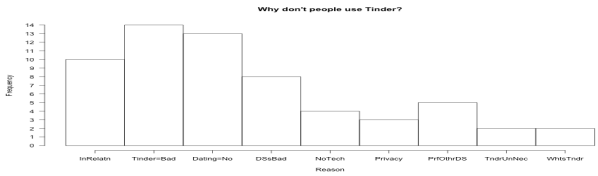

Figure 3- This histogram shows the distribution of responses to the question "Why don't you use Tinder?" Only three people cited privacy as the reason for not having a Tinder account.

Next, we asked non-users the question "Why don't you use Tinder?" From Figure 3, we can conclude that the majority of Tinder non-users either aren't looking for a significant other or don't like Tinder as a dating site. What's surprising about the data is that only 3 people (~2.7% of all respondents and ~4.8% of Tinder non-users) avoid using Tinder for privacy reasons. This suggests that our respondents evaluate dating apps mostly by their effectiveness as social media. To see whether or not there was a correlation between Tinder use and privacy awareness, we compared the mean frequency which respondents check their privacy settings between users who use Tinder and users who don't. Responses to the question "How often do you check the privacy settings on your social media accounts?" were coded to be the following integer values: 2 = Daily, 3 = Weekly, 4 = Monthly, 5 = Every 2-3 Months, 6 = Twice a year, 7 = Yearly, and 8 = Never.

We then compared the distribution of frequencies for Tinder users, non-users, and the overall distribution. The mean for Tinder users is 5.429, and the mean for Tinder non-users is 5.919. This indicates that respondents check their privacy settings every 3-6 months on average. We ran a two-sample t-test with the null hypothesis that the difference in means between Tinder users and non-users is 0. The t-test generated statistically-insignificant p-value of 0.085. This indicates that Tinder users and non-users showed no statistical difference in the frequency of checking privacy settings on their social media sites.

When asked "What does privacy mean to you?", ~80.2% of respondents equated privacy to having control over personal information. Around 7.2% of people said that privacy is important, 5.4% indicated that they were confused by the question, 2.7% said privacy doesn't exist, and 2.7% said that privacy means having control over personal information but achieving privacy a futile goal. These responses indicate that most people consider privacy desirable. However, with regard to privacy practices on social media, few people exhibit their privacy concerns when choosing dating applications or managing their social media accounts. As seen earlier, only 3 respondents indicated privacy concerns as a detracting factor from using Tinder.

4. CONCLUSIONS

Through our two-part exploration of dating site privacy tendencies, we discovered that user's opinions on privacy have very little to do with their privacy habits in practice. A user's reported interest in privacy had no bearing on their actual privacy practices. This held true for both dating site users and dating site non-users. This finding provides support for the privacy paradox phenomenon – in which a user's privacy beliefs in hypothetical or abstract scenarios is unable to be used to predict actual behaviors [1]. While those surveyed were largely of the opinion that privacy was to be prized, an alarming percentage did not reflect this in their reported privacy maintenance habits. In fact, about 20% of respondents said they had never checked their privacy settings.

Our study also reflected interesting findings on the tendencies of Tinder users in particular. Our survey participants who responded in the affirmative to our question "Do you use Tinder?" were then asked what information could be gathered on them based on their presence on the app. Many respondents correctly assumed that their Facebook profiles would likely be easy to link to their Tinder profile. However, very few users mentioned the idea of other online profiles being linked to their Tinder profiles. This tendency shows that while Tinder users are aware of Tinder's connection to Facebook, they are seemingly unaware of the idea of a linkage attack. This does not reflect the reality of our findings in our re-identification results, since information gathered on an individual was not limited to that which could be found on a Facebook profile. In the files assembled on each of the members of our sample population, information gathered also extended to other social media sites, as well as personal details gathered from a multitude of other online and publicly available sources.

5. ACKNOWLEDGMENTS

Our thanks to our professor Darakhshan Mir who advised us throughout our research.

6. REFERENCES

[1] Acquisiti, A. and R. Gross. "Information Revelation and Privacy in Online Social Networks." In pre-proceedings version. ACM Workshop on Privacy in the Electronic Society (WPES), 2005. http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf.

[2] McRae, Brent, and Jessica McKnight. "Privacy and Online Dating." *Convenient or Invasive: The Information Age*. By Adam Barreras, Kai R. Larsen, and Zoya A. Vronovich. Boulder, CO: Ethica, 2007. http://www.ethicapublishing.com/inconvenientorinvasive/2CH13.pdf.

[3] Woodruff Et Al. "Would a Privacy Fundamentalist Sell Their DNA for $1000... If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences." *Usenix Association* (2014). Tenth Symposium On Usable Privacy and Security. https://www.usenix.org/system/files/conference/soups2014/soups14-paper-woodruff.pdf.