



Article

Exploring Personal Data Processing in Video Conferencing Apps

Georgios Achilleos ¹, Konstantinos Limniotis ^{1,2,*}  and Nicholas Kolokotronis ³ ¹ School of Pure and Applied Sciences, Open University of Cyprus, Latsia, Nicosia 2220, Cyprus² Hellenic Data Protection Authority, Kifissias 1-3, 11523 Athens, Greece³ Department of Informatics and Telecommunications, University of Peloponnese, 22100 Tripolis, Greece

* Correspondence: konstantinos.limniotis@ouc.ac.cy or klimniotis@dpa.gr

Abstract: The use of video conferencing applications has increased tremendously in recent years, particularly due to the COVID-19 pandemic and the associated restrictions on movements. As a result, the corresponding smart apps have also seen increased usage, leading to a surge in downloads of video conferencing apps. However, this trend has generated several data protection and privacy challenges inherent in the smart mobile ecosystem. This paper aims to study data protection issues in video conferencing apps by statistically and dynamically analyzing the most common such issues in real-time operation on Android platforms. The goal is to determine what these applications do in real time and verify whether they provide users with sufficient information regarding the underlying personal data processes. Our results illustrate that there is still room for improvement in several aspects, mainly because the relevant privacy policies do not always provide users with sufficient information about the underlying personal data processes (especially with respect to data leaks to third parties), which, in turn, raises concerns about compliance with data protection by design and default principles. Specifically, users are often not informed about which personal data are being processed, for what purposes, and whether these processes are necessary (and, if yes, why) or based on their consent. Furthermore, the permissions required by the apps during runtime are not always justified.

Keywords: Android; personal data protection; privacy; video conferencing apps



Citation: Achilleos, G.; Limniotis, K.; Kolokotronis, N. Exploring Personal Data Processing in Video Conferencing Apps. *Electronics* **2023**, *12*, 1247. <https://doi.org/10.3390/electronics12051247>

Academic Editor: Hung-Yu Chien

Received: 2 February 2023

Revised: 22 February 2023

Accepted: 2 March 2023

Published: 5 March 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The COVID-19 pandemic considerably changed our daily lives in several aspects. One of the main changes was the rapid expansion of remote work, which resulted in investments in video conferencing software. Indeed, as a characteristic example, in March 2020, video conferencing apps on Android and iOS were downloaded 62 million times per week [1]. However, this trend seems to be continuing despite the fact that lockdowns and restrictions on movements imposed during the pandemic seem to have passed (some related statistics for 2022 can be found in [2]).

This increase in the use of video conferencing apps (VCAs) brings with it an increase in privacy and personal data protection risks. Indeed, smart applications typically process large amounts of personal data, including information stored in the user's device, and this can occur in a non-transparent way and/or can be quite excessive [3,4]. Specifically, an app may collect personal data without the user being aware or without the user being given the option to disable this feature. This becomes an issue if the data collection is not essential for the purpose for which the user installed the app. Additionally, these privacy and data protection issues are compounded by the fact that data may be transmitted to third parties, including trackers. Therefore, in the smart mobile ecosystem, privacy and personal data protection present both technical and legal challenges, and, including in the case of video conferencing apps.

It has been said that although people typically use 8-9 apps daily, a smartphone has, on average, around 80 apps installed [5], and the number of smartphone subscriptions worldwide is constantly increasing [6]. Regarding the underlying platform, smartphones running on the Android operating system, which is the most popular operating system, accounted for more than 70% of the global app market in 2022 [7,8]. On the Android platform, the user is required to grant permissions for each app in order for it to operate properly. The vast majority of apps utilize third-party libraries to integrate with social networks or facilitate programming procedures by easily embedding functionalities such as statistical information collection (see, e.g., [9]). However, these libraries obtain the same access rights as the host app since the Android security model does not support the separation of privileges between apps and the embedded libraries (see, e.g., [10]). This, in turn, creates significant risks with respect to users' privacy and personal data protection, for example:

- Libraries can abuse the privileges granted to the host applications.
- Libraries can track users.
- Libraries can aggregate multiple signals for detailed user profiling, even from different host apps that are installed on the user's device (known as the *intra-library collusion* problem [10]).

Hence, privacy and data protection issues depend not only on what the app provider does with the user's data but also on which third parties have access to the user's data and how they use them, as well as the overall transparency of the data processing. As demonstrated in previous studies (see, e.g., [11]), there is an increased collection of personally identifiable information across app versions, with a large number of third parties being able to link user activity and locations across different apps.

The right to privacy has been recognized as a fundamental human right by the United Nations Declaration of Human Rights, the International Covenant on Civil and Political Rights, the Charter of Fundamental Rights in the European Union, and other international treaties. Hence, it is essential for any organization involved in personal data processing, including app providers, to fulfill the relevant legal requirements. This is not an easy task, given the high fragmentation among stakeholders in the smart app ecosystem, including app developers, app owners, app stores, operating systems, and device manufacturers, as well as the third parties involved in the collection and processing of personal data from smart devices, such as analytics and advertising providers [12]. Moreover, there is also fragmentation in the corresponding legal frameworks worldwide, which is particularly relevant in the case of video conferencing apps that employ real-time communication between users residing in different countries or even continents, presenting additional challenges in terms of legal compliance.

This paper focuses on analyzing the underlying personal data processing that takes place within popular video conferencing apps in Android environments. Specifically, we aim to determine the permissions that are granted to these apps and whether these permissions are necessary, identify any data leaks to third parties and the types of data that are being sent to these third parties, and assess whether the app provides sufficient information to users about the data processing that takes place. We also analyze the legal requirements related to data protection, with an emphasis on the provisions stemming from the European legal framework and the General Data Protection Regulation (GDPR), which can serve as a useful model for other regulations to follow in terms of rights and principles (see, e.g., [13]).

The aim of the paper is not to suggest that some video conferencing apps are better than others or to perform a legal analysis of the personal data processing they perform. Rather, we aim to examine a typical usage scenario of these popular apps, including whether the user is fully aware of the actual underlying personal data processing that takes place, and identify any common characteristics in the data processing required for these apps to function. Hence, given that some VCAs provide more services than others, and

thus have different characteristics, this paper should not be considered a guideline for selecting a VCA.

The paper is organized as follows. First, a short discussion of the main legal provisions is provided in Section 2, along with a presentation of device identifiers that should be considered personal data. Section 2.2 provides a short overview of the privacy and data protection issues related to the Android permission model, with an emphasis on the so-called high-risk permissions in terms of privacy. Section 3 presents a summary of the relevant previous works in this field. Section 4 provides the research questions and methodology adopted to address the identified issues. In Section 5, the results of our analysis of the video conferencing applications are presented, and a discussion of the main findings is presented in Section 6. Finally, the concluding remarks and suggestions are presented in Section 7.

2. Preliminaries

2.1. *The Notions of Privacy and Personal Data Protection*

Both privacy and personal data protection are considered fundamental human rights in Europe. According to the Charter of Fundamental Rights of the European Union, which consolidates the most important personal freedoms and rights enjoyed by citizens of the European Union, all people have the right to respect for their private and family life, home, and communications (art. 7 of the Charter), including the right to the protection of their personal data (art. 8 of the Charter). Although privacy and personal data protection are strongly related, they are not synonymous.

The General Data Protection Regulation or GDPR [14] is considered the main legal instrument for personal data protection in Europe. Although the GDPR is a European regulation, it applies to all organizations, regardless of location, if they are involved with processing the personal data of individuals residing in the European Union. As stated in [15], the intentionally global reach of the GDPR, in conjunction with the relevant threat of huge fines if fundamental rights are not properly protected, has led to companies around the world adjusting their privacy practices and countries around the world updating their privacy laws.

The term personal data refers to any information related to an identified or identifiable natural person. As explicitly stated in the GDPR, an identifiable natural person is one who can be identified, either directly or indirectly, particularly in terms of an identifier such as a name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. Personal data processing means any operation that is performed on personal data, including the collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure by transmission, dissemination, combination, and erasure. The entity that, either alone or in conjunction with others, determines the purposes and means of the processing of personal data, is the so-called data controller, whereas the entity that processes the personal data on behalf of the controller is the data processor.

The concept of personal data is quite broad and in general, device and network identifiers should be regarded as personal data since they can potentially identify a user when combined with other information. Specifically, in this work, we focus on the Android operating system, which is associated with two identifiers (see, e.g., [16]):

- The Android ID, which is a permanent 64-bit randomly generated number.
- The Google Advertising ID (GAID), which is a 32-digit alphanumeric identifier that can be reset at any time by the user.

Other device and network identifiers, such as medium access control (MAC) and Internet protocol (IP) addresses, are also considered personal data.

Generally, data processing should be always transparent in that users should be fully informed about the processing upfront in a comprehensive, accessible, and easy-to-understood manner. Such information should include the data to be processed, the parties involved in the processing, and the purposes for which the data will be used.

The GDPR outlines the fundamental principles and the specific obligations of entities that process personal data, including data controllers and data processors. These principles include purpose limitations, which require personal data to be collected for specified, explicit, and legitimate purposes and not further processed for other purposes; data minimization, which ensures that the use of the personal data is limited to what is necessary for the purposes for which they are processed; and data security, which requires appropriate technical or organizational measures to protect against unauthorized or unlawful processing, as well as accidental loss, destruction, or damage. In this regard, any processing of personal data must have a lawful basis, which should also be included in the aforementioned information notice. If an individual's consent is the lawful basis, the consent must meet specific requirements to be considered valid. Specifically, the consent must be freely given, specific, informed, and unambiguous, and must be expressed through a statement or a clear affirmative action (art. 4 of the GDPR).

The GDPR outlines the specific rules and obligations for data controllers. Among them, the so-called data protection by design and data protection by default constitute important challenges involving various technological and organizational aspects [17]. In essence, data protection by design means that data protection should be integrated into processing activities from the early design stage and throughout the life cycle. In other words, organizations should consider data protection issues in everything they do. On the other hand, data protection by default, which could be seen as a substantiation of data protection by design, implements rules to limit data processing to what is necessary for its purposes by requiring the selection and implementation of proper default settings [18]. As explicitly stated in [18], the selection of the defaults is not trivial, even when considering data protection by design, as it requires an assessment of the necessity of each processing purpose, balanced with other equally important requirements such as the usability and expected behavior of the system or service. This challenge becomes particularly important in smart apps.

In relation to the above, Recital 78 of the GDPR states that the appropriate measures for addressing the above two principles of data protection by design/default could consist of, inter alia, minimizing the processing of personal data, pseudonymizing personal data as soon as possible, transparency with regard to the functions and processing of personal data, allowing the data subject to monitor the data processing, and allowing the controller to create and improve security features. In the same Recital, there is also an explicit reference to the providers of the products, services, and applications used for data processing (where these providers are typically not data controllers or processors), and they are encouraged to take into account the right to data protection when developing and designing their products, services, and applications.

It should be pointed out that depending on the technique used, the tracking of a mobile user may fall under the scope of the legal framework outlined in the ePrivacy Directive (Directive 2002/58/EC) which takes precedence over the more general provisions of the GDPR. The e-Privacy Directive currently applies only to the European Union. As with many cases involving data processing, informed consent is a legal prerequisite.

2.2. Privacy and Data Protection Issues in Android Applications

One of the core features of the Android system is that applications are executed in their own private environment, which is referred to as a sandbox, and applications are unable to access resources or perform operations outside of their sandbox that would adversely impact system security (e.g., by downloading malicious software) or the user's privacy (e.g., by reading contacts, emails, or other personal information) (see, e.g., [19]). An application must explicitly request the permissions needed either at installation time via its `AndroidManifest.xml` file or at runtime. Our experimental environments, which are discussed later, involved Android version 8.0, and thus, the permissions granted to the applications were requested at runtime.

The permissions granted to applications are classified into several protection levels based on their ability to harm the system or the end user, of which three levels affect third-party applications:

1. Normal permissions: these cover areas where an application needs to access data or resources outside its sandbox but there is a low risk to the user's privacy or the operation of other applications.
2. Signature permissions: these are granted only if the application that requests the permission is signed by the same certificate as the application that requests the permission.
3. Dangerous permissions: these cover areas where an application requests access to data or resources that involve the user's private information and could potentially affect the user's stored data or the operation of other applications.

In the smart mobile ecosystem, the permissions model is related to the user's consent, and thus, it deserves special attention [4]. Unfortunately, most users have a limited understanding of the risks associated with granting permissions to (or accessing) certain apps, and many app developers have difficulties in comprehending and appropriately handling permissions [4]. Moreover, the permissions model does not facilitate the provision of legally valid consent for any third-party functionalities that may be integrated into the app (since in Android platforms, third-party libraries inherit the privileges of the host app); hence, data protection risks arise whenever a third-party library uses personal data for profiling and targeting without the user's consent or without informing the user.

In addition to the above, other privacy and data protection risks that are inherent in the smart mobile ecosystem can be summarized as follows (see, e.g., [4] and the references therein):

- The processing of personal data should not be limited to the bare minimum. For example, app providers should allow an app to access a phone's sensors (location, camera, microphone, etc.) and the data stored on the user's device (pictures, contacts, etc.) when it is relevant for the proper functioning of the app, e.g., it is acceptable for a weather app to request permission to access a device's location but access to the exact location seems unnecessary.
- Confidentiality of personal data is insufficient. For example, encrypting all communications should be a prerequisite (which is not always the case); however, this may not always be sufficient. An app should at least use certificate pinning or preinstalled keys to prevent man-in-the-middle attacks on encrypted sessions (see, e.g., [20]). Moreover, users should be fully aware of what encryption means, for example, if an end-to-end encryption scheme is not used, this means that the app provider is technically able to decrypt and read the data. Additionally, it should also be made clear whether or not metadata are encrypted.
- There are insufficient mechanisms to allow users to control their data processing. Apart from the aforementioned intra-library collusion issue, users should have clear free choices when providing consent, for example, deceptive designs and manipulative patterns that "force" users to provide consent (such as pre-checked boxes) are highly problematic. Moreover, when an app requests permission to access a device's sensors (location, camera, microphone, etc.) and/or locally stored data, the app should still work even when the user does not agree to this access, with possibly limited functionality.

3. Previous Work

Data protection and privacy issues in the general framework of the mobile ecosystem have been extensively studied in the literature (see, e.g., [21–27]), and a generic report has been also issued by the European Union Agency for Cybersecurity [4]. Specifically, the privacy implications of ads in Android applications were studied in [21], and it was shown that many ad libraries required more permissions than what was described in their documentation. The work in [22] focused on checking and evaluating the behavior of

apps with respect to privacy issues through static analysis to identify possible data leaks, for example, whether the application releases the user's location or device ID without their consent. To achieve this, the researchers designed concrete semantics that formalized how the expressions generated by the program's execution maintained the footprints of personal data stored locally on the mobile device. Additionally, in [24], it was shown that even so-called anonymous social networks process personal data and these should not be considered anonymous applications. Privacy implications with respect to the use of wearables and fitness-tracking applications were studied in [25] and the work in [26] focused on privacy issues stemming from the use of fitness applications and GPS navigators. In [27], mobile health applications were studied in terms of both security and privacy characteristics, illustrating that many of the analyzed applications did not follow well-known practices, including the relevant legal obligations. In all the above-mentioned works, some common issues were identified: (i) several hidden or not fully transparent personal data processes occurred without the user's awareness (such as the leaking of device identifiers to third parties), and (ii) many dangerous permissions were granted to apps that were not fully justified.

The security and privacy risks stemming from video conferencing apps have received much attention over the past few years due to the pandemic. For example, the well-known Zoom app issued a patch in 2019 to address a flaw that allowed hackers to hijack webcams [28] and enhanced its encryption features following the outbreak of the pandemic (see, e.g., [29]).

However, despite the fact that all these apps now use encryption—and some of them also use end-to-end encryption, meaning that neither service providers nor other parties have access to the contents of communications aside from the end users—there are still several concerns because, as mentioned above, privacy is not synonymous with confidentiality. For example, in [30], it was shown that, through the use of these apps, various user data can be derived from the characteristics of encrypted media streams, such as whether the camera is on/off or whether there is increased activity in front of the camera, even if end-to-end encryption is used.

There are also several issues stemming from the amount of personal data, including metadata, that VCAs collect and process, in conjunction with what is outlined in the relevant privacy policies. For example, in a 2020 report [31], it was stated that according to their privacy policies, some popular VCAs collect more data than consumers realize. In [32], it was shown that the leaking of users' personal data from smart devices to third-party websites takes place through apps such as VCAs. Since they can lead to the exposure of users' personal data without their consent, the privacy risks related to the recording services provided by VCAs were examined in [33], where a privacy-preserving publishing system that automatically processes video and audio information in VCRs for personal data protection was proposed. Recently, in [34], video conferencing apps were analyzed in terms of their behavior when a user clicks the mute button. Surprisingly, the researchers managed to trace raw audio flow in many popular apps since some apps continuously monitored the microphone input during mute, whereas others did this periodically. Moreover, fragmentation was also found in the relevant policies. Additionally, in [35], the researchers illustrated how private information can be extracted from collage images of meeting participants that are publicly posted online. To achieve this, image processing and text recognition tools, as well as social network analysis, were efficiently utilized.

4. Research Methodology

This section presents the main goals of the current research and the methodology that was adopted.

4.1. Contribution of This Work

This work aims to analyze VCAs by identifying the processing of personal data during usage of these apps through static and dynamic analysis while taking into account the

intra-library collusion issue in the Android environment. We also examine the information provided to users through privacy policies to assess their sufficiency and evaluate whether data protection by design and default principles are in place.

Our work further extends the work in [32] by examining more apps than those studied therein and by studying and evaluating all the relevant privacy policies in connection with the results of our analysis.

4.2. Research Questions

In this work, we mainly focus on the following research questions regarding messaging and video conferencing applications:

1. Do these applications collect only data that are absolutely necessary? Are any required permissions fully justified?
2. What types of data are being leaked to third parties through the use of these apps?
3. Are all these processes fully transparent to the users, i.e., is clear and comprehensive information provided about the underlying processing of personal data?

Based on these research questions, we proceed with the testing environment and the analysis of the selected video conferencing apps.

4.3. The Testing Environment

For our research, we utilized an Android device (version Nougat 8) on which we installed and further examined the selected video conferencing apps, as described in the next section.

To analyze these smart apps by investigating whether they send personal data to third parties and checking the permissions they request, we utilized two well-known tools, namely Exodus Privacy (hereafter referred to as Exodus) [36] and the Lumen Privacy Monitor (hereafter referred to as Lumen) [37]. These tools provide the following functionalities:

- Exodus, which is supported by a French non-profit organization, can statically analyze Android applications by looking for embedded trackers and listing them as an output report. In addition, this tool presents the permissions that are being requested by an app and highlights the dangerous permissions.
- Lumen is at the core of the ICSI Haystack project and is an initiative of independent academic researchers. After its installation, the Lumen app uses VPN installation permissions on Android to analyze the outgoing traffic from the applications installed on the device. Therefore, the VPN acts as middleware between the applications and the packets they send by identifying their endpoints. In order for the application to be able to read and analyze the outgoing encrypted data through the TLS and traffic from the applications, the installation of a TLS certificate is required. Through the analysis, users can see the personal data that an application collects, block unwanted flows, and configure the application permissions so that they have better control over their personal data. This tool has been used in several studies to analyze smart apps with respect to privacy issues (see, e.g., [38,39]).

After setting up the appropriate testing environment, we proceeded to analyze several video conferencing apps. In order to select a representative set of apps, we used several selection criteria, such as (i) a high number of downloads according to the statistics from the app store (i.e., popular apps), and (ii) a variety of countries/continents of origin spanning Asia, America, and Europe. The latter allows for checking how the different legal frameworks on privacy and personal data protection affect the design and operation of an app. Based on the above criteria, our study selected eighteen (18) popular video conferencing apps: (1) Discord, (2) Element, (3) KakaoTalk, (4) Line, (5) Messenger, (6) Phoenix, (7) Session, (8) Signal, (9) Skype, (10) Teams, (11) Telegram, (12) Viber, (13) Webex Meet, (14) WeChat, (15) WhatsApp, (16) Wire, (17) Zalo, and (18) Zoom.

Finally, having identified the specific data processes that take place through the use of the aforementioned VCAs, we proceeded to examine their privacy policies to identify

possible discrepancies and determine whether the information provided to the user was clear, easily understood, and comprehensive. In the process, we attempted to find possible violations of data protection by default principle.

Next, we present the results of our analysis. The dynamic analysis was performed during the period of January–March 2022. The static analysis was also performed during this period but it was repeated in November 2022 to identify any possible changes that had occurred. The privacy policies were monitored during the entire period. The analyses presented in this paper rely on the most recent versions (December 2022).

5. Results

5.1. Permissions Analysis of the Video Conferencing Apps

By using Exodus in conjunction with the Lumen tool, we analyzed the permissions granted to each of the selected applications. We noticed that all applications requested some access rights that were classified as dangerous; some of them were classified as dangerous by Exodus but as high or medium risk by the Lumen tool. All the permissions that were characterized as high risk by the Lumen tool were also considered dangerous by Exodus. We summarize our observations in Table 1, with an emphasis on the high-risk permissions. Each app was assigned a descriptive number, as described in Section 4.3.

As evident from the above analysis, although all the applications provided similar services, there were variations in the permissions that each of them required. Permissions such as accessing the camera or recording audio can be considered necessary in order to provide the relevant video services, and thus, the fact that all apps required these permissions was not considered strange (of course this does not mean that camera and audio recording can be enabled at any time without the user being fully aware). However, other high-risk permissions could not be considered, by default, absolutely necessary, and thus, it was of interest that each app required, more or less, different permissions.

To avoid any misconceptions, it should be explicitly pointed out that none of these permissions should be considered, by default, unacceptable in the context of a video conferencing app; depending on the exact services provided by the app, we may find that all the required permissions are necessary. However, the crucial issue is that any permission should be fully justifiable and, of course, appropriate and comprehensive information should be provided to users regarding the necessity of these permissions with respect to the desired purpose of the processing. As discussed below, it is questionable that these conditions are always in place.

The above variations in terms of the different permissions that are requested among the different video conferencing apps may yield privacy and data protection concerns due to the intra-library collusion threat, for example, according to the data in Table 1, if the same third-party library is being simultaneously used (e.g., KakaoTalk, Viber, WeChat, and Zalo), this library will obtain all the high-risk permissions that are shown in Table 1.

Additionally, we found that the video conferencing apps that required the largest number of high-risk permissions were KakaoTalk and Signal, each requiring 19 high-risk permissions, followed by Messenger and Line, requiring 18 and 17 high-risk permissions, respectively. On the other hand, the app that required the lowest number of high-risk permissions was Session, requiring only five such permissions, followed by Discord, Element, and Wire, which required seven high-risk permissions.

Table 1. Dangerous permissions obtained by video conferencing apps (where × denotes the relevant permission being requested).

Permissions/VCA	Discord	Element	KakaoTalk	Line	Messenger	Phoenix	Session	Signal	Skype	Teams	Telegram	Viber	Webex Meet	WeChat	WhatsApp	Wire	Zalo	Zoom
ACCESS_COARSE_LOCATION			×	×	×	×		×	×	×	×	×	×	×	×		×	×
ACCESS_FINE_LOCATION			×	×	×	×		×	×	×	×	×	×	×	×	×	×	×
ANSWER_PHONE_CALLS																		×
BODY_SENSORS														×				
CALL_PHONE			×	×	×			×	×	×	×	×	×				×	×
CAMERA	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
GET_ACCOUNTS	×		×	×	×			×	×	×	×	×	×	×	×		×	
READ_CALENDAR			×		×			×										×
READ_CALL_LOG											×	×						
READ_CONTACTS	×	×	×	×	×			×	×	×	×	×	×	×	×	×	×	×
READ_EXTERNAL_STORAGE	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
READ_PHONE_NUMBERS			×	×	×			×				×	×		×			×
READ_PHONE_STATE			×	×	×	×		×	×		×	×	×	×	×	×	×	×
READ_SMS			×	×	×			×										
RECEIVE_SMS			×	×	×			×										
RECEIVE_MMS			×	×	×			×							×			
RECORD_AUDIO	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
SEND_SMS			×		×			×							×			
SYSTEM_ALERT_WINDOW	×	×	×	×	×	×			×	×	×	×	×	×			×	×
WRITE_CALENDAR			×					×										×
WRITE_CONTACTS			×	×	×			×	×	×	×	×		×	×		×	
WRITE_EXTERNAL_STORAGE	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
WRITE_SETTINGS		×		×			×	×	×	×		×		×	×		×	
Total number	7	7	19	17	18	8	5	19	13	12	13	15	12	13	14	7	14	13

5.2. Trackers Analysis of the Video Conferencing Apps

In January 2022, we analyzed the video conferencing apps using Exodus and found that all but three of them contained at least one tracker. Interestingly, we observed that a Google tracker was present in almost all of the apps, with the exception of Wire.

In November 2022, we re-examined the trackers present in these apps. Notably, the number of trackers had decreased in seven of the apps, which demonstrated efforts by the app providers to be more privacy friendly. However, in Messenger, the number of trackers had increased from four to five.

The number of trackers found in each application is summarized in Table 2.

The presence of trackers indicates possible privacy threats depending on the types of trackers present and the data collected by each tracker. In principle, a small number of trackers may not present threats, whereas the presence of no trackers can alleviate the so-called intra-library collusion issue. In this regard, the data in Tables 1 and 2 should be considered together, for example, it can be seen that Signal requested a large number of high-risk permissions but, at the same time, it did not contain any trackers.

In Tables 1 and 2, it can be seen that the app with the highest number of trackers was Viber, which also required a high number of high-risk permissions. On the other hand, the apps mentioned previously that required the smallest number of high-risk permissions, in general, also contained a small number of trackers. In particular, Element, Session, and Wire did not contain any trackers (Wire contained one tracker in January 2022, which was not a Google tracker). However, Discord, which also required a small number of high-risk permissions, included a significant number of trackers, that is, six, in January 2022. By November, this number had decreased to two. Interestingly, popular apps such as Skype, Teams, Webex Meet, and Zoom, which are frequently used by organizations for video conferencing, did not contain a large number of trackers.

Table 2. Number of trackers embedded into video conferencing apps.

App	Number of Trackers (January 2022)	Number of Trackers (November 2022)
(1) Discord	6	2
(2) Element	0	0
(3) KakaoTalk	3	3
(4) Line	4	4
(5) Messenger	4	5
(6) Phoenix	3	3
(7) Session	0	0
(8) Signal	0	0
(9) Skype	2	1
(10) Teams	3	3
(11) Telegram	1	1
(12) Viber	12	6
(13) Webex Meet	2	2
(14) WeChat	5	2
(15) WhatsApp	1	1
(16) Wire	1	0
(17) Zalo	7	5
(18) Zoom	1	0

Relationships with Other Apps

When studying the permissions required by an app, together with the trackers that the app uses, we should also take into account the large number of other apps that the user already has installed on their device. For example, according to the data in Table 2, Viber contained six trackers, which, based on the information obtained using the Exodus tool, included some well-known ATS such as Google AdMob and MixPanel, and some well-known analytics services such as Google CrashLytics and Google Firebase Analytics. If another app, for example, a fitness app, that was installed on the user's device also utilized one or more of these trackers, then the intra-library collusion threat can lead to serious data protection concerns. To observe this, we could simply conclude that this fitness app requires different permissions to those granted to Viber (e.g., the RECEIVE_SMS permission) while it also sends different types of personal data to the tracker(s) compared to those sent by Viber. Then, this third party receives personal information from both apps, which becomes a superset of information containing more than it would had only one of these two apps been installed on the device.

The user, when installing and using apps, is typically not aware of this threat. As we discuss later, this kind of information cannot be gleaned from privacy policies, even those that are fairly comprehensive.

5.3. Analyzing the Data Flow from the Video Conferencing Apps

Using the Lumen tool, we observed that for some of the video conferencing apps, there was data traffic to third-party domains. For example, Figure 1 illustrates the case of Viber, where there was data traffic to third-party domains, which were characterized as advertising or tracking services (ATS).

The output of the Lumen tool with regard to the traffic being transmitted to ATS by the video conferencing apps is shown in Table 3. All the domains corresponding to

ATS were third-party domains, with the exception of the domain line-apps.com, which corresponded to the Line app. The Lumen tool did not identify any other traffic from the other applications to ATS.

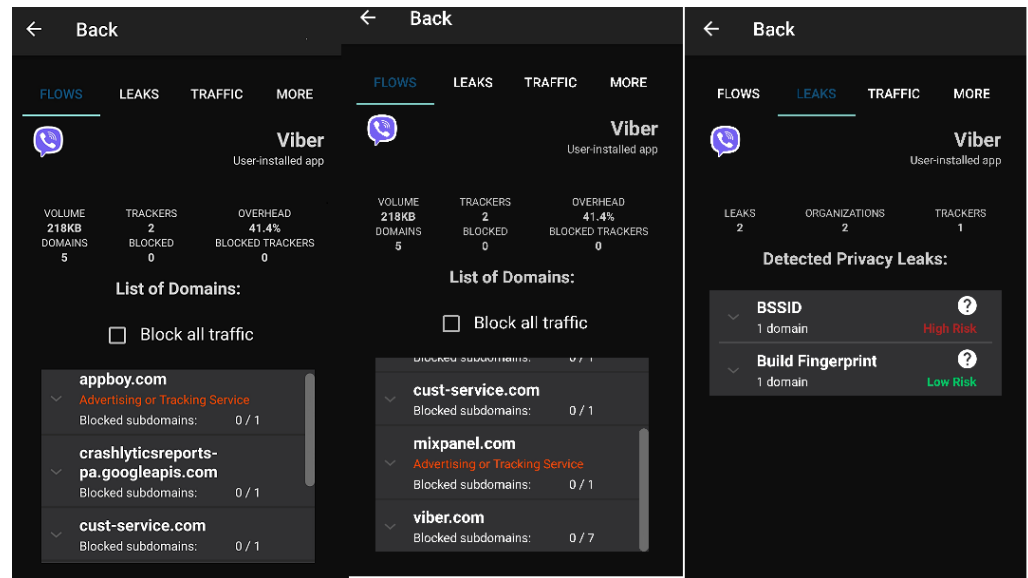


Figure 1. Data flow to ATS from Viber.

Table 3. Captured traffic from video conferencing apps to ATS (where “×” indicates that traffic to the relevant domain has been captured).

	Discord	KakaoTalk	Line	Phoenix	Viber
adjust.com	×				
appboy.com					×
appsflyer.com				×	
collection-endpoint-prod.herokuapp.com				×	
crashlytics.com	×	×			
line-apps.com			×		
mixpanel.com					×

Moreover, according to the output of the Lumen tool, some leaks were considered high risk with respect to privacy (see, e.g., Figure 1 for the case of Viber). A summary of the leaks captured by the Lumen tool is given in Table 4. Red indicates high risk, whereas green and blue indicate low and medium risk, respectively.

Table 4. Captured data leaks from video conferencing apps.

App	Account (com.facebook.messenger)	Android Serial	Build BSSID	Build Fingerprint	Private IP	Timezone
Line				×	×	
Phoenix				×		
Skype	×	×				×
Teams				×		
Viber			×	×		
Webex Meet				×	×	×
Whatsapp				×		

Based on the findings of the Lumen tool, Skype was able to access information about the user's Facebook Messenger account, as well as the Android serial number. Both these data leaks were characterized as high risk, whereas no other app was found to require access to these data. Moreover, Viber was able to access the Basic Service Set Identifier (BSSID), which was also considered high risk. Indeed, the BSSID can provide access to the geolocation of the user even if the GPS is disabled [40]. Other data leaks that were captured were the time zone (Skype and Webex Meet) and the private IP address (Line and Webex Meet) of the user. The latter is a range of IP addresses used in an internal network that is provided by network devices such as routers using network address translation. According to the Lumen tool, these data leaks were considered medium risk in terms of privacy. As shown in Table 4, six apps were found to process the so-called Build Fingerprint, which is a value that is used to uniquely identify the type and version of the Android operating system.

5.4. Transparency of the Processing

Next, we studied the privacy policies of video conferencing apps to evaluate whether they provide sufficient information to their users or, equivalently, whether they fulfill the transparency requirements. By taking into account the results from the tools, the study of the privacy policies indicated that there were apps that sent data to advertisers without the user's permission, and in some cases, the privacy policy was not clear with respect to the underlying purposes of the data processing. The main findings can be summarized as follows:

1. Discord: The privacy policy (<https://discord.com/privacy> (accessed on 28 December 2022)) classifies the personal data that the app processes into two main categories:
 - (a) Data provided by the user to the company such as account information, content created by the user, etc.
 - (b) Data automatically collected by the company such as information about the user's device (e.g., the IP address, operating system information, browser information, device settings related to the microphone and/or camera, and information about the use of the app or website when the user utilizes one of the company's services. Additionally, there may be other cases, for example, when the user clicks on an ad on a third-party platform on which the company advertises for Discord, the company may receive information about which ad the user saw and on which platform.

The Discord privacy policy also describes all the purposes of the data processes that take place and the legal basis for each purpose; however, there is no explicit mapping of each purpose to the exact user data processed.

Moreover, although Discord's privacy policy states that the user may be able to configure their privacy settings, it seems that the data protection by default principle may not be always present, for example, the privacy policy states that "If you turn off the "Use data to improve Discord" setting, we will stop collecting and using certain event and log information to help us understand how users use our services, what features or products they may want, or to otherwise improve our services", which implies that this option is activated by default.

Regarding third-party trackers, the relevant information in Discord's privacy policy states that "We may share information with vendors we hire to carry out specific work for us (...) We may also share limited information with advertising platforms to help us reach people that we think will like our product and to measure the performance of our ads shown on those platforms. We do this to help bring more users to Discord, and provide only the information required to facilitate these services. This may include information like the fact that you installed our app or registered to use Discord.". Given the number of embedded trackers found in the dynamic analysis, it is unclear exactly which user information is being sent to which third parties.

2. Element: The privacy policy (<https://element.io/privacy> (accessed on 28 December 2022)) states that the company collects information when the user registers for an account, including their email address, an identified authentication (which is further explained in the policy), their password (stored in a salted hashed form with a server-side pepper secret), their Twitter id, and their Google id. Additionally, the company may collect the user's location data if the user chooses to use static or live location-sharing features within the app. Moreover, the company collects the user's IP address to support operational maintenance and protect against malicious actions against its infrastructure. The company also uses analytics services that are hosted entirely within the company's network and states explicitly that the company does not share any analytics data with third parties.

In principle, Element's privacy policy and the app itself are consistent with the findings of our dynamic analysis of the app, that is, it does not contain any trackers.

3. KakaoTalk: The privacy policy (<https://www.kakao.com/policy/privacy> (accessed on 28 December 2022)) defines some data that are always collected, including basic personal information such as the user's email address, password, name (nickname), profile picture, list of friends, contacts, and history of service usage, among others. The purposes of the data processes are explicitly stated and include a description of each process involving personal data.

The policy also states that some other information may be collected during the use of the provided services such as the operating system, screen size, device ID, and IP address, among others.

According to the policy, the company does not provide personal information to any third party without the user's consent or unless demanded by law. However, there is a reference to pseudonymized data that cannot identify an individual, which may be used for archiving, scientific research, or statistical purposes. According to the findings of our dynamic analysis, the app sends data to the crashlytics tracker, which is an analytics service. However, it is unclear whether the data that are sent to this tracker are indeed pseudonymous or the level of pseudonymization applied to them.

4. Line: The privacy policy (<https://line.me/en/terms/policy/> (accessed on 28 December 2022)) classifies the data processing with respect to data that are automatically collected by the app provider (such as information provided during the user's registration process, e.g., the user's phone number, as well as information collected externally, e.g., information collected by an app plug-in installed in a third-party app such as "Like") and data that are optionally provided by the user, such as those in the context of the "Auto Add Friends" feature, which automatically adds friends to the app's services when the user uploads information about their friends to their device's address book.

An interesting point in Line's privacy policy is that the app provider may disclose public information containing personal data in news published on the Internet. The purpose of this processing is not clearly stated in the policy.

Additionally, according to the policy, the app may collect the location information of the user's device when the user shares their location information with friends in order to provide optimized search results or customized content or ads. If the user does not agree to share their location information, the app's policy states that the app may approximate the user's location from network information such as their IP address.

With regard to the use of third-party modules, the policy states that the app may use modules from a third-party software development kit (SDK) in its services to analyze the usage of its services or distribute ads and measure their effectiveness. Moreover, the policy states that in cases where data are being processed by a third party through a module provided by that third party, the privacy policy of that third party applies. A list of these third parties is provided, which includes, among others, companies such as Google, Firebase, and Facebook. Interestingly, the exact data collected by each of them and the purpose of the processing are not clearly stated.

5. Messenger: The privacy policy (<https://www.facebook.com/policy.php> (accessed on 28 December 2022)) contains text that is common to all apps provided by Meta, which could be considered a possible weak point since the user may not have a clear understanding of the personal data processed by each app. In any case, this general privacy policy classifies the personal data that are collected into four main categories:
 - (a) The user's activity and the information provided by the user (with an emphasis on the fact that the company cannot see the content of end-to-end encrypted messages). Metadata are also included in this category.
 - (b) The user's friends, followers, and other connections. In this regard, the policy states that the company also collects information on the user's contacts, whereas, interestingly, this information may be collected even if the user's contacts do not use Meta products.
 - (c) The app, browser, and device information, including the type of device, details about its operating system, the battery level, identifiers that can distinguish the user's device from other users' devices, the IP address, and device signals such as GPS, Bluetooth, and nearby Wi-Fi access points.
 - (d) Information from partners, vendors, and third parties.

The policy states that the user's data are used to provide, personalize, and improve the company's products. These goals are further classified into sub-goals, including the provision of measurements, analytics, and business services. Moreover, the policy has a separate section on partners, which are classified as advertisers and audience network publishers, partners who use the company's analytics services, partners who offer goods or services on the company's commercial platforms, and integrated partners.

The policy also explains, in detail, the relevant legal basis for each type of data processing; however, a detailed description of which personal data are used for each purpose is unavailable.

6. Phoenix: The Phoenix app is a Facebook wrapper that shows Facebook and Messenger in a mobile-friendly web interface. It offers in-app messages, calls, and video calls, providing the user with the same aesthetics as the original Facebook app. The privacy policy of Phoenix was available during the time of our initial dynamic analysis at privacy.unimania.xyz/privacy_policy_pnx.html (accessed on 12 February 2022); however, by November 2022 when we re-examined the privacy policies, this link had become inactive. We later found the app's privacy policy at <https://www.apkmirror.com/apk/unimania/phoenix-facebook-messenger/> (accessed on 4 January 2023), which states that the company collects anonymous, non-personal user demographics and ad data for market research purposes only to gain special advertising-related insights and conduct analyses for brands that work with the company. The company does not collect, store, use, share, or sell any of the user's personal information. However, it appears that this policy is not fully consistent with our findings since the app includes third-party trackers and collects the build fingerprint of the device, but neither of these can directly identify the user and they are not considered high-risk processes. However, this information can still be considered personal and not anonymous data.
7. Session: The privacy policy (<https://getsession.org/privacy-policy> (accessed on 28 December 2022)) is very brief and states that the app does not know who the user is, who they are talking to, or the contents of messages as it does not collect or share any personal information. The policy also states that the app does not store any identifying information about the user's device, such as the IP address or the user agent, or any personal data such as the user's phone number, e-mail address, or any information tied to the user's real identity when they create a Session account. The above points are consistent with our findings that Session does not use any trackers.

8. Signal: The privacy policy (<https://signal.org/legal/#privacy-policy> (accessed on 28 December 2022)) begins by stating that “Signal is designed to never collect or store any sensitive information. Signal messages and calls cannot be accessed by the company or other third parties because they are always end-to-end encrypted, private, and secure”. The policy, which is quite brief, also states that a user’s phone number is needed when they create an account and additional optional data such as the user’s photo may be also processed.
Moreover, Signal’s policy states that the app can optionally determine which contacts in the user’s address book are Signal users by using a service designed to protect the privacy of the contacts based on cryptographic hashes. Specifically, as stated on a dedicated web page (<https://signal.org/blog/contact-discovery/> (accessed on 28 December 2022)), Signal overcomes this problem by utilizing Bloom filters to explore contacts lists to identify users that also Signal while preserving users’ privacy. There is also a reference to third parties and the policy states that the company works with third parties to provide some of its services. For example, these third-party providers send a verification code to the user’s phone number when they register. These providers are bound by their privacy policies to safeguard that information. No other information is provided about third parties, which is consistent with our findings that the app contained no trackers.
9. Skype and Teams: These are two Microsoft apps and although they are intended for different uses (Teams is geared toward professional/academic activities), they share the same privacy policy (<https://privacy.microsoft.com/en-us/privacystatement> (accessed on 28 December 2022)). As in the case of Meta’s general privacy policy, this could be considered a weak point with respect to the clarity of the information provided to users.
According to the policy, the company collects data from users by interacting with them and through the company’s products. The data collected by the company depends on the context of the user’s interactions with the company and their choices, including the privacy settings, products, and features used. The company also obtains user data from third parties. Moreover, the policy describes a list of purposes for data processing (including targeted advertising, among others) and states that to carry out these purposes, it combines data from different contexts (for example, when a user uses two Microsoft products) or obtains data from third parties to provide the user with “a more seamless, consistent, and personalized experience in order to make informed business decisions, as well as for other legitimate purposes”. There is also a reference to automated processes based on artificial intelligence techniques. The policy includes several other sections such as “cookies and similar technologies” and “Microsoft account”. However, as stated above, the policy is generic and does not explicitly state which personal data are used by each app and for what purpose or the legal basis on which personal data are processed. Thus, despite the generic statement in the policy that the user has control over their data usage, it is uncertain whether the apps meet the data protection by design and default principles.
10. Telegram: The app’s privacy policy (<https://telegram.org/privacy> (accessed on 28 December 2022)) begins by stating two privacy principles: (1) the company does not use the user’s data to customize ads, and (2) the company only stores the data that Telegram needs to function as a secure and feature-rich messaging service.
According to the policy, the personal data used by the app includes the basic account details (telephone number, e-mail address, account name, etc.), messages exchanged through the cloud chat (which are stored on its servers and are encrypted using cryptographic keys stored in separate data centers) or secret chats (which use end-to-end encryption, and thus, there is no way for the company or anybody else without direct access to the user’s device to discover the content of those messages; the company does not store secret chats or store the logs for messages sent in secret chats), and the user’s contacts where consent is requested before synchronization. Moreover,

if the user shares their location in a chat, this location data is treated the same as the content of other messages in cloud or secret chats.

The policy also provides a list of the purposes for which the user's data are processed and explicitly states that the company does not use the user's data for ad targeting or other commercial purposes. However, as described above, our experiments illustrated that there is a tracker in the app, that is Google Firebase Analytics, which is not explicitly stated in the app's privacy policy.

11. Viber: The app's privacy policy (<https://www.viber.com/en/terms/viber-privacy-policy/> (accessed on 28 December 2022)) presents a list of all personal data that are collected by the company, including several types of identifiers (such as device and network identifiers) and GPS-based location depending on the user's agreement. The policy explicitly states that some personal data are collected automatically from the user's device through device-identifying technologies. To this end, the policy clarifies that cookies and tracking technologies are used for advertising and marketing purposes and provides a list of all third parties that are involved in the data processing; however, they are mainly presented in the 'cookies section' of the privacy policy, thus implying that they are related to third-party cookies rather than other tracking mechanisms.

Moreover, the policy describes the purposes of all the data processes and, interestingly, for each purpose, there is a description of the types of personal data that are needed (a feature that is not common in other policies). However, these descriptions are somewhat generic. For example, with respect to the advertising purpose, the policy states that the company shares different types of personal data, which may include a device identifier and the user's age range, inferred gender, and reduced IP address (or GPS location data if the user allows this) with third-party advertising partners for the purpose of presenting personalized ads. However, an exact reference to the processing of the BSSID that was captured by our dynamic analysis is missing from the information provided to users.

12. Webex Meet: A generic privacy policy (<https://www.cisco.com/c/en/us/about/legal/privacy.html> (accessed on 28 December 2022)) is provided by the company (Cisco). In this generic policy, the description of the user's personal data that is processed by the company is also quite generic. The policy states that "We collect personal information for a variety of reasons, which may include processing your order, providing our various websites and other products and services ("Solutions"), providing you with a newsletter subscription, sending business and marketing communications, personalizing your experience, and processing job applications" and "We may also collect information relating to your use of our websites and web-based Solutions through the use of various technologies, including cookies".

However, in the generic policy are links to more specific privacy policies, where a privacy datasheet is available (<https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf> (accessed on 28 December 2022)), which describes the processing of personal data by Webex Meet. This datasheet contains a detailed description, along with the purposes, of the personal data that are processed. There is also an explicit reference to the sub-processors, i.e., service providers, contractors, or authorized third parties that assist in providing and improving the services. The datasheet also contains a detailed description of all the third parties, the personal data that are processed by each of them, and for what purposes. Moreover, for each case, information is also provided about the location where the data are stored.

13. WeChat: There are two privacy policies for this app—one for users whose phone numbers are not the +86 China country code and another for China-based users. Here, we focus on the first privacy policy, which is available at https://www.wechat.com/mobile/htdocs/en/privacy_policy.html#pp_how (accessed on 28 December 2022). This policy is quite detailed with respect to the personal data that are collected

and further processed, as well as for what purposes and on which legal basis the data are used. Additionally, the data retention period is also provided. However, there may be some concerns with respect to data protection by design and by principle. For example, regarding location data, the policy defines that “location data is information that is derived from your GPS (GPS coordinates), WiFi (approximate city location), IP address (country location), or public posts that contain location information (the location you geo-tag)”, while the legal basis for processing these data is that it is necessary to fulfill the contract; however, the policy also states that the user may disable the collection and use of their location data through device-level settings, thus rendering the necessity of collecting such data questionable.

With respect to data transfers to third parties, the policy states that the company engages with service providers to supply services to support or improve the app and that the company may share with advertising partners reports about the trends and performance of their advertisements to help them better understand their audience. To this end, the policy states that the company does not share information that personally identifies the user, such as their name or email address unless the user consents to this. Along the same line, the policy also states that the company may also pseudonymize or aggregate personal information for analytical purposes to provide to third-party service providers. There is no explicit reference to the names of these providers (our analysis found, for example, the existence of the Google Firebase Analytics tracker) and there is also no explicit information about the types of pseudonymized/aggregated information provided to them.

Finally, our analysis illustrated that the app requests the `BODY_SENSORS` permission (it is the only app requiring this access), and this data process is not explained in the app’s privacy policy.

14. Whatsapp: The app’s privacy policy (<https://www.whatsapp.com/legal/privacy-policy-eea> (accessed on 28 December 2022)), which begins with a generic statement that the app provides end-to-end encryption and that this will never change, is quite detailed in a structured way, presenting the purposes for which data are being processed and the types of personal data that are processed for each purpose, as well as the relevant legal basis. Interestingly, apart from this detailed description, there is also a more general section of the policy that explains in simple words what personal data the company generally collects and why. This generalized text identifies the following cases with respect to personal data collection:
 - Information that the user provides. This includes account information and user content, as well as the user’s connections (if the user makes use of the contact upload feature, whereas the policy states that if any of the user’s contacts are not yet using the service, the company will manage this information in a way that is designed to ensure that those contacts cannot be identified).
 - Automatically collected information: This includes device and connection information (whereas, as a special case, it is explicitly mentioned that this includes identifiers unique to Meta products associated with the same device or account) and general location information (for precise location information, the user must provide consent).
 - Information that third parties provide about the user. This includes data processed by the company through the aforementioned upload contacts feature, as well as cases where users report other users (e.g., for violation of terms).
 - Information shared by the user and by WhatsApp with third parties. This includes third-party service providers, but these third parties, as described in the app’s privacy policy, do not include advertising or analytics companies. In terms of the latter, the policy states that the company works with other Meta companies in the UK, Israel, and the United States that provide business analytics services.

The above points are consistent with our findings. Of course, in such a complex data processing framework with the many services provided, the fulfillment of data

protection by design and default principles needs to be very cautiously assessed. In any case, the privacy policy seems to present all the necessary information.

15. Wire: The app's privacy policy (<https://wire.com/en/legal/> (accessed on 28 December 2022)) is very different from the other privacy policies since it does not contain detailed information about which personal data are processed or for what purposes. However, the app's provider presents the characteristics of the app that make it privacy friendly, and the policy states that there is always end-to-end encryption, meaning that each device and user access request is fully authenticated, authorized, and encrypted before granting access. In addition, the policy states that there are no ads, and thus, the user's personal data and the content of their conversations will never be sold or shared with anyone and nor will they ever be used by any third-party advertiser.

The above points are generally consistent with our findings since no tracker was found through our analysis and Wire requests a relatively small number of high-risk permissions. In any case, even if the data processing is generally privacy friendly—and it is also highly possible that the data minimization principle is fulfilled—sufficient information should be provided to users.

16. Zalo: Zalo's privacy policy (<https://zalo.me/zalo/policy/> (accessed on 28 December 2022)) is the briefest of all the privacy policies we examined in this work. It consists of three very compact sections. The first briefly describes the information the company collects, that is, information about the user's account, device information such as the hardware model, location information, and information about the user's contacts (address book). The latter is stored on the company's servers to optimize the app experience. The second section briefly described how the collected information is used (no advertising or statistics purposes are given therein). The third section concerns how the company shares the information and it is simply stated that encryption is used and that the information is not shared with any third parties.

The privacy policy is so compact that it is very difficult to claim that sufficient information is provided to users. It is unclear exactly which personal data are collected and on what legal basis (e.g., whether some data are collected only after the user provides consent). Moreover, our analysis found that this app contained five trackers and this is not reflected in the privacy policy. In addition, the fact that the contact list is, by default, stored on the company's servers raises some concerns regarding the fulfillment of the data protection by default principle.

17. Zoom: The app's privacy policy (<https://explore.zoom.us/en/privacy/> (accessed on 28 December 2022)) contains several sections. The first section describes the types of personal data that are generally collected. This includes the device information, together with a description that it is consistent with the high-risk permissions required, i.e., this device information "may include information about the speaker, microphone, camera, OS version, hard-disk ID, PC name, MAC address, IP address (which may be used to infer the general location at a city or country level), device attributes such as the operating system version and battery level, WiFi information, and other device information such as Bluetooth signals". The second section contains a description of how the personal data are used and includes an explicit reference to marketing, promotions, and third-party advertising. However, there is no explicit mapping of the first two sections, i.e., the types of personal data that are used and for what purposes. There is another section in the policy concerning data sharing, which states that the company uses third-party marketing, advertising, and analytics providers. Moreover, there is a specific section about the cases in which European law (such as the GDPR) is applicable, including the legal basis for each data process and users' rights). However, there is no explicit mapping of the purposes of the data processes described in the policy to the corresponding legal bases.

In Table 5, we summarize the main findings of our evaluation of the privacy policies of video conferencing applications. The table focuses on the following aspects:

- Whether the privacy policy provides a detailed description of the types of personal data that are collected and further processed and for what purposes;
- Whether there is a detailed description of the third parties that collect data and which data are collected by which provider and for what purposes;
- Whether the results of our static and dynamic analysis of the apps are consistent with the app's corresponding privacy policy.

It is important to note that when even in cases where the privacy policy contains a detailed description of the underlying personal data processes, no justification is provided about which Android permissions are required by the app or why. Hence, it remains difficult to fully evaluate the necessities of the permissions shown in Table 1.

Table 5. Summary of the examination of the privacy policies of the VCAs.

App	Detailed Description of Personal Data Collected (Types of Data and Purposes)	Detailed Description of Third Parties	The Privacy Policy Is Consistent with Our Findings
Discord	Yes *	No	Yes †
Element	Yes	No third parties	Yes
KakaoTalk	Yes	Yes *	Yes ‡
Line	Yes **	Yes *	Yes
Messenger	Yes *	Yes *	Yes
Phoenix	Only anonymous data ◊	No	No (see Tables 3 and 4)
Session	Only anonymous data ◊	No third parties	Yes
Signal	Yes ◊	No third parties	Yes
Skype	No detailed description	No	No (see Table 4)
Teams	No detailed description	No	Yes
Telegram	Yes *	No third parties (only payment services)	Yes †
Viber	Yes	Yes *	No (see Table 4)
Webex Meet	Yes	Yes	Yes
WeChat	Yes	Categories of parties *	No (see Tables 1 and 2)
WhatsApp	Yes	Categories of parties	Yes
Wire	Yes ◊	No third parties	Yes
Zalo	No	No	No (see Table 2)
Zoom	Yes *	Categories of parties *	Yes

* No direct mapping of the types of data processed to the relevant purposes of the processing. † Some traffic to third parties was captured but is not stated clearly in the policy. ‡ Unclear what pseudonymized data are provided to third parties. • No detailed information about the processing of public information from the Internet. ◊ Unclear whether data considered anonymous are indeed anonymous. ◊ Minimal information is provided but the app collects minimal personal data.

It should be pointed out that Table 5 does not include information about whether the legal basis, according to the GDPR provisions, is also given for each data process (this occurs only in a few cases, as stated above, i.e., with Discord, Messenger, and Zoom). Moreover, as stressed above, in a few cases, there are concerns that some default configurations are not privacy friendly (e.g., Discord, Line, WeChat, and Zalo) based on what is stated in the corresponding privacy policy; however, this is not reflected in Table 5.

5.5. Security Aspects

For the sake of completeness, we subsequently present information regarding the security aspects of VCAs. This includes identifying which VCAs support end-to-end encryption and investigating the publicly disclosed related cybersecurity vulnerabilities related to these VCAs based on the well-known Common Vulnerabilities Exposure (CVE) list [41]. Since it is logical to assume that vulnerabilities found several years ago have been efficiently resolved by the current versions of the apps, we focused on the vulnerabilities found over the last two years (2021–2022), although these recent vulnerabilities may have already been resolved. It should be stressed that in Table 6, we present the number of known vulnerabilities identified over these two years in any version of the application, regardless

of the underlying platform (i.e., we do not confine ourselves only to Android versions). Moreover, we also present the relevant CVSS scores of the identified vulnerabilities to allow us to extract some information about the severity of these vulnerabilities since CVSS scores are commonly used for this purpose (a CVSS score can be between 0.0 and 10.0, with 10.0 being the most severe).

The basic information about the security aspects is provided in Table 6. However, the data in this table though should not be considered a security evaluation since they are not the result of a thorough security analysis of VCAs.

Table 6. Security aspects of VCAs.

App	End-to-End Encryption	Total Number of CVEs (2021–2022)	Corresponding CVSS Scores
Discord	No	2	5.0, 7.5
Element	Yes	2	0.0, 5.1
KakaoTalk	No	0	-
Line	Yes	7	0.0, 4.3, 4.3, 4.3, 4.4, 4.6, 5.0
Messenger	No *	1	4.3
Phoenix	No	0	-
Session	Yes	1	2.1
Signal	Yes	1	5.0
Skype	No	8 ‡	4.0, 4.0, 5.0, 5.8, 5.8, 6.5, 6.5, 7.5
Teams	No	2	3.5, 5.0
Telegram	No	14	2.1, 3.5, 4.3, 4.3, 4.3, 4.3, 4.3, 4.3, 4.3, 5.0, 5.0, 5.8, 5.8, 7.5
Viber	Yes	0	-
Webex Meet	No *	18 ◊	0.0, 0.0, 2.1, 2.1, 3.5, 4.0, 4.0, 4.3, 4.3, 4.3, 4.3, 5.0, 5.5, 5.8, 5.8, 6.5, 6.8, 6.9
WeChat	No	2	0.0, 4.3
WhatsApp	Yes	8	0.0, 0.0, 5.0, 6.4, 6.4, 7.5, 7.5, 10.0
Wire	Yes ◊	8	0.0, 2.1, 4.0, 4.0, 4.0, 4.3, 5.0, 7.5
Zalo	Yes †	0	-
Zoom	Yes *	3	0.0, 0.0, 4.3

* This feature is supported but is not enabled by default. † Not enough information about this was discovered. ‡ These vulnerabilities were found in the Skype for Business software and one additional vulnerability was found in the Skype extension for Chrome (CVSS: 2.6). ◊ These include vulnerabilities for Webex Meet, Webex Meet Online, and Webex Meet Desktop.

6. Discussion

The above analysis illustrates that VCAs, in general, still need to address several data protection issues. Although it seems that all relevant service providers, regardless of their location, are making efforts to comply with the legal provisions regarding transparency in data processing as required by the GDPR, our analysis has highlighted the following concerns:

- In their privacy policies, all the apps describe the types of personal data they process and the purposes of the data processes. However, in many cases, the exact types of personal data that are processed are not explicitly stated (e.g., some general information is stated in some cases such as “we process account information, device information”, etc.). Moreover, in the majority of cases, there is no explicit mapping between the personal data that are processed and the purpose of the process, i.e., the users cannot distinguish which of their data are used and for what purpose(s).
- The corresponding legal basis for each data process is not always explicitly stated (some privacy policies do provide this information but not always in a comprehensive way, e.g., by associating a specific data process with a specific legal basis. Therefore, it is not obvious whether or not some processes require the user’s consent (i.e., whether the legal basis is the user’s consent).
- Further to the previous issue, it seems that there are cases where some specific data processes are enabled by default and the user is simply informed that they can disable these processes if desired. The idea that these processes rely on the user’s consent is

inaccurate since the processes are initially activated without the user providing explicit consent prior to the start of the process. Such cases also raise concerns regarding the fulfillment of the data protection by default principle.

- When permission is requested by an app, it is not always clear to the user which specific data processes are associated with which high-risk Android permissions. Although the need to grant access to these permissions is clear in many cases (e.g., access to the camera is needed for a video call), some permissions seem to be necessary only for specific processes or, even worse, their necessity is not clear at all. More generally, each of these permissions should be mapped to one or more data processes with well-determined characteristics (i.e., which personal data are needed for these processes, what are the legal bases, etc.); however, this type of mapping is not reflected in the privacy policies.
- In a few cases (see Table 4), we identified some underlying personal data processes that are not defined, either clearly or at all, in the corresponding privacy policies.
- It is not always clear who the exact third parties are that collect personal data or for what purposes. Even in the few cases where third parties are explicitly stated, it is not clear which personal data they collect, and the issue of third-party libraries inheriting the privileges of the host app is absent from all privacy policies.
- Further to the previous issue, our analysis illustrated that in a few cases, there are data leaks to third parties without providing information to the users about this.
- A few privacy policies state that when users' data are transmitted to third parties, the relevant privacy policies of those parties apply. However, such cases should be meticulously studied; if data are transmitted to third parties by a VCA provider, it is questionable whether the VCA provider can simply refer to the privacy policies of these parties, especially if the users do not have the option to object to this transmission.
- Some privacy policies tend to define device data that do not allow for the easy identification of the user (at least, directly) as anonymous information; however, at least according to the GDPR provisions, these data are still considered personal data, and even if these processes are not high risk, it should be made clear that such types of device information are considered personal data.
- A few large companies that provide several different types of applications with different scopes adopt a unified privacy policy that covers all these applications. However, in this approach, it is difficult to ensure that users who only use a specific application provided by these companies receive the appropriate information about personal data processing.

The above findings indicate that the underlying personal data processes that occur through VCAs still have room for improvement under the assumption that the relevant European legal framework is used as a baseline. Even in cases where the underlying personal data processes seem to satisfy the data minimization process, i.e., there are no trackers or excessive collection of personal data and end-to-end encryption is used, the relevant information that is provided to users could be further improved and more comprehensive. Moreover, the aforementioned privacy and data protection concerns should be taken into account, along with the known problem of intra-library collusion in the Android ecosystem, especially because, as described earlier in the text, there are variations among VCAs with respect to the high-risk permissions that are required for their operation.

As a general conclusion, we believe that the data protection by design and default principles are not being fulfilled by all VCAs. Although some issues are related to the Android ecosystem itself, other issues could be efficiently addressed by the VCA providers, which seems not to be the case.

7. Conclusions

This work examined video conferencing apps, which have become tremendously popular in recent years, and assessed whether they fulfill basic data protection requirements.

Specifically, we focused on Android apps by investigating which personal data they process, how well justified these data processes are in the corresponding privacy policies, and how data transfer to third parties (especially to trackers) is handled by the app providers. As discussed in Section 6, not all privacy policies are clear and/or comprehensive and some underlying data processes are not described at all in these policies.

Therefore, recalling the research questions stated in Section 4.2, the main conclusions can be summarized as follows:

1. In all cases, there is no direct mapping of the required Android permissions to the relevant data processes. Therefore, when the user is required to grant access to permissions required by the app, they are not fully aware of whether the permissions are necessary and what happens with their personal data when granting this access. More generally, the app provider does not ensure that all data processes that are taking place by default are indeed necessary.
2. There is not always accurate information about the types of data that are being sent to third parties and for what purposes. Furthermore, in a few cases, there are data leaks without any information being provided to the user. It also seems that in some cases, there are some misconceptions with respect to what constitutes anonymous data, and thus data transmitted to third parties (especially to analytics services) are characterized as anonymous, although it is questionable whether this is indeed the case.
3. Some privacy policies do not provide details about the types of personal data that are being processed and for what purposes. This observation was more prevalent when data are transferred to third parties. In this context, considering the structure of the Android ecosystem, granting access to an app requiring permission is highly likely to allow access not only to the app provider but also to third parties, and this is not transparent to the users. Therefore, all relevant stakeholders must make efforts to ensure that users are fully and effectively informed about what personal data processes will occur if such access is granted.

With regard to the limitations of this research, it should be first pointed out that our findings concerning data leaks do not necessarily constitute an exhaustive list and there is still room for further analysis of these apps as the free Lumen tool has some limitations. One of these limitations is its ability to properly analyze encrypted traffic (see, e.g., [11]), and thus, some leaked encrypted personal data may not have been captured in our analysis. Moreover, we did not perform an extensive study on what exactly take place in the underlying data processes in the various configurations of these apps (e.g., by switching off the camera and/or the microphone) or evaluate the apps with respect to other privacy-friendly techniques that they may adopt (e.g., the background blurring feature). Finally, we did not study the exact security features that are implemented by these apps (e.g., what type of encryption is being used, with which parameters, etc.).

Moreover, as previously stated in the introductory section, this work should not be considered an in-depth legal analysis. The privacy policies were not thoroughly assessed for all possible data protection issues, several of which were outside the scope of our study. For instance, the GDPR outlines very strict rules regarding the international transfer of personal data, i.e., data transfer outside the European Union. This is of particular importance in VCAs, especially if the service provider is located outside the European Union. Our work did not perform such a legal assessment.

An interesting direction for further research would involve conducting a systematic study of the main third-party libraries used by various popular apps, regardless of their category, and estimating the number of these apps that are likely to be simultaneously installed on a single device. This would enable the assessment of the potential severity of the threat posed by intra-library collisions.

In conclusion, all software/product producers and service providers should prioritize data protection by design and default principles. This would allow them to fulfill their legal data protection obligations and increase users' trust in their services. In this regard,

we believe that all VCA providers should consider implementing end-to-end encryption to assure users that their private communications are indeed private. Although there is no explicit legal requirement for end-to-end encryption, its importance is significant given the potential risks to individuals' rights and freedoms when using VCAs.

Author Contributions: The experiments were set up and performed by G.A.; K.L. and N.K. contributed to the conceptualization and methodology; G.A., K.L. and N.K. contributed to the writing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable

Acknowledgments: The authors would like to thank the anonymous reviewers for their valuable comments that helped to improved the paper.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ATS	Advertising and Tracking Services
BSSID	Basic Service Set Identifier
CVE	Common Vulnerability Exposure
CVSS	Common Vulnerability Scoring System
GDPR	General Data Protection Regulation
GPS	Global Positioning System
ICSI	International Computer Science Institute
ID	Identifier
IP	Internet Protocol
MAC	Media Access Control
OS	Operating System
SDK	Software Development Kit
TLS	Transport Layer Security
VCA	Video Conferencing Application
VPN	Virtual Private Network

References

1. Techcrunch. Videoconferencing Apps Saw a Record 62M Downloads during One Week in March. 2020. Available online: <https://techcrunch.com/2020/03/30/video-conferencing-apps-saw-a-record-62m-downloads-during-one-week-in-march/> (accessed on 10 November 2022).
2. Beauford, M. The State of Video Conferencing in 2022. GetVoIP. 2022. Available online: <https://getvoip.com/blog/state-of-conferencing/> (accessed on 7 January 2023).
3. Degirmenci, K. Mobile users' information privacy concerns and the role of app permission requests. *Int. J. Inf. Manag.* **2020**, *50*, 261–272. [CrossRef]
4. European Union Agency for Cybersecurity: Privacy and Data Protection in Mobile Applications—A Study on the App Development Ecosystem and the Technical Implementation of GDPR. 2018. Available online: <https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications> (accessed on 10 December 2022).
5. Wise, J. 40+ Mobile App Statistics 2023: Usage 'I&' Downloads Data. Earthweb. 2022. Available online: <https://earthweb.com/app-statistics/> (accessed on 10 January 2023).
6. Statista. Number of Smartphone Users Worldwide from 2016 to 2021. 2020. Available online: <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/> (accessed on 18 December 2022).
7. Statcounter. Mobile Operating System Market Share Worldwide. 2022. Available online: <https://gs.statcounter.com/os-market-share/mobile/worldwide> (accessed on 20 January 2023).
8. Statista. Share of Global sMARTphone Shipments by Operating System from 2014 to 2023. 2019. Available online: <https://www.statista.com/statistics/272307/market-share-forecast-for-smartphone-operating-systems/> (accessed on 20 January 2023).
9. Binns, R.; Lyngs, U.; Van Kleek, M.; Zhao, J.; Libert, T.; Shadbolt, N. Third Party Tracking in the Mobile Ecosystem. *arXiv* **2018**, arXiv:1804.03603v3.
10. Taylor, V.F.; Beresford, A.R.; Martinovic, I. Intra-Library Collusion: A Potential Privacy Nightmare on Smartphones. *arXiv* **2017**, arXiv:1708.03520v1.

11. Ren, J.; Lindorfer, M.; Dubois, D.J.; Rao, A.; Choffnes, D.; Vallina-Rodriguez, N. Bug Fixes, Improvements, ... and Privacy Leaks. In Proceedings of the 25th Annual Network and Distributed System Security Symposium (NDSS 2018), San Diego, CA, USA, 18–21 February 2018.
12. Article 29 Data Protection Working Party. Opinion 02/2013 on Apps on Smart Devices. 2013. Available online: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf (accessed on 1 November 2022).
13. Michael, J.; Kuhn, R.; Voas, J. Security or Privacy: Can You Have Both? *Computer* **2020**, *53*, 20–30. [CrossRef]
14. European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Off. J. European Union* **2016**, *119*, 1–88. Available online: <https://gdpr-info.eu/> (accessed on 1 December 2022).
15. Kaminski, M. A recent renaissance in privacy law. *Commun. ACM* **2020**, *63*, 24–27. [CrossRef]
16. Son, S.; Kim, D.; Shmatikov, V. What Mobile Ads Know About Mobile Users. In Proceedings of the Network and Distributed System Security Symposium, San Diego, CA, USA, 21–24 February 2016.
17. Alshammari, M.; Simpson, A. Towards a Principled Approach for Engineering Privacy by Design. In *Privacy Technologies and Policy. APF 2017, LNCS*; Schweighofer, E., Leitold, H., Mitrakas, A., Rannenber, K., Eds.; Springer: Heidelberg, Germany, 2017; Volume 10518, pp. 161–177.
18. European Union Agency for Cybersecurity. Recommendations on Shaping Technology According to GDPR Provisions—Exploring the Notion of Data Protection by Default. 2019. Available online: <https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2> (accessed on 1 December 2022).
19. Grammatikakis, K.-P.; Ioannou, A.; Shiaeles, S.; Kolokotronis, N. Are cracked applications really free? An empirical analysis on Android devices. In Proceedings of the 16th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), Athens, Greece, 12–15 August 2018; pp. 730–735.
20. Moonsamy, V.; Batten, L. Mitigating man-in-the-middle attacks on smartphones—A discussion of SSL pinning and DNSSEC. In Proceedings of the 12th Australian Information Security Management Conference (AISM), Perth, Australia, 1–3 December 2014; pp. 5–13.
21. Stevens, R.; Gibler, C.; Crussell, J.; Erickson, J.; Chen, H. Investigating User Privacy in Android Ad Libraries. In Proceedings of the IEEE Workshop on Mobile Security Technologies (MoST), San Francisco, CA, USA, 24 May 2012.
22. Barbon, G.; Cortesi, A.; Ferrara, P.; Pistoia, M.; Tripp, O. Privacy Analysis of Android Apps: Implicit Flows and Quantitative Analysis. In *Computer Information Systems and Industrial Management. CISIM 2015*; Lecture Notes in Computer Science; Saeed, K., Homenda, W., Eds.; Springer: Cham, Switzerland, 2015; Volume 9339.
23. Bracamonte, V.; Pape, S.; Löbner, S. “All apps do this”: Comparing Privacy Concerns Towards Privacy Tools and Non-Privacy Tools for Social Media Content. *Proc. Priv. Enhancing Technol.* **2022**, *3*, 57–78. [CrossRef]
24. Chatzistefanou, V.; Limniotis, K. Anonymity in social networks: The case of anonymous social media. *Int. J. Electron. Gov. (IJEG)* **2019**, *11*, 361–385. [CrossRef]
25. Ioannidou, I.; Sklavos, N. On General Data Protection Regulation (GDPR) Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications. *Cryptography* **2021**, *5*, 29. [CrossRef]
26. Monogios, S.; Magos, K.; Limniotis, K.; Kolokotronis, N.; Shiaeles, S. Privacy issues in Android applications: The cases of GPS navigators and fitness trackers. *Int. J. Electron. Gov. (IJEG)* **2022**, *14*, 83–111. [CrossRef]
27. Papageorgiou, A.; Strigkos, M.; Politou, E.; Alepis, E.; Solanas, A.; Patsakis, C. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE Access* **2018**, *6*, 9390–9403. [CrossRef]
28. Newman, L.H. Zoom Will Fix the Flaw that Let Hackers Hijack Webcams. *Wired*. 2019. Available online: <https://www.wired.com/story/zoom-flaw-web-server-fix/> (accessed on 18 December 2022).
29. Schneier, B. Securing Internet Videoconferencing Apps: Zoom and Others. Available online: https://www.schneier.com/blog/archives/2020/04/secure_internet.html (accessed on 18 December 2022).
30. Altschaffel, R.; Hielscher, J.; Kiltz, S.; Dittmann, J. Meta and Media Data Stream Forensics in the Encrypted Domain of Video Conferences. In Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, Virtual Event, Belgium, 22–25 June 2021; pp. 23–33.
31. Consumer Reports. It’s Not Just Zoom. Google Meet, Microsoft Teams, and Webex Have Privacy Issues, Too. 2020. Available online: <https://www.consumerreports.org/video-conferencing-services/videoconferencing-privacy-issues-google-microsoft-webex-a7383469308/> (accessed on 18 December 2022).
32. Kalapodi, A.; Sklavos, N. The concerns of personal data privacy, on calling and messaging, networking Applications. In *Security in Computing and Communications SSCC 2020*; Communications in Computer and Information Science; Thampi, S.M., Wang, G., Rawat, D.B., Ko, R., Fan, C.I., Eds.; Springer: Singapore, 2021; Volume 1364.
33. Sun, Y.; Zhu, S.; Chen, Y. ZoomP³: Privacy-Preserving Publishing of Online Video Conference Recordings. *Proc. Priv. Enhancing Technol. (POPETS)* **2022**, *3*, 630–649. [CrossRef]
34. Yang, Y.; West, J.; Thiruvathukal, G.K.; Fawaz, K. Are You Really Muted?: A Privacy Analysis of Mute Buttons in Video Conferencing Apps. *arXiv* **2022**, arXiv:2204.06128.
35. Kagan, D.; Alpert, G.F.; Fire, M. Zooming Into Video Conferencing Privacy. *IEEE Trans. Comput. Soc. Syst.* **2023**. [CrossRef]
36. Exodus Privacy. Available online: <https://exodus-privacy.eu.org/en/> (accessed on 5 November 2022).

37. International Computer Science. Lumen Privacy Monitor. 2021. Available online: <https://www.icsi.berkeley.edu/icsi/projects/networking/haystack> (accessed on 5 November 2022).
38. Reyes, I.; Wijesekera, P.; Razaghpanah, A.; Reardon, J.; VallinaRodriguez, N.; Egelman, S.; Kreibich, C. Is our children's apps learning? automatically detecting coppa violations. In Proceedings of the IEEE Workshop on Technology and Consumer Protection (ConPro), San Jose, CA, USA, 22–24 May 2017.
39. Razaghpanah, A.; Nithyanand, R.; Vallina-Rodriguez, N.; Sundaresan, S.; Allman, M.; Kreibich, C.; Gill, P. Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem. In Proceedings of the Network and Distributed System Security Symposium, San Diego, CA, USA, 18–21 February 2018.
40. Zhou, X.; Demetriou, S.; He, D.; Naveed, M.; Pan, X.; Wang, X.; Gunter, C.A.; Nahrstedt, K. Identity, location, disease and more: Inferring your secrets from Android public resources. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, Berlin, Germany, 4–8 November 2013; pp. 1017–1028.
41. MITRE. CVE List. Available online: <https://cve.mitre.org/cve/> (accessed on 18 February 2023).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.