ISSN: 2167-1508
v11 n 4823

Privacy and Security Issues Associated with Mobile Dating Applications

Dr. Darren R. Hayes
dhayes@pace.edu
Pace University
Sapienza Università di Roma

Christopher Snow
csnow@pace.edu
Pace University
New York, NY

Abstract

Mobile dating application (app) usage has grown exponentially, while becoming more effective at connecting people romantically. Given the sensitive nature of the information users are required to provide, to effectively match a couple, our research sought to understand if app permissions and privacy policies were enough for a user to adequately determine the amount of personal information being collected and shared. Based on a static and dynamic analysis of three popular dating apps for Android and iPhone, our conclusion is that dating app developers are collecting and sharing personal information that extends well beyond publicly stated privacy policies, which tend to be vague at best. Furthermore, the security protocols, utilized by dating app developers, could be deemed relatively inadequate, thereby posing potential risk to both consumers and organizations. While social media companies have been the primary focus for discussions surrounding the implementation of the General Data Protection Regulation (GDPR) in the European Union, our research findings indicate that third-party analytical companies and big data gatherers need to be more closely examined for potential violations.

Keywords: GDPR, Privacy, Mobile Advertising, Big Data, Mobile Forensics, Android

1. INTRODUCTION

There were 3.6 million applications (“apps”) on Google Play and 2.1 million iOS applications on Apple’s App Store in 2017 and a mere 8.5% of those apps were cross-platform, meaning that they were available for both iOS and Android (App store Insights from Appfigures, 2018). Adults in the United States are using mobile devices in ways that could not be imagined just 15 years ago. According to Pew Research Center’s report on mobile dating, 15% of adults (ages 18 and older), in the United States, reported they have used online dating sites or mobile dating apps. Dating site usage has nearly tripled for young adults (18 through 24) in just two years, from 10% to 27% (Smith and Anderson, 2016). Therefore, it is important for individuals to clearly understand the potential security risks and privacy issues associated with dating apps. Moreover, the prevalence of social engineering, using data derived from social media accounts, means that dating apps are a cause for concern in terms of organizational risk, as this paper will later highlight.

Mobile dating applications for the iPhone and iPad are referred to as iOS apps and they can be downloaded by users, with an Apple iTunes account, from the Apple Store. Similarly, Android users, with a Google account, can download these apps to a smartphone or

Android tablet, from the Google Play Store. During app installation, the customer enters her personal information and selects what permissions that the user will allow; for example, permit the app to track the user's location (WiFi, cell towers, GPS) or perhaps allow the app to connect to the Internet.

During app installation, a SQLite database will be installed on the user device. This is a relational database that is comprised of tables. The data stored in these tables may or may not be encrypted. A table may contain a user's contacts, while a related table may store communications with contacts, for example. It is important to understand that these databases contain an extraordinary amount of personal information and, when unencrypted, may put an individual at risk for social engineering. Conversely, while this study found that the data stored in these databases is unencrypted, for the most part, this finding is advantageous for criminal investigators, who may find relevant evidence on the user device and may not need to subpoena a third-party service provider for evidence.

The General Data Protection Regulation (GDPR) was enacted in the European Union (EU) in May 2018. While GDPR is an EU law, any company that maintains the personal records of EU citizens is impacted, regardless of whether the company is American or the company maintains their operations within the USA. Any entity that processes or controls the records of an EU citizen, including cloud services, is subject to GDPR. Thus, it can be inferred that the producer of a dating app, and third-party analytics companies, associated with that dating app, are subject to GDPR. As you will later note, our research findings raise many concerns in terms of potential GDPR violations.

With the recent increase in online match-making connections, in a post-Snowden era where privacy has become a major concern, one must questions whether these dating applications are utilizing personal data ethically. For example, in March 2018, a security flaw in the Grindr app disclosed user location data, which could have exposed app users to harassment (Latimer, 2018); Grindr is a dating app, primarily used to connect gay men. Therefore, the research question we address in this paper is: Do dating applications pose a security threat or raise concerns about user privacy?

2. BACKGROUND

Concerns about data collection by app developers and associated third-parties, beyond what is stated in the privacy policy, continue to grow. Generally, there are potential security risks associated with third-party geolocation requests from apps (Liu et al., 2017), while many apps connect to known malware server domains (Vigneri et al., 2015). Consumers are concerned about how mobile apps are collecting personal information, as reported in a recent study (Wijesekera et al., 2015). Companies collect vast amounts of analytics from mobile apps and their users for performance metrics, marketing purposes and potential revenue-generating opportunities. It is abundantly clear that Big Data is tremendously lucrative for companies and, therefore, apps will continue to collect large quantities of data (Jang and Kwak, 2015; Erevelles et al., 2016). In addition to the value of Big Data, which compels companies to collect more information from apps, than disclaimed in their privacy policies, another potential risk for individuals is the appropriation of data through malware (Wijesekera et al., 2015). The potential for the leakage of personal information, through mobile apps, implies that the risk for social engineering individuals exists (Abraham and Chengalur-Smith, 2010; Krombholz et al., 2015; Mouton et al., 2016; Hayes and Cappa, 2018). Moreover, corporations continue to be at risk of cyber-attack.

The research herein contributes to the existing academic literature by analyzing the privacy issues associated with mobile apps (Jain and Shanbhag, 2012; Yun, 2013; Vigneri et al., 2015; Snow et al., 2016; Wang et al., 2016) and highlights the potentially unethical behavior of some app development companies that collect invasive personal data and subsequently derive value from that data. Using a combination of static and dynamic analyses of mobile dating apps, we uncovered a number of threats to organizational security. Our research focuses on apps that are commonly used by millennials (Generation Y). A thorough analysis of the three mobile apps identified how analytics (Big Data) companies are collecting vast quantities of data about users, beyond individual consent, which in turn increases organizational risk, primarily through social engineering and also with the potential for data breaches. Broadly speaking, these research findings could also extend to national security, as highlighted in a recent article about how fitness apps can be used to track military personnel and identify military bases (Sly et al., 2018).

3. RELATED WORK

The research group at Pace University previously published research that detailed how geolocation information, from mobile apps, could theoretically be used by governments to track users in an article entitled "Leakage of Geolocation Data by Mobile Ad Networks" (Snow, Hayes, Dwyer, 2016). More specifically, this research focused on the claims of the NSA whistleblower, Edward Snowden, who declared that mobile apps are collecting and sending data, about the user, without her knowledge; data including but not limited to: current and previous locations in longitude and latitude, age, name, and email. In addition, recent research by the same team uncovered how Uber tracks user location in ways that contradict their privacy policies (Hayes et al., 2018).

Recent research published in arXiv and entitled "Privacy Risks in Mobile Dating Apps" (2015) analyzed nine dating applications, using mobile forensics tools, and were able to find Facebook tokens, full plain-text conversational messages, and private images that the user never received (Farnden, Martini, Choo, 2015). A similar research paper, entitled "Playing Hide and Seek with Mobile Dating Applications", was presented at the *International Information Security Conference*. This research identified how hackers can exploit data collected by dating applications. The research explored bad actors spoofing their location and chatting with users on dating applications in an effort to socially engineer people into revealing their true location, thereby creating the potential for cyber-stalking (Qin, Patsakis, Bouroche, 2014).

4. METHODOLOGY

Our experimental research involved two phases of analysis: (1) a static and dynamic analysis of the mobile app and (2) a review of the app developer's publicly available privacy policy. A static analysis is focused on a review of (a) the application code and (b) the corresponding SQLite database. The privacy policies that were examined were retrieved from (a) the developer's Website and (b) the end-user license agreement (EULA) displayed at time of installation.

The mobile applications, selected for this case study research, were as follows: Tinder, Bumble, and Grindr. The rationale for selecting these apps was the popularity of these apps, in terms of downloads, in the USA. Our selection was also based on dating apps that were cross-platform (iOS and Android). Moreover, Grindr has recently come under fire in Europe for its sharing practices of very personal user data (Lomas, 2018). It is understood that dating applications need to collect personal details that users are prepared to share with others. The Apple Store provides a ranking for each application based on a particular category. Tinder and Bumble are ranked #1 and #4 under the "Lifestyle" category respectively, while Grindr ranks #57 under "Social Networking", which is a more competitive category. Each of these dating applications maintains partnerships and information sharing with social media services. This practice of sharing between apps has become increasingly popular and is referred to as "deep linking"; a mobile app seamlessly links with another app or with a Web browser. Again, the three mobile apps are cross-platform, i.e. available for both iOS (iPhone/iPad) and Android mobile devices.

Tinder and Bumble have similar features and functionality, whereby people within close proximity of each other are revealed to the user. The user can then either swipe right or left depending on whether they want to connect with a person (swipe right) or dismiss a displayed profile (swipe left). A match is made when both individuals indicate that they want to meet, i.e. both swiped right on each other's profile. However, on Bumble, conversations only begin when a woman initiates a conversation. Both Tinder and Bumble applications are inclusive of same-sex matches. Grindr, on the other hand, is a men-only application that shows a list of people in close proximity to the user; chat can be initiated regardless of whether a match is made.

Experimental Process

Our analysis involved (a) reverse-engineering the code encapsulated in the mobile application for both iOS and for Android (b) a review of the application SQLite database, including its structure and content and (c) an analysis of the application's HTTP requests. The rationale for reverse-engineering the code was to identify the permissions that the application sought to establish and then subsequently identify if any of these permissions potentially violated the application developer's privacy policy. Furthermore, we sought to assess if any of the requested permissions were moderate to high risk, thereby posing a threat to the individual and their respective organization. Our static analysis included a review of the Android application package (APK) file. This code review displayed the app manifest, which included the app permissions. An app manifest can include location-tracking permissions based on cell sites (cell towers) or user location based on proximity to access points (WiFi hotspots). Moreover, a manifest can include permissions that extend to activation of the user's device microphone or potentially manipulate files on a computer that the mobile device synchronizes to through a USB connection. There are numerous tools available for examining the code in an APK, including dex2jar and FileViewer Plus. During our analysis, we chose to use an online APK decompiler application (Java Decompilers, 2018) and BlackLight (BlackBag Technologies). The rationale for selecting these tools is that they are trusted; the APK decompiler allows APK uploads directly to the Website, without downloading any potentially harmful software while BlackLight is a highly reputable digital forensics tool.

Our static analysis included a review of the mobile app's SQLite database using both the APK decompiler and the BlackLight software. Virtually every mobile app, on a smartphone or tablet, stores information in a relational (SQLite) database. Each database is comprised of tables that are linked with a primary and foreign key. Each table has rows and columns – similar to Microsoft Excel. As mentioned, all tables in the SQLite database are linked by a key, as is the case with any relational database, to maintain referential integrity. Ultimately, it is up to the developer what information, contained in each table of the SQLite database, should be encrypted. All information in these tables should be encrypted: (1) on the device, (2) during transmission and (3) at rest on the company's server, to protect the user. The experimental research we performed concluded that this critical component of information security, i.e. encryption, is not being followed by app developers in most cases, which puts both the user and organizations at risk.

Privacy Policy Analysis

Under U.S. law, there is no single federal privacy law that requires companies to maintain a privacy law on their Website. Nevertheless, there are state and federal laws, like the Consumer Credit Reporting Control Act or the CalOPPA (California Online Privacy Protection Act), that imply that companies should provide a written privacy policy about the collection and sharing of personally identifiable information (PII) with third-parties. Apart from personal healthcare information, which is protected under HIPAA (Health Insurance Portability and Accountability Act), consumers are extremely limited in preventing PII from being shared with third-parties. Therefore, we judiciously examined the privacy policies of the three dating apps to identify whether they properly disclose all of the PII that they collect and share.

5. APPLICATION FINDINGS

In this section we report the findings of the static and dynamic analyses conducted on each of the three apps examined. Our research findings clearly indicate that each of these dating apps expose individuals to some type of privacy risk that could not be determined from a review of the app developer's privacy policy.

Tinder

The Tinder app utilizes a customer's location to determine potential matches within the vicinity of the user. However, the app stores location information for the user locally on the device and in plaintext. Tags referring to ZLASTVIIST TIMESTAMP, ZLATITUDE FLOAT, and ZLATITUDE FLOAT were all found within the app's SQLite database. We expected to see to see these tags because a user must opt-in to locational services permissions to enable the app to identify potential matches in close proximity.

The Tinder app utilizes deep-linking to connect to the Spotify and Facebook applications if installed on the user device. We observed this connection, during our static analysis of the Tinder app SQLite database, which contained the Spotify user ID and Spotify playlist. We ascertained that Tinder utilizes a user's music playlist, from Spotify, to improve its algorithm, which enhances match-making. Figure 1 displays the link to Facebook, while the in-app browser opens and requests the user's link verification. That message briefly describes what information Tinder will receive and it allows the user to edit that information. However, information about how Tinder is using and distributing this shared data is unavailable. Information about deep-linking is unavailable within the company's privacy policy. This is perhaps a concern for the user and how they are being profiled by Tinder.

The Tinder app also uses Taplytics, a mobile app analytics company (Taplytics Inc., 2018). Within Tinder's Taplytics SQLite database we identified the following personal information for the user: birthday, city, country, county, data provider, gender, language, location radius, device model, iOS version, UID and age. Interestingly, we determined that this information could only have been derived from the user's Facebook account because it is not information obtained directly from the user; the Facebook app was installed on the iPhone used in our experimentation. Once again, this personal identifiable information (PII) is not disclosed in the company's privacy policy. Information from user social media accounts is also being captured within the Tinder app, which should be a concern for Tinder subscribers, especially given that all of this information is being shared with third-party providers.

Moreover, throughout Tinder's SQLite databases, there are lines referring to a Crashlytics key. Much like Taplytics, Crashlytics is hugely popular with developers seeking performance data analytics. The tool is often integrated into applications to allow developers to improve app performance and determine how users are navigating through their application. An example of a Crashlytics key can be seen below.

```
<key>com.crashlytics.iuuid</key>
<string>90400EEE-8809-4146-B11B-
83FB6FD022B0</strong>
```

Figure 2 shows how Tinder saves user messages in plaintext. This sample conversation includes an incoming message that says "Hello Chris," i.e. the name of the user. Interestingly, the SQLite database does not save the user responses and only incoming messages. The Tinder2.SQLite database maintains links to images of each match uploaded to the domain "images-ssl.gotinder.com". These links are saved in plaintext and beneath each of these are the incoming messages from that user. Therefore, Tinder locally stores the conversation of each match and also all of their profile photos. We should note that the domain "images-ssl.gotinder.com" does use the "secure socket layer" security protocol which indicates that this information is encrypted during transmission across the Internet.

An analysis of the HTTP connections, during application execution, indicated that all communications are encrypted using TLS/HTTPS. The packet-capture tool, Debookee, was unable to decrypt the wireless communications between Tinder and many other companies, which included AppsFlyer, a marketing analytics provider. This analytics company could not be found in our static analysis of the SQLite database. Figure 3 displays the numerous DNS connections initiated by Tinder. Although the TLS protocol is not impervious, our analysis indicated that a man-in-the-middle (MITM) attack would be difficult.

Bumble

During our static analysis of the Bumble app, we tracked multiple connections to outside companies, including Microsoft, Google, Badoo, and Facebook. Like Tinder, we can infer that many of these server connections are used to provide analytical user data to developers or perhaps serve up mobile advertisements to the user. Specifically, we observed that server connections are made to AppsFlyer and HockeyApp (by Microsoft). Both services are described, on their homepages, as traffic analyzers that provide developers with data on crashes, incoming traffic sources, and other data that will assist developers enhance performance based on user data. We can assume that both of these services are very similar to the Crashlytics and Taplytics services associated with Tinder.

We analyzed the Bumble SQLite database with BlackLight. This static forensic analysis revealed that user profile photos are saved on Bumble's server yet they are accessible through unencrypted links on the user device. Bumble essentially saves data from profiles viewed by the user in addition to the user's own profile. Figure 4 displays the user profile "Krista", whom is from Newark, New Jersey and Krista has multiple photos that were uploaded to Bumble's domain "bumbcdn.com". These photos are accessible on the Web using the same type of links uncovered in Tinder's SQLite database. Figure 4 also indicates that the URLs for the photos are assigned a key on the Bumble server where their photos are uploaded. Therefore, each image's URL contains a key, like "1346904409". This key also appears on the "encounters:" line.

We ran the Bumble app for approximately five minutes while Debookee captured HTTP requests. Unlike Tinder, Bumble initiatives fewer server connections per second. Figure 5 displays Bumble's the HTTP requests captured in the space of approximately five minutes; we can clearly see fewer requests recorded by Debookee. Unlike Tinder, Bumble is surprisingly quiet in terms of server requests compared to other apps. Moreover, all of the server connections we expected to see, based on our static analysis of the SQLite database, were visible: Badoo, AppsFlyer and Facebook.

Grindr

A forensic analysis of the Grindr iOS application, using BlackLight, did not yield any personal information about the user. The only available data were application assets such as connections with ad networks and in-app graphics. However, an analysis of the HTTP requests made during execution of Grindr application yielded more interesting results. Figure 6 displays the numerous secure server connections were made. Interestingly, there were connections to Smaato and Octopus-X (not pictured) that were unsecured (unencrypted) communications.

Upon further analysis, we determined that Smaato and Octopus-X describe themselves as a service for developers that can monetize use of an application. In other words, they are companies that tailor advertising for the user. Snippets of both HTTP requests are seen below in Tables 2 and 3 (certain lines were redacted for privacy).

```
http://soma.smaato.net/oapi/reqAd.jsp?adspace
=130000706&[…]&gender=m
&iosadid=***1920-****-47F9-**4F-
2D40****5940&iosadtracking=true&fcid=630
7****-9F07-4033-871A-
4D1B9843F077&countrycode=US&country
=United+States&region=NY&city=New+Yo
rk&zip=10032&connection=wifi&coppa=0&b
eacon=true&mraidver=2&apiver=503&client=sd
kios_8-2-
3&extensions=moat&mediationversion=2&devic
emodel=iPhone9%2C2&devicebrand=Apple&devi
cetype=0&carriercode=311480&osversion=11.
3.1&carrier=Verizon[…]&bundle-for-
tq=com.grindrguy.grindrx&response=JSON
```

Table 2. Smaato HTTP request

```
http://rtb.octopus-
x.com/t/ev?app_key=7f0c0025028dc7e56e0f77
3c32078c0b&idfa=D42F1920-24A0-47F9-
A14F-
2D406B855940&strategy_name=adx_cpm&ts
=1528773641&id=7_539936325&ip=**.174.*
*.80&country=US&[…]creative_id=7_5399363
25&redir_url=https%3A%2F%2Ftracking.octo
pus-x.com%2Fcpc%2Fshow%3Fid%
3D7_539936325%26country%3DUS%26oid%3D
130000706%26strategy_name%3Dadx_cpm%2
6gaid%3D%26idfa%3DD42F1920-24A0-47F9-
A14F-[…] %3D0%26agency%3Dopenx&
type=1&pub_type=app&os=IOS
```

Table 3. Octopus-X HTTP request

In the Smaato request, we observed accurate locational information and personal information, including the device owner’s gender and type of smartphone. The locational information is most likely available because the Grindr app has access to user location, while it searches for nearby users. In the Octopus-X request, the most alarming piece of information is the IP address that was included in the (unencrypted) request. Both requests infer that user advertising tracking is enabled and there is a key unique to the user. It is clearly evident that these requests came from the advertiser, which is displayed in Figure 7.

In the Grindr privacy policy, they do disclose that advertisers use their own cookies and other tracking technologies that collect information from Grinder users. Their privacy policy also indicates that they may not have control over what personal information these advertisers collect. Grindr’s privacy policy discloses MoPub as one of their sanctioned advertisers and also provides links to MoPub’s privacy policy. However, during our analysis, we did not find any HTTP requests associated with MoPub (Grindr, 2018).

6. CONCLUSIONS

While many developers integrate some type of analytic reporting or advertising system into their applications, it is interesting to see that the information collected by these third-parties is not disclosed. It is understandable that a developer wants to determine the identity and location of their users and also gain feedback about the app user experience. We know from the unencrypted communications performed by Smaato and Octopus-X that these companies can take advantage of an app’s permissions – particularly permissions related to location. However, it is not clear from our app analysis whether or not the user is aware that their information is being shared with both the app developer and also numerous analytics and advertising providers. We also know from previous experiments performed in “Leakage of Geolocation Data by Mobile Ad Networks” (Snow, Hayes, Dwyer, 2016) that assigning a key to a user does not prevent users from being personally identified. From a forensic investigator’s perspective, it would be fairly easy to comprehensively profile a user of a dating app using the aforementioned static and dynamic analysis tools. Therefore, it can be argued that user data is being shared well beyond what is outlined in their stated privacy policy.

The data collected by third-party companies, like Crashanalytics and Taplytics, can be compared to data collection techniques on the Web where cookies from companies, like Google Analytics, are used to track Website visitors. However, the difference with Web tracking is that users have a choice of Web browsers, including those that provide plug-in tools that limit user tracking. Traditional Internet users are becoming more aware that their information is being used to provide a "tailored" Web browsing experience, which in turn raises privacy concerns for many users. It can be argued that users should always have control over their data and data being shared with third-party companies; even if it means sacrificing a more personalized experience. In terms of dating applications, it could be argued that a user should be able to opt-out of certain third-party tracking services. In 2018, the European Union implemented the General Data Protection Regulation (GDPR). However, the primary focus of GDPR compliance has been on traditional Websites but the research herein clearly shows that PII being captured and shared by mobile app developers should be more closely monitored for non-compliance.

Our experimental findings also show how deep-linking, between the dating applications and other applications, like social media services, is not clearly disclosed to the app user. Facebook has attempted to inform the user about exactly what type of information is requested from an application containing deep-links. Other services could improve their disclosure about deep-link connections, the connected services and the type of user data being shared. In the case of Tinder, what user data from their Facebook friends list and interests are being culled and how that data is being used. In terms of privacy policies, disclosing information sharing with Facebook is a grey area. It can be assumed that application developers believe that the use of personal information, by Facebook, does not need to be explicitly outlined since the user has to manually opt-in, view the information being used, and agree to the terms of service before a connection is made; an example can be viewed in Figure 1. Nevertheless, companies should be required to disclose how their personal information is being used and shared. Of the applications researched, Bumble was the only company to disclose specifics about how Facebook data is used to "see current location, display mutual friends with matches, provide photos to matches," and more (Bumble, 2018). Grindr and Tinder make a generalized blanket statement that "Facebook information will be shared with us" (Tinder, 2018; Grindr, 2018). As far as observing Facebook data, where Facebook was not authorized to do so, it is possible that advertising agencies assigned a key to the device analyzed and data was pulled from other applications where Facebook was authorized and stored with that key.

7. IMPORTANCE OF RESEARCH

The findings, presented in this paper, clearly illustrate how location tracking and the collection of PII are more extensive and invasive than a public privacy policy discloses. Furthermore, privacy policies and app permission requests are poor indicators of how safe an app is in terms of information sharing. These findings may raise concerns for smartphone users and also for many companies. Mobile app should be a consideration for organizational security and IT risk. One can no longer trust a privacy policy to determine if a user's data is being protected. Additionally, our findings should imply that privacy and security are very different concerns; encryption of PII and PII sharing are completely different concepts. With all of the analytic and advertising companies found in just a few dating applications, it is impossible for a company to state that user privacy is being protected when the company themselves cannot be entirely sure that the integration of analytics keeps their user's data safe. Additionally, it is not clear when a user allows an application to use location services how third-parties with take advantage of that authorization. In the example of Bumble, a potential bad actor could hack into their servers and navigate to user "1346904409" where they will not only determine the user's name is "Krista" but also be able to find photos related to her and learn that she is from New Jersey. Privacy protection does not mean assigning a non-personally identifiable number to a user, it should also mean ensuring that bad actors cannot potentially steal the records of an entire user database to learn more about them. Our recommendation is that data on the user device and on the Bumble servers should be encrypted.

We know that Smaato and Octopus-X are services that facilitate application developers to easily deliver advertising to their users in an effort to monetize their free application. However, those same developers may not fully comprehend the security protocols utilized by the services that they are connecting to. Reasons for connecting with a service can range from ease of use to the promise of a bigger payout. It is unclear why application developers would not use a service that they know is secure and reputable, like Google Ads. However, many advertising services collect personal information to identify user interests, while no advertising agency is inherently "safe."

Application developers should understand the importance of data encryption – at rest and in transit. There is always the risk of a man-in-the-middle attacks. During our experiments, the app data that we collected was via HTTP protocols. Application developers should be utilizing the more secure HTTPS transmission protocol to all of their Web-connected communications. Like advertising, it is unclear why developers do not inherently choose HTTPS when deciding to connect their application to the Web as there are free options or low-cost annual certificate subscriptions using trusted domains.

It appears that Apple understands the privacy concerns of consumers, who can be frustrated with developers and advertisers gaining access to personal information that was not explicitly requested. Over the past 3 years, Apple has implemented changes to iOS app developer rules; users now have the ability to limit ad tracking, disable the sharing of analytical data to developers, and even view the information that has been collected by ad networks. Apple may push developers to permit users to limit the sharing of even more personal information. Interestingly, Apple still has no requirement for developers to encrypt PII saved on the user device. One could argue that Apple should consider forcing developers to encrypt PII.

The research presented in this paper may educate individuals and organizations about how developers are collecting PII and sharing this information with third-parties, regardless of the app permission options selected by the user. With the recent controversy, involving Facebook and Cambridge Analytica, companies, and individuals, should be more cautious about the mobile applications that they install.

REFERENCES

Abraham, S., Chengalur-Smith, I. (2010) An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, 32, 183–196.

App store Insights from Appfigures. 2018. Consultado 28 Apr. 2018. Disponible en https://blog.appfigures.com/ios-developers-ship-less-apps-for-first-time/ (appfigures).

Bumble Privacy Policy. (2018, May 24). Retreived from https://bumble.com/privacy

Farnden, J., Martini, B., & Choo, K. K. R. (2015). Privacy risks in mobile dating apps. *arXiv preprint arXiv:1505.02906*.

Grindr Privacy Policy. (n.d.). Retrieved from https://www.grindr.com/privacy-policy

Hayes, D., Cappa, F. (2018) Open Source Intelligence for Risk Assessment. *Business Horizons*, In Press, .

Hayes, D., Snow, C., Altuwayjiri, S. (2018) A Dynamic and Static Analysis of the Uber Mobile Application from a Privacy Perspective. *Journal of information systems applied research.*, 11, 11–22.

Jang, Y.-J., Kwak, J. (2015) Digital forensics investigation methodology applicable for social network services. *Multimedia Tools and Applications*, 74, 5029–5040.

Java Decompilers. 2018. Decompilers Online. Disponible en www.javadecompilers.com/apk

Krombholz, K., Hobel, H., Huber, M., Weippl, E. (2015) Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113–122.

Latimer, B. (2018, Mar 28). Grindr security flaw exposes users' location data. *NBC Universal*. Retrieved from https://www.nbcnews.com/feature/nbc-out/security-flaws-gay-dating-app-grindr-expose-users-location-data-n858446

Lomas, N. (2018, April 05). Grindr hit with privacy complaint in Europe over sharing user data. Retrieved from https://techcrunch.com/2018/04/03/grindr-hit-with-privacy-complaint-in-europe-over-sharing-user-data/

Qin, G., Patsakis, C., & Bouroche, M. (2014, June). Playing hide and seek with mobile dating applications. In *IFIP International Information Security Conference* (pp. 185-196). Springer, Berlin, Heidelberg.

Shackelford, S.J. (2012) Should your firm invest in cyber risk insurance? *Business Horizons*, 55, 349–356.

Smith, A., & Anderson, M. (2016, February 29). 5 facts about online dating. Retrieved June 11, 2018, from http://www.pewresearch.org/fact-tank/2016/02/29/5-facts-about-online-dating/#

Snow, C., Hayes, D., Dwyner, C. (2016) Leakage of Geolocation Data by Mobile Ad Networks.

Journal of Information Systems Applied Research, 9, 24–33.

Taplytics Inc. 2018. Taplytics. Disponible en https://taplytics.com/what-is-taplytics

Thurm, S., Kane, Y.I. (2010) Your Apps Are Watching You. *The Wall Street Journal*, 2010.

Tinder. 2018. Consultado 29 Apr. 2018. Disponible en https://tinder.com/?lang=it

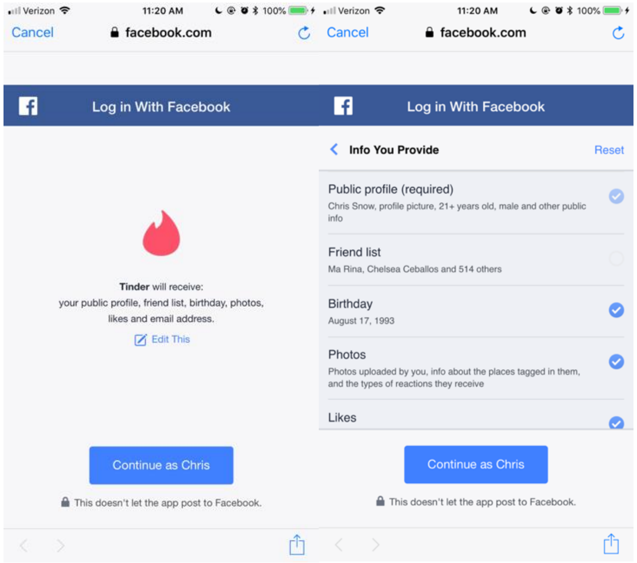
Taming the Android appstore: Lightweight characterization of Android applications (2015, s.l.). 2015. Ed. Vigneri, L., Chandrashekar, J., Pefkianakis, I., Heen, O. s.l.,

Tinder Privacy Policy. (2018, May 25). Retrieved from https://www.gotinder.com/privacy

Wang, T., Duong, T.D., Chen, C.C. (2016) Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, 36, 531–542.

Yun, H. (2013) Understanding the use of location-based service applications : Do privacy concerns matter ? *Journal of Electronic Commerce Research*, 14, 215–230.

Appendix



Tinder will receive:
your public profile, friend list, birthday, photos, likes and email address.

This doesn't let the app post to Facebook.

Public profile (required)
Chris Snow, profile picture, 21+ years old, male and other public info

Friend list
Ma Rina, Chelsea Ceballos and 514 others

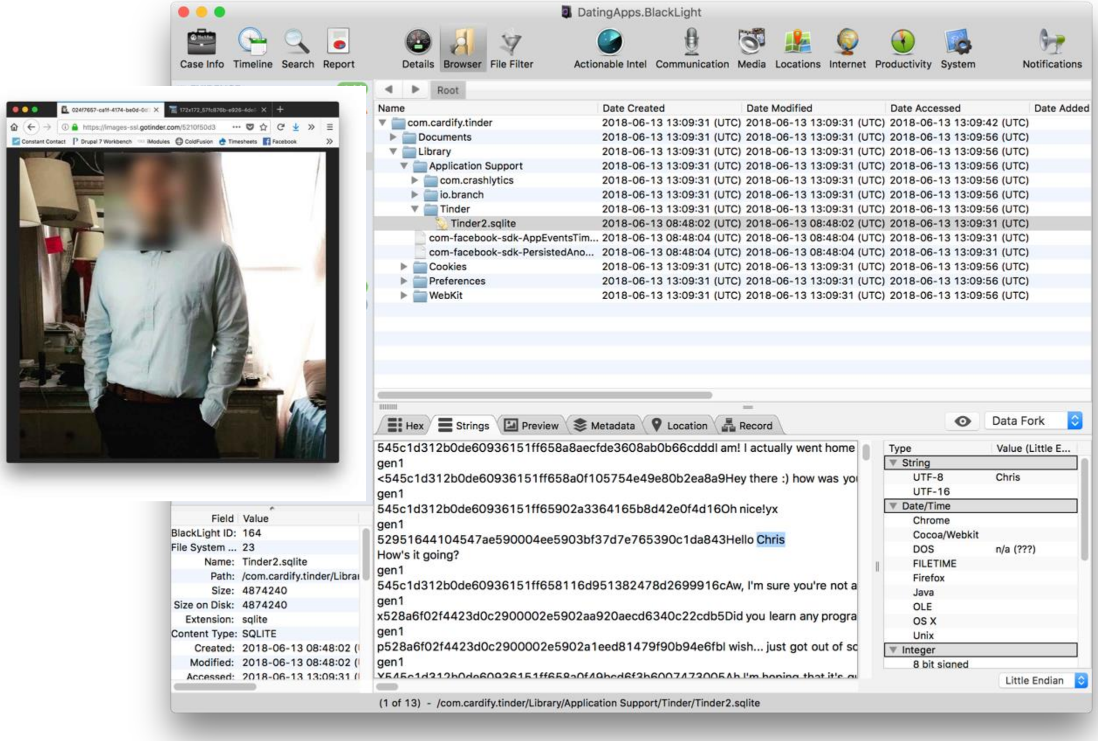
Birthday
August 17, 1993

Photos
Photos uploaded by you, info about the places tagged in them, and the types of reactions they receive

Likes

This doesn't let the app post to Facebook.

Figure 1 | Tinder Facebook Authorization



Name	Date Created	Date Modified	Date Accessed	Date Added
com.cardify.tinder	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:42 (UTC)	
Documents	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:56 (UTC)	
Library	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:56 (UTC)	
Application Support	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:56 (UTC)	
com.crashlytics	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:56 (UTC)	
io.branch	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:56 (UTC)	
Tinder	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:56 (UTC)	
Tinder2.sqlite	2018-06-13 08:48:02 (UTC)	2018-06-13 08:48:02 (UTC)	2018-06-13 13:09:31 (UTC)	
com-facebook-sdk-AppEventsTim...	2018-06-13 08:48:04 (UTC)	2018-06-13 08:48:04 (UTC)	2018-06-13 13:09:31 (UTC)	
com-facebook-sdk-PersistedAno...	2018-06-13 08:48:04 (UTC)	2018-06-13 08:48:04 (UTC)	2018-06-13 13:09:31 (UTC)	
Cookies	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:56 (UTC)	
Preferences	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:56 (UTC)	
WebKit	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:31 (UTC)	2018-06-13 13:09:56 (UTC)	

Field	Value
BlackLight ID:	164
File System ...	23
Name:	Tinder2.sqlite
Path:	/com.cardify.tinder/Librai
Size:	4874240
Size on Disk:	4874240
Extension:	sqlite
Content Type:	SQLITE
Created:	2018-06-13 08:48:02 (
Modified:	2018-06-13 08:48:02 (
Accessed:	2018-06-13 13:09:31 (

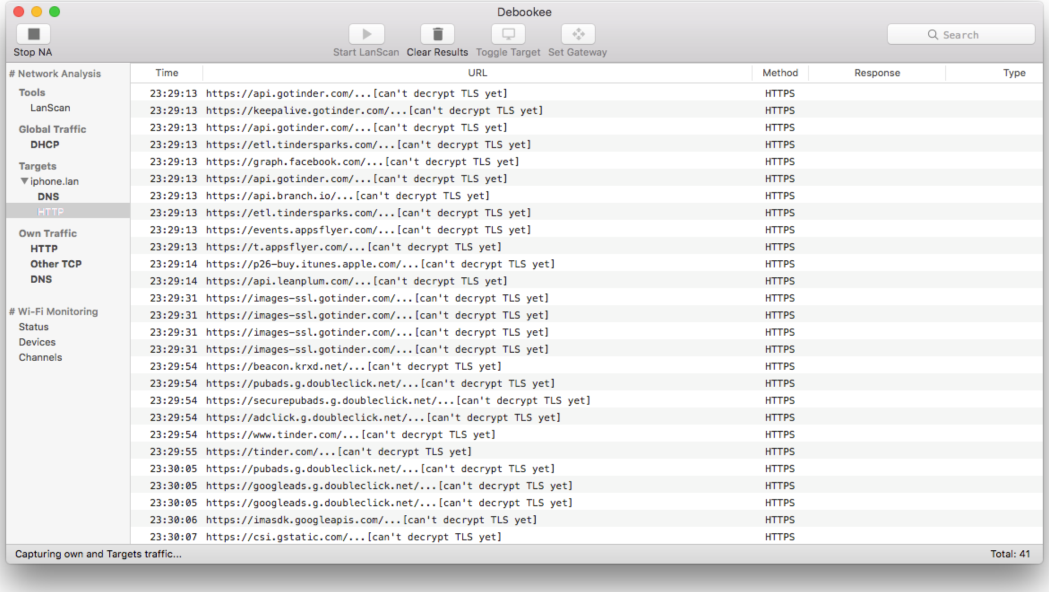
```
545c1d312b0de60936151ff658a8aecfde3608ab0b66cdddl am! I actually went home
gen1
<545c1d312b0de60936151ff658a0f105754e49e80b2ea8a9Hey there :) how was yo
gen1
545c1d312b0de60936151ff65902a3364165b8d42e0f4d16Oh nice!yx
gen1
52951644104547ae590004ee5903bf37d7e765390c1da843Hello Chris
How's it going?
gen1
545c1d312b0de60936151ff658116d951382478d2699916cAw, I'm sure you're not a
gen1
x528a6f02f4423d0c2900002e5902aa920aecd6340c22cdb5Did you learn any progra
gen1
p528a6f02f4423d0c2900002e5902a1eed81479f90b94e6fbl wish... just got out of sc
gen1
```

Type	Value (Little E...
String	
UTF-8	Chris
UTF-16	
Date/Time	
Chrome	
Cocoa/Webkit	
DOS	n/a (???)
FILETIME	
Firefox	
Java	
OLE	
OS X	
Unix	
Integer	
8 bit signed	

(1 of 13) - /com.cardify.tinder/Library/Application Support/Tinder/Tinder2.sqlite

Figure 2 | Tinder keeps plain-text conversations and links to images (blurred for privacy)

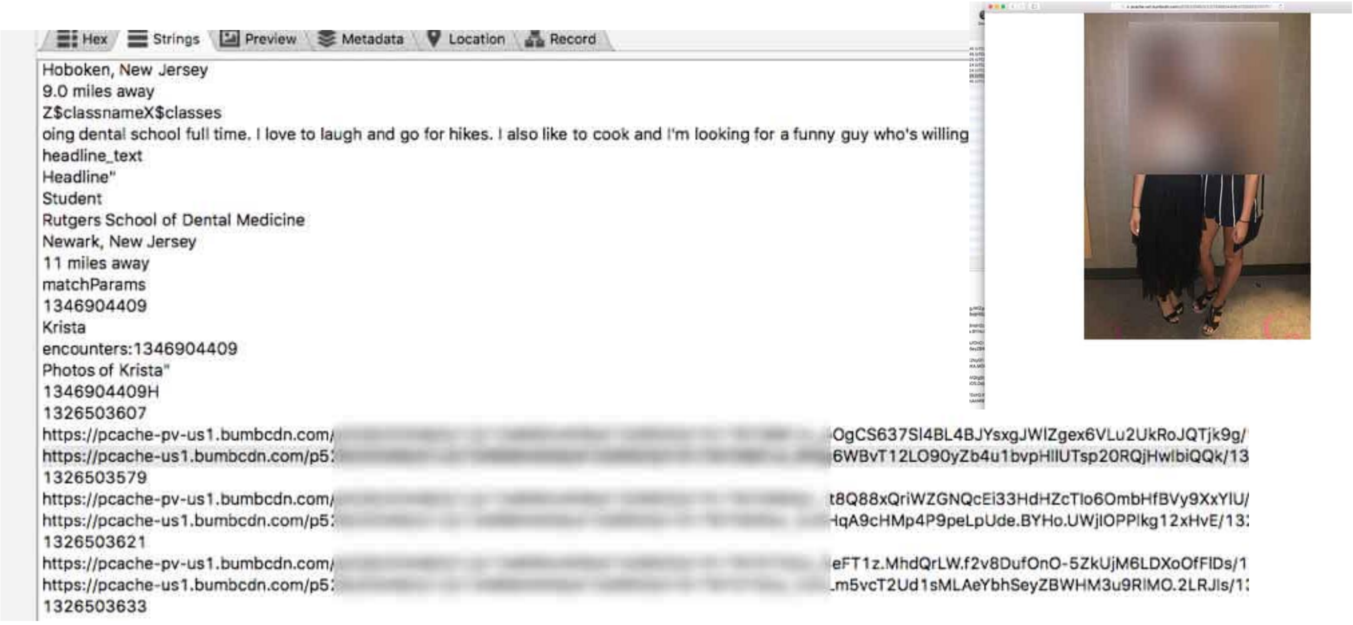
ISSN: 2167-1508
v11 n 4823



```
Time      URL                                                              Method   Response   Type
23:29:13  https://api.gotinder.com/...[can't decrypt TLS yet]               HTTPS
23:29:13  https://keepalive.gotinder.com/...[can't decrypt TLS yet]         HTTPS
23:29:13  https://api.gotinder.com/...[can't decrypt TLS yet]               HTTPS
23:29:13  https://etl.tindersparks.com/...[can't decrypt TLS yet]           HTTPS
23:29:13  https://graph.facebook.com/...[can't decrypt TLS yet]             HTTPS
23:29:13  https://api.gotinder.com/...[can't decrypt TLS yet]               HTTPS
23:29:13  https://api.branch.io/...[can't decrypt TLS yet]                  HTTPS
23:29:13  https://etl.tindersparks.com/...[can't decrypt TLS yet]           HTTPS
23:29:13  https://events.appsflyer.com/...[can't decrypt TLS yet]           HTTPS
23:29:13  https://t.appsflyer.com/...[can't decrypt TLS yet]                HTTPS
23:29:14  https://p26-buy.itunes.apple.com/...[can't decrypt TLS yet]       HTTPS
23:29:14  https://api.leanplum.com/...[can't decrypt TLS yet]               HTTPS
23:29:31  https://images-ssl.gotinder.com/...[can't decrypt TLS yet]        HTTPS
23:29:31  https://images-ssl.gotinder.com/...[can't decrypt TLS yet]        HTTPS
23:29:31  https://images-ssl.gotinder.com/...[can't decrypt TLS yet]        HTTPS
23:29:31  https://images-ssl.gotinder.com/...[can't decrypt TLS yet]        HTTPS
23:29:54  https://beacon.krxd.net/...[can't decrypt TLS yet]                HTTPS
23:29:54  https://pubads.g.doubleclick.net/...[can't decrypt TLS yet]       HTTPS
23:29:54  https://securepubads.g.doubleclick.net/...[can't decrypt TLS yet] HTTPS
23:29:54  https://adclick.g.doubleclick.net/...[can't decrypt TLS yet]      HTTPS
23:29:54  https://www.tinder.com/...[can't decrypt TLS yet]                 HTTPS
23:29:55  https://tinder.com/...[can't decrypt TLS yet]                     HTTPS
23:30:05  https://pubads.g.doubleclick.net/...[can't decrypt TLS yet]       HTTPS
23:30:05  https://googleads.g.doubleclick.net/...[can't decrypt TLS yet]    HTTPS
23:30:05  https://googleads.g.doubleclick.net/...[can't decrypt TLS yet]    HTTPS
23:30:06  https://imasdk.googleapis.com/...[can't decrypt TLS yet]          HTTPS
23:30:07  https://csi.gstatic.com/...[can't decrypt TLS yet]                HTTPS
```

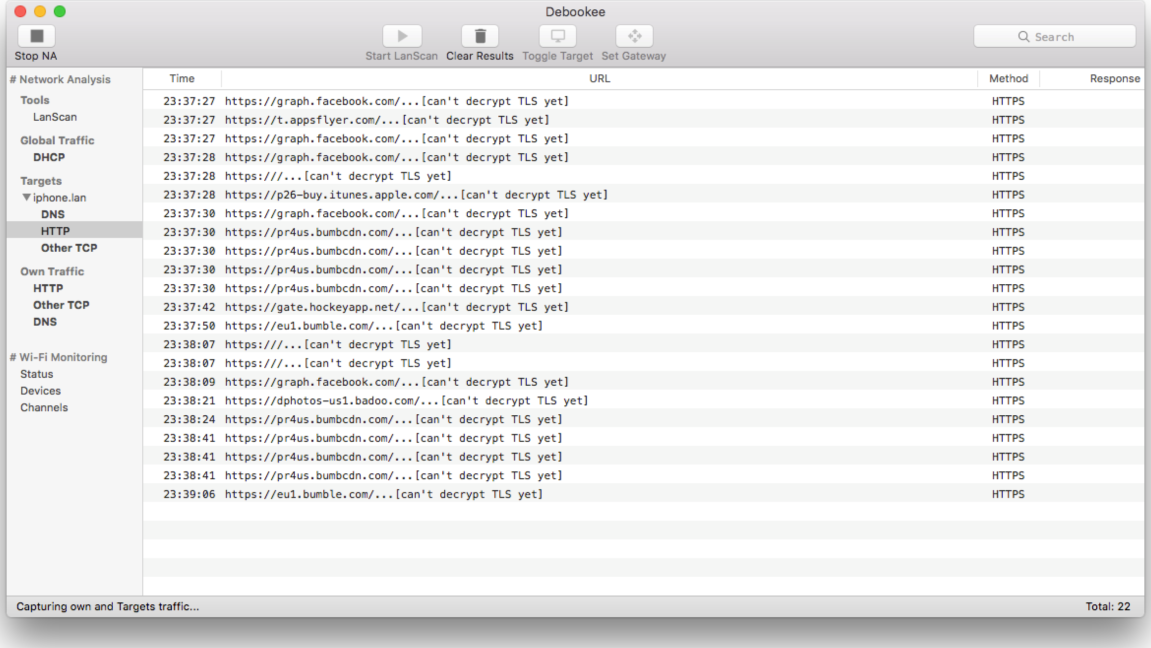
Capturing own and Targets traffic...   Total: 41

Figure 3 | Tinder's HTTP requests from Debookee



```
Hoboken, New Jersey
9.0 miles away
Z$classnameX$classes
oing dental school full time. I love to laugh and go for hikes. I also like to cook and I'm looking for a funny guy who's willing
headline_text
Headline"
Student
Rutgers School of Dental Medicine
Newark, New Jersey
11 miles away
matchParams
1346904409
Krista
encounters:1346904409
Photos of Krista"
1346904409H
1326503607
https://pcache-pv-us1.bumbcdn.com/[redacted]OgCS637SI4BL4BJYsxgJWlZgex6VLu2UkRoJQTjk9g/
https://pcache-us1.bumbcdn.com/p5[redacted]6WBvT12LO90yZb4u1bvpHllUTsp20RQjHwlbiQQk/13
1326503579
https://pcache-pv-us1.bumbcdn.com/[redacted]t8Q88xQriWZGNQcEi33HdHZcTlo6OmbHfBVy9XxYlU/
https://pcache-us1.bumbcdn.com/p5[redacted]HqA9cHMp4P9peLpUde.BYHo.UWjlOPPlkg12xHvE/13
1326503621
https://pcache-pv-us1.bumbcdn.com/[redacted]eFT1z.MhdQrLW.f2v8DufOnO-5ZkUjM6LDXoOfFIDs/1
https://pcache-us1.bumbcdn.com/p5[redacted]m5vcT2Ud1sMLAeYbhSeyZBWHM3u9RIMO.2LRJls/13
1326503633
```

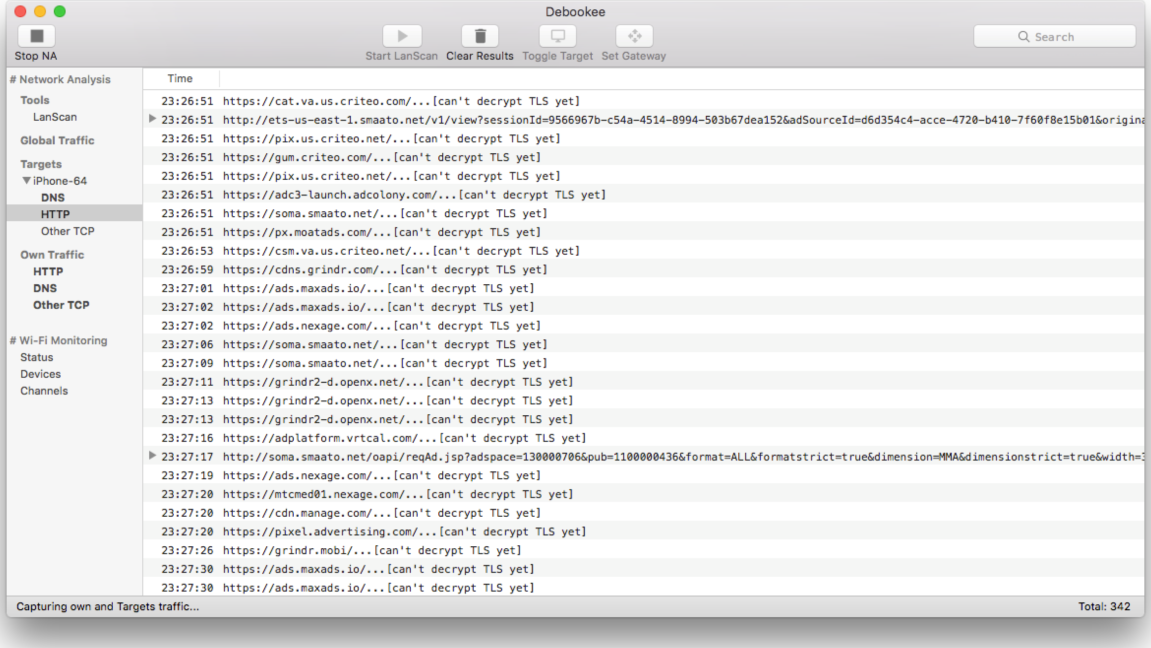
Figure 4 | User "Krista's" profile on Bumble with plain-text links to profile images



```
Time      URL                                                        Method   Response
23:37:27  https://graph.facebook.com/...[can't decrypt TLS yet]        HTTPS
23:37:27  https://t.appsflyer.com/...[can't decrypt TLS yet]           HTTPS
23:37:27  https://graph.facebook.com/...[can't decrypt TLS yet]        HTTPS
23:37:28  https://graph.facebook.com/...[can't decrypt TLS yet]        HTTPS
23:37:28  https:///...[can't decrypt TLS yet]                          HTTPS
23:37:28  https://p26-buy.itunes.apple.com/...[can't decrypt TLS yet]  HTTPS
23:37:30  https://graph.facebook.com/...[can't decrypt TLS yet]        HTTPS
23:37:30  https://pr4us.bumbcdn.com/...[can't decrypt TLS yet]         HTTPS
23:37:30  https://pr4us.bumbcdn.com/...[can't decrypt TLS yet]         HTTPS
23:37:30  https://pr4us.bumbcdn.com/...[can't decrypt TLS yet]         HTTPS
23:37:30  https://pr4us.bumbcdn.com/...[can't decrypt TLS yet]         HTTPS
23:37:42  https://gate.hockeyapp.net/...[can't decrypt TLS yet]        HTTPS
23:37:50  https://eu1.bumble.com/...[can't decrypt TLS yet]            HTTPS
23:38:07  https:///...[can't decrypt TLS yet]                          HTTPS
23:38:07  https:///...[can't decrypt TLS yet]                          HTTPS
23:38:09  https://graph.facebook.com/...[can't decrypt TLS yet]        HTTPS
23:38:21  https://dphotos-us1.badoo.com/...[can't decrypt TLS yet]     HTTPS
23:38:24  https://pr4us.bumbcdn.com/...[can't decrypt TLS yet]         HTTPS
23:38:41  https://pr4us.bumbcdn.com/...[can't decrypt TLS yet]         HTTPS
23:38:41  https://pr4us.bumbcdn.com/...[can't decrypt TLS yet]         HTTPS
23:38:41  https://pr4us.bumbcdn.com/...[can't decrypt TLS yet]         HTTPS
23:39:06  https://eu1.bumble.com/...[can't decrypt TLS yet]            HTTPS

Capturing own and Targets traffic...                                  Total: 22
```

Figure 5 | Bumble's HTTP requests from Debookee



```
  Time
  23:26:51 https://cat.va.us.criteo.com/...[can't decrypt TLS yet]
▶ 23:26:51 http://ets-us-east-1.smaato.net/v1/view?sessionId=9566967b-c54a-4514-8994-503b67dea152&adSourceId=d6d354c4-acce-4720-b410-7f60f8e15b01&origina
  23:26:51 https://pix.us.criteo.net/...[can't decrypt TLS yet]
  23:26:51 https://gum.criteo.com/...[can't decrypt TLS yet]
  23:26:51 https://pix.us.criteo.net/...[can't decrypt TLS yet]
  23:26:51 https://adc3-launch.adcolony.com/...[can't decrypt TLS yet]
  23:26:51 https://soma.smaato.net/...[can't decrypt TLS yet]
  23:26:51 https://px.moatads.com/...[can't decrypt TLS yet]
  23:26:53 https://csm.va.us.criteo.net/...[can't decrypt TLS yet]
  23:26:59 https://cdns.grindr.com/...[can't decrypt TLS yet]
  23:27:01 https://ads.maxads.io/...[can't decrypt TLS yet]
  23:27:02 https://ads.maxads.io/...[can't decrypt TLS yet]
  23:27:02 https://ads.nexage.com/...[can't decrypt TLS yet]
  23:27:06 https://soma.smaato.net/...[can't decrypt TLS yet]
  23:27:09 https://soma.smaato.net/...[can't decrypt TLS yet]
  23:27:11 https://grindr2-d.openx.net/...[can't decrypt TLS yet]
  23:27:13 https://grindr2-d.openx.net/...[can't decrypt TLS yet]
  23:27:13 https://grindr2-d.openx.net/...[can't decrypt TLS yet]
  23:27:16 https://adplatform.vrtcal.com/...[can't decrypt TLS yet]
▶ 23:27:17 http://soma.smaato.net/oapi/reqAd.jsp?adspace=130000706&pub=1100000436&format=ALL&formatstrict=true&dimension=MMA&dimensionstrict=true&width=3
  23:27:19 https://ads.nexage.com/...[can't decrypt TLS yet]
  23:27:20 https://mtcmed01.nexage.com/...[can't decrypt TLS yet]
  23:27:20 https://cdn.manage.com/...[can't decrypt TLS yet]
  23:27:20 https://pixel.advertising.com/...[can't decrypt TLS yet]
  23:27:26 https://grindr.mobi/...[can't decrypt TLS yet]
  23:27:30 https://ads.maxads.io/...[can't decrypt TLS yet]
  23:27:30 https://ads.maxads.io/...[can't decrypt TLS yet]

Capturing own and Targets traffic...                                  Total: 342
```

Figure 6 | Grindr's HTTP requests from Debookee

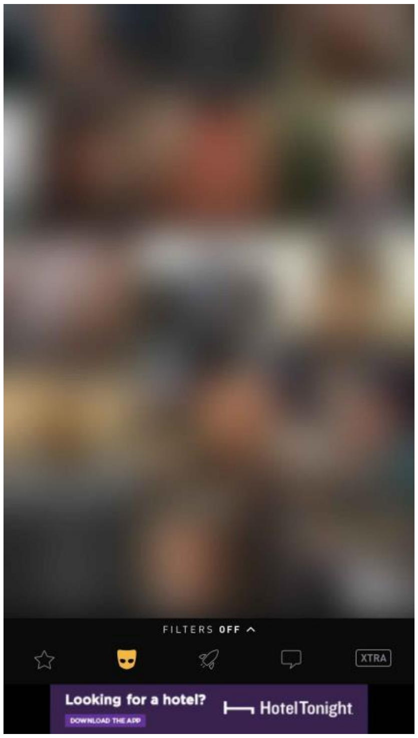


Figure 7 | Grindr’s lower advertisement (blurred for privacy)