ICOOAI83 Privacy and Social Engineering

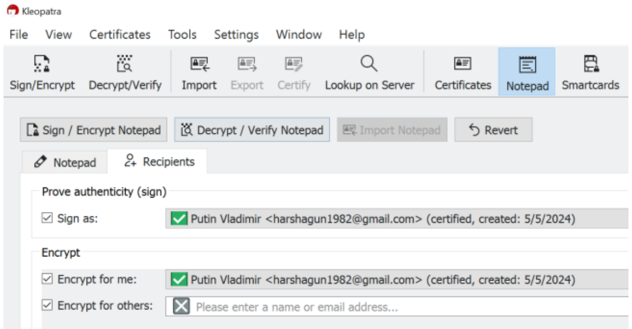
Harsha Gunasekara

Study Right No. 2401908

Week 2: Messaging and mobile privacy

Task 1: Private and authentic messaging

You are allowed to have one unencrypted message, but it must be from an unknown address.


Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards
Sign / Encrypt Notepad
Decrypt / Verify Notepad
Import Notepad
Revert
Notepad
Recipients

Prove authenticity (sign)

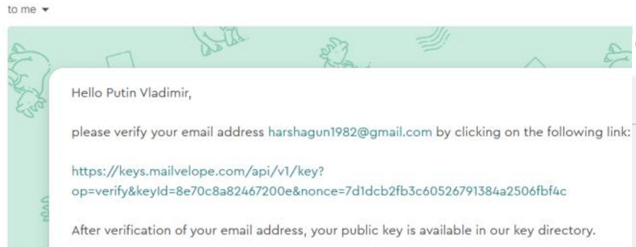
☑ Sign as: Putin Vladimir <harshagun1982@gmail.com> (certified, created: 5/5/2024)

Encrypt

☑ Encrypt for me: Putin Vladimir <harshagun1982@gmail.com> (certified, created: 5/5/2024)

☑ Encrypt for others: Please enter a name or email address...

Document your actions precisely, and name software or services used to the best of your ability.



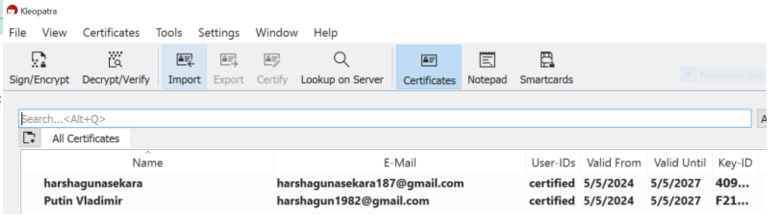
to me

Hello Putin Vladimir,

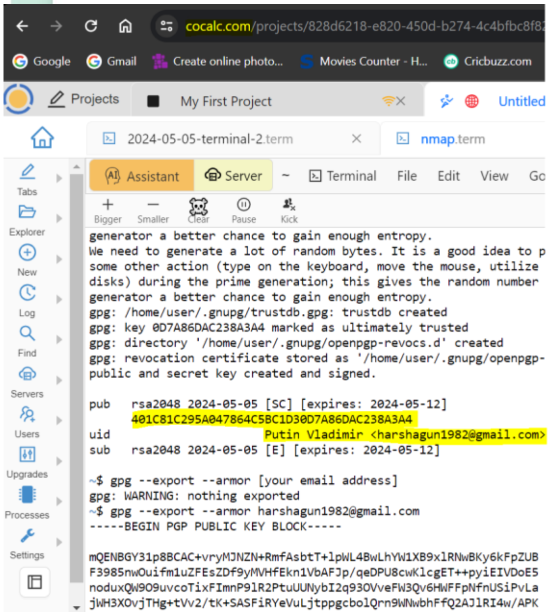
please verify your email address harshagun1982@gmail.com by clicking on the following link:

https://keys.mailvelope.com/api/v1/key?op=verify&keyId=8e70c8a82467200e&nonce=7d1dcb2fb3c60526791384a2506fbf4c

After verification of your email address, your public key is available in our key directory.


Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards
Search...<Alt+Q>
All Certificates

Name	E-Mail	User-IDs	Valid From	Valid Until	Key-ID
harshagunasekara	harshagunasekara187@gmail.com	certified	5/5/2024	5/5/2027	409...
Putin Vladimir	harshagun1982@gmail.com	certified	5/5/2024	5/5/2027	F21...


cocalc.com/projects/828d6218-e820-450d-b274-4c4bfbc8f8
Google Gmail Create online photo... Movies Counter - H... Cricbuzz.com
Projects My First Project Untitled
2024-05-05-terminal-2.term nmap.term
Assistant Server ~ Terminal File Edit View Go
Bigger Smaller Clear Pause Kick
Tabs Explorer New Log Find Servers Users Upgrades Processes Settings

```
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to p
some other action (type on the keyboard, move the mouse, utilize
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: /home/user/.gnupg/trustdb.gpg: trustdb created
gpg: key 0D7A86DAC238A3A4 marked as ultimately trusted
gpg: directory '/home/user/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/user/.gnupg/openpgp-
public and secret key created and signed.

pub   rsa2048 2024-05-05 [SC] [expires: 2024-05-12]
      401C81C295A047864C5BC1D30D7A86DAC238A3A4
uid                      Putin Vladimir <harshagun1982@gmail.com>
sub   rsa2048 2024-05-05 [E] [expires: 2024-05-12]

~$ gpg --export --armor [your email address]
gpg: WARNING: nothing exported
~$ gpg --export --armor harshagun1982@gmail.com
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBGY31p8BCAC+vryMJNZN+RmfAsbtT+1pWL4BwLhYW1XB9xlRNwBKy6kFpZUB
F3985nwOuifm1uZFEsZDf9yMVHfEkn1VbAFJp/qeDPU8cwKlcgET++pyiEIVDoE5
noduxQW9O9uvcoTixFImnP9lR2PtuUUNybI2q93OVveFW3Qv6HWFFpNfnUSiPvLa
jWH3XOvjTHg+tVv2/tK+SASFiRYeVuLjtppgcbolQrn9WNwbhFfQ2AJlRI4w/APK
```

https://cocalc.com

https://www.techspot.com/downloads/6650-gpg4win.html

https://chatgpt.com/

You are expected to generate PGP keys, exchange them (public keys only!), encrypt, sign, verify and decrypt the message contents. Would anyone logged in on your account on the machine be able to read the messages? Why or why not?

No, anyone logged in to the account on the machine would not be able to read the messages exchanged in the encrypted email conversation. Because PGP encryption ensures that only the sender and the intended recipient can decrypt and read the messages.

Describe the experience and how difficult you found this to be.

Generating PGP keys, exchanging them, encrypting, and signing, verifying, and decrypting message contents can be a straightforward process with the right tools and guidance, but it requires attention to detail and understanding of the concepts involved. Experience and the perceived difficulties such as Exchanging Public Keys, Verifying Signatures, Generating PGP Keys and Exchanging Public Keys are reasons to be that.

Task 2: Metadata and messaging

2A) Compare messaging platforms

Write an essay of at least 300 words based on the previous sources and examples, including app comparison and considering also the importance of E2E encrypted metadata.

Similarities

Schedule: Both users communicate every Thursday, around 1:00 PM. suggest a planned or routine interaction.

Location: User B seems to be near "The Nice Cafe" in Helsinki city on Thursdays, possibly meeting User A there.

User A

Device: Uses an iPhone 14 Pro Max, suggesting a preference for Apple products.

Location: Consistently sends messages from "The Nice Cafe" which could be their workplace, a regular meeting spot, or their home base.

User B

Device: Uses a Windows machine (Acer Nitro) and an Android phone (Nokia G21). This suggests they might be comfortable with different operating systems or have multiple devices for work and personal use.

Location: Their initial message comes from a specific Wi-Fi network ("Best Wi-Fi") with a static IP address (123.45.67.89). This suggests a work or home location. Later messages come from a mobile device (Nokia G21) near an Elisa cell tower within a 3-kilometer radius of "The Nice Cafe." This strongly suggests they move to meet User A at the cafe after their initial message.

Unknowns

Relationship: We don't know if they're friends, colleagues, romantic partners, or something else.

Message Content: The content of the messages would be crucial to understand the nature of their interaction.

Possible Scenarios

User A sends a reminder for a weekly cafe meeting, while User B confirms and joins them via personal phone. This pre-arranged business meeting involves User A waiting at the cafe and User B providing updates.

In conclusion - Communication pattern suggests planned Thursday interaction between User A and User B at "The Nice Cafe" in Helsinki City, with potential social element, but message content uncertain.

App comparison,

	WhatsApp	Signal	Telegram	Meta's Messenger
Privacy & Security	Chats are encrypted by default, but Meta stores user data such as phone numbers and contacts.	Focuses heavily on privacy. Open-source code, end-to-end encryption by default, no user data collection	Offers end-to-end encryption for "Secret Chats" only. Regular chats store data on servers	Meta collects user data for targeted advertising, despite offering end-to-end encryption in "Secret Conversations" mode
Features	Most popular, large user base, simple interface, voice/ video calls, group chats, file sharing	Focuses on secure communication, similar features to WhatsApp, but smaller user base	Large file sharing limit, large groups & channels, feature-rich with bots & integrations. Less focus on user-friendliness.	Integrates with Facebook for easy contact discovery, features like games, polls, & payments. May feel cluttered compared to others
Device Compatibility	All four apps are available on Android, iPhone, and desktop	All four apps are available on Android, iPhone, and desktop	All four apps are available on Android, iPhone, and desktop	All four apps are available on Android, iPhone, and desktop
Cloud Storage & Backup	Messages stored on user's phone by default. Backup options to cloud services	No default cloud storage, messages disappear when uninstalled from both devices. Encrypted backups possible	Messages stored on Telegram servers, accessible from any device. Encrypted chat backups available.	Messages stored on Meta servers, accessible from any device.
Target Audience	Most popular, good for casual users & those with large social circles already on the platform	Ideal for privacy-conscious users who prioritize secure communication.	Suited for large groups, file sharing, and those who need advanced features.	Best for those already invested in Facebook ecosystem and want easy integration with social features.
Choosing the right app depends on priorities	WhatsApp offers a familiar, feature-rich experience with large user base. However, privacy concerns exist.	Signal prioritizes security with strong encryption and minimal data collection.	Telegram offers more flexibility but comes with less focus on user-friendliness and potential privacy concerns.	Meta's Messenger provides seamless connection with Facebook contacts but collects user data for targeted ads.

Cross-Platform Support	Available on multiple platforms, including iOS, Android, and web browsers.	Available on multiple platforms, including iOS, Android, and web browsers.	Available on multiple platforms, including iOS, Android, and web browsers.	Available on multiple platforms, including iOS, Android, and web browsers.

Importance of E2E encrypted metadata,

Signal, Telegram, WhatsApp, and Messenger are popular for privacy and security, with Signal offering strong encryption and minimal data collection, while Telegram faces security criticism.

Protects Sensitive Details - E2E encryption scrambles metadata, including sender/receiver identities, timestamps, location data, and communication frequency, making it unreadable to only the intended recipient.
Limits Data Exposure - E2E encryption safeguards metadata stored by service providers, preventing valuable data from being used for targeted advertising, user profiling, or legal situations.
Hinders Tracking and Analysis - Third parties can analyze communication patterns, while E2E encryption makes tracking communication patterns harder, making it crucial for journalists, activists, and those concerned about surveillance.

E2E encryption enhances privacy, minimizes user data exposure, and allows service providers to know usage frequency, making it a crucial feature in selecting secure communication platforms.

Note also the use of the same phone number across different services. For example, WhatsApp shares phone numbers and other information with Meta Company outside of the European Union 14. What does this mean in the context of social graphs and the accuracy of possible behavior and knowledge modelling?
Write one paragraph of your thoughts.

Use of the same phone number across different services can significantly impact social graphs and the accuracy of behavior and knowledge modeling.

<u>Impact on Social Graphs:</u>

Enhanced Connections - The linking of phone numbers across services owned by the same company enhances the connection between profiles in the social graph, providing a more comprehensive view of a user's social circle.
Data Sharing - Sharing phone numbers across services can potentially merge social circles, revealing connections users may not have intended to share publicly.

<u>Impact on Behavior and Knowledge Modeling:</u>

Improved Accuracy - Companies can gather user data across platforms, including location history, app usage patterns, and potential contacts, to create more accurate models of user behavior and preferences.
Privacy Concerns - Sharing phone numbers across services raises privacy concerns as companies can create detailed profiles about users, potentially used for targeted advertising or third-party sales.
Limited Scope - Relying solely on phone numbers for connection can lead to inaccuracies as people may use different numbers for different purposes or some services may not require phone numbers.

User A and User B's social graph connection is enhanced by WhatsApp and Meta's location data access, potentially highlighting their Thursday visit to "The Nice Cafe."

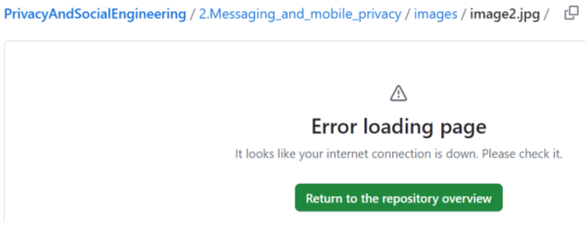
Additionally, what privacy risks "last seen" or showing "online status" can include? Imagine a situation, where someone who has the same contact list as you have, automates to process of checking the online status of every contact for every second and finally stores this information for a longer period.
Write one paragraph of your thoughts.

The feature of "last seen" or showing "online status" in messaging platforms can pose significant privacy risks, especially when automated processes are used to continuously monitor these statuses for every contact.

A friend automates checking online statuses, raising privacy concerns. This can reveal activity patterns, exposing sensitive information about availability, habits, and interactions. The data collected over time creates a detailed profile of online behavior, potentially exploited for targeted advertising, social engineering, or stalking. While online status indicators can enhance communication, misuse raises ethical and privacy concerns that platform developers must address.

2 B) Image metadata

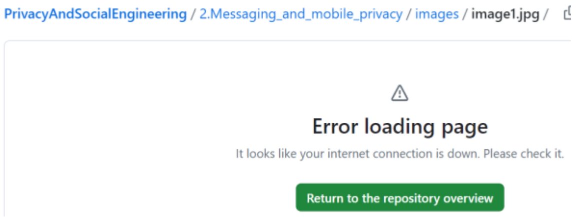
Unable to download (error) image1.jpg and image2.jpg



PrivacyAndSocialEngineering / 2.Messaging_and_mobile_privacy / images / image2.jpg /

Error loading page

It looks like your internet connection is down. Please check it.



PrivacyAndSocialEngineering / 2.Messaging_and_mobile_privacy / images / image1.jpg /

Error loading page

It looks like your internet connection is down. Please check it.

Task 3: Application permissions and trackers

Choose two (2) applications yourself to analyze with the help of Exodus, and find a third application that has obvious unnecessary dangerous permissions, such as a flashlight application accessing your contacts.

1. **How many trackers and permissions each application has?**

	trackers	permissions
Facebook	0	83
TikTok	5	43
Flashlight App	14	18

2. **How many "dangerous" (runtime) and/or "special" permissions does each have? (Red exclamation mark, see these in Google's guide 15)**

	"dangerous" (runtime) and/or "special"
Facebook	15
TikTok	9
Flashlight App	2

3. **Did the applications have permission to access such data they could use or sell for monetary gain? Which permissions and trackers are these?**

   Facebook and TikTok use user data for targeted advertising, profiling, and third-party sales. However, flashlight apps may request permissions for camera or location functionality, raising concerns about potential misuse of user data and potential spamming.

	trackers	permissions
Facebook	Facebook Login & Places, Cookies, Analytics	Camera, Contacts, Location, Microphone
TikTok	TikTok Login & Places, Cookies, Analytics	Camera, Contacts, Location, Microphone
Flashlight	Analytics & 3rd party Trackers, Advertising SDKs	Camera, Contacts, Location, Microphone

4. **Describe two attack vectors enabled by these permissions for each application, had an attacker gained access into the application and/or their database.**

   Facebook's extensive permissions could allow unauthorized access to the app, enabling various attack vectors that could compromise user privacy and security,

   - Social Engineering and Account Takeover

Access to Friend List and Contact Information -

Facebook permissions can potentially grant access to a user's friend list or contact information, allowing an attacker to exploit this data.

Targeted Phishing Attacks -

Individuals could create personalized phishing attacks by presenting emails or messages as friends or contacts, potentially containing malicious links or requests for personal information.

Social Engineering Scams -

An attacker can use friend list information to create social engineering scams, impersonating a friend or family member to manipulate the victim into revealing sensitive information or clicking malicious links.

- Profile Data for Identity Theft or Targeted Attacks

Targeted Attacks -
The attacker could exploit user profile data for targeted attacks, targeting location-specific malware or spam, or analyze user interests for convincing phishing or social engineering scams.
Identity Theft -
An attacker with this information could potentially use it for identity theft purposes. They might create fake IDs or use the information to gain access to other accounts associated with the victim.
Extracting Personal Information - Permissions can grant access to a user's profile data, including birthday, location, and potentially private messages, depending on past permissions.

5. Compare Android and iOS privacy labels (if it is available on both platforms) to your findings about trackers

Trackers

Limited Disclosure - The privacy labels on Android and iOS do not explicitly mention "trackers" but instead focus on broader data collection categories like location, contacts, photos, and identifiers.

Android

Focus on Data Collection - Android labels categorize data into "Data collected on device" and "Data shared with third parties," providing transparency but not specifying data collection methods like cookies or embedded trackers.

Limited Detail - The broad categories in Android labels can make it challenging to comprehend the specific types of trackers being utilized.

iOS

Similar Focus - iOS labels, similar to Android, categorize data like "Location" or "User Contact Information" but do not explicitly mention trackers.

Data Use Descriptions - iOS labels may include "Data Used to Track You" section, but details may be vague and not fully reveal tracking extent through cookies, third-party integrations, or other methods.

Recommendations

Research Beyond Labels - Users should conduct further research to understand an app's tracking practices, including app reviews, privacy policies, or contacting the app developer directly.

Consider Alternatives - If an app's privacy label raises concerns about extensive data collection or tracking, consider alternative apps with more privacy-focused practices.

Privacy labels are still evolving, and future iterations might include more detailed information about the types of trackers used within apps goods for Potential Improvements

Task 4: Application SDKs, code signatures, Tags and Pixels (bonus)

What is the motivation behind advertising business and trackers?

Advertising businesses use trackers to deliver targeted ads to users, based on their interests, preferences, behaviors, and demographics, generating revenue through relevant and engaging content.

Mobile Advertising -

Mobile advertisers use apps, websites, and social media to reach users. Tracking devices, cookies, and SDKs gather data on user interactions, enabling detailed profiles and targeted ads based on interests.

Web Advertising -

Web environment governed by principles of cookies, pixels, and tracking technologies, which monitor user browsing history, preferences, interactions, and help advertisers' measure campaign effectiveness and retarget users.

Motivation -

Advertising and trackers enhance campaign effectiveness by providing personalized ads, capturing user attention, and enhancing click-through rates, while user data analysis optimizes strategies, reduces waste, and generates revenue. Advertising and trackers aim to foster a symbiotic relationship between advertisers, publishers, and users, but privacy, data security, and user consent concerns have led to regulatory actions.

4A) Legacy technologies

Look for research articles regarding the impact of this change. Write 2-3 paragraphs based on at least 3 sources.

- A Survey on Web Browser Fingerprinting Techniques (2020) by Haya et. al.

This article provides a thorough analysis of web browser fingerprinting techniques, examining various data points, mitigating methods, and discussing the privacy implications of this technology.

Negative Impacts:

Privacy Intrusion - Fingerprinting creates unique device identifiers, potentially revealing browsing habits and online identity without consent, raising privacy concerns as companies track users across websites
Targeted Advertising - Advertisers can use fingerprint data to create personalized ads, potentially affecting your online experience and presenting irrelevant content.
Website Blocking or Tracking - Websites may employ fingerprinting to detect and prevent bots or malicious actors, but this method can also be misused to block legitimate users or track their activities for non-security purposes.
Difficulty Escaping Tracking - Fingerprinting, unlike cookies, relies on unchangeable device characteristics, making it harder to avoid web tracking compared to cookies that can be cleared.

Positive Impacts -

Fraud Detection - Fingerprinting aids in identifying and preventing online fraud by creating unique user profiles, thereby detecting suspicious behavior and safeguarding users from scams.
Website Personalization - Websites could use fingerprinting to personalize user experiences by remembering preferences or tailoring content based on browsing habits, but transparency and user consent are essential.
Enhanced Security - Fingerprinting can be utilized as an additional layer of security in online accounts, aiding in the identification and blocking of unauthorized login attempts.

Web browser fingerprinting, while potentially beneficial for fraud detection and website personalization, raises privacy concerns. Mitigation strategies include using privacy-focused browsers or blocking tracking scripts.

- Detection Potential of Recently Discovered Techniques for Recovering Latent Fingerprints: A Review (2019) by Asoh et. al.

Positive Impacts

Bot Detection - Browser fingerprinting can distinguish between real users and bots, detecting inconsistencies in device fingerprints, thereby preventing malicious activities like data scraping or fake account creation.

Enhanced Security - Fingerprinting enhances online security by preventing bots from impersonating real users, especially beneficial for websites or platforms susceptible to bot attacks.

Limitations

Evolving Techniques - The article highlights the ongoing battle between developers and bot creators due to the potential for bots to adapt and spoof fingerprints due to changes in browser versions and user privacy settings.

Privacy Concerns - Fingerprinting for anti-spoofing raises privacy concerns, as users may not appreciate their browser data being collected and analyzed to determine their identity.

Inaccuracy - Fingerprinting is not foolproof, as user behavior changes or legitimate browser extensions can alter the fingerprint, potentially leading to false positives and blocking genuine users.

Fingerprinting can potentially combat bots, but its limitations and privacy concerns must be carefully considered alongside other security measures, emphasizing user privacy.

4B) the use of the advanced technologies

What kind of tracking pixels you are finding?

motonet.fi - Google Analytics, Facebook Pixel, Others like conversion tracking pixels from payment processors.

masku.com - Likely similar setup to motonet.fi with Google Analytics and Facebook Pixel being common.

wolt.com - The food delivery service likely utilizes Google Analytics for app/website usage analysis, possibly Facebook Pixel for ad targeting, and internal tracking pixels for order flow and delivery efficiency.

verkkokauppa.com - Google Analytics, Facebook Pixel, and potentially others.

power.fi - Likely uses Google Analytics, Facebook Pixel, and possibly others for affiliate marketing or CRM

etuovi.com - The real estate marketplace may utilize Google Analytics for website traffic, Facebook Pixel for ad targeting, and potentially tracking pixels from lead generation services.

huutokaupat.com - The auction platform, Utilize Google Analytics and Facebook Pixel, along with conversion tracking pixels specifically designed for online auctions.

tentree.ca - As an e-commerce store, expect Google Analytics, Facebook Pixel, and potentially others depending on their marketing strategy.

crypto.com - Cryptocurrency platforms rely on analytics, including Google Analytics and web tools, and may have their own conversion tracking pixels for user actions like signups and trades.

investing.com - Financial information websites often utilize Google Analytics and Facebook Pixel for targeted advertising related to financial products or services.

Have you encountered ads when using some of the social platforms?

Social media platforms offer analytics tools for advertisers and can be brief analytics Integrations as below,
Facebook/Instagram - Integrates with Facebook Pixel for ad performance tracking.
Twitter - Offers Twitter Conversion Tracking to measure ad campaign effectiveness.
YouTube - Uses Google Ads for analytics and conversion tracking.
TikTok - Provides TikTok Pixel for ad campaign measurement.

Impact of Ads,

Disrupted experience - Ads can break the flow of your social media browsing.
Privacy concerns - Social media platforms track activity to target ads, which can be unsettling for some users.
Potential manipulation - Ads may use emotional triggers or misleading information to control opinions or actions.

Do you find similar analytics from their apps? Do you have any idea where your data is going and what is even tracked? Also, consider what is the impact of using advertiser-provided log-in options. E.g. for using Google login or Facebook login to some service, which has integrated relevant tracking software.

When considering AppFlyer's integration into social media apps and impact of using advertiser-provided login options, here's what might be tracked and potential implications and analytics tracked with AppFlyer Integration,

App Installs - Tracking the number of users who install the app after clicking on an ad.
In-App Events - App is monitoring user interactions, including purchases, registrations, level completions, and other predefined actions.

Attribution - Objective is to identify the marketing strategies that are driving app installs and user engagement.
Retention Rate - Study aims to assess number of users who continue to use app over time after its installation.
User Segmentation - Process involves sorting users based on factors like demographics, behavior & engagements.

Where the Data Goes and Implications,

Data Usage - AppFlyer integration collects data within the app ecosystem, which can be shared with app developers, advertising partners, or analytics providers.
Privacy Considerations - Users are advised to understand the app's privacy policy regarding data collection and sharing practices, including their usage for advertising and analytics.
Targeted Advertising - AppFlyer integration may use user data to personalize ad targeting and optimize campaigns, potentially resulting in more relevant ads, but raising privacy concerns.
Third-Party Sharing - App developers can share aggregated and anonymized data with third parties for analytics and advertising, requiring user consent and compliance with privacy regulations.

Impact of advertiser-provided login options is significant,

Convenience vs. Privacy - Google and Facebook login options offer user convenience but also allow access to user data to these platforms and their advertising partners.
Data Sharing - Users may accidentally share additional data with app developers and third-party analytics providers by logging in using their social media profiles.
Tracking - AppFlyer, an integrated tracking software, allows users to track interactions within and across platforms, providing comprehensive profiles for targeted advertising.

AppFlyer integration provides valuable insights for app developers and marketers, but users must be mindful of privacy implications, consent, and adherence to privacy regulations.