Meike Molitor

Data security and data protection impact assessment of Tinder

Final Master's Project

directed by Dr. Josep Domingo-Ferrer

Master's Degree in Computer Security Engineering and Artificial Intelligence

UNIVERSITAT ROVIRA i VIRGILI

Tarragona

2021

Table of contents

1. Introduction

Location-based online dating services gained significant attraction during the last years. One of the most popular dating services worldwide is Tinder [1]. Tinder is part of the Match Group business and offers its service for mobile devices (iOS and Android) and as desktop-version. Since the introduction of Tinder in 2012, the app was downloaded more than 340 million times in 190 countries and 40 languages. [2] When using Tinder, users reveal sensitive personal data, such as their geolocation, biometric data, information about their personality, and sexual orientation. Given the amount and sensitivity of the affected personal data, it is essential to ensure data security and data privacy.

The General Data Protection Regulation (GDPR) aims to protect personal data by regulating its processing and giving natural persons control over their data. As Tinder processes personal data of millions of users in the EU alone and because Tinder has a headquarter within the EU, they are obliged to comply with the GDPR.

This work evaluates the security and privacy of Tinder user's personal data by conducting a Data Protection Impact Assessment (DPIA) according to Article 35 GDPR of Tinder's processing operations. Our assessment identifies and demonstrates multiple GDPR infringements that pose risks to Tinder users and proposes technical and organizational measures for risk mitigation. Tinder repeatedly violates the GDPR principles of transparency, data minimization, and purpose limitation. Additionally, Tinder infringes the rights of the data subjects by providing incomplete and unspecific information in their privacy policy. Furthermore, we show that Tinder deviates from its own specifications by using analytics cookies even though disabled by the user. In addition, Tinder violates the security of processing, privacy by design approach, and integrity and confidentiality principle. First of all, by storing the users' profile pictures at an external service provider without prohibiting unauthorized requests. Secondly, by permitting weak cipher suites and an outdated protocol. And finally, by using inadequate API rate limiting. Moreover, Tinder's practice of gaining consent of the data subjects is not valid pursuant to the GDPR. As a result, Tinder might process parts of the users' data unlawfully.

2. Current state and related work

In 2013, Security and privacy concerns regarding Tinder and other dating applications gained attention when the media reported vulnerabilities. Also, academic research about privacy in geosocial apps started. There are the following research areas:

- location privacy/trilateration [3], [4], [5], [6], [7], [8].
- mobile forensic analysis [9], [10], [11].
- network traffic analysis [3], [10], [12].

In July 2013, the press reported the first significant vulnerability of the Tinder app. By analyzing Tinder's network traffic, a researcher detected that when querying the Tinder Application Programming Interface (API), it sent exact latitude and longitude coordinates of other app users to the iOS client. The API also sent Facebook IDs, with which an attacker can infer a person's name, surname, and, depending on the privacy settings, further personal information. [13]

Tinder closed the location vulnerability by no longer sending the exact GPS coordinates. However, at the end of 2013, the computer and network security company "Include Security"[1] detected that the distance information between two users sent by the API was still too precise. In their experiment, the examiners created three test profiles and then used trilateration to locate a user with a precision of 100 ft. [14] As a countermeasure, Tinder decided to send approximate numbers. [3]

In 2017, *Carman and Choo* [3] documented these attacks on Tinder academically, analyzed whether Tinder's countermeasures were sufficient and whether there were still privacy concerns. The analysis showed that the attacks were no longer practical (Tinder sent no exact GPS coordinates and no Facebook ID). In fact, "*the distance returned is now a whole number, rounded to the nearest mile*." The usage of whole and rounded numbers resulted in a less accurate calculation using trilateration. By using existing trilateration methods, the researchers narrowed a user's location down to an area of 3-4 km². However, they examined that Tinder used only UUID tokens for authentication, did not adequately validate the users' location updates, sent user images over HTTP, and included the user's Tinder ID in the image path. In addition, they were able to associate a Facebook profile with the Tinder account, enhancing the risk of reverse image search. To our best knowledge, after Carman and Choo, no academic paper investigated trilateration on Tinder again.

Further research about location attacks on other geosocial apps:

In 2017, *Hoang et al.* [4] proposed a trilateration model called "colluding-trilateration" to estimate dating app users' location. The model takes advantage of the fact that some dating apps list their users in ascending order depending on their distance from the searching user. First, the attacker generates an account to obtain the list. The attacker then generates two more accounts and manipulates their location in such a way that one account is listed immediately before and immediately after the victim. The locations can now be gradually adjusted to reduce the distance to the victim and ultimately determine the victim's exact location. The researchers successfully estimated the user's location for all three dating apps (Grindr, Hornet, and Jack'd) even though they implemented distance hiding functions and location obfuscation. *Qin et al.* [6] and *Argyros et al.* [7] also reported that a user's location could be found even though the geosocial apps used obfuscation methods.

Other research papers about location attacks were published by *Fattori et al.* [8] in 2013 and *Zhao et al.* [5] in 2016.

[1] https://includesecurity.com/

Forensic analysis

In forensic analysis, an attacker has (physical or remote) access to the storage files of the victim's device.

In 2015, *Farnden et al.* [9] carried out a forensic analysis of dating apps, including Tinder, installed on Android devices. They discussed that the examined apps stored sensitive and partly unencrypted data (messages and location readings, seen profiles, Facebook tokens, further records) on the device. Regarding Tinder, the researchers retrieved unencrypted messages in the device's database as well as profile images, the exact user location over the network, the Facebook Token, and Tinder Token.

In 2018, *Kim et al.* [10] evaluated the security of five Android dating apps (Tinder, Amanda, Glam, DangYeonsi, Noondate) by analyzing the network traffic and using reverse engineering techniques. Two apps (Glam and DangYeonsi) disclosed user-profile information as they used ongoing profile indexes. Four apps (Glam, Tinder, DangYeonsi, and Noondate) disclosed location information. The server responses from three out of these four apps (Glam, Tinder, and Noondate) contained the distance between the attacker and the victim. For all five apps, it turned out that an attacker who has access to the victim's smartphone storage files might gain user credential data. Four apps stored the credentials in the shared preferences (local storage in Android) and one app (DangYeonsi) as a cookie. Additionally, this kind of attacker could also read chat messages written in the Tinder App, as the chat history was stored in the database without being encrypted.

Further research regarding forensic examinations was conducted by *Mata* [11] in 2018.

Network traffic analysis

In 2017, *Shetty* [12] analyzed seven Android mobile dating apps, including Tinder. They conducted a MITM attack to intercept and manipulate the communication between the dating app and the dating app provider's server. For some apps, the researchers were able to gain personal information in plaintext and access a victim's dating app profile. Regarding Tinder, they were able to

- intercept profile pictures, which an attacker then can use for a reverse image search,
- eavesdrop and intercept exchanged text messages,
- upload Not Safe for Work (NSFW) images by making use of the GIPHY API via an intercepted URL and
- restrict and block certain packets sent.

In 2018 the *Checkmarx Security* Research Team discovered that attackers in the same network were able to infer whether a Tinder iOS or Android app user swiped right, left, or made a match due to the fixed sizes of the HTTPS responses (see CVE-2018-6018). In addition, images were not encrypted during transmission, allowing an attacker in the same network to see and replace them (see CVE-2018-6017). So, by combining both, the whole user experience was reconstructable. [15] In June 2018, Tinder stated that they padded the swipe data and that the transmitted images are encrypted now.

Since 2018, technical research regarding the security and privacy of Tinder has decreased significantly. However, companies are beginning to recognize the necessity to protect personal data and address the users' increasing privacy concerns. Some big players are driving data protection forward by restricting tracking practices and enhancing user control and transparency. For instance, in January 2021, Apple announced that with the iOS14 and iPadOS 14 versions, they introduce two privacy features to enable users to make informed decisions. Firstly, Apple requires every app developer to deliver a distinctly understandable privacy practice summary. This summary includes the categories of processed data and information about whether the data is used to track, link, or not link them. So, Apple users can quickly check which personal data the app processes prior to and after installing the app. Additionally, Apple obliges app developers to ask the users for consent before tracking them across apps or websites owned by other companies. [16] The shift in privacy practices was also evident when Google stated in March 2021 that Chrome would stop the support of third-party cookies. [17] Instead, Google plans to prevent individual tracking by using a privacy-preserving mechanism called Federate Learning of Cohorts (FLoC) API. Cohorts are groups of users with comparable interests. Depending on the user's browser history, the FLoC API uses an algorithm that assigns the cohort id to a user. Google Chrome wants to enhance privacy by requiring every group to contain at least k distinct users. [18] This privacy-first anonymization model is called k-anonymity. While using k-anonymity is a step in the right direction, there are still attacks to consider (homogeneity attack and background knowledge attack).

Apart from the technical point of view, there is a lack of documented research about the compliance of dating apps with applicable laws and regulations. An exception is the publication of an open letter to the dating app Grindr by Datatilsynet [19], which explicates that Grindr violates the GDPR by sharing personal data to third parties without a valid legal basis. In addition to the GDPR, which handles any processing of personal data, there are other regulations companies like Tinder have to follow. For instance, in April 2021, the European Commission published a draft of a regulation defining mandatory requirements for designing, developing, and using artificial intelligence systems [20].

All in all, there is a deficiency of academically documented research regarding the GDPR-compliance of Tinder. Also, there is a lack of up-to-date technical research. To our best knowledge, this is the first extensive work about the GDPR compliance of Tinder which combines technical and legal evaluations.

3. The GDPR

The application of the General Data Protection Regulation (GDPR) in 2018 was a significant step towards the rights and freedoms of natural persons. The objective of the GDPR is to protect personal data by regulating its processing and giving natural persons control over their data. (Article (1)(2) GDPR).

GDPR-compliance is mandatory for enterprises within the European Economic Area that are processing personal data. So, as Tinder has a headquarter within the EU where they process personal data of European users, they must comply with the GDPR. Processing "*means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*" (Article (4)(2)GDPR).

The GDPR defines personal data and its subtypes as follows.

- **Personal data** is "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*" (Article (4)(1) GDPR).
- **Special categories of data** are "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*" (Article (9)(1) GDPR).
- **Biometric data** is "*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data*" (Article (4)(14) GDPR).

Tinder processes following personal data:

- Geolocation
- Login credentials
- If applicable social media login credentials and information from social media
- Gender, date of birth, personality, lifestyle, interests, job
- For subscribers: financial information like the credit card number
- User interaction and activity
    - the users connected and interacted with, chats, time and date of the exchanges, number of messages received and sent
    - login date and time, used features, searches, clicks and websites, website address, clicks on ads
- Device information (hardware and software information, network connections, device sensors)
- Special categories of data: sexual orientation, data concerning sex life, racial or ethnic origin, religious belief
- Biometric data: photos and videos

4. Methodology

The security and privacy of Tinder user's personal data are evaluated by conducting a Data Protection Impact Assessment (DPIA) pursuant to Article 35 GDPR of Tinder's processing operations. A DPIA aims to assess the "*origin, nature, particularity and severity*" (Recital 84 GDPR) of the risk of natural persons.

In the scope of the GDPR, risk can be understood as the likelihood that physical, material or non-material damage regarding the rights and freedoms of a data subject could occur. The risk can have a varying likelihood and severity. (Recital 75 GDPR) Within this work, the severity of the risks is divided into medium and high. The classification is based on Article 83 GDPR, which distinguishes between provision infringements as summarized in the table below.

Severity	
Medium	Infringements against controller obligations (Art. 8, 11, 25-39 GDPR).
High	Infringements against - principles of processing and conditions for consent (Art. 5, 6, 7, 9 GDPR). - the data subject's rights (Art. 12-22 GDPR). - third-country data transfer (Art. 44-49 GDPR).

Table 1: Severity of risks.

The overall risk can be classified as low risk, medium risk, and high risk. This categorization aligns with the recommendations of the DSK (Datenschutzkonferenz), a German association of data protection authorities. [21]

A DPIA is an ongoing procedure and consists in

- describing processing operations performed on personal data and explaining the processing purposes,
- evaluating the necessity and proportionality of processing while considering the processing purposes,
- conducting a risk assessment, and
- define countermeasures to tackle the risk. (Article (35)(7) GDPR)

This work is written from an external perspective, so the DPIA is based on the information provided by Tinder and derived by using Tinder's service. We analyze whether the provided information in Tinder's privacy policy is GDPR compliant for each regarded processing operation. Where applicable, we carry out a practical analysis of the Tinder app or its browser version to detect deviations from the privacy policy and other GDPR violations. By taking into account the required steps of a DPIA, for each evaluated processing operation, the results are bundled in tables examining

- the description, purpose, and legal basis of the processing operation provided by Tinder,
- the necessity and proportionality of Tinder's processing operations,
- the findings which result in a risk to the data subjects,
- the measures to mitigate the risk, and
- the residual risk.

5. Data Protection Impact Assessment

5.1. Requirements

Tinder must meet the following GDPR aspects, which necessitate a prior definition.

5.1.1. Transparency

Transparency is a fundamental principle of the GDPR which requires that "*personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*" (Article (5)(1)(a) GDPR). The controller is responsible for providing all

- information regarding Article 13 and 14 GDPR and
- notifications regarding Article 15-22 and Article 34 GDPR

concerning the processing operations "*to the data subjects in a **concise, transparent,** intelligible and easily accessible form**, using clear and plain language**"* (Article (12)(1) GDPR).

The Article 29 Working Party (WP29) further defines in the *Guidelines on transparency under Regulation 2016/679* that for clear and plain language,

> *"Language qualifiers such as "may", "might", "some", "often" and "possible" should also be avoided. Where data controllers opt to use indefinite language, they should be able, in accordance with the principle of accountability, to demonstrate why the use of such language could not be avoided and how it does not undermine the fairness of processing"* [22]

In addition, WP29 gives examples of good practice and poor practice:

- **Poor practice example** which is "*not sufficiently clear as to the purposes of processing*": *"'We may use your personal data to develop new services' (as it is unclear what the 'services' are or how the data will help develop them)"* [22]
- **Good practice example**: "'*We will retain your shopping history and use details of the products you have previously purchased to make suggestions to you for other products which we believe you will also be interested in' (it is clear that what types of data will be processed, that the data subject will be subject to targeted advertisements for products and that their data will be used to enable this)*" [22]

Recital 39 of the GDPR outlines that the data subjects must be aware

- that their personal data are processed (for instance, collected or used).
- to what extent the personal data is processed.
- of the purposes of the processing.
- of their rights, risks, rules, and safeguards.
- of the identity of the controller.

5.1.2. Purpose limitation

The principle of purpose limitation indicates that personal data shall only be processed for the specified, explicit, and legitimate purposes it was collected. Further processing differing from the original purpose is prohibited. (Article (5)(1)(b) GDPR)

5.1.3. Data minimization

The data minimization principle states that personal data shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*" (Article (5)(1)(c) GDPR)

According to the DSK data are [23]

- *adequate* if their content has a concrete link to the processing purpose.
- *relevant* if their processing contributes to achieving the purpose. The relevance of data links with the proportionality assessment within the DPIA.
- *limited to what is necessary* if they are required for the purpose. Without them, the purpose cannot be fulfilled. The limitation of processed data links with the necessity assessment within the DPIA.

5.1.4. Lawfulness of processing

Consistent with the GDPR, the processing of personal data is only lawful if it relies on legal bases (Article (6)(1) GDPR). Tinder relies on the following legal bases for its processing operations:

- Data subjects gave consent to the processing. (Article (6)(1)(a) GDPR)
- Processing is necessary to perform a contract with the data subject. (Article (6)(1)(b) GDPR)
- The controller has a legitimate interest in the processing. (Article (6)(1)(f) GDPR)

5.2. Collection of information

Tinder collects personal data directly provided by the data subject, indirectly provided while the data subjects use Tinder's service, and they get personal data from others (social media, partners, other users).

The following personal data collecting processes pose a risk to the data subjects.

5.2.1. Collect personal information provided by the data subjects

01	**Processing operation:**	Collect personal information provided by the data subjects to provide service

Provided information:

"*When you create an account, you provide us with at least your login credentials, as well as some basic details necessary for the service to work, such as your gender and date of birth. When you complete your profile, you can share with us additional information, such as details on your personality, lifestyle, interests and other details about you, as well as content such as photos and videos […] racial or ethnic origins, sexual orientation and religious beliefs. By choosing to provide this information, you consent to our* ***processing*** *of that information. […] Of course, we also* ***process*** *your chats with other users as well as the content you publish, as part of the operation of the services."* [24]

Processing purpose: provide service

Legal basis: performance of a contract according to Art(6)(1)(b)

It is assumed that most of the above-listed processing operations rely on the following provided legal basis:

> "*Most of the time, the reason we process your information is to perform the contract that you have with us. For instance, as you go about using our service to build meaningful connections, we use your information to maintain your account and your profile, to make it viewable to other users and recommend other users to you*."[24]

Necessity and proportionality of processing:

The data processed seem to be relevant and necessary for the processing operation. The procedure complies with the data minimization principle.

Risk: the data subjects are "*deprived of their rights and freedoms or prevented from exercising control over their personal data*" (Recital 75 GDPR) due to the following provision infringement.

<u>Violation of the transparency principle</u>

Tinder states that they "process" the listed sensitive data of the user profiles and the chats with other users. Processing by its definition means every operation on personal data (Article (4)(2) GDPR), including collection and storage but also disclosure by transmitting, making available, and combining. Given this highly sensitive personal information, clarification on the processing operations must be provided.

Tinder describes further processing operations in subsequent and separate policy sections. However, even when reading these sections, it is unclear which and how this personal information is further processed (see tables 04-10).

Tinder's formulations are not precise enough to comply with the transparency principle defined in Article (5)(1)(a) GDPR and Article (12)(1) GDPR.

Severity: high
Measures: To comply with the transparency principle, Tinder must specify to what extent the personal data is processed.
Residual risk: low When Tinder updates its policy with more specific information, the data subjects are well informed and hence able to decide whether they agree with Tinder's processing.

5.2.2. Collect personal information received by partners

02	**Processing operation:**	Collect personal information received by partners

Provided information:
"*We **may receive info** about you from **our partners**, **for instance** where Tinder ads are published on a partner's websites and platforms (in which case they **may** pass along details on a campaign's success)." [24]*

Processing purpose: NA

Provided legal basis: NA

Necessity and proportionality of processing:
Tinder does not specify which data or which category of data are involved in the processing operation, which makes it impossible to assess the necessity and proportionality.

Risk: the data subjects are "*deprived of their rights and freedoms or prevented from exercising control over their personal data*" (Recital 75 GDPR) due to the following provision infringements.

a) <u>Violation of the right of the data subjects (providing information about collected personal data not obtained from the data subject)</u>

If Tinder relies on legitimate interest, the policy misses an explanation about those interests (Article (14)(2)(b) GDPR). If Tinder does not rely on legitimate interests, there is no legal basis provided at all, which is a violation of Article (14)(1)(c) GDPR. Additionally, Tinder names only one example of the received categories of personal data: details on a campaign's success. However, all categories of the concerned personal data must be provided according to Article (14)(1)(d) GDPR.

Moreover, there is no clear information about who Tinder's partners are or which category of partners they refer to in this section. Providing a single example (advertising partners) is not enough and leaves the question from which other sources they "may" get information. This seems to be in contrast with Article 14(2)(f) GDPR.

b) <u>Violation of the transparency principle</u>

Due to the vague modal verb "may", it is not sufficiently clear under which circumstances Tinder receives information from partners about the data subjects. As discussed in section a), there is no explanation about which kind of data they receive from partners, the purpose of receiving data from third parties (except for the given advertising example), and the sources of the personal data. Hence, in contrast to Article (5)(1)(a) GDPR and Article (12)(1) GDPR, the necessary information for fair and transparent processing is missing.

The missing specification of the processing purpose allows Tinder a gradual widening of its processing activities. This procedure is called *function creep* and results in the risk that data subjects might lose control over their data *[25]*, as the unknown kind of data received by Tinder and sent by unknown third parties could be used for unexpected purposes.

Severity: high

Measures:

a) Tinder must provide a legal basis for collecting personal information received by partners. If Tinder relies on legitimate interests, the controller must explain those interests. Furthermore, the controller needs to add all categories of collected data and partners to the privacy policy.

b) In addition to the categories of data and partners, Tinder must explain the processing purpose. Moreover, Tinder must avoid vague modal verbs.

Residual risk: low

When Tinder updates its policy with more specific information, the data subjects are well informed and hence able to decide whether they agree with Tinder's processing.

A precondition for low risk is

- that the processing purposes are in accordance with the GDPR and limited to the defined purpose to comply with the purpose limitation principle.
- that Tinder only collects necessary data to comply with the data minimization principle.
- that the controller seeks user consent if applicable.

Otherwise, the risk is still high.

5.2.3. Collect personal information generated while service usage

03	**Processing operation:**	Collect personal information generated while service usage

Provided information:

"When you use our services, we collect […]

- ***Usage Information*** *We collect information about your activity on our services**, for instance** how you use them (**e.g.,** date and time you logged in, features you've been using, searches, clicks and pages which have been shown to you, referring webpage address, advertising that you click on) and how you interact with other users (e.g., users you connect and interact with, time and date of your exchanges, number of messages you send and receive).*
- ***Device information*** *We collect information from and about the device(s) you use to access our services, including:*
  - *hardware and software information **such as** IP address, **device ID** and type, device-specific and apps settings and characteristics, app crashes, advertising IDs (such as Google's AAID and Apple's IDFA, both of which are randomly generated numbers that you can reset by going into your device' settings), browser type, version and language, operating system, time zones**,** identifiers associated with cookies or other technologies that **may uniquely identify your device or browser** (e.g., **IMEI/UDID and MAC address**);*
  - *information on your wireless and mobile network connection, **like** your service provider and signal strength;*
  - *information on device sensors **such as accelerometers, gyroscopes and compasses**.*
- ***Other information with your consent*** *If you give us permission, we can collect your **precise geolocation** (latitude and longitude) through various means, depending on the service and device you're using, including GPS, Bluetooth or Wi-Fi connections. The collection of your geolocation may occur in the **background** even when you aren't using the services if the permission you gave us expressly permits such collection. If you decline permission for us to collect your geolocation, we will not collect it. Similarly, if you consent, we may collect your photos and videos (for instance, if you want to publish a photo, video or streaming on the services)."* [24]

Processing purpose: NA

Provided legal basis:

All the provided legal basis statements partly apply to the collection.

*"**Provide our service to you**: Most of the time, the reason we process your information is to perform the contract that you have with us. For instance, as you go about using our service to build meaningful connections, we use your information to maintain your account and your profile, to make it viewable to other users and recommend other users to you.*

***Legitimate interests**: We may use your information where we have legitimate interests to do so. For instance, we analyze users' behavior on our services to continuously improve our offerings, we suggest offers we think might interest you, and we process information for administrative, fraud detection and other legal purposes.*

***Consent**: From time to time, we may ask for your consent to use your information for certain specific reasons. You may withdraw your consent at any time by contacting us at the address provided at the end of this Privacy Policy."[24]*

Necessity and proportionality of processing:

Data is necessary and proportional if it is required and relevant to reach the purpose. As Tinder does not describe the processing purpose in this section, there is only a limited possibility to evaluate the necessity and proportionality of processing. However, regardless of the possible processing purposes, the following assumptions can be made:

- **Usage information:** The listed personal information seems to comply with the data minimization principle.
- **Device information:** Collecting the device ID, IMEI/UDID, MAC address, and device sensor information, including accelerometers, gyroscopes, and compasses, is not necessary to provide service to the users and is not in accordance with the data minimization principle.
- **Other information:** It is unnecessary to collect the precise geolocation of a user. An approximate number or just the town name should be enough. Moreover, collecting the data subject's geolocation in the background is not necessary. Even when asking the users for consent, this collection seems not appropriate. It opens the possibility to track a user's locations 24/7 to generate a location profile.

Risk: the data subjects are "*deprived of their rights and freedoms or prevented from exercising control over their personal data*" (Recital 75 GDPR) due to the following provision infringements.

a) <u>Violation of the data minimization principle</u>

Tinder violates the data minimization principle according to Article (5)(1)(c) GDPR by collecting personal data which are not relevant to provide their service (see details above).

b) <u>Violation of the right of the data subjects (providing information about collected personal data obtained from the data subject)</u>

Tinder does not explain the purposes of collecting personal information, and the reader needs to guess the legal bases for processing. This is not in accordance with Article (13)(1)(c) GDPR, which requires the controller to provide the purposes and legal basis for the processing of personal data.

c) <u>Violation of the transparency principle</u>

Tinder states that they collect photos and videos if the data subjects "for instance" want to publish a photo or video. Given this formulation, we have to assume that the photos and videos are collected in further ways.

Moreover, it is not sufficiently clear for which purposes Tinder collects the listed personal data. Not describing the specific purposes, is not in the sense of the transparency principle (Article (5)(1)(a) and (12)(1) GDPR).

Additionally, as discussed in table 02, an unspecific purpose raises the risk of function creep.

d) <u>Violation of the privacy by design approach, the integrity and confidentiality principle, and the security of processing</u>

For complying with the security of processing requirement (Article 32 GDPR), an appropriate level of data security must be ensured by taking into account the state of the art and implementation costs (Recital 83 GDPR). Data security requires strong encryption mechanisms and protocols to prevent unauthorized disclosure or access to the Tinder user's highly sensitive personal data. However, Tinder's server supports a deprecated protocol (TLS 1.1) and does not prohibit weak cipher suites (see chapter 5.2.4 for details). This increases the risk of attacks that undermine data security.

The lack of appropriate technical safeguards for data protection also contradicts the data protection by design and by default approach (Article 25 GDPR) and the integrity and confidentiality principle (Article (5)(1)(f) GDPR).

Hence, Tinder's practice does not comply with the GDPR's requirement for security of processing, integrity and confidentiality, and data protection by design and default.

Severity: high

Measures:

a) To comply with the data minimization principle, Tinder must stop collecting the personal data named above. In addition, Tinder should recheck the necessity and proportionality of all collected data generated during the data subjects' service usage, which might not be listed in the privacy policy.

b) Tinder must provide specific information about the purposes and legal basis for collecting personal data generated while service usage.

c) Tinder needs to explain the processing purposes.

d) Tinder's server should not support TLS 1.1 and prohibit weak cipher suites.

Residual risk: low

When Tinder updates its policy with more specific information, the data subjects are well informed and hence able to decide whether they agree with Tinder's processing.

A prerequisite for low risk is that the

- processing purposes are in accordance with the GDPR and limited to the defined purpose to comply with the purpose limitation principle.
- controller seeks user consent if applicable.
- recheck of the collected data has been carried out conscientiously, that the processing of data recognized as not required is stopped, and Tinder therefore only collects necessary data.

Also, if Tinder stops the support of TLS 1.1 and uses only strong ciphers, the risk is low.

Otherwise, the risk is still high.

5.2.4. Practical analysis of the cryptographic schemes used by Tinder

In the current chapter, we analyze the security of Tinder's Android app and web interface by sniffing the network traffic and reviewing the used cryptographic schemes.

5.2.4.1. Web interface

Tinder processes highly sensitive data, like the users' sexual orientation and chats, which necessitate a high degree of data security. In particular, Tinder must provide data confidentiality, integrity, availability, and authenticity continuously. Appropriate encryption is essential for reaching these security goals. As Tinder outsources data availability to AWS, this security goal is not part of the analysis.

Experiment setup

- We first assess which cipher suites and protocols are used when browsing tinder.com with an up-to-date Firefox browser (version 88.0.1).
- Then, we check which other ciphers and protocols the Tinder API accepts using the *Qualys SSL Labs tool*[2].

When using the Firefox browser in version 88.0.1 on Windows 10, the page information of Tinder's web interface shows that the connection is encrypted using TLS_AES_128_GCM_SHA256 (see figure 1). So, Tinder uses

- the Transport Layer Security (TLS) [26] protocol in version 1.3,
- the Advanced Encryption Standard (AES) [27] with a 128-bit key in Galois/Counter mode (GCM) [28], and
- the Secure Hash Algorithm (SHA) [29] with a 256-bit message digest.

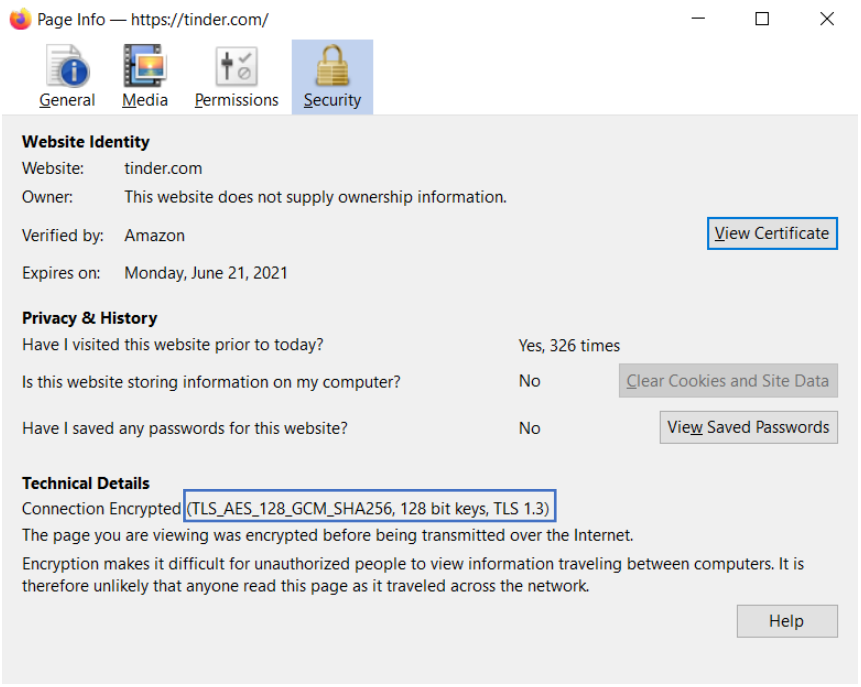


Figure 1: Page information of Tinder's web interface.

[2] https://www.ssllabs.com/ssltest/analyze.html?d=tinder.com&s=13.227.75.10&hideResults=on&ignoreMismatch=on

TLS 1.3 is the latest TLS protocol version and is documented in the RFC 8446 standard by the Internet Engineering Task Force (IETF). TLS 1.3 enables confidentiality, data integrity, and authentication between two communicating parties. Moreover, TLS 1.3 provides perfect forward secrecy, which means that "*the compromise of a long-term private key after it has been used to establish a session key does not cause the compromise of that session key*." [30]

The evaluation of the used cipher suites is based on the cryptographic key management guidance NIST SP 800-131A [31] by the National Institute of Standards and Technology (NIST). According to the guideline, when using **AES-128** and **SHA-256** correctly, the schemes are safe to use, and the security risk is low. **GCM** was standardized by NIST in the SP 800-38D [28] and shown to be secure [32] as well. Using AES in GCM ensures data confidentiality. Moreover, GCM aims to ensure data authenticity, and SHA provides integrity.

So, the discussed selection of cryptographic schemes is adequate, and if used correctly, confidentiality, integrity, and authenticity are reached.

However, depending on the user's browser version and operating system, other cryptographic schemes can be used. An *SSL/TLS Server test* of tinder.com using the *Qualys SSL Labs tool*[3] showed that in addition to TLS 1.3, the server also supports TLS 1.2 and the deprecated TLS 1.1 version.

Protocols	
TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	No

Figure 2: Supported TLS versions.[2]

Regarding TLS 1.2, nine out of 12 supported cipher suites are classified as weak (see figure 3). Additionally, the server prefers two weak ciphers to two more secure ciphers. Furthermore, all four supported TLS 1.1 suites are weak (see figure 4).

# TLS 1.2 (suites in server-preferred order)		
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK		128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK		256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK		128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK		256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK		128

Figure 3: Supported TLS 1.2 cipher suites.[2]

[3] https://www.ssllabs.com/ssltest/analyze.html?d=tinder.com&s=13.227.75.10&hideResults=on&ignoreMismatch=on

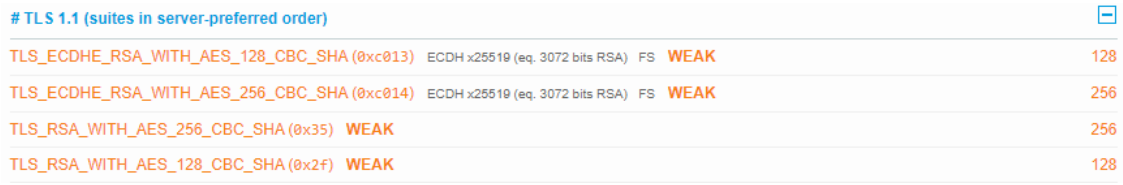


Figure 4: Supported TLS 1.1 cipher suites.[2]

Using deprecated protocol versions and weak ciphers known to enable attacks is not following the GDPR's requirement for security of processing, the integrity and confidentiality principle, and the data protection by design and default approach.

5.2.4.2. Android app

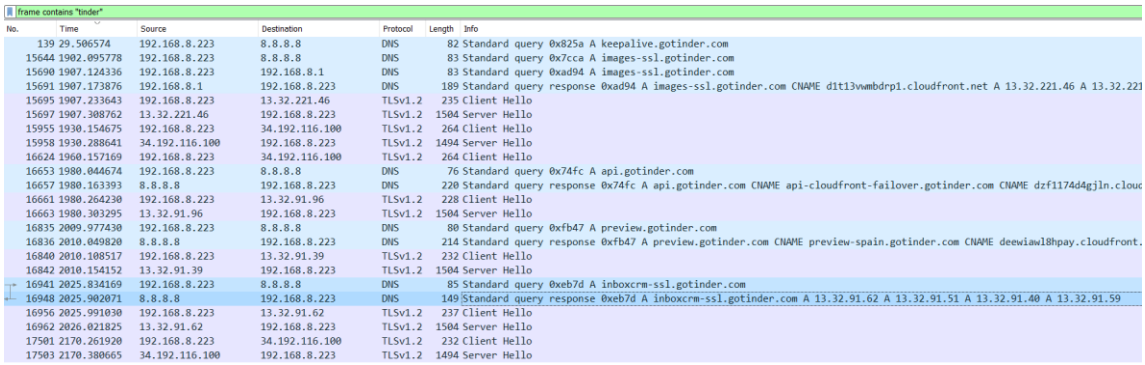
We analyzed the network traffic of the Tinder Android app installed on an emulated Android device using Wireshark to approve that the communication is sufficiently encrypted, especially with regard to the users' images which have not been encrypted during transmission prior to 2018 (see chapter 2 and CVE-2018-6017).

Experiment setup

- We used the BlueStacks emulator, enabling running Android apps on Microsoft Windows (and macOS).
- After installation, we signed in using a Google account and downloaded the Tinder app.
- Then, we generated traffic by using the app while capturing the network traffic using Wireshark.

The network dump reveals that the communication is encrypted using TLS 1.2, including user profile pictures. So, the CVE-2018-6017 vulnerability is still fixed.

All in all, nothing exceptional was found.


frame contains "tinder"

No.	Time	Source	Destination	Protocol	Length	Info
139	29.506574	192.168.8.223	8.8.8.8	DNS	82	Standard query 0x825a A keepalive.gotinder.com
15644	1902.095778	192.168.8.223	8.8.8.8	DNS	83	Standard query 0x7cca A images-ssl.gotinder.com
15690	1907.124336	192.168.8.223	192.168.8.1	DNS	83	Standard query 0xad94 A images-ssl.gotinder.com
15691	1907.173876	192.168.8.1	192.168.8.223	DNS	189	Standard query response 0xad94 A images-ssl.gotinder.com CNAME d1t13vwmbdrp1.cloudfront.net A 13.32.221.46 A 13.32.221
15695	1907.233643	192.168.8.223	13.32.221.46	TLSv1.2	235	Client Hello
15697	1907.308762	13.32.221.46	192.168.8.223	TLSv1.2	1504	Server Hello
15955	1930.154675	192.168.8.223	34.192.116.100	TLSv1.2	264	Client Hello
15958	1930.288641	34.192.116.100	192.168.8.223	TLSv1.2	1494	Server Hello
16624	1960.157169	192.168.8.223	34.192.116.100	TLSv1.2	264	Client Hello
16653	1980.044674	192.168.8.223	8.8.8.8	DNS	76	Standard query 0x74fc A api.gotinder.com
16657	1980.163393	8.8.8.8	192.168.8.223	DNS	220	Standard query response 0x74fc A api.gotinder.com CNAME api-cloudfront-failover.gotinder.com CNAME dzf1174d4gjln.cloud
16661	1980.264230	192.168.8.223	13.32.91.96	TLSv1.2	228	Client Hello
16663	1980.303295	13.32.91.96	192.168.8.223	TLSv1.2	1504	Server Hello
16835	2009.977430	192.168.8.223	8.8.8.8	DNS	80	Standard query 0xfb47 A preview.gotinder.com
16836	2010.049820	8.8.8.8	192.168.8.223	DNS	214	Standard query response 0xfb47 A preview.gotinder.com CNAME preview-spain.gotinder.com CNAME deewiawl8hpay.cloudfront.
16840	2010.108517	192.168.8.223	13.32.91.39	TLSv1.2	232	Client Hello
16842	2010.154152	13.32.91.39	192.168.8.223	TLSv1.2	1504	Server Hello
16941	2025.834169	192.168.8.223	8.8.8.8	DNS	85	Standard query 0xeb7d A inboxcrm-ssl.gotinder.com
16948	2025.902071	8.8.8.8	192.168.8.223	DNS	149	Standard query response 0xeb7d A inboxcrm-ssl.gotinder.com A 13.32.91.62 A 13.32.91.51 A 13.32.91.40 A 13.32.91.59
16956	2025.991030	192.168.8.223	13.32.91.62	TLSv1.2	237	Client Hello
16962	2026.021825	13.32.91.62	192.168.8.223	TLSv1.2	1504	Server Hello
17501	2170.261920	192.168.8.223	34.192.116.100	TLSv1.2	232	Client Hello
17503	2170.380665	34.192.116.100	192.168.8.223	TLSv1.2	1494	Server Hello

Figure 5: Android network traffic.

5.3. Cookies and similar technologies

5.3.1. Collect and use personal information generated by cookies

04	**Processing operation:**	Collect and use personal information generated by cookies

Provided information:

"We use and may allow others to use cookies and similar technologies (e.g., web beacons, pixels) to recognize you and/or your device(s). You may read our Cookie Policy for more information on why we use them (such as authenticating you, remembering your preferences and settings, analyzing site traffic and trends, delivering and measuring the effectiveness of advertising campaigns, allowing you to use social features) and how you can better control their use, through your browser settings and other tools." [24]

Cookie policy: *"we use cookies to provide, secure and improve our services, including by remembering your preferences, recognizing you when you visit our website and personalizing and tailoring ads to your interests. To accomplish these purposes, we also may link information from cookies with other personal information we hold about you."* [33]

Processing purpose: provide, improve, and secure their service

Legal basis: NA

Necessity and proportionality of processing:

Tinder does not specify which data or which category of data are involved in the processing operation, which makes it impossible to assess the necessity and proportionality.

Risk: the data subjects are "*deprived of their rights and freedoms or prevented from exercising control over their personal data*" (Recital 75 GDPR) due to the following provision infringements.

a) **<u>Violation of the right of the data subjects (providing information about collected personal data obtained from the data subject)</u>**
   In Tinder's policies is no information about the legal basis of their processing operation. This is not in accordance with Article (13)(1)(c) GDPR.

b) **<u>Violation of the principle of the lawfulness of processing</u>**
   While strictly necessary cookies for providing the service can be based on legitimate interest, analytics cookies cannot. So, in practice, Tinder correctly requests consent for using these cookies. However, despite refusing analytics cookies, they are created and used. As the data subjects did not consent to this processing operation, Tinder has no legal basis and processes personal data unlawfully. Hence, Tinder violates Article (6)(1) GDPR.
   Chapter 5.3.2 provides further details about how this violation was found.

Severity: high

Measures:

a) Tinder must provide a legal basis for collecting and using personal data generated by cookies. If Tinder relies on legitimate interests, the controller must explain those interests.

b) Tinder must stop using analytics cookies if the data subjects did not give consent for them.

Residual risk: low
If Tinder implements the countermeasures, the risk for the data subjects is low.

5.3.2. Practical analysis of Tinder's cookie practice

This experiment aims to evaluate whether Tinder is in accordance with its privacy policy and cookie policy.

Experiment setup

- The initial part of the experiment checks how Tinder gains consent for cookies when browsing tinder.com.
- Based on that follows an analysis of which cookies are stored on the user device while using the service.

Theory: How Tinder gains consent for cookies

When revoking Tinder's website, the following request is made.

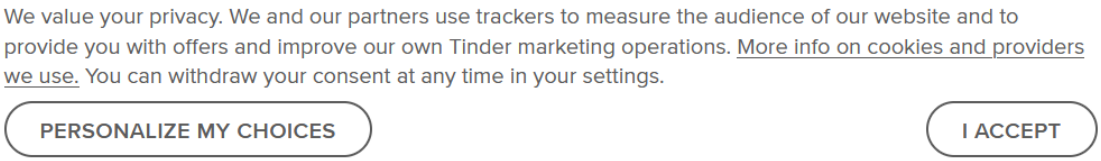


Figure 6: Consent for cookies.

By clicking "personalize my choices", the user is led to Tinder's privacy preference center, where the data subjects can adjust their consent settings. The strictly necessary trackers are obligatory, but the users can decide whether they give marketing and analytics permissions. So, by refusing all optional cookies, Tinder should neither use marketing nor analytics cookies.

Practice:

(1) Before accepting or refusing cookies

Primarily, all cookies, the site data, and the cache of the (Firefox) browser are cleared. Then, tinder.com is loaded. By using Firefox's inspection tool, one can see that two cookies are created.

Name	Value
AWSALBCORS	Lo+cbu3m9xoIXXgOWdPd0
AWSALB	Lo+cbu3m9xoIXXgOWdPd0

Figure 7: List of generated Amazon cookies.

AWSALB and AWSALBCORS are first-party cookies with a lifetime of one week. The purpose of these AWS (Amazon Web Services) cookies is load balancing. Both cookies are listed on Tinder's list of trackers, which are strictly necessary to provide service. So far, Tinder's practice is in accordance with the GDPR.

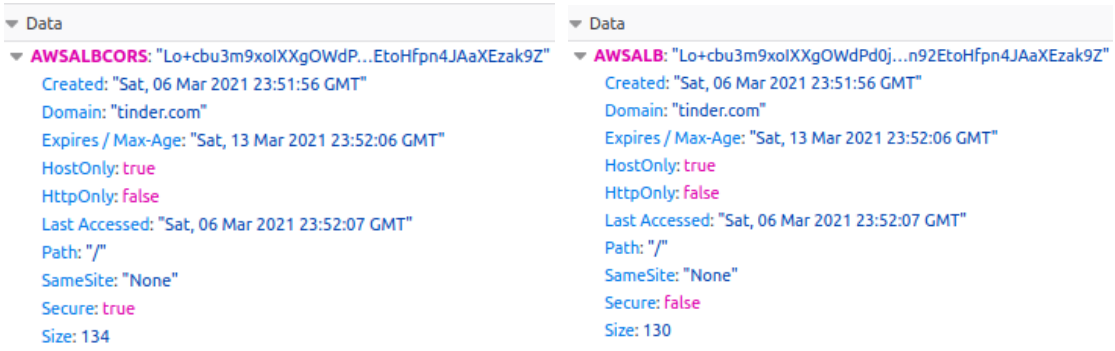


Figure 8: Details of Amazon cookies.

(2) Refusing all cookies

After refusing all cookies in Tinder's privacy preference center, two additional cookies appear in the cookies list.

Name	Value
_ga_CDPT3R4PG7	GS1.1.1615074890.1.0.1615074891.0
_ga	GA1.1.764989617.1615074891
AWSALBCORS	Lo+cbu3m9xoIXXgOWdPd0jvLsr9tiH5WaaQER
AWSALB	Lo+cbu3m9xoIXXgOWdPd0jvLsr9tiH5WaaQER

Figure 9: List of generated cookies after refusing all cookies.

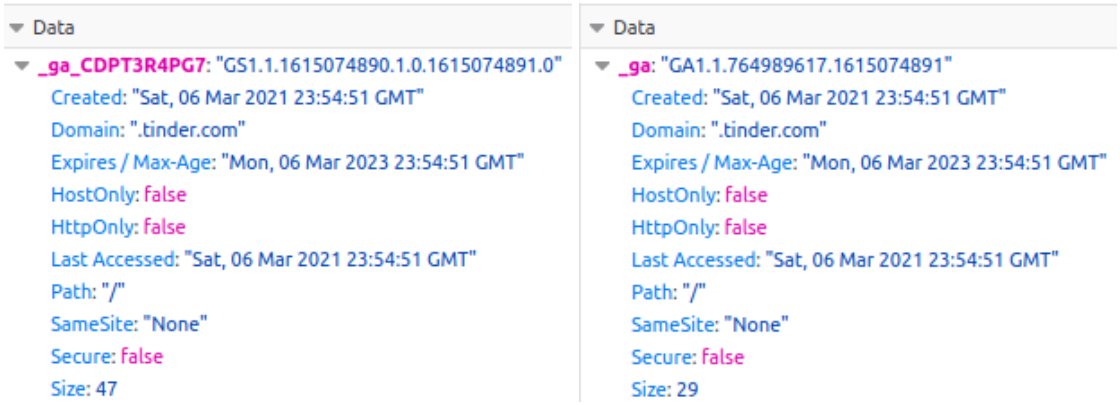


Figure 10: Details of Google Cookies.

The "_ga cookies" are not part of Tinder's list of strictly necessary trackers. Instead, they appear on the analytics permission list. These cookies are third-party Google Analytics cookies, have a lifetime of two years, and are used "*to distinguish unique users to measure the audience of the website*".

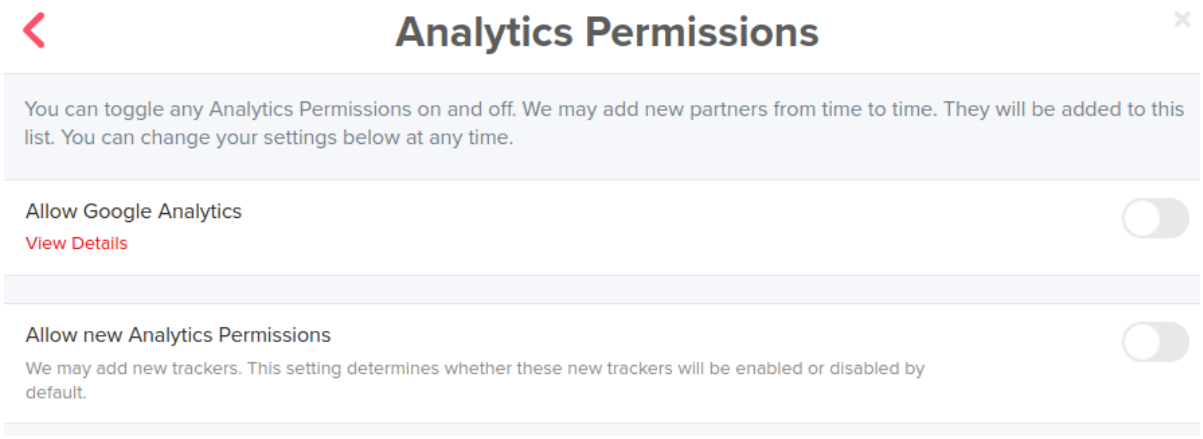


Figure 11: Tinder's analytics permission request within the privacy preference center.

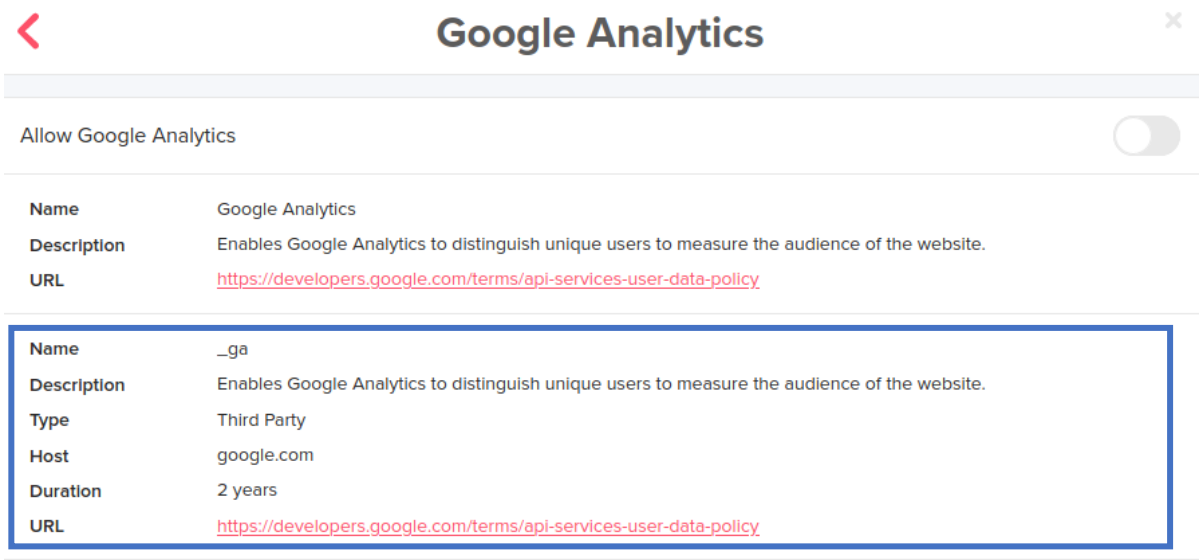


Figure 12: Tinder's Google analytics permission request within the privacy preference center

By rechecking the settings, we validated that all cookies should be disabled. But they are not:

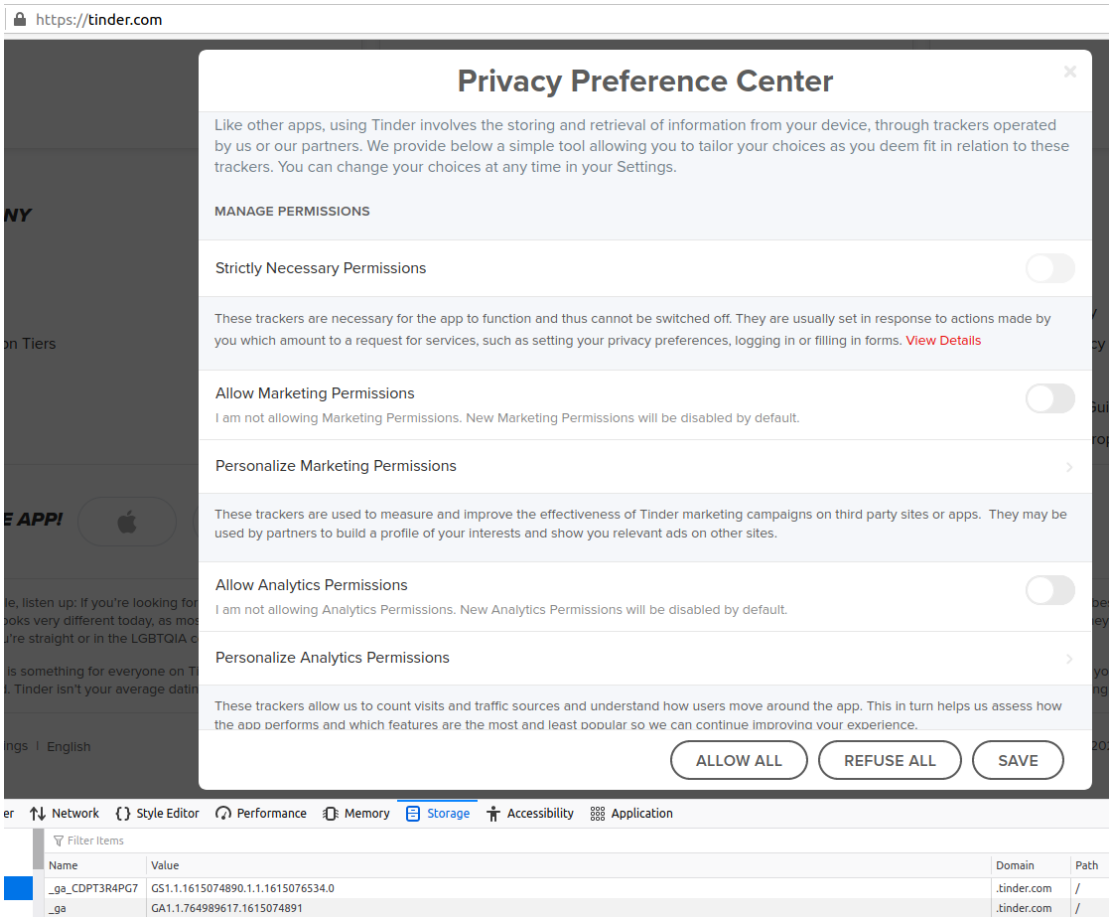


Figure 13: Google cookies stored on the user device even though all permissions were refused.

(3) After logging in

After logging in and interacting on the website, the _ga_CDPT3R4PG7 Google Analytics cookie stays active (value changes). With every cookie access, the expiration age is set again to two years.

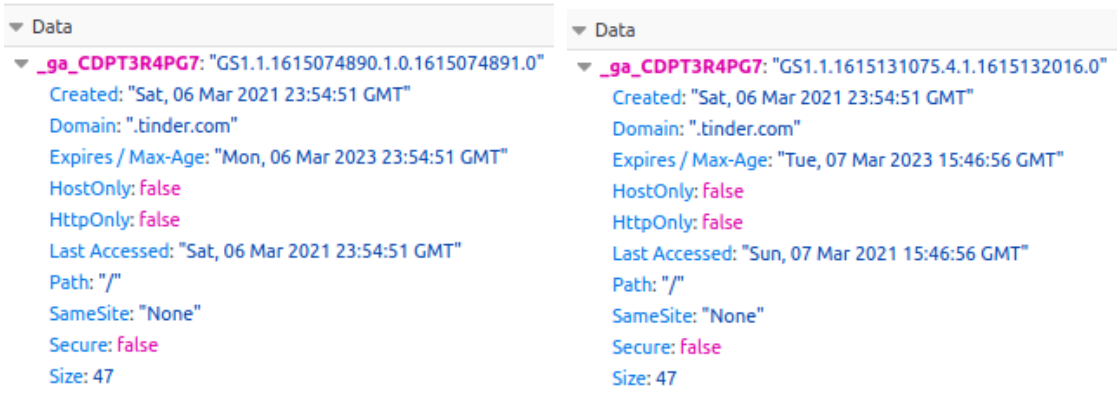


Figure 14: Cookie details at creation time (left) and after service usage on the next day (right).

To sum up, even though consent for Google Analytics cookies was denied, they were created after refusing them, and they stay active during the usage of Tinder's service.

5.4. Sharing of information

Tinder shares personal data with other Match Group brands, partners, and service providers.

5.4.1. Share personal information with other Match Group brands

05	**Processing operation:**	Share personal information with other Match Group brands for several processing operations

Provided information:

"With other Match Group businesses

Tinder is part of the Match Group family of businesses which, as of the date of this Privacy Policy, includes websites and apps such as Tinder, OkCupid, Plenty of Fish, Match, Meetic, BlackPeopleMeet, LoveScout24, OurTime, Pairs, ParPerfeito, and Twoo (for more details, click here).

*We share your information with other Match Group companies for them to assist us in **processing your information**, as service providers, upon our instructions and on our behalf. Assistance provided by other Match Group companies **may include** technical processing operations, such as data hosting and maintenance, customer care, marketing and **targeted advertising**, finance and accounting assistance, better understanding how our service is used and **users' behavior** to **improve our service**, securing our data and systems and fighting against spam, abuse, fraud, infringement and other wrongdoings.*

*We **may** also share information with other Match Group companies for legitimate business purposes **such as** corporate audit, **analysis** and consolidated reporting as well as compliance with applicable laws. We **may** also share user information with other Match Group companies to remove users who violate our terms of service, or have been reported for criminal activity and/or bad behavior. In some instances, we **may** remove that user from all platforms."[24]*

Processing purpose: get assistance in processing information

Legal basis: NA

Necessity and proportionality of processing:

Tinder does not specify which data or which category of data are involved in the processing operation, which makes it impossible to assess the necessity and proportionality.

Risk: the data subjects are "*deprived of their rights and freedoms or prevented from exercising control over their personal data*" (Recital 75 GDPR) due to the following provision infringements.

a) **<u>Violation of the transparency principle</u>**

Tinder names different processing operations operated by other Match Group companies using the words "may include" and "such as". This indicates that the list is incomplete, and further processing operations could occur. In addition, the repeated usage of "may" in this paragraph is highly likely not to be in accordance with the fairness of processing (Article (5)(1)(a) GDPR). Tinder's controller must demonstrate that this ambiguous language cannot be avoided. Otherwise, they are non-compliant with the principle of accountability [22] as well.

Furthermore, Tinder neither names the legal basis nor the categories of personal data processed by other Match Group companies. Consequently, the requirement for transparency is not met.

b) <u>Violation of the principle of purpose limitation</u>

While Tinder names ten examples, Match Group owns more than 45 dating brands [34], with which the personal data can be shared for different processing purposes, like marketing, targeted advertising, and to improve their service.

Tinder indicates in their collection chapter that the primary purpose of collecting the users' personal information is to provide their service (see chapter 5.2.1), which is showing the users suitable matches. Making personal data available to possibly 44 other dating brands for targeted advertising and other purposes is not in the sense of Article 5(1)(b) GDPR, which states that personal data must not be processed in further ways which are not in accordance with the original purposes.

Hence, Tinder violates the principle of purpose limitation.

Severity: high

Measures:

a) Tinder must describe all processing operations operated by other Match Group companies, define the legal bases, and avoid vague modal verbs.

b) As discussed in table 07, Tinder should request data subjects' opt-in consent for automated individual decision-making and profiling for targeted advertising and marketing purposes. For the processing operations not listed, Tinder must assess whether the purposes are compatible with the original purpose and on which legal basis (Article (6)(1) GDPR) they can rely for the processing. Finally, the data subjects must be informed about the outcomes (purpose, affected personal data, legal basis) in the privacy policy, and if applicable, user consent must be gained prior to the processing.

The processing operations should be reviewed regularly to identify processes that differ from the original purposes. If applicable, the data subjects must be informed again.

Residual risk: low

If Tinder implements the measures and conducts regular reviews of processing operations, the residual risk is low.

5.4.2. Share personal information with providers and partners

06	**Processing operation:**	Share personal information with providers and partners to operate and improve services

Provided information:
*"We use **third parties** to help us operate and improve our services. These third parties assist us with various tasks, **including** data hosting and maintenance, **analytics**, customer care, **marketing**, **advertising**, payment processing and security operations.*
*We **may** also share information with **partners** who distribute and assist us in advertising our services. **For instance**, we **may** share **limited information** on you in hashed, non-human readable form to advertising partners.*
We follow a strict vetting process prior to engaging any service provider or working with any partner. All of our service providers and partners must agree to strict confidentiality obligations." [24]

Processing purpose: operate and improve service

Provided legal basis: NA

Necessity and proportionality of processing:
Tinder does not specify which data or which category of data are involved in the processing operation, which makes it impossible to assess the necessity and proportionality.

Risk: the data subjects are "*deprived of their rights and freedoms or prevented from exercising control over their personal data*" (Recital 75 GDPR) due to the following provision infringements.

a) **<u>Violation of the transparency principle</u>**
Tinder does not provide details on which personal information is shared. Additionally, in the first text section, Tinder does not explain in particular how the third parties assist them in improving their service. Regarding the second text section, there is no information about which conditions must apply to share user information for advertising purposes and to whom. Tinder repeatedly gives a single example regarding sharing information with partners, which raises again the question of which other scenarios exist. Moreover, it is not sufficiently clear when Tinder shares hashed personal data and when they do not.
So, the provided information does not meet the requirement of transparency pursuant to Article (5)(1)(a) GDPR.

b) <u>Violation of the privacy by design approach, the integrity and confidentiality principle, and the security of processing</u>

For meeting the privacy by design approach, it must be assured that personal data is not accessible to an indefinite number of natural persons without the individual's intervention. (Article (25)(2) GDPR) So, Tinder profile pictures should be only visible to other Tinder users. However, the profile pictures of all 57 million users are hosted and accessible on AWS without requesting any authentication (see details in chapter 5.4.3). As a result, the privacy by design approach is not met.

Additionally, the missing authentication does not comply with the security of processing pursuant to Article 32 GDPR and the integrity and confidentiality principle according to Article (5)(1)(f) GDPR, as both articles demand ongoing confidentiality of personal data.

c) <u>Violation of the principle of purpose limitation</u>

Tinder shares personal data with third parties for analytics, marketing, and advertising purposes. However, the data was mainly collected to show matches to Tinder users and provide service.

So, unlike Article (5)(1)(b) GDPR, the personal data is processed in further ways which are not in accordance with the original purpose. Hence, Tinder violates the principle of purpose limitation.

Severity: high

Measures:

a) Tinder must provide the categories of the affected personal data. Additionally, they must inform the data subjects with which third parties their personal data is shared and how the third parties assist them. Furthermore, Tinder must specify in which cases the personal data will be hashed before sharing and in which cases it will not. Ideally, Tinder should anonymize all personal data shared with their partners.

b) Tinder needs to implement technical measures to ensure that only authorized entities can access the data subjects' profile pictures. This could be solved using session cookies, tokens, or other authentication mechanisms. Tinder must evaluate the adequacy of the chosen mechanism in terms of potential attacks that could negatively affect the security of processing.

c) As discussed in tables 05 and 07, Tinder should request data subjects' opt-in consent for automated individual decision-making and profiling for targeted advertising and marketing purposes.

Residual risk: low

After the correct implementation of the measures, the risk is low. The prerequisite is that the chosen authentication mechanism is secured at least against common and widely used attacks.

5.4.3. Practical analysis of Tinder's personal data sharing

While analyzing Tinder's network traffic, it turned out that the profile picture of the test user can be retrieved with the following link.

https://images-ssl.gotinder.com/5ff60c6db44ee70100038475/640x800_822c855e-bdb6-4365-88ca-958ce2186ec1.jpg

Further analysis revealed that images of Tinder users are stored following the format: https:// images-ssl.gotinder.com/userID/resolution/imageID.jpg

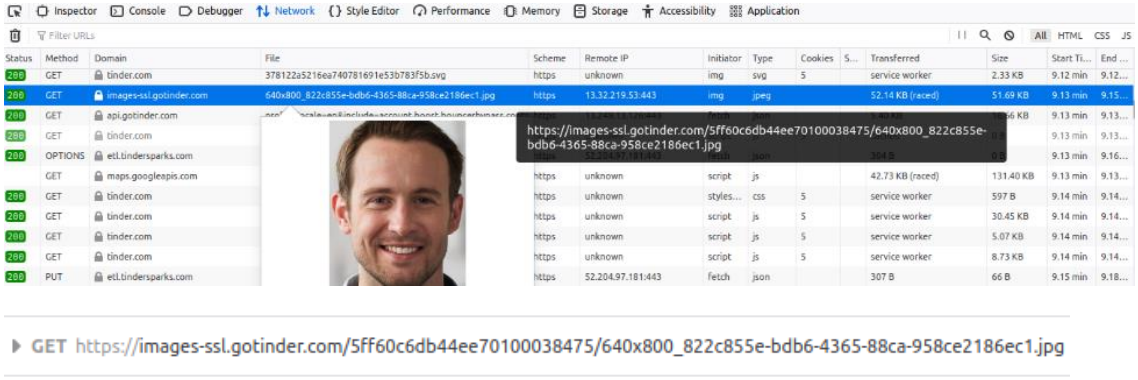


Figure 15: Network traffic.

To prevent using biometric information of natural persons, we used a synthetic image for the test user. The profile picture was generated by a Generative Adversarial Network (GAN) and shows a non-existent person obtained from https://thispersondoesnotexist.com/ by Karras et al. and Nvidia [35].

The page information and certificate reveal that the pictures are stored on an AWS server (Server CA 1B) in the US.

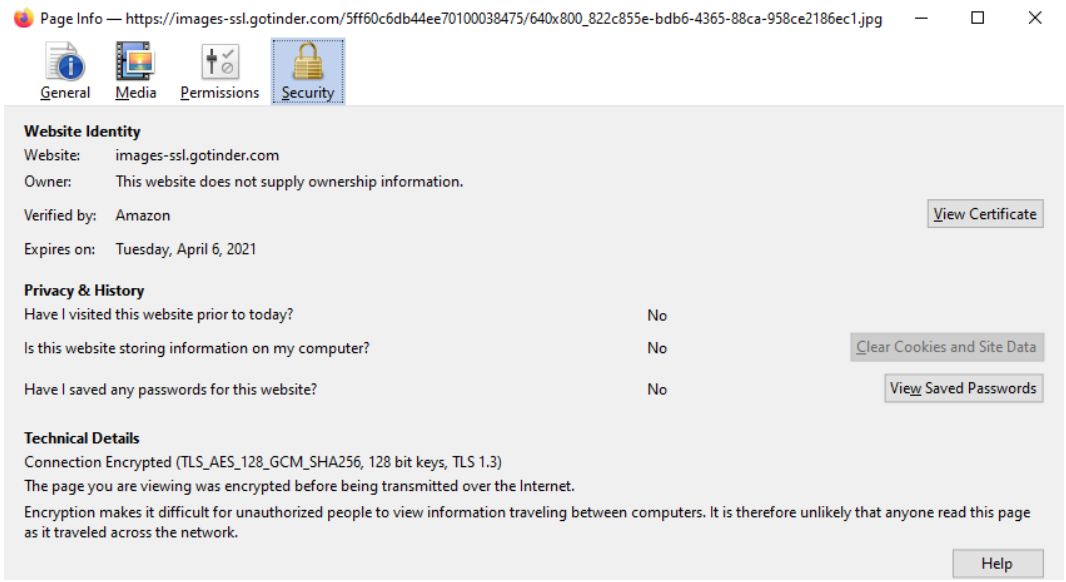


Figure 16: Page information of images-ssl.gotinder.com.

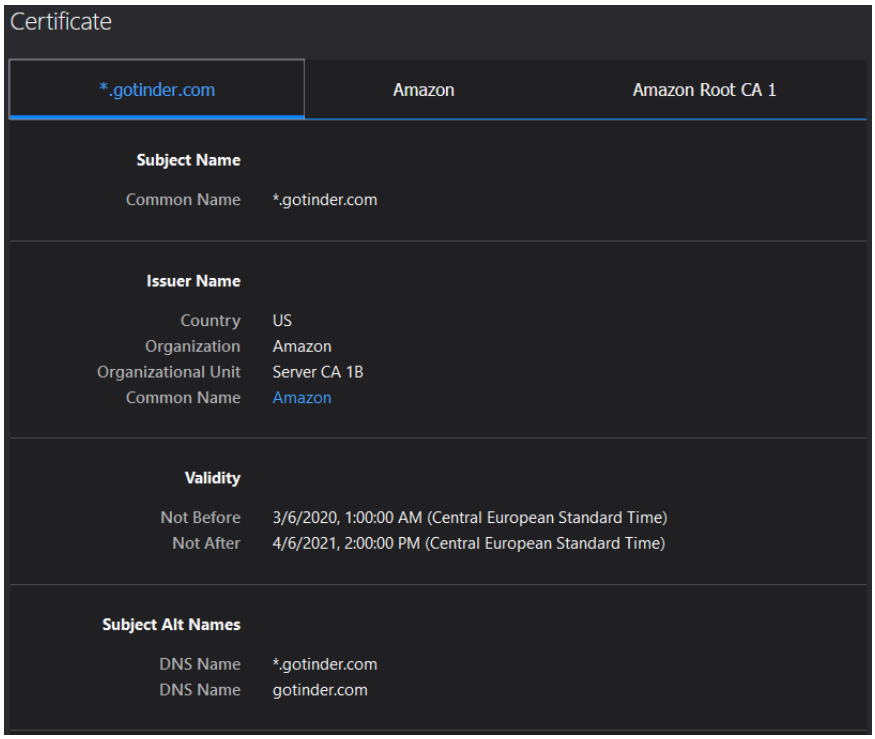


*Figure 17: Certificate of *gotinder.com*

While analyzing the network traffic, it turned out that the profile picture is accessible on AWS without providing any authentication. It can be retrieved by anyone if the URL is known.

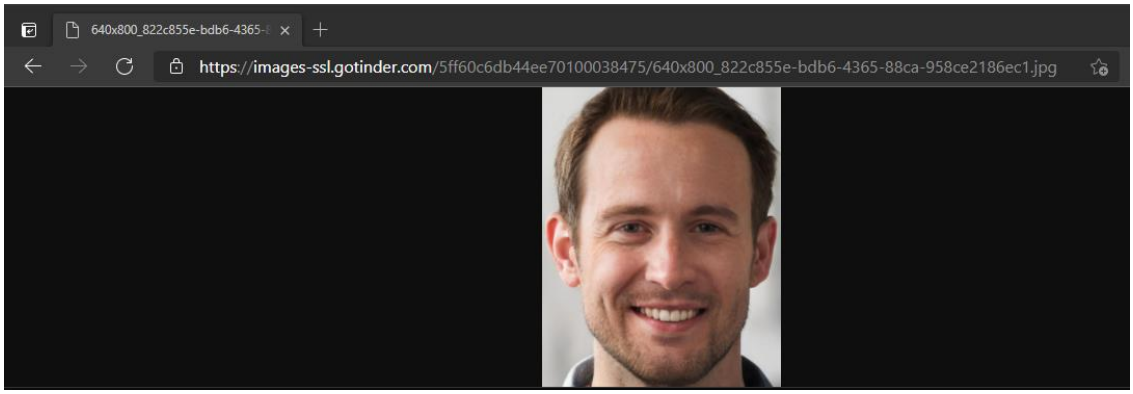


Figure 18: Freely accessible profile picture of our test user.

This can be reproduced with any image of any Tinder user. Hence, the profile pictures of all 57 million users are hosted and accessible on AWS and can be accessed by anyone without providing authentication, which violates the integrity and confidentiality principle pursuant to Article (5)(1)(f) GDPR, the privacy by design approach according to Article 25 GDPR, and the security of processing pursuant to Article 32 GDPR.

5.5. Usage of information

Tinder conducts automated individual decision-making and profiling to serve relevant ads and offers, improve and develop new services, and prevent illegal and unauthorized activities.

The GDPR defines profiling as

> *„any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements"* (Article (4)(4) GDPR).

5.5.1. Automated individual decision-making and profiling for ads and offers

07	Processing operation:	**Automated individual decision-making and profiling to serve relevant ads and offers**

Provided information:

"*To serve you relevant offers and ads*

- *Administer sweepstakes, contests, discounts or other offers*
- *Develop, display and **track** content and advertising **tailored** to your interests on our services and other sites*
- *Communicate with you by email, phone, social media or mobile device about products or services that we think may interest you*" [24].

Processing purpose: serve relevant offers and ads

Legal basis: legitimate interests according to Art(6)(1)(f).

> *"We **may** use your **information** where we have legitimate interests to do so. **For instance**, we **analyze users' behavior** on our services to continuously improve our **offerings**, we **suggest offer**s we think might interest you, […] and other legal purposes"[24].*

Necessity and proportionality of processing:

Tinder does not specify which data or which category of data are involved in the processing operation, which makes it impossible to assess the necessity and proportionality.

Risk: the data subjects are "*deprived of their rights and freedoms or prevented from exercising control over their personal data*" (Recital 75 GDPR) due to the following provision infringements.

a) <u>Violation of the transparency principle</u>

Decision-making and profiling are processes that are often invisible to the data subjects and, depending on their knowledge, challenging to comprehend. [36] Specific information must be provided by the controller so that the data subjects can fully understand the procedure. As profiling generates new personal data not provided by the data subjects themselves [36], the categories of the indirectly derived personal data must be provided (Article 14(1)(d) GDPR). However, in the case of Tinder, it is unclear which kind of personal data will be derived during the decision-making and profiling processes.

While Tinder states that they tailor contents and advertising based on the data subjects' interests, they do not explicate how they identified them. Providing the information that they "for instance" analyze user's behavior to improve their services is not specific.
As a result, Tinder violates the transparency principle.

b) <u>Violation of the principle of the lawfulness of processing</u>

In general, legitimate interest can apply for direct marketing purposes (Recital 47 GDPR). However, according to Article 6(1)(f) GDPR this only applies if the interest of the controller does not outweigh the interests or fundamental rights and freedoms of the data subject. The decision of whether the controller's interest outweighs the interest of the data subject requires an assessment (Recital 47 GDPR). The WP29 states that in general, it is "*difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering*" [36]. [37]
Also according to the DSK, intervention-intensive measures like profiling used for advertising purposes implies that the controller's interests outweigh the data subjects' interests and hence, the data subjects should be excluded of the data processing. Additionally, in that case, the data subject's right to object (Article 21 GDPR) is not sufficient. [38] So, profiling with advertising purpose cannot be based on Article 6(1)(f) GDPR. Instead, tracking-based digital market research, advertising, and direct marketing based on tracking and profiling almost always requires free, specific, informed and unambiguous "opt-in" consent. [39] [37]
Consequently, Tinder cannot rely on legitimate interest for the automated individual decision-making and profiling for advertising and marketing purposes.

Severity: high

Measures:

a) Tinder must provide specific information about the decision-making and profiling so that the data subjects can fully understand how the personal data was retrieved. Also, the categories of the indirectly derived personal data must be named.
Additionally, Tinder should evaluate if their artificial intelligence systems comply with the "*Proposal for a Regulation laying down harmonised rules on artificial intelligence*" published by the European Commission [20].

b) Tinder should request opt-in consent from the data subjects for conducting automated individual decision-making and profiling for advertising and marketing purposes.

Residual risk: low
If Tinder informs the data subjects adequately and requests valid consent, the risk is low.

5.5.2. Automated individual decision-making and profiling for Tinder services

08	**Processing operation:**	Automated individual decision-making and profiling to improve and develop new services

Provided information:

"*To improve our services and develop new ones*

- *Administer focus groups and surveys*
- *Conduct **research and analysis of users' behavior** to improve our services and content (**for instance, we may** decide to change the look and feel or even substantially modify a given feature based on users' behavior)*
- *Develop **new features and services (for example, we may** decide to build a new interests-based feature further to requests received from users)*" [24].

Processing purpose: improve and develop services

Legal basis: legitimate interests according to Art(6)(1)(f)

"*We may use your information where we have legitimate interests to do so. For instance, we analyze users' behavior on our services to continuously improve our offerings, we suggest offers we think might interest you, […] and other legal purposes*" [24].

Necessity and proportionality of processing:

Tinder does not specify which data or which category of data are involved in the processing operation, which makes it impossible to assess the necessity and proportionality.

Risk: the data subjects are "*deprived of their rights and freedoms or prevented from exercising control over their personal data*" (Recital 75 GDPR) due to the following provision infringement.

<u>Violation of the transparency principle</u>

- **Bullet-point 2:** As discussed in table 07, Tinder must inform the data subjects about the categories of the newly and indirectly derived personal data (Article (14)(1)(d) GDPR). Additionally, the statement gives no information about which contents and services they want to improve. The lack of precision in Tinder's formulation and providing only a single example is not in the sense of the transparency principle.
- **Bullet-point 3:** This sentence has a high similarity with the poor practice example from chapter 5.1.1. It is unclear which kind of features and services Tinder wants to develop and to which specific purpose. In addition, they do not list which type of data they want to process and how this data can serve to build the features and services. Again, providing a single possible example is not specific enough and allows Tinder unrestricted freedom of action.

As a result, Tinder violates the transparency principle.

Severity: high

Measures: Tinder must specify the features and services they want to improve, the categories of the indirectly derived personal data, how this data is used, and for which purposes. Additionally, Tinder should evaluate if their artificial intelligence systems comply with the "*Proposal for a Regulation laying down harmonised rules on artificial intelligence*" published by the European Commission [20].
Residual risk: low If Tinder informs the data subjects adequately, the risk is low. Tinder could consider to requests valid consent for the automated decision-making and profiling procedure.

5.5.3. Automated individual decision-making and profiling for security purposes

09	**Processing operation:**	Automated individual decision-making and profiling to prevent illegal and unauthorized activities

Provided information:

"*To prevent, detect and fight fraud or other illegal or unauthorized activities*

- *Address ongoing or alleged misbehavior on and off-platform*
- *Perform **data analysis** to better understand and design countermeasures against these activities*
- *Retain data related to fraudulent activities to prevent against recurrences*" [24]

Processing purpose: prevent, detect and fight illegal and unauthorized activities

Legal basis: legitimate interests according to Art(6)(1)(f)

"*We **may** use your **information** where we have legitimate interests to do so. For instance, […] we **process information** for administrative, fraud detection and other legal purposes*" [24].

Necessity and proportionality of processing:

Tinder does not specify which data or which category of data are involved in the processing operation, which makes it impossible to assess the necessity and proportionality.

Risk: the data subjects are "*deprived of their rights and freedoms or prevented from exercising control over their personal data*" (Recital 75 GDPR) due to the following provision infringement(s).

a) <u>Violation of the transparency principle</u>

Tinder does not describe which personal data is processed and how the data serves to prevent, detect, and fight fraudulent activity. Also, Tinder does not list the categories of newly and indirectly derived personal data created during the profiling process as required in Article (14)(1)(d) GDPR.

As a result, Tinder violates the transparency principle.

b) <u>Violation of the privacy by design approach, the integrity and confidentiality principle, and the security of processing</u>

The Tinder API's rate limiting allows accessing four user profiles per second for an unlimited time (see chapter 5.5.4). For regular app usage, this threshold seems to be too high. Given this rate limit, datasets containing the Tinder users' information can be created efficiently by constantly querying the API. Attackers can use such datasets for querying any information of interest. For instance, this information can be used to spy or blackmail employees working in certain companies or discriminate, surveil, or threaten particular users. Additionally, the database can be sold or made publicly available.

To comply with the integrity and confidentiality principle, Tinder must use appropriate technical measures to protect the users' data against unauthorized or unlawful processing (Article (5)(1)(f)). Also, the data protection by design and by default approach (Article 25 GDPR) and the security of processing requirement (Article 32 GDPR) necessitate appropriate safeguards to protect the data subjects' rights. Hence, Tinder is not in accordance with these GDPR articles.

Severity: high

Measures:

a) Tinder must explain which categories of personal data are processed, which types of personal data are derived, and how the decision-making and profiling procedure serves to prevent, detect, and fight fraudulent activity.
Additionally, Tinder should evaluate if their artificial intelligence systems comply with the "*Proposal for a Regulation laying down harmonised rules on artificial intelligence*" published by the European Commission [20].

b) Tinder should adjust the rate limit to a reasonable threshold.

Residual risk: medium
If Tinder implements an adequate rate limit, building a user dataset is less efficient. However, the risk is still present. Consequently, the residual risk is medium.

5.5.4. Practical analysis of the effectiveness of Tinder's bot prevention

Tinder states that they conduct profiling to prevent illegal and unauthorized activities. This chapter assesses the effectiveness of Tinder's profiling prevention system. To do so, we are directly querying Tinder's API without using any of their apps or web frontend.

Experiment setup

(1) We use a python script to establish a connection to the Tinder API in order to access information about Tinder users, including their name, user id, age, birthdate, distance, Instagram user name, bio, gender, job, and sexual preference. The data will be temporarily stored in a local SQLite database for further analysis. Our script uses a tool called "pynder" which is used to query the Tinder API. It can be found on Github[4].
(2) By using our python script, we test Tinder's rate limit.
(3) We use Apache Superset[5], a business analytics tool, to access the SQLite database, run SQL queries, and visualize the data on a dashboard.

The following figure summarizes the first step of the experiment.

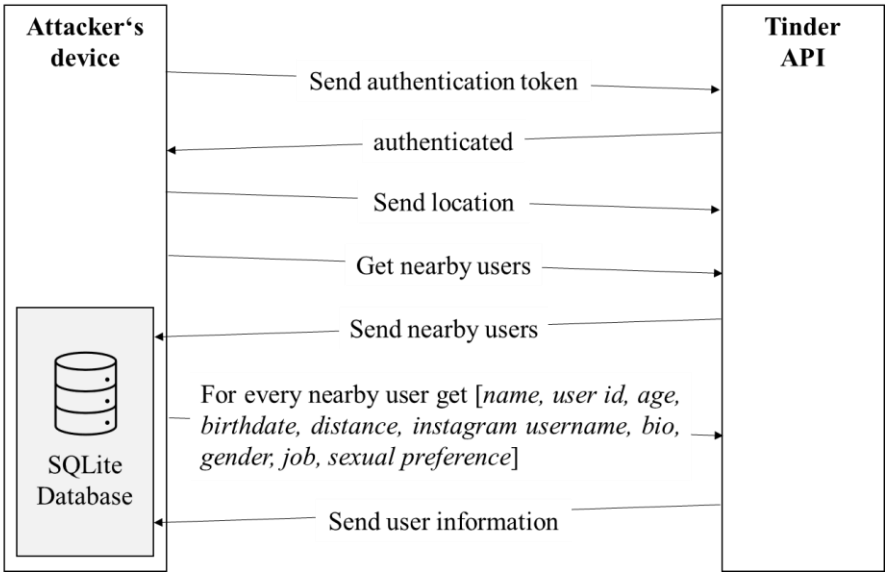


Figure 19: Requesting user information from the Tinder API.

[4] https://github.com/charliewolf/pynder
[5] https://superset.apache.org/

(1) Obtaining the authentication token, setting the location, and run the script

First, we need to obtain a valid authentication token. The authentication token can be extracted from the network traffic during an authenticated session by analyzing a GET request header to api.gotinder.com.

We insert the authentication token into the respective variables, provide a location and start querying the Tinder API. The API returns the data of nearby users.

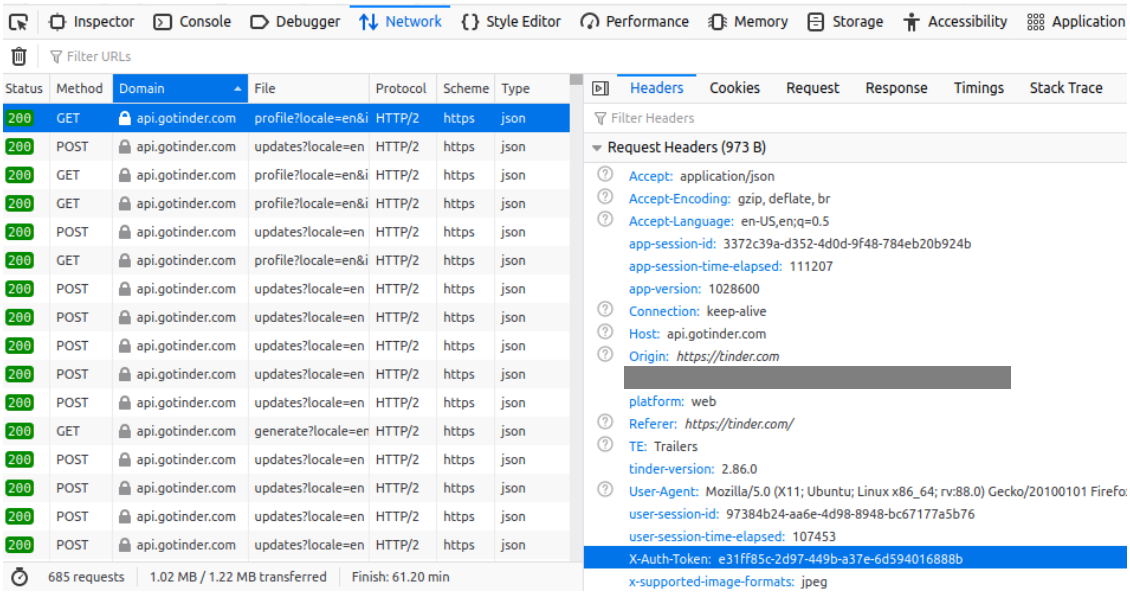


Figure 20: Gaining the X-Authentication Token.

```
root@ubuntu:/home/meike# nano filldb.py
```

```
# TINDER API
X_Auth_Token = 'e31ff85c-2d97-449b-a37e-6d594016888b'
session = pynder.Session(XAuthToken=X_Auth_Token)
print('authenticated: ' + str(session.profile))
```

Figure 21: Inserting the authentication token into the script.

The script establishes a connection to our SQLite database and authenticates our test user named "Max" to the Tinder API. Then, it proceeds with requesting nearby users. In order to be able to visualize the data, we insert it into our SQLite database.

To ensure GDPR compliance with our Proof-of-Concept, we need to make sure not to store personal data without having the consent of data subjects. Consequently, we aim to store minimal data and avoid storing (biometric) images. As Tinder stores images on AWS without requiring any authentication, we can just store a link. The image itself resides on AWS. (Noise is added to variables such as birthdate by Tinder to prevent the identification of individuals.)

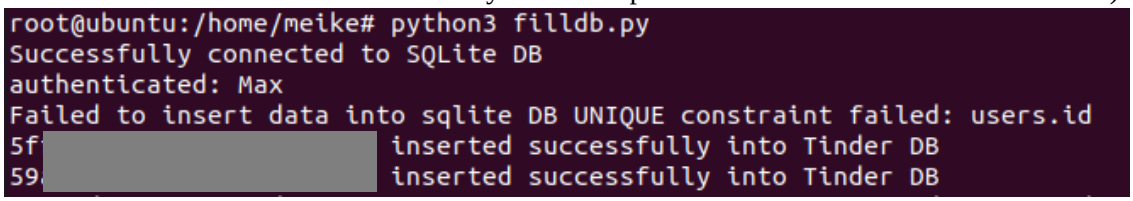


Figure 22: Executing the python script.

The following algorithm explains how our script requests the user data and saves them into the SQLite database (see annex and https://github.com/Meike-m/getProfiles for details and the code of this attack). As our test user is male, the script assigns the proposed male users to LGBTQ (Lesbian, Gay, Bisexual, Transsexual, Queer).

Algorithm Gaining user data of Tinder users interested in men

```
1:  Input: location l, authentication token aT, database DB
2:  Output: DB filled with user information
3:  Procedure:
4:    establish a connection with the Tinder API using aT
5:    send l to the Tinder API
6:    request profiles of nearby users N
7:    for every user i in N do
8:      id = id(i)
9:      age = age(i)
10:     birthdate = birthdate(i)
11:     distance = distance(i)
12:     instagram = instagram(i)
13:     biography = biography(i)
14:     gender = gender(i)
15:     job = job(i)
16:     if gender = male then
17:         LGBTQ = 1
18:     end if
19:     if gender = female then
20:         LGBTQ = 0
21:     end if
22:     photos = photos(i)
23:     if id(i) does not exist in DB
24:         save all information of i in DB
25:     end if
26:   end for
27: end procedure
```

(2) Test the rate limit

To verify whether Tinder's profiling to prevent illegal and unauthorized activities is effective, we tested the rate limit of their API. When waiting for less than 250ms between queries on average, Tinder begins temporarily blocking our account. The time until we are being blocked depends on the rate of request per second. Hence, we are able to retrieve the personal information (non-images) of four users per second or four image links of a given user.

Delay between requests in ms	Time before being blocked
0 - 50	10 min 40 sec
25 - 75	18 min 10 sec
50 - 100	25 min
100 - 150	39 min 46 sec
200 - 300	60 min +

Table 2: Results of testing Tinder's rate limit.

Our experiment shows that the Tinder API rate limiting is effective when accessing more than four user profiles per second. However, the threshold appears to be too high considering the typical user behavior of dating apps.

While completely avoiding the attack is hard to accomplish, Tinder could adjust the rate to a reasonable limit.

(3) Draw conclusions about the users

Using Apache Superset, we created a dashboard that shows selected metrics about the Tinder users queried in the step above, such as the number of cached users, sexual preferences, and a bar chart showing the age distribution by gender. Additionally, the user table is visualized below. Note that we do not store the images themselves, but only a link.

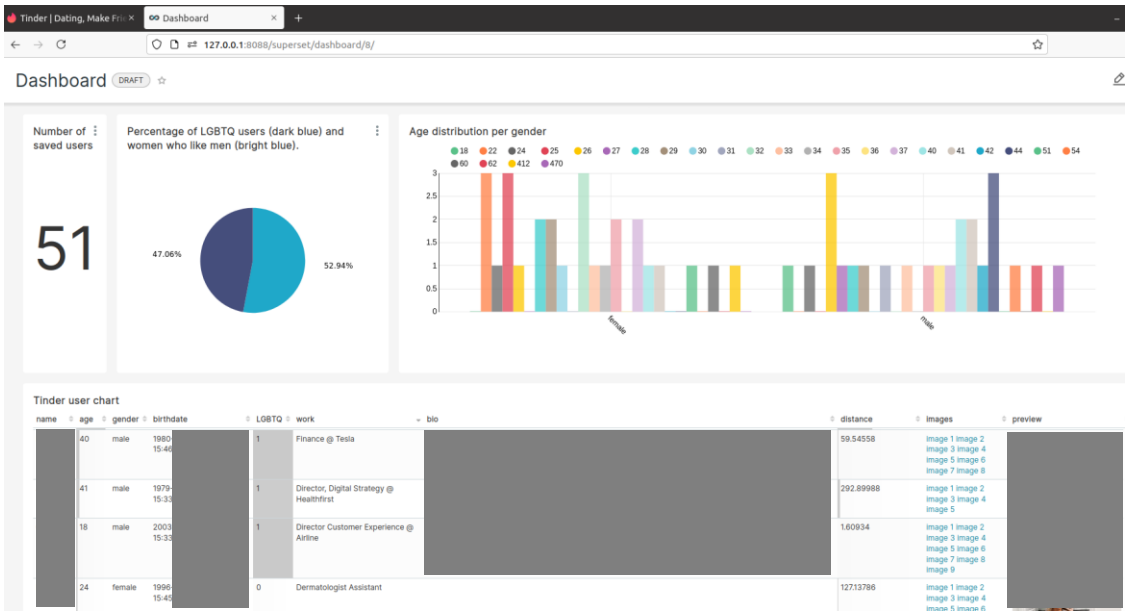


Figure 19: Tinder user dashboard.

<u>Being able to query the Tinder API from any device has the following security implications:</u>

Such a dataset allows querying any information of interest, which an attacker can exploit in various ways. For instance, considering espionage, an intelligence agency or criminal organization can filter the dataset for job positions in certain companies to locate and deceive or blackmail employees.

Moreover, the insights of the dataset could pose risks of discrimination, surveillance, and physical security to LGBTQ users. Recent history shows that this threat is existent [40] [41].

Also, the database can be sold or made publicly available. For instance, in 2020, it was reported that account credentials and user data from Tinder and other dating apps were published on dark web markets [41].

The database can be used further for recognizing a person by conducting a reverse image search. So, an attacker could use a person's picture and check whether the person is saved in the database to gain its personal information.

5.6. Cross-border transfer of information

10	**Processing operation:**	Cross-border sharing of information

Provided information:
"Sharing of information laid out in Section 6 ***sometimes involves*** *cross-border data transfers,* ***for instance*** *to the United States of America and other jurisdictions. As an* ***example****, where the service allows for users to be located in the European Economic Area ('EEA'), their* ***personal information*** *is transferred to countries outside of the EEA. We use standard contract clauses approved by the European Commission or other suitable safeguard to permit data transfers from the EEA to other countries. Standard contractual clauses are commitments between companies transferring personal data, binding them to protect the privacy and security of your data."* [24]

Processing purpose: enable third party data sharing

Provided legal basis: NA

Necessity and proportionality of processing:
Tinder does not specify which data or which category of data are involved in the processing operation, which makes it impossible to assess the necessity and proportionality.

Risk: the data subjects are "*deprived of their rights and freedoms or prevented from exercising control over their personal data*" (Recital 75 GDPR) due to the following provision infringement.

<u>Violation of the transparency principle</u>
Section six of Tinder's privacy policy ("How We Share Information") does not specify which personal information is processed by third parties and partners, so by simply referring to the section, it is neither in this section. The statement that the unknown personal information is "sometimes" cross-border transferred adds additional uncertainty as the conditions on when this happens are not explained. Tinder does not explicitly state which services concern the cross-border transmission of personal data of citizens within the EU, which personal data is affected, and how it serves for the processing.
Hence, the provided information of Tinder does not comply with the transparency principle.

Severity: high

Measures:
Tinder must state which services require a cross-border transfer, specify which categories of personal data are cross-border transferred and why the processing is necessary.

Additionally, Tinder should consider the caveats about cross-border transfer discussed in the "*COMMISSION IMPLEMENTING DECISION on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*"[42], published on June 4, 2021. According to the decision, Tinder must approve that the processors ensure appropriate data protection measures that meet the requirements of EU law. As discussed in table 6 and chapter 5.4.3, the Tinder users' profile pictures are hosted on a server in the US, where the pictures' security and privacy are not ensured. This is the first indication that Tinder's third-party service providers might not meet the

requisitions of the European Parliament and Council. Hence, Tinder should ensure that its service providers comply with EU law.
Additionally, the decision discusses that a copy of the standard contractual clauses should be provided to the data subjects to increase transparency. Also, the data subjects must be informed about the concerned categories of personal data, their right to get a copy of the standard contractual clauses, and onward transfers. At the moment, Tinder does not inform the data subjects about their right to obtain a copy of the standard contractual clauses. So, Tinder should inform the data subjects adequately. While this section highlighted two caveats, there are further requirements that Tinder should consider.

Residual risk: low
If Tinder informs the data subjects adequately, and as long as Tinder takes measures for appropriate safeguards, the risk is low.

5.7. Gaining consent

A data subjects' consent to the processing of their personal data is only valid if it was given by a **clear affirmative** action that was **freely given, specific, informed, and unambiguous**. (Article (4)(11) GDPR). Recital 42 of the GDPPR further states that "*a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using **clear and plain language** and it should not contain unfair terms.*"

Tinder's practice of gaining consent is discussed below. The examination takes into account the *Guidelines 05/2020 on consent under Regulation 2016/679* [25], published by the EDPB (European Data Protection Board).

How Tinder gains consent:

When creating an account, Tinder provides the information that:

> "*By clicking Log In, you agree to our Terms. Learn how we process your data in our Privacy Policy and Cookie Policy*."

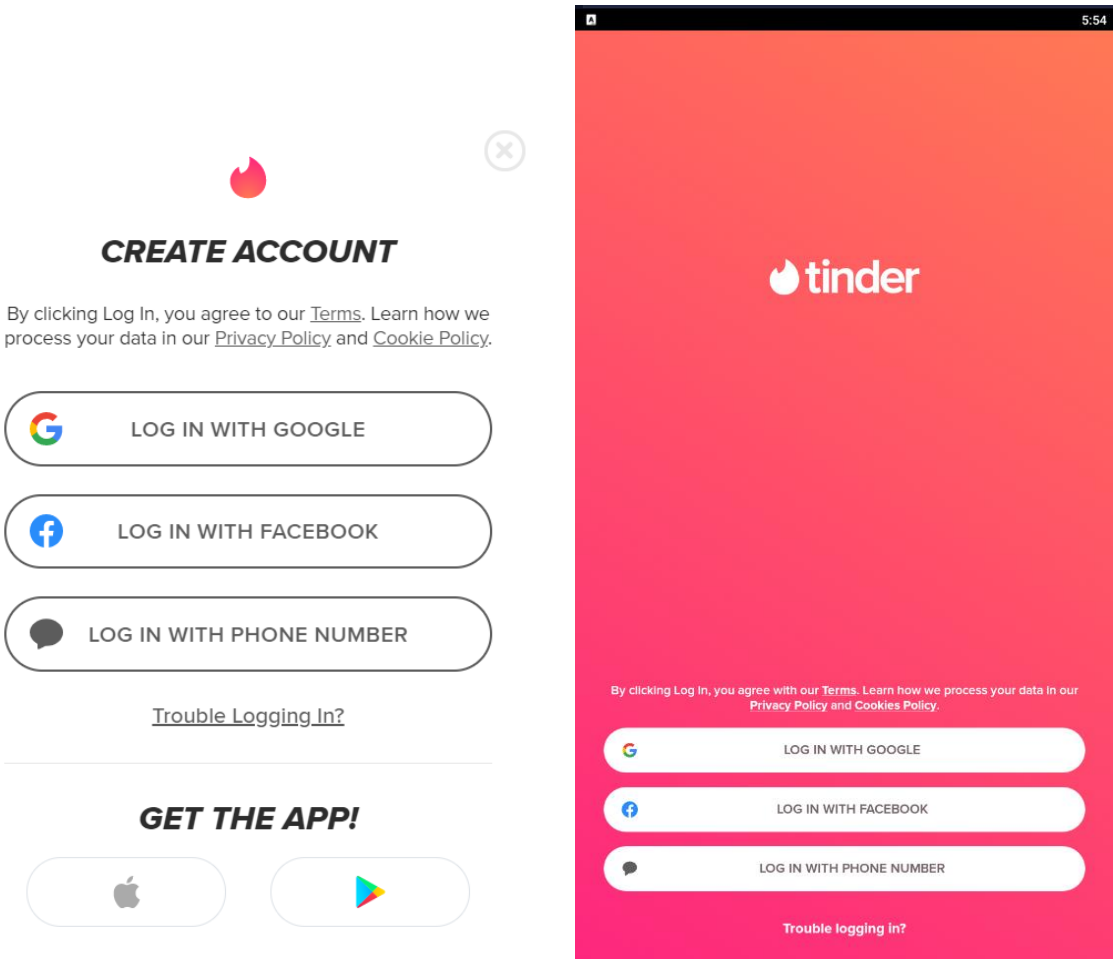


Figure 23: Login using the browser version (left) and the Android app (right).

The privacy policy is not directly shown during the account creation. Details about the privacy policy can be found by following the provided links to the terms and policies. When revoking the terms of use link, the user can read that

> "*By creating a Tinder account, whether through a mobile device, mobile application or computer (collectively, the "Service") you agree to be bound by (i) these Terms of Use, (ii) our Privacy Policy, Cookie Policy, […]*". [43]

This practice contradicts with the elements of valid consent [25] as follows.

Informed

A request for consent must be concise and clear. [25] But the statement provided by Tinder when creating an account does not clearly ask whether the users accept the processing of their data, and it does not inform the data subject that they accept the privacy policy when creating an account. Instead, it only says that they can learn how Tinder processes their data. However, according to the EDPB, "*the declaration of consent must be named as such. Drafting […] does not meet the requirement of clear language*." [25]

So, Tinder's request for consent is neither concise nor clear. The user can only infer that if they accept the terms of use, they accept the privacy policy as well by following the link to the terms of use to read them. While Tinder states in its terms of use that creating an account is bound with agreeing to the privacy policy, this still does not meet the requirements of the GDPR because "*if consent is requested by electronic means, the consent request has to be separate and distinct, it cannot simply be a paragraph within terms and conditions, pursuant to Recital 32*." [25]

Additionally, as discussed in chapters 5.2-5.6, when reading Tinder's information about processing operations is not always clear which personal data is involved or what the purposes are. However, according to the EDPB, this information is required for informed consent. [25]

So, Tinder does not comply with the requirement of informed consent.

Unambiguous indication of wishes

For valid consent, the data subjects must agree actively to the processing of their data, and it must be obvious to the data subjects that they are giving consent. As discussed above (informed consent), before creating an account, Tinder provides the information that the users can learn how Tinder processes their information in their privacy policy. However, it is not evident that by clicking "Log in," the user gives consent to the processing. Tinder's statement in the Terms of Use is also not sufficient when it comes to the requirement of an unambiguous indication of wishes, as

> "*consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal data. The GDPR does not allow controllers to offer pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement (for example 'opt-out boxes')*." [25]

So, the data subjects do not give consent in a clear affirmative act.

Freely given

Consent is freely given if the data subject has a real choice. There must not be an imbalance of power, conditionality, a lack of granularity, and detriment.

Tinder's practices lead to a violation of freely given consent because of the consent's conditionality and lack of granularity:

- **Granularity**
  According to Recital 43 of the GDPR, consent is not freely given if there is no possibility to give separate consent to different personal data processing operations, even though it would be appropriate. Additionally, Recital 32 GDPR declares that

  > "*Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them."*

  Tinder's service includes several processing operations for different purposes (see chapter 5.2-5.6). However, even though it is appropriate, the data subjects cannot granularly give consent to them. For instance, Tinder conducts automated decision-making and profiling to show the users ads on and off their service, to measure the effectiveness of ads, and to provide offers and discounts tailored to the user profile. Another example is that Tinder does not give the data subjects the opportunity to give granular consent to the sharing of personal data with third parties. These procedures differ from and are not necessary for serving Tinder's core service: showing suitable matches to the users. Hence, it is appropriate to allow separate consent to these different personal data processing operations. As this opportunity is not provided, the user's consent is not freely given.

- **Conditionality**
  Tinder bundles consent to not strictly necessary processing operations (see above) with consent to the contract and the provision of its service, which contrasts with Article (7)(4) GDPR:

  > *"When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."*

  The only choice a data subject has is either using the app and accepting all the additional processing purposes or not using the app at all. However, according to the EDPB, "*Compulsion to agree with the use of personal data additional to what is strictly necessary limits data subject's choices and stands in the way of free consent*." [25]

Specific

Consent must be given for a specific purpose or specific purposes (Article (6)(1)(a) GDPR). The requirement for specificity is closely linked to the requirements for informed consent and granularity and aims to give the data subjects control and transparency. So, for the consent to be specific, the controller must ensure that for every consent request, it is clear which data is involved in the processing and for which purpose. Additionally, the consent request must be granular. [25]

As already discussed, Tinder bundles different processing purposes in one policy without enabling the data subject to give granular consent. Also, Tinder repeatedly does not specify which data are affected in certain processing operations and lacks specificity in its purpose definitions.

As a result, Tinder does not meet the elements of valid consent. Hence, the data subjects' consent to the privacy policy is invalid. Consequently, Tinder could violate Article 6 GDPR, which means that the processing of the personal data concerned would be unlawful.

6. Conclusion

Tinder processes personal data, including name, age, gender, geolocation, job, and details on the personality of its users. Moreover, Tinder processes special categories of personal data according to Article 9 GDPR, such as biometric data and sexual orientation. Tinder is accountable for protecting this sensitive data and is obliged to comply with the GDPR. However, our assessment shows that Tinder does not comply with the following GDPR articles.

- **The transparency principle pursuant to Article (5)(1)(a) and (12)(1) GDPR**
  Tinder's privacy policy is comparatively long but at the same time contains very little information. All in all, Tinder provides incomplete and unspecific information about their processing operations regarding the affected personal data, the sources of personal data, the legal bases for processing, and the processing purposes.
  This practice hinders data the subjects from making informed decisions and from keeping control over their data.

- **The purpose limitation principle pursuant to Article 5(1)(b) GDPR**
  Tinder processes the data subjects' personal data for purposes not compatible with the original purpose. So, the data subjects' data is processed in a way they cannot reasonably expect.

- **The data minimization principle pursuant to Article (5)(1)(c) GDPR**
  By collecting personal data not relevant for providing service, Tinder violates the data minimization principle.

- **The lawfulness of processing pursuant to Article (6) GDPR**
  Tinder uses analytics cookies without the users' consent, gains invalid consent to the privacy policy, and does not request consent for decision-making and profiling for marketing and advertising purposes.

- **The "Information to be provided where personal data are collected from the data subject" pursuant to Article (13) GDPR**
  Tinder infringes the data subjects' rights by providing no legal basis for collecting personal data received by partners, not describing all categories of processed personal data, giving insufficient information about their partners, and keeping back the purposes for collecting personal data during the users' service usage.

- **The "Information to be provided where personal data have not been obtained from the data subject" pursuant to Article (14) GDPR**
  Tinder violates the data subjects' rights by providing no legal basis and data categories for collecting personal data received from unknown types of partners.

- **The data protection by design and by default approach pursuant to Article (25) GDPR, the security of processing according to Article (32) GDPR, and the integrity and confidentiality principle pursuant to Article (5)(1)(f) GDPR**
  Tinder violates articles 5, 25 and 32 GDPR by storing the user's profile pictures on AWS without avoiding unauthorized access, permitting weak cipher suites and deprecated protocols, and using inadequate API rate limiting.

These findings pose a high risk to the data subjects, as Tinder deprives them of their rights and freedoms and hinders them from controlling their data. So, Tinder must take measures to mitigate these risks. This work proposes countermeasures to comply with European law and to accomplish an acceptable risk level.

7. Future research

The assessment of Tinder's processing operations was done using information that is accessible and derivable from an external perspective. Further findings might arise when assessing additional internal information. Especially Tinder's matching system, which is profiling according to the GDPR, could be another point of investigation. The assessment could include an analysis of Tinder's undisclosed matching algorithm to approve GDPR compliance, for instance, concerning the data minimization principle.

Further research could also assess the possibility of calculating the approximate location of Tinder users by using several nearby accounts and applying a trilateration algorithm.

Moreover, future research could examine the GDPR compliance of other Match Group's dating brands, where we assume similar violations.

8. Bibliography

[1] SEMrush, *Most popular online dating websites worldwide in March 2020, by average monthly visits.* [Online]. Available: https://www.statista.com/statistics/1115157/most-popular-dating-sites-globally/

[2] Tinder, *What is Tinder?* [Online]. Available: https://www.help.tinder.com/hc/en-us/articles/115004647686-What-is-Tinder-

[3] M. Carman and K.-K. R. Choo, "Tinder Me Softly – How Safe Are You Really on Tinder?," in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 198, *Security and Privacy in Communication Networks: 12th International Conference, SecureComm 2016, Guangzhou, China, October 10-12, 2016, Proceedings*, R. Deng, J. Weng, K. Ren, and V. Yegneswaran, Eds., Cham, s.l.: Springer International Publishing, 2017, pp. 271–286.

[4] N. P. Hoang, Y. Asano, and M. Yoshikawa, "Your neighbors are my spies: Location and other privacy concerns in GLBT-focused location-based dating applications," in *Opening era of smart society!: The 19th International Conference on Advanced Communications Technology : Phoenix Park, Pyeongchang, Korea (South), Feb. 19-22, 2017 : proceeding & journal*, 2017.

[5] S. Zhao *et al.*, "I Know Where You All Are! Exploiting Mobile Social Apps for Large-Scale Location Privacy Probing," in *Lecture Notes in Computer Science*, vol. 9722, *Information Security and Privacy: 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part I*, J. K. Liu and R. Steinfeld, Eds., Cham, s.l.: Springer International Publishing, 2016, pp. 3–19. Accessed: Feb. 23 2021. [Online]. Available: https://www.researchgate.net/profile/Shuang-Zhao/publication/304621107_I_Know_Where_You_All_Are_Exploiting_Mobile_Social_Apps_for_Large-Scale_Location_Privacy_Probing/links/5f3f684392851cd3020ee6b4/I-Know-Where-You-All-Are-Exploiting-Mobile-Social-Apps-for-Large-Scale-Location-Privacy-Probing.pdf

[6] G. Qin, C. Patsakis, and M. Bouroche, "Playing Hide and Seek with Mobile Dating Applications," in 2014, pp. 185–196. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-55415-5_15

[7] G. Argyros, T. Petsios, S. Sivakorn, A. D. Keromytis, and J. Polakis, "Evaluating the Privacy Guarantees of Location Proximity Services," *ACM Trans. Priv. Secur.*, vol. 19, no. 4, pp. 1–31, 2017, doi: 10.1145/3007209.

[8] A. Fattori, A. Reina, A. Gerino, and S. Mascetti, "On the Privacy of Real-World Friend-Finder Services," in *2013 IEEE 14th International Conference on Mobile Data Management (MDM 2013): Milan, Italy, 3 - 6 June 2013 ; [proceedings ; including workshops*, Milan, Italy, 2013, pp. 331–334. Accessed: Mar. 1 2021.

[9] J. Farnden, B. Martini, and K.-K. R. Choo, "Privacy Risks in Mobile Dating Apps," in *Proceedings of 21st Americas Conference on Information Systems (AMCIS 2015).* [Online]. Available: http://arxiv.org/pdf/1505.02906v1

[10] K. Kim, T. Kim, S. Lee, S. Kim, and H. Kim, "When Harry Met Tinder: Security Analysis of Dating Apps on Android," in *Lecture Notes in Computer Science*, vol. 11252, *Secure IT systems: 23rd Nordic conference, NordSec 2018, Oslo, Norway, November 28-30, 2018 : proceedings*, N. Gruschka, Ed., Cham: Springer, 2018, pp. 454–467. Accessed: Jan. 29 2021. [Online]. Available: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Your+neighbors+are+my+spies%3A+Location+and+other+privacy+concerns+in+GLBT-focused+location-based+dating+applications.&btnG=

[11] N. Mata, N. Beebe, and K.-K. R. Choo, "Are Your Neighbors Swingers or Kinksters? Feeld App Forensic Analysis," in *The 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2018)/the 12th IEEE International Conference*

on Big Data Science and Engineering (IEEE BigDataSE 2018): 2018 IEEE Trustcom/BigDataSE : proceedings : 31 July-3 August 2018, New York, New York, New York, NY, USA, 2018, pp. 1433–1439.
[12] R. Shetty, G. Grispos, and K.-K. R. Choo, "Are You Dating Danger? An Interdisciplinary Approach to Evaluating the (In)Security of Android Dating Apps," *IEEE Trans. Sustain. Comput.*, p. 1, 2017, doi: 10.1109/TSUSC.2017.2783858.
[13] Z. M. Seward, *Dating app Tinder briefly exposed the physical location of its users.* [Online]. Available: https://qz.com/106731/tinder-exposed-users-locations/ (accessed: Feb. 22 2021).
[14] M. Veytsman, *How I was able to track the location of any Tinder user.* [Online]. Available: https://blog.includesecurity.com/2014/02/how-i-was-able-to-track-the-location-of-any-tinder-user/
[15] A. Greenberg, *Tinder's Lack of Encryption Lets Strangers Spy on Your Swipes.* [Online]. Available: https://www.wired.com/story/tinder-lack-of-encryption-lets-strangers-spy-on-swipes/
[16] S. Bauer and F. Sainz, "Data Privacy Day at Apple: Improving transparency and empowering users," 2021. [Online]. Available: https://www.apple.com/newsroom/2021/01/data-privacy-day-at-apple-improving-transparency-and-empowering-users/
[17] D. Temkin, "Charting a course towards a more privacy-first web," Mar. 2021. Accessed: May 17 2021.
[18] D. Ravichandran and S. Vassilvitskii, "Evaluation of Cohort Algorithms for the FLoC API," Accessed: May 18 2021. [Online]. Available: https://raw.githubusercontent.com/google/ads-privacy/master/proposals/FLoC/FLOC-Whitepaper-Google.pdf
[19] J. Dyrkorn and B. E. Thon, "Advance notification of an administrative fine," 2021. Accessed: Mar. 21 2021. [Online]. Available: https://www.datatilsynet.no/contentassets/da7652d0c072493c84a4c7af506cf293/advance-notification-of-an-administrative-fine.pdf
[20] European Commission, Ed., "Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)," 2021.
[21] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz), "Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen, Version 2.0," 2018. [Online]. Available: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf
[22] Article 29 Working Party, "Guidelines on transparency under Regulation 2016/679," 2017.
[23] Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, Ed., "The Standard Data Protection Model: A method for Data Protection advising and controlling on the basis of uniform protection goals," Accessed: Jan. 24 2021. [Online]. Available: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V2.0b.pdf
[24] Tinder, *Privacy Policy.* [Online]. Available: https://policies.tinder.com/cookie-policy/intl/en
[25] European Data Protection Board, Ed., "Guidelines 05/2020 on consent under Regulation 2016/679," Version 1.1, 2020. Accessed: Mar. 24 2021. [Online]. Available: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf
[26] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," [Online]. Available: https://datatracker.ietf.org/doc/html/rfc8446
[27] NIST Computer Security Division (CSD), "Advanced Encryption Standard (AES) (FIPS PUB 197).," 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
[28] M. Dworkin, "Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC," 2007. Accessed: May 24 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf
[29] Q. H. Dang, "Secure Hash Standard (SHS) (FIPS PUB 180-4)," 2015. Accessed: May 24 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[30] K. A. McKay and D. A. Cooper, “Guidelines for the selection, configuration, and use of Transport Layer Security (TLS) implementations: NIST Special Publication 800-52 Revision 2,” Gaithersburg, MD, 2019. Accessed: May 25 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf
[31] E. Barker and A. Roginsky, “Transitioning the use of cryptographic algorithms and key lengths,” Gaithersburg, MD, 2019. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf
[32] D. A. McGrew and J. Viega, “The Security and Performance of the Galois/Counter Mode (GCM) of Operation,” 2004. [Online]. Available: https://eprint.iacr.org/2004/193.pdf
[33] Tinder, *Cookie Policy.* [Online]. Available: https://policies.tinder.com/cookie-policy/intl/en
[34] M. Meisenzahl, “These charts from Match Group show more people are turning to online dating during the pandemic,” *Business Insider India*, 06 Aug., 2020. https://www.businessinsider.in/tech/news/these-charts-from-match-group-show-more-people-are-turning-to-online-dating-during-the-pandemic/articleshow/77382961.cms
[35] T. Karras, S. Laine, M. Aittala, J. Hellsten, J. Lehtinen, and T. Aila, “Analyzing and Improving the Image Quality of StyleGAN,” 2019. [Online]. Available: https://arxiv.org/pdf/1912.04958.pdf
[36] Article 29 Working Party, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,” 2018.
[37] Article 29 Working Party, “Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC,” 2014. [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
[38] Bayerisches Landesamt für Datenschutzaufsicht, “Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO),” 2018. [Online]. Available: https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Entschliessungen_Datenschutzkonferenz/Inhalt/96_-Konferenz/Orientierungshilfe-der-Aufsichtsbehoerden-zur-Verarbeitung-von-personenbezogenen-Daten-fuer-Zwecke-der-Direktwerbung-unter-Geltung-der-Datenschutz-Grundverordnung-_DS-GVO_/OH_Werbung_Stand_07_11_2018.pdf
[39] Article 29 Working Party, “Opinion 03/2013 on purpose limitation,” 2013. [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
[40] M. Haider, *Two men in Detroit were shot for being gay, prosecutors say.* [Online]. Available: https://edition.cnn.com/2019/07/12/us/detroit-men-shot-for-being-gay-trnd/index.html
[41] Insikt Group®, “Online Surveillance, Censorship, and Discrimination for LGBTQIA+ Community Worldwide,” [Online]. Available: https://go.recordedfuture.com/hubfs/reports/cta-2020-0714.pdf
[42] European Commission, Ed., “COMMISSION IMPLEMENTING DECISION on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council,” Accessed: Jun. 5 2021. [Online]. Available: https://ec.europa.eu/info/sites/default/files/1_en_act_part1_v5.pdf
[43] Tinder, *Terms of use.* [Online]. Available: https://policies.tinder.com/terms/intl/en

9. List of figures

10. Annex

The python script getProfiles establishes a connection to the Tinder API to access Tinder user data and store them in a local SQLite database. The code can be found on Github[6]. To query the Tinder API, we use a tool called pynder, accessible on Github[7].

Prerequisites

Install SQLite:

> apt-get install sqlite3

> apt-get install sqlitebrowser

Install Python:

> apt-get install python3-venv

Clone and install pynder:

> git clone https://github.com/charliewolf/pynder.git

> cd pynder

> git fetch origin +refs/pull/211/merge

> git checkout -qf FETCH_HEAD

> python3 -m pip install --force-reinstall --no-deps

> pip3 install pynder

After installation, insert

- the path to the SQLite database,
- a valid authentication token, and
- the preferred location

into the python script.

Run the script

When running the following command, a connection to the SQLite database will be created, the test user will be authenticated, the location will be updated, and the data of nearby users will be stored in the SQLite database.

> python3 getProfiles.py

[6] https://github.com/Meike-m/getProfiles
[7] https://github.com/charliewolf/pynder