KATHOLIEKE UNIVERSITEIT LEUVEN

DEPARTMENT OF ENGINEERING SCIENCE

Privacy Impact Assessment for Tinder

Authors:	Hui Zeng (r0923438) Marcelina Kowalska (r0924651) Marko Cvjetko (r0924245)
Submission Date:	03.01.2023

Contents

1 Introduction

The increasing amount of data being collected worldwide, combined with sophisticated data analysis methods, has been paramount for advances in various domains, but it also led to an increase of concerns over privacy. Online dating services, which use data-savvy matching algorithms and have millions of users, provide a particularly interesting case study in terms of privacy. The business model of Tinder, the world's most popular dating service, incentivizes the collection of a large amount of data to power its machine learning algorithms and is entangled with all seven types of privacy defined by Finn, Wright and Friedewald [1] : privacy of the person, thoughts and feelings, behavior and action, personal communication, association, data and image, and privacy of location and space.

This paper discusses Tinder's functionality, stakeholders and data collection practices. Finally, we utilize the LINDDUN method to conduct a privacy impact assessment and provide recommendations aiming at enhancing user privacy.

2 Product Description and Functionality

2.1 Functionality

Tinder's basic function is swiping and matching (see Figure 1). If the user swipes the shown person right (green heart on the screen), it means that the user likes the person and would like to chat. The user can also swipe the person left (red cross on the screen) if they do not find the currently shown person interesting. The match is made only when both users swipe each other right. Then they can send messages to each other.

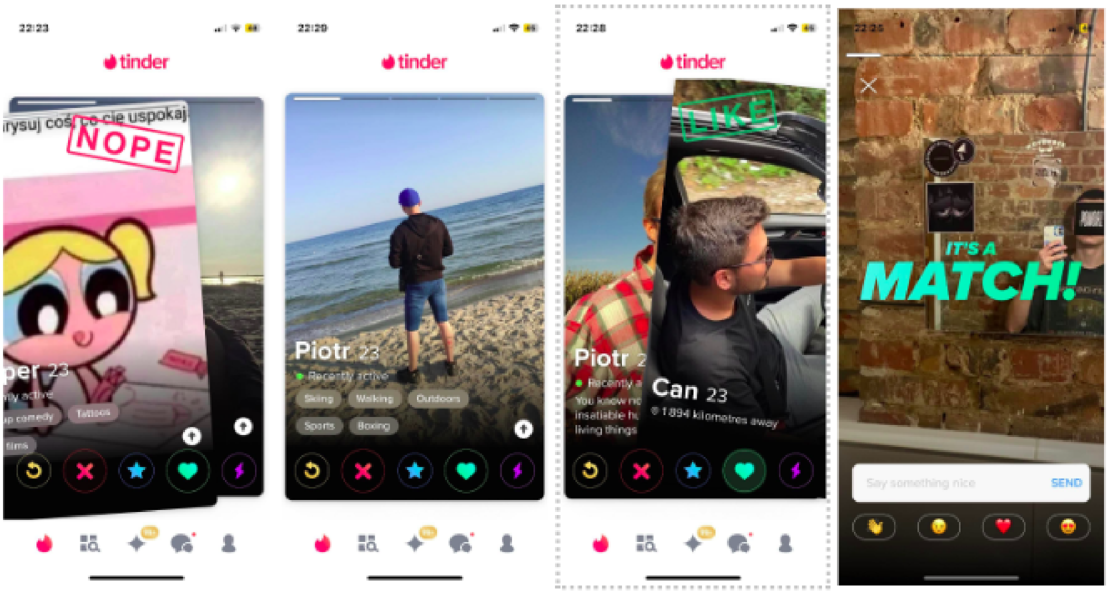


Figure 1: Tinder's user interface

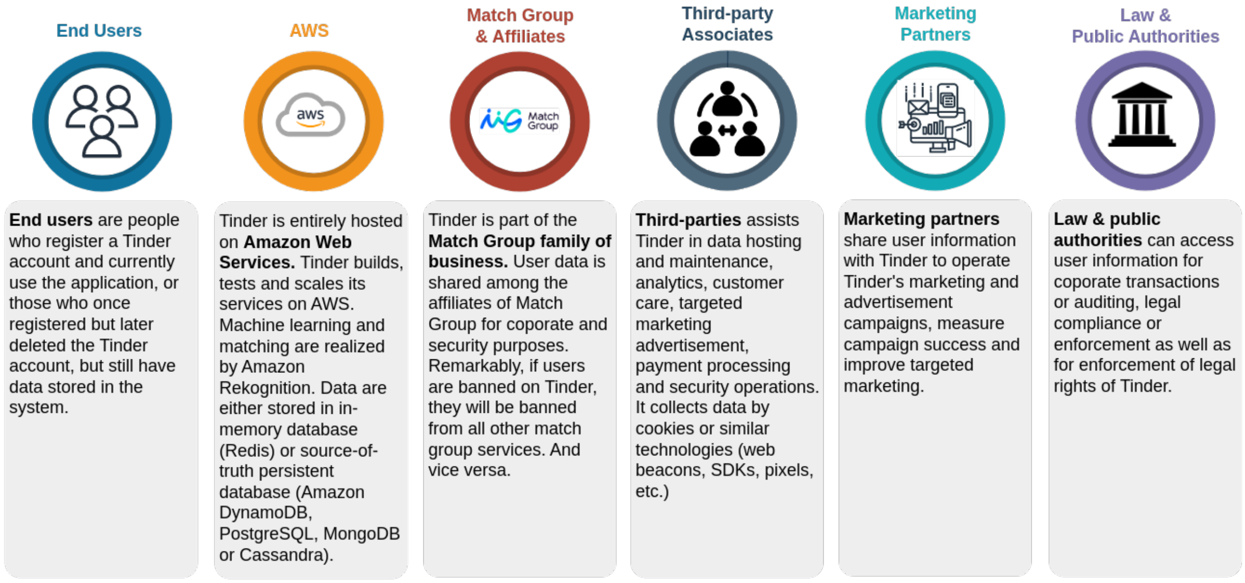
A recommendations algorithm is learning an individual profile map of potential matches in the background. It focuses mainly on the following aspects [2]:

- The activity on the application – people who use the application frequently are prioritized by the algorithm; they are more often shown to other users than less active ones,
- The proximity to other users – most potential matches are from the nearest area,
- Previous liked profiles - photo tags generated from the previous likes will be learned and profiles with similar tags will be introduced [3].

To increase user's attractiveness, the user may upgrade their profile to one of available paid premium plans. All of them offer unlimited amounts of likes and rewinds. The more expensive profiles unlock more advanced options, e.g., Tinder Plantinum users are allowed to send a message without matching with another person.

2.2 Stakeholders

The stakeholders of Tinder are those individuals or organizations that are involved in the data life-cycle (generation, transmission, computation, sharing, storage and deletion) of Tinder. With Tinder as the central data controller, six stakeholders: end users, AWS, Match Groups & affiliates, third-party associates, marketing partners as well as law & public authorities are identified [4]. A detailed explanation of each stakeholder is explicated in Figure 2.



End users are people who register a Tinder account and currently use the application, or those who once registered but later deleted the Tinder account, but still have data stored in the system.

Tinder is entirely hosted on **Amazon Web Services.** Tinder builds, tests and scales its services on AWS. Machine learning and matching are realized by Amazon Rekognition. Data are either stored in in-memory database (Redis) or source-of-truth persistent database (Amazon DynamoDB, PostgreSQL, MongoDB or Cassandra).

Tinder is part of the **Match Group family of business.** User data is shared among the affiliates of Match Group for coporate and security purposes. Remarkably, if users are banned on Tinder, they will be banned from all other match group services. And vice versa.

Third-parties assists Tinder in data hosting and maintenance, analytics, customer care, targeted marketing advertisement, payment processing and security operations. It collects data by cookies or similar technologies (web beacons, SDKs, pixels, etc.)

Marketing partners share user information with Tinder to operate Tinder's marketing and advertisement campaigns, measure campaign success and improve targeted marketing.

Law & public authorities can access user information for coporate transactions or auditing, legal compliance or enforcement as well as for enforcement of legal rights of Tinder.

Figure 2: Stakeholders of Tinder

2.3 Data Collection

Data collected by Tinder surrounds its core purpose: match recommendation and user profiling. Thus, we categorize these data into four groups [4]:

- direct data collected from user;
- indirect data collected upon usage;
- data for recommendation service;
- data collected or processed by third-party services.

An overview of data collected by Tinder is illustrated in Figure 3.

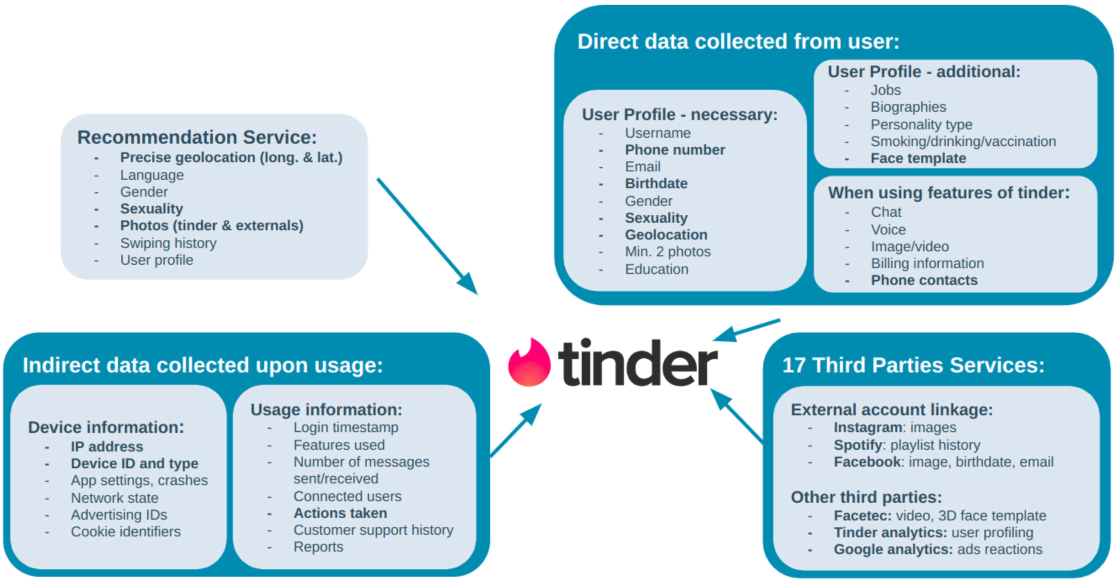


Figure 3: Stakeholders of Tinder

2.3.1 Direct data collection

Direct data mainly includes user's profile and feature data. When two users are matched, their interactions (text, images, voice and video calls) are transmitted to Tinder's server. Additional ID verification requires a selfie video that generates a 3D face template. Another feature *"Block my contact"* accesses user's phone contacts to block the profile from all selected contacts. With consent, the precise geo-location (latitude and longitude) can be retrieved both during active usage and inactively from background.

For subscribers, payment information will be collected. Moreover, subscribers of Tinder enjoy further privacy customization in keeping besides gender and sexuality (basic users) their age and distance private [5]. However, all this information is still collected by Tinder.

2.3.2 Indirect data collection upon usage

Indirect data constitutes usage and device information. The most prominent usage data are actions (left/right swipe, superlike, boost). Metadata, such as login timestamp, number of messages sent or received are collected simultaneously. Device information includes IP address, device ID and type. Such information is collected for internal technical operation analysis or forwarded to third parties.

Data about users can also be collected from other participation parties: other users, affiliates or partners of Tinder. This happens when a) a report against this user is submitted; or when b) critical information from other Match Group affiliates or c) marketing analysis from partners is received.

2.3.3 Data for recommendation

For its recommendation model, Tinder firstly filters profiles based on user's preference (e.g., language, sexuality, distance and age), then learns a profile map of potential matches by comparing profiles and reacting to their swiping history and characteristics (e.g., photo tags, number of photos viewed, time stayed on one profile).

2.3.4 Data collected or processed by third-parties

In total, Tinder places 19 third-party services, with 11 absolute necessary cookies, 2 optional marketing cookies and 5 optional advertising cookies and 1 social network access cookies. An extensive analysis of Tinder's third-party services is demonstrated in Table 1.

3 Third Parties Analysis

Table 1: Tinder's 19 Third-party Services
(Service-irrelevant data is boldfolded.)

Service Type	**Name**	**Purpose**	**Collected Data**
absolute necessary	Google Firebase [6]	release status, crash free metrics monitoring	IP address
	Tinder Analytics [7]	user analytics	device and usage data, OS, language, **location**
	Google login	login via Google	email
	Facebook login	login via Facebook	email, **photos, birthdate**
	Adyen [8]	financial transaction	IP address, **Google Analytics ID**, device type, **location**, payment (card number, expiry date, amount, currency, timestamp, category, merchant ID)
	Firebase Crashlytics [6]	app stability monitoring	Crashlytics Installation UUIDs, crash traces
	BugSnag [9]		log files, pixel tags, web bugs, web beacons
	Vonage [10]	video chats	time and duration of usage, source and destination, **job, employer, business contacts, location**, roaming status, IP address
	Spotify [11]	external profile linkage	name, email, **phone number, birthdate, gender**, country, **search queries, streaming history, playlists, library, browsing history**
	Instagram [12]	external profile linkage	name, **photos**, followers, subscribers
	Facetec [13]	identity verification	face image, photo ID document, session length, IP address, OS, SDK version, device ID, **phone model**

optional marketing	Appsflyer [14]	tracking and measurement of Tinder promotion campaigns	name, email, **phone number**, app usage data, OS, device type, IP address
	Branch [15]	profile sharing	IP address, link data, engagement data
optional advertising	Tinder direct ads Google ads [16] Tinder promotions Facebook ads	external targeted marketing	web request, IP address, browser type, language, **gender birthyear**, internet service provider, domain, timestamp, app, response
	Video Amp [17]	marketing effectiveness measurement	URL, **location**, click stream
social media permission	Adjust [18]	bridges social network access	traffic data, **location**, server logs, IP address, OS, browser type

4 Privacy Impact Assessment using LINDDUN Approach

The privacy impact assessment of Tinder is primarily inspired by a quote from the *Terms of Use* [19], which makes one wonder the extent of power Tinder has on its users:

> *"By creating an account, you grant to Tinder a worldwide, transferable, sub-licensable, royalty-free, right and license to host, store, use, copy, display, reproduce, adapt, edit, publish, modify and distribute information you authorize us to access from third parties such as Facebook, as well as any information you post, upload, display or otherwise make available (collectively, "post") on the Service or transmit to other members (collectively, "Content")."*

Technically, the assessment follows the workflow of the LINDDUN approach [20]. To start with, a data flow diagram is created. Then, potential privacy risks are discussed and mapped onto the LINDDUN table.

4.1 Data flow diagram

Figure 4 illustrates the data flow of Tinder. A microservice architecture is implemented for scalability. To begin with, the profile creator service and database collect user profile data. Then users swipe on Tinder, all right swipes will be processed in match workers and are waiting for matches, while left swipes are stored temporarily in a low-cost database. Once matched, the chat service is activated for interactions. To generate new candidates, the recommendation service uses machine learning to create a profile map of potential matches. These data will be further shared with other stakeholders (e.g., third parties, Match Group affiliates and marketing partners). [21]

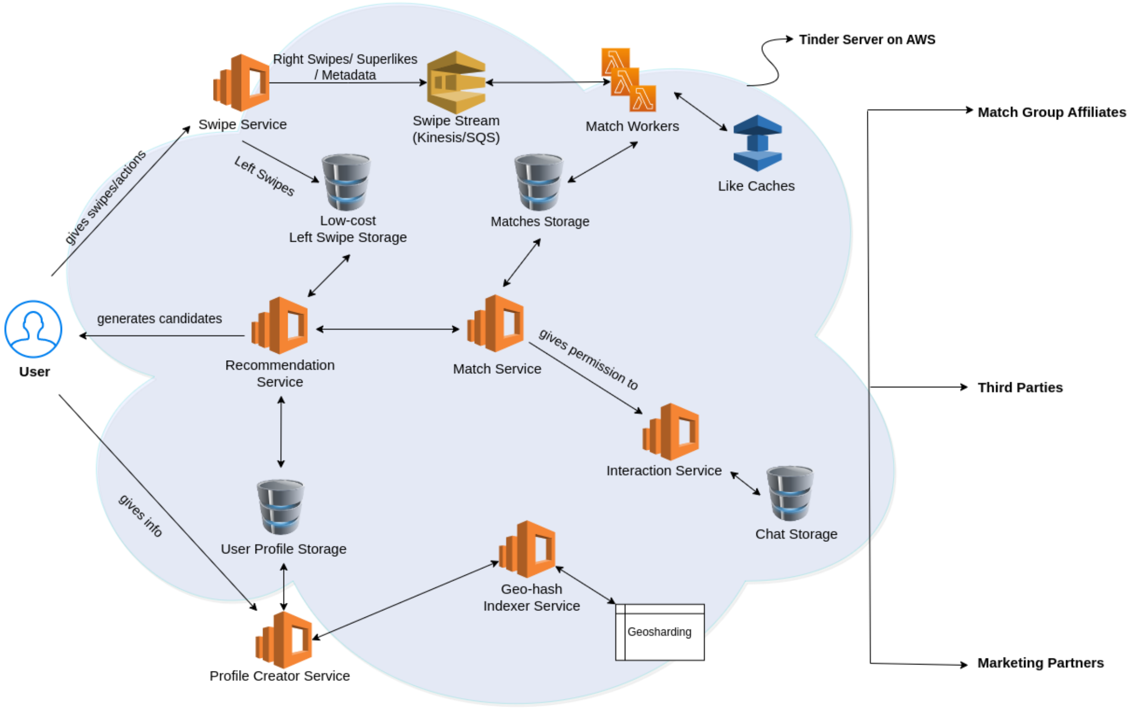


Figure 4: Data flow diagram

4.2 LINDDUN risk analysis

Based on the data flow, an abstract table (Table 2) is used to map the possible risks of DFD elements onto corresponding LINDDUN elements. The table contains four DFD elements: data storage, data flow, process and entity. Each element touches on different threat targets and points out their violated LINDDUN properties.

Table 2: Mapping table to DFD for Tinder (from left to right: L-Linkability, I-Identifiability, N-Non-Repudiation, D-Detectability, D-Information Disclosure, U-Unawareness, N-Non-compliance)

	Threat targets	**L**	**I**	**N**	**D**	**D**	**U**	**N**
Data store	User profile storage, chat storage, matches storage, low-cost left swipe storage		x			x		
Data flow	User → User Interaction		x			x		
	User's geolocation → Tinder server			x		x		
	ID documents → third party		x		x			
	Tinder server → third party	x	x					
Process	Harassment detection			x		x	x	
	Machine Learning	x			x	x		
	Targeted marketing	x					x	
Entity	Amazon Web Service	x	x		x	x		
	Third party analytics	x	x			x		
	User				x			

4.2.1 Identification verification by document

Besides its current age verification process [22], Tinder recently announced their plans in creating a safer platform by further verifying users by driver's licenses or identification documents [23]. Depending on the country, the original file would be stored from 30 up to 90 days. Later, only the result of verification would be stored. A verification may be processed by a third-party company since currently it is common in the development of similar platforms. Nevertheless, this kind of verification may lead to:

- **Eavesdropping unprotected data**: risk of **identifiability** and **detectability**, as a Man-In-The-Middle attack may capture unprotected data during transmission to the company which provides verification.
- **Data leakage on server**: risk of **identifiability**, as it is unknown how secure verification data are stored before, during and after the verification process, since the data contains sensitive identifiable information. Moreover, there imposes risk of **detectability**, since the data appearance in the verification dataset directly implies that someone has a Tinder account.

4.2.2 Not end-to-end encrypted interaction

When two matched users interact on Tinder, their interaction is not end-to-end encrypted. Tinder acts as a middleman between the sender and recipient and listens to all messages.

The message transmission from/to the Tinder server is secured and authenticated under the TLS-protocol against third parties. However, in Tinder's implementation, the protocol messages are unencrypted in plaintext during transmission. Messages are only encrypted on the server using Amazon KMS. Keys and messages are stored and can be decrypted on demand. [24]
Such implementation may impose various risks, as sensitive personal information is exchanged during interaction, such as names, phone numbers, home addresses or other meet-up locations.

- **Attack during data transmission**: risk of **identifiability** in case of TLS interception, POODLE attack followed by a Man-In-The-Middle attack [25], where personal information can be directly extracted to re-identify each user.

- **Data breach of server**: risk of **data disclosure** and **identifiability** of users in case of data breaches, where keys stored in KMS can be used to decrypt all messages.

- **Data monitoring, processing and publication**: risk of d**ata disclosure** as Tinder could decrypt all messages on demand for either its own purposes or share it with other affiliates or third parties. Furthermore, in the event of law enforcement, all data could be publicly disclosed.

4.2.3 Third party data sharing

Tinder uses third-party services to supports its operational functionalities. In this case, it is crucial to ensure proper security of sharing data. However, anonymization methods are not clearly stated in any Tinder's document. A user does not have any knowledge or control over which and how their data is pseudonymized. There exist risks associated to:

- **Sending data to other companies**: risk of **linkability** and **identifiability**, because the transmission process itself can be a source of vulnerability as well as what kind of data is shared with other companies – unsecured data or communication channel may reveal shared data.

- **Processing and storage of data by a third-party**: Tinder does not have impact on the way of processing and storage of data by other company. Thus, Tinder should only share encrypted data and as little data as possible with third parties, since it may lead to violation of **linkability** and **identifiability**. For instance, the fact of having Tinder account and information included in it may be revealed in a data leak happening in another company. Even an attack aimed at the third-party may cause harm to Tinder user without any interference with Tinder itself.

4.2.4 Inference on users for targeted marketing

In Tinder's *Privacy Policy*, it is stated that data collected from users is used to create profiles containing information preferences, characteristics, psychological trends, behavior, attitudes and more. Moreover, such information is used and shared with third party vendors and professional services organizations for the same purposes. [26]

This raises various privacy concerns, as the information mentioned above is extremely sensitive and there should be clear outreach from Tinder to explain the specifics of how this information is inferred, with whom and in what from it is. The following risks were identified:

- **Extremely sensitive data shared with third parties for marketing**: risk of **data disclosure**, as sharing data increases the possibility of a data leak or misuse and should be avoided whenever possible.
- **The process of inference and data sharing methods with third parties are vague**: risk of **unawareness**, as the nature of this data is sensitive, the user should have more understanding and control of how it is handled. This data is not available through the *Download My Data* service either [27].

Additionally, one might also question whether inferring such sensitive information for commercial purposes is ethically acceptable, especially since it is the kind of information which might easily be used for discrimination.

4.2.5 Centralized machine learning

Of no doubt should we forget the machine learning algorithms, one of Tinder's most powerful tools. As the world's most successful dating app, machine learning is implemented everywhere in Tinder: from match recommendations to harassment detection, smart photo placement, etc.

Tinder utilizes AWS Rekognition model [28] for its image/video analysis and implements TinVec [29] to generate recommendations. These large models take unencrypted data as input and are applied in a centralized fashion. That is, all users data is uploaded onto, trained or tested at the cloud server, then the results and sent back.

Such a centralized architecture creates not only high communication overheads, but also vendor lock-in, as all models are trained and deployed at one cloud provider. More importantly, this architecture is more susceptible to multiple privacy risks:

- **Training set membership inference** [30]: risk of **detectability**. Models are prone to perform better on their training data. Without having direct access to the user's data or the model, adversaries can simply observe the model performance and reconstruct data samples used for training.
- **Attribute inference attacks** [31]: risk of **data disclosure**, as an adversary could infer missing attributes of a data instance by collecting its publicly available information on other platforms.
- **User profiling and inference**: risk of **linkability**, as the model aggregates and builds user clusters using their personal information. Thus, when one user has certain properties, it easily assumes its neighbouring members within a cluster share such characteristics and members from a distanced cluster would have opposing properties.

4.2.6 Centralized data storage

Tinder utilizes in general a microservice architecture, which divides its operation into many microservices with its independent data storage. This architecture introduces some data distribution, but within its whole cloud infrastructure, all data is stored in a centralized fashion at its cloud provider AWS [32].

Like the machine learning architecture, such centralization could inflict some privacy threats:

- **Data breach from cloud provider**: risk of **data disclosure**. As Tinder is fully hosted on AWS, risks brought by AWS are automatically attached to Tinder and its users. Though there hasn't been data leakage of Tinder due to AWS, a long history of AWS data breaches [33] still raises concern for storing all information at one single cloud provider.

- **Data breach from Tinder**: risk of **data disclosure** and **identifiability**. Using centralized storage, a data instance is stored altogether with its metadata. In case of data breaches, personal information can be retrieved to re-identify users. One of the most recent examples are the photo breach from Tinder, where 70,000 female figures together with their metadata (timestamp, location) and the corresponding unique Tinder IDs are leaked, affecting 16,000 users [34].

4.2.7 Excessive collection of geolocation

As part of its matching service, Tinder allows users to filter potential matches based on their proximity. To this end, Tinder collects the geolocation of the user's device both in active and inactive usage.

Historically, Tinder's geolocation data collection and sharing was a cause of multiple high profile privacy related incidents [35, 36]. Even though the processing of geolocation data has improved, there are leftover concerns:

- **Device location is always tracked**: risk of **non-repudiation**, as users cannot turn location tracking without losing access to Tinder services. This may be unnecessary in certain situations, such as when users only wants to chat with their existing matches.

- **Mandatory GPS access for phone users**: on the contrary to phone users, Tinder can be used via computer without built-in GPS. This raises further concerns in **data disclosure** in the usage and collection of geolocation data.

4.2.8 General lack of clarity in Privacy Policy

Overall, it appears that Tinder lacks transparency in its handling of user data. The company's *Privacy Policy* and *Terms of Use* are often vague, particularly regarding the inferences made as part of its matching algorithms and marketing efforts [4]. It is also unclear whether the *Download my Data* feature provides users with all their data. A risk emerges:

- **Specifics of how data is collected and used are hard or impossible to find**: risk of **unawareness**. The lack of transparency leaves users unaware of the extent to which they are sacrificing their privacy to use the service. Furthermore, the information provided in these official statements is often insufficient to allow users to make informed decisions regarding their privacy.

4.2.9 Other risks

Full information retrieval after changing phone number: As a Tinder account is uniquely binding to a phone number, there is a risk of **data disclosure** and **detectability**. If person A changes their phone number without deleting their Tinder account, a person B who gets A's previous phone number could check if A uses Tinder by checking a verification SMS. If yes, a full information retrieval about A is possible by just logging in Tinder.

Compulsory and intransparent harassment detection: In order to fight against sexual harassment, Tinder introduces *"Does it bother you"* feature, which automatically detects possible offensive messages or nudity in photos using machine learning. [37]

This feature could lead to erroneous ban of user accounts, as offensiveness relies highly on context and personal perception, which is a risk of **non-repudiation**. Furthermore, it inflicts risk of **unawareness** and **data disclosure**, as there is no way to opt out of this feature, nor did Tinder explain the algorithm to its users explicitly in *Privacy Policy* or upon usage.

5 Recommendations

5.1 Secure storage of sensitive information

Sensitive identifiable data which should be stored in a much more protected database. Access to these databases should be allowed only after performing two-factor authentication and depend on user's privileges. A minimum number of employees should have access to databases and their privileges should be restricted to the minimum necessary level for them to do their work [38]. A proper defense against SQL injections should also be applied. It can be done by creating SQL statements with placeholders for the parameters provided by a user. A cloud provider should take care of the physical security of databases.

All stored data should be secured by the best possible available encryption while it is at rest and so in transit. Encryption keys should be handled in compliance with best-practice methods. Besides, any images, backups or copies should have provided the same security and access as the original database.

5.2 End-to-end encryption

As user interaction is one of the main features of Tinder, Tinder is supposed to provide users with higher privacy protection by encrypting the interactions end-to-end. An end-to-end encryption ensures that no one else can access or process the interaction except for the sender and recipient. By using public key encryption, the public key could although be viewed by anyone including Tinder, the private key is stored only on the device of the two participating parties, which can be used to decrypt messages [39].

If user A un-matches user B, the private key to their interaction should be invalidated, thus neither of them are able to decrypt their conversation, even the locally cached copies.

5.3 Privacy-preserving machine learning

Above all, Tinder should clarify and ask for specific consent on every feature that concerns machine learning with its users. Moreover, more privacy-preserving machine learning architectures should be implemented.

From the perspective of data, machine learning models can implement differential privacy by perturbing either the input data, the optimal parameters, the objective function or the gradients with noise. What's more, models can be also trained or tested on encrypted data by implementing Fully Homomorphic Encryption (FHE) [40].

From the perspective of learning, Tinder can implement a decentralized architecture, namely federated learning [41]. User data is stored locally, while only the model weights are sent. Learning is performed locally and independently based on each user's data, which enables personalization in, for instance, match recommendation and harassment detection. Individual weights are sent back, aggregated centrally and distributed again, which provides some global optimization. Furthermore, the transmitting parameters can also be encrypted to secure the model. In this case, learning doesn't stand in the way of end-to-end encryption.

5.4 Data anonymization in data sharing and transmission

It may be worth implementing a data masking mechanism if it has not been applied yet. Such an operation will make data useless to an attacker if they somehow capture data during its transit [42]. It also reduces risks connected to cloud adoption.

The architecture should be adapted to include components that use state-of-the-art k-anonymity and differential privacy techniques to obtain anonymized users' data. With techniques like quasi-identifier data generalization, the possibility of user identification could be lowered.

5.5 Decentralized data storage

A decentralized data storage infrastructure helps mitigate the risk of full data disclosure in case of data breaches. It allows for fractional amounts of data to be stored in multiple locations. For example, instead of storing one complete photo and its metadata at one location, the photo and its metadata are partitioned into many pieces and stored in different locations. Even if the attackers obtain access to one database, data is incomplete to re-identify users.

5.6 Option to opt-out unnecessary data collection or additional features

Tinder should allow its users to opt-out of giving information not necessary for Tinder's services to function, e.g. geolocation, device ID and screen size. The biggest concern is geolocation which is collected at all times. Additionally, phones should be able to turn off GPS, as the service works on devices without it.

Users should also be given the option to opt-out features such as *"Does it bother you"*, if they are concerned about their personal data being processed by the harassment detection model. Depending on Tinder's balance tradeoff between privacy protection and harassment elimination, user's decision on this feature can be displayed to notify other end-users.

5.7 Reconstruction of a clearer Privacy Policy

The *Privacy Policy* and *Terms of Use* should be expanded with a more detailed description of how data is handled. For example, more needs to be said about which data the matching and marketing inferences algorithms use. The methods of data anonymization methods should also be listed. The *Download My Data* service currently only returns raw data, and it is even unclear if all raw data is provided. None of the many inferences Tinder makes are available to the user.

6 Conclusion

In this paper, a privacy impact assessment was conducted based on the LINDDUN methodology. Legal and technical aspects of Tinder's privacy were discussed. An extensive list of recommendations were given at the end of the assignment.

Though Tinder has made progress in resolving previous severe vulnerabilities, as world's most popular dating app, Tinder still has a long way to go to become privacy oriented for its 75 million users. It should shoulder more responsibility in creating a safer, more transparent and fair environment for its users.

References

[1] R. L. Finn, D. Wright, and M. Friedewald. "Seven types of privacy." In: *European data protection: coming of age*. Springer, 2013, pp. 3–32.

[2] Tinder. *Powering Tinder® — the method behind our matching*. https://www.help.tinder.com/hc/en-us/articles/7606685697037-Powering-Tinder-The-Method-Behind-Our-Matching. Accessed on 02.01.2023.

[3] K. Tiffany. *The Tinder algorithm, explained*. https://www.vox.com/2019/2/7/18210998/tinder-algorithm-swiping-tips-dating-app-science. Accessed on 02.01.2023. Feb. 2019.

[4] Tinder. *Privacy policy*. https://policies.tinder.com/privacy/intl/2022-12-13/en. Acessed on 02.01.2023. Jan. 2022.

[5] Tinder. *Privacy settings*. https://policies.tinder.com/web/safety-center/tools/privacy/in/en/. Acessed on 02.01.2023.

[6] G. Firebase. *Privacy and Security in Firebase*. https://firebase.google.com/support/privacy. Accessed on 02.01.2023. Sept. 2022.

[7] T. Insights. *Privacy Policy*. https://tinderinsights.com/privacy. Accessed on 02.01.2023. Feb. 2020.

[8] Adyen. *Privacy Statement*. https://www.adyen.com/policies-and-disclaimer/privacy-policy. Accessed on 02.01.2023. Apr. 2022.

[9] S. BugSnag. *SmartBear Privacy Notice*. https://smartbear.com/privacy/. Accessed on 02.01.2023. July 2022.

[10] Vonage. *Vonage Privacy Policy*. https://www.vonage.com/legal/privacy-policy/. Accessed on 02.01.2023. May 2022.

[11] Spotify. *Spotify Privacy Poicy*. https://www.spotify.com/us/legal/privacy-policy/. Accessed on 02.01.2023. Jan. 2023.

[12] Instagram. *Data Policy*. https://help.instagram.com/155833707900388. Accessed on 02.01.2023. Jan. 2022.

[13] facetec. *FaceTec Privacy Shield, GDPR, Website, App and Email Privacy Policies*. https://dev.facetec.com/privacy-site. Accessed on 02.01.2023. June 2021.

[14] Appsflyer. *Website Privacy Policy*. https://www.appsflyer.com/legal/privacy-policy/. Accessed on 02.01.2023. Aug. 2021.

[15] Branch. *Privacy Policy*. https://branch.io/policies/privacy-policy/. Accessed on 02.01.2023. Feb. 2022.

[16] Google. *Google Privacy & Terms*. https://policies.google.com/technologies/ads?hl=en-US. Accessed on 02.01.2023. Dec. 2022.

[17] VideoAmp. *Privacy Policy*. https://videoamp.com/privacy-policy/. Accessed on 02.01.2023. June 2022.

[18] Adjust. *Privacy Policy*. https://www.adjust.com/terms/privacy-policy/. Accessed on 02.01.2023. May 2022.

[19] Tinder. *Terms of use*. https://policies.tinder.com/terms/intl/en. Acessed on 02.01.2023.

[20] D. R. Group. *Linddun Framework*. https://www.linddun.org/linddun. Acessed on 02.01.2023. 2020.

[21] T. Takshila. *Design dating platform - Tinder*. https://techtakshila.com/system-design-interview/chapter-5/. Acessed on 02.01.2023. Sept. 2020.

[22] Tinder. *How does age verification work? – Tinder*. https://www.help.tinder.com/hc/en-us/articles/360040592771-How-does-age-verification-work-. Acessed on 02.01.2023.

[23] Tinder. *Tinder will add ID verification option following the successful rollout of photo verification*. https://www.tinderpressroom.com/2021-08-16-Tinder-Commits-to-ID-Verification-for-Members-Globally,-a-First-in-the-Dating-Category. Acessed on 02.01.2023. Aug. 2021.

[24] K. Ho, A. Nistala, K. Tu, and R. Rivest. "End-To-End Message Encryption for Tinder." In: (2016).

[25] Wikipedia. *Transport layer security*. https://en.wikipedia.org/wiki/Transport_Layer_Security. Acessed on 02.01.2023. Dec. 2022.

[26] Tinder. *CCPA addendum*. https://policies.tinder.com/ccpa-addendum/us/en. Acessed on 02.01.2023.

[27] Tinder. *How do I request a copy of my personal data? – Tinder*. https://www.help.tinder.com/hc/en-us/articles/115005626726-How-do-I-request-a-copy-of-my-personal-data-. Acessed on 02.01.2023.

[28] AWS. *What is Amazon Rekognition?* https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html. Acessed on 02.01.2023.

[29] S. Liu. *Personalized Recommendation at Tinder: The TinVec Approach*. https://www.slideshare.net/SessionsEvents/dr-steve-liu-chief-scientist-tinder-at-mlconf-sf-2017. Acessed on 02.01.2023. 2017.

[30] B. Dickson. *Machine learning: What are membership inference attacks?* https://bdtechtalks.com/2021/04/23/machine-learning-membership-inference-attacks/. Acessed on 02.01.2023. Apr. 2021.

[31] N. Z. Gong and B. Liu. "Attribute inference attacks in online social networks." In: *ACM Transactions on Privacy and Security (TOPS)* 21.1 (2018), pp. 1–30.

[32] C. Staff. *Decentralized Cloud Storage Comparisons*. https://www.gemini.com/cryptopedia/crypto-cloud-storage-decentralized-cloud-storage-providers. Acessed on 02.01.2023. Dec. 2021.

[33] M. X. Heiligenstein. *Amazon Web Services (AWS) data breaches: Full timeline through 2022*. https://firewalltimes.com/amazon-web-services-data-breach-timeline/. Acessed on 02.01.2023. June 2022.

[34] W. Heasman. *Tinder's data loss shows the perils of centralization*. https://decrypt.co/17167/tinders-hack-shows-the-perils-of-centralization. Acessed on 02.01.2023. Jan. 2020.

[35] J. V. Grove. *Tinder flaw may have exposed members' exact whereabouts for months*. https://www.cnet.com/tech/services-and-software/tinder-flaw-may-have-exposed-members-exact-whereabouts-for-months/. Accessed on 02.01.2023. Feb. 2014.

[36] R. Heaton. *How Tinder keeps your exact location (a bit) private*. https://robertheaton.com/2018/07/09/how-tinder-keeps-your-location-a-bit-private/. Accessed on 02.01.2023. July 2018.

[37] A. Pardes. *Tinder swipes right on AI to help stop harassment*. https://www.wired.com/story/tinder-does-this-bother-you-harassment-tools/#:~:text=Thepopularonlinedatingapp,themtoitsreportform. Accessed on 02.01.2023. Jan. 2020.

[38] IBM. *Database security: An essential guide*. https://www.ibm.com/topics/database-security. Accessed on 02.01.2023.

[39] Cloudflare. *What is end-to-end-encryption?* https://www.cloudflare.com/learning/privacy/what-is-end-to-end-encryption/. Accessed on 02.01.2023.

[40] Inpher. *What is fully homomorphic encryption?* https://inpher.io/technology/what-is-fully-homomorphic-encryption/. Accessed on 02.01.2023. Apr. 2021.

[41] Wikipedia. *Federated learning*. https://en.wikipedia.org/wiki/Federated_learning#Properties_of_federated_learning. Accessed on 02.01.2023. Dec. 2022.

[42] Imperva. *What is data masking?: Techniques amp; Best Practices: Imperva*. https://www.imperva.com/learn/data-security/data-masking/. Accessed on 02.01.2023. Dec. 2022.