An Investigative Study on the Privacy Implications of Mobile E-scooter Rental Apps

Nisha Vinayaga-Sureshkanth
University of Texas at San Antonio
San Antonio, Texas, USA
vsnisha@ieee.org

Raveen Wijewickrama
University of Texas at San Antonio
San Antonio, Texas, USA
raveen.wijewickrama@utsa.edu

Anindya Maiti
University of Oklahoma
Norman, Oklahoma, USA
am@ou.edu

Murtuza Jadliwala
University of Texas at San Antonio
San Antonio, Texas, USA
murtuza.jadliwala@utsa.edu

ABSTRACT

E-scooter rental services have significantly expanded the micromobility paradigm of short-distance urban and suburban transportation since their inception in 2017. Service providers around the world have followed a common rental model wherein customers (i.e., riders or users) download and install a mobile application for locating (finding) and renting e-scooters. Unlike many other app categories, e-scooter rental apps require a set of privacy-sensitive user data as a functional requirement. Unfortunately, privacy-related questions such as *how much user data is being collected by these apps?*, *is user data being safely handled once acquired?*, and *with whom the collected user data is being shared?* are not readily known to customers. Answering such questions can be critical for users in determining which e-scooter rental services are sufficiently trustworthy per their personal privacy preferences. In this paper, we conduct a comprehensive analysis of e-scooter rental apps to answer these and other research questions related to user data collection, third-party involvement, usefulness of privacy policies, and evolution of user data management by different e-scooter apps/services over time. Our findings will create awareness among consumers vis-à-vis the data they share with service providers in return for the received e-scooter rental service, and it can also evoke more accountability and transparency from service providers towards their efforts and processes on protecting consumer privacy.

CCS CONCEPTS

• **Security and privacy → Web application security**; • **Human-centered computing → Mobile devices**; • **Computer systems organization → Sensors and actuators**.

KEYWORDS

E-scooter Mobile Apps, Application Analysis, Privacy Policies.

WiSec '22, May 16–19, 2022, San Antonio, TX, USA

ACM ISBN 978-1-4503-9216-7/22/05…$15.00
https://doi.org/10.1145/3507657.3528551

ACM Reference Format:
Nisha Vinayaga-Sureshkanth, Raveen Wijewickrama, Anindya Maiti, and Murtuza Jadliwala. 2022. An Investigative Study on the Privacy Implications of Mobile E-scooter Rental Apps. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '22), May 16–19, 2022, San Antonio, TX, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3507657.3528551

1 INTRODUCTION

Micromobility vehicles such as electric scooters (a.k.a e-scooters) have become a popular means for short commutes and last-mile transportation in urban areas. The relatively easy and cost-effective process to rent (or own) and operate one, without requiring recurring or expensive maintenance, is one of the main driving factors for their popularity over conventional private/public transportation modes such as cars and buses. Their popularity has soared among the general urban population, specifically among students and tourists, due to the inexpensive ride costs, ease of availability and unique ability to navigate crowded pedestrian streets and hot-spots. It is even anticipated that the rental e-scooter market will continue to grow in the post-pandemic era due to a renewed awareness on social-distancing and hygiene while commuting [72].

Despite their relatively low ownership cost, rentals continue to be the more popular and convenient means to gain access to these micromobility vehicles [31]. To cater to this burgeoning need for e-scooter rentals, several local, national and multi-national service providers have emerged in urban communities [22]. These service providers operate by deploying and maintaining a fleet of e-scooters within a community or urban space, and enabling convenient access to them for potential renters or customers using smartphone or mobile apps. Besides the physical vehicles and user-facing apps, these service providers also operate and maintain a back-end command/control hardware and software framework for accounting, business analytics, vehicle tracking, and other operational and logistical tasks.

The rise in popularity of this upcoming transportation paradigm has also brought forward significant technical and research challenges. Among others, open research problems in the areas of rider and pedestrian safety [56, 58, 89], and urban planning or civil engineering [47, 85] have received the most attention. Besides this, there have been several academic and hobbyist-style efforts towards

studying the security and reliability of the various software frameworks and interfaces within the entire e-scooter ecosystem. In the midst of all this progress, one issue that has gone relatively unnoticed and unaddressed by the research community is that of *privacy* of renters (or riders) who are the consumers in this e-scooter rental ecosystem.

A comprehensive analysis of the state of user (or consumer) privacy in the e-scooter rental ecosystem is extremely important and timely. Due to the extremely sensitive nature of data that is generated from e-scooter and other micromobility rides, for example, users' locations, schedules, preferences, etc., it is important to clearly understand what type of, and how much, user-related data is collected by these applications (and service providers), and how this data is shared with affiliated third-parties. In addition, it is equally important to study the privacy policies, and other mechanisms, adopted by these service providers to protect users' private data, and to analyze how effectively they are enforced within their apps. Users typically agree to service provider data-collection and privacy policies at application install time without careful scrutiny, which makes a careful quantitative and qualitative analysis of such policies, and their enforcement, paramount [76]. Given the large numbers and diversity of service providers, with varying degrees of reputations, and the fact that they may be able to collect, infer and/or share different types of sensitive information, potentially without their customers' complete knowledge and/or without abiding to local data/privacy regulations, a large-scale and longitudinal study of all applications and service providers is critical to shed light on the state of user-privacy within this upcoming transportation paradigm.

In this paper, we conduct the first such comprehensive analysis of Android e-scooter rental applications and service provider privacy policies in order to gain an insight into the data collection and handling processes practiced by e-scooter service providers, their relationship with third-party entities regarding sharing and exchange of sensitive user data, and how these processes evolved over time to reflect their privacy policies and local regulations. In contrast to the plethora of research efforts in the literature on mobile app and policy analysis (Table 4 in Appendix), which narrowly address a particular privacy aspect (e.g., sensitive data leakage, privacy policy analysis, etc.) for a large set of popular but unrelated mobile apps, our work is unique and novel in that it comprehensively analyzes all these aspects of privacy for an upcoming and important group of apps (related to e-scooter/micromobility rentals) that have significant privacy implications.

Our analysis begins by first creating a large representative dataset of Android e-scooter rental applications (APK files), comprising of a diverse set of service providers and regions where these apps operate in. With the help of state-of-the-art static and dynamic analysis tools and techniques from the literature, we carry out an in-depth examination of the various user data and resources that are accessible to these apps. In addition to characterizing the type of data being collected, this step also focuses on identifying the data shared by service providers and the recipients of this data. Using well-known natural language processing (NLP) and policy analysis tools, we characterize the privacy policies defined by these apps (and service providers), and employ the outcome of the previous task to verify if the user data collected by each app is clearly documented in its privacy policy. Lastly by analyzing prior (historical) versions of these apps, we study how the data collection and sharing behavior and privacy policies of these apps have (temporally) evolved, especially in relation to some of the significant data privacy laws/regulations enacted around the world. In this work, our goal is to create awareness among consumers vis-à-vis the data they (explicitly or implicitly) share with service providers in return for the received e-scooter rental service, and at the same time to evoke more accountability and transparency from service providers towards their efforts and processes on protecting consumer privacy.

2 ADVERSARY MODEL AND RESEARCH OBJECTIVES

E-scooter rental services follow a very straightforward service model, as outlined in Figure 1. Rental service providers effectively operate two high-level interfaces: (i) a *vehicle-facing* interface, and (ii) a *user-facing* interface. The vehicle-facing interface comprises of an on-board computer, hardware sensors such as GPS and a long-range wireless (e.g., 4G/5G) communication interface that is present on each vehicle through which the provider monitors and tracks the health, location and usage of its vehicle fleet. The user-facing interface comprises of a software such as a mobile or smartphone app and is the primary means through which a service provider communicates with its customer, tracks their rides and receives payments for the rental service provided. Rental users (riders) typically download the desired service provider's app on their smartphones, sign-up for the service by providing some personal information, and add a payment option in order to start using the service, i.e., to rent and ride an e-scooter.

Additionally, due to the nature of the e-scooter services, the user may have to explicitly permit the app to access a set of privacy-sensitive sensors (e.g., GPS) and other on-device data. Occasionally, due to business obligations or other operational requirements, service providers may also communicate with third-parties (e.g., advertisers, government regulators, etc.) by sharing user or fleet data. In this work, our focus is not on the vehicle-facing interface, but rather on the user-facing interface (i.e., the mobile app) and the privacy implications of interacting with that interface.

Thus, the adversary in our case is the untrusted service provider who operates this user-facing interface or mobile app. From an adversarial standpoint, we know that location tracking alone can be used to infer a variety of personal information [40], and the availability of additional on-device and user-entered data can further aid a potential adversary trying to infer users' personal information. As the problem of permission over-claim in mobile ecosystems have been largely curbed [70, 84], only a few categories of apps require as many permissions (to access on-board sensor data) and as much user-entered information as e-scooter rental apps. Moreover, while app categories such as travel and navigation utilize similar type of information, they are heavily dominated by a select few large corporations (such as Google Maps and Apple Maps) that are often accepted as 'trusted' by most users.

Micromobility apps, on the other hand, are much more heterogeneous in nature with a variety of service providers with varying

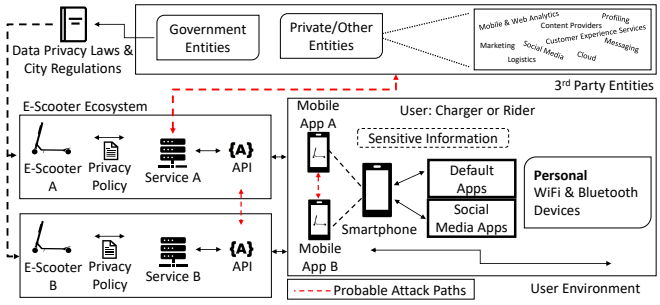

Figure 1: Components of a typical e-scooter rental service ecosystem.

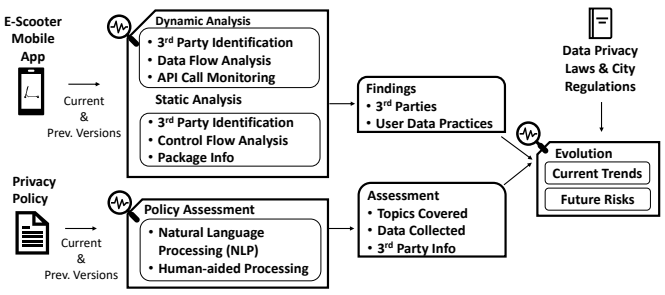

Figure 2: App and policy analysis process flow pipeline and outcomes.

degrees of reputation and operating in different (multiple) geographical regions. Consequently, there is significant uncertainty currently as to how users' data is collected and handled by the dozens of popular e-scooter apps in the wild, which are readily downloadable from the app stores. Accordingly, the first objective of our investigative research effort is to:

> RO1 *Investigate e-scooter rental services' potential to risk user privacy by analyzing service providers' data-related (access, collection, storage) practices in their mobile apps.*

In addition to collecting and using user data for enabling the e-scooter rental service, service providers have also been known to share this collected user data with government and municipal officials of the cities they operate in for planning and regulatory purposes [17]. Such rich and fine-grained user data also has strong potential of being shared with other unknown or non-obvious third-parties by providers, in order to meet commercial and/or business obligations. Therefore, our second research objective is to:

> RO2 *Investigate e-scooter rental services' potential to risk user privacy by analyzing service providers' data sharing practices with third-parties.*

An important accompaniment to any mobile app is a (service provider provided) privacy policy document, which clearly outlines (to the users) the provider's practices in terms of the type and frequency of the data collected and retained by the app. Such policy documents are not only a standard practice for mobile apps, but often also a legal/regulatory requirement in most jurisdictions in which the app operates. Despite their importance towards creating a transparent operating environment in protecting users' private data, accessibility (part of which is readability) of such policies has always been an issue as lengthy and overly technical privacy policies are often ineffective in unambiguously informing users about the privacy implications of using a particular service [38]. Moreover, service providers may also be incongruent with their privacy policies. Therefore, our third research objective is to:

> RO3 *Investigate e-scooter rental services' data collection and handling transparency and trustworthiness by analyzing the coverage, accessibility and terminology similarity in service provider supplied privacy policy documents.*

When a service provider becomes popular and has an increased customer base, it is often subject to more scrutiny about its data collection and handling practices than before. Intuitively, this could mean that as service providers grow in popularity and scale, they may change their data collection/handling practices and privacy policies to mitigate any legal/regulatory concerns. Similarly, changes in local and state privacy regulations and laws could also force service providers to change (and adapt) their data practices and policies. Thus, our fourth research objective is to:

> RO4 *Investigate e-scooter rental services' potential risk factor (pertaining to user privacy) over a period of time, by identifying its historical perspectives and trends through a chronological analysis of different versions of individual apps.*

3 RESEARCH METHODOLOGY

Next, we present a detailed description of our analysis methodology and work flow (Figure 2) that was employed to accomplish the research objectives outlined earlier.

3.1 Analysis Dataset

The first step in our analysis is to create a carefully curated dataset of mobile e-scooter rental apps and their corresponding privacy policies. Accordingly, we created a dataset comprising of Android e-scooter rental apps (all available versions from their inception date until March 2021) and their corresponding privacy policies (all available versions until July 2021). In order to create this dataset used in Sections 4 to 6, we first search for English-supported apps on Google Play [4] using different combinations of e-scooter related keywords across countries. Specifically, by using different variations of the term "e-scooter" in the search, together with action verbs such as "share", "rent" and "ride", we obtain an initial set of apps. However, as this set also contained apps irrelevant to this study

(for example, moped rental apps), we filter it manually to contain only e-scooter rental apps. After finalizing the set of apps (we will refer to this as the *appset*), we also save additional metadata such as package name and privacy policy link extracted from the associated Google Play webpage. In this paper, we only consider Android apps because of the open-source nature of the Android OS, which makes app debugging and all related analyses feasible. Due to lack of appropriate analysis tools and debugging restrictions, our appset does not include iOS (or Apple) apps. Once finalized, we download all available versions of application packages (APKs) corresponding to apps in our appset from the AndroZoo web service [13] used in Section 7. Our final dataset contains a total of 1079 APKs corresponding to 102 unique e-scooter rental services. In addition to the APKs, we also download different versions of privacy policies for each app in our appset by using the URL extracted from the app store (Google Play) page. Past (cached) versions of the privacy policy were also downloaded from Internet archives [16], whenever available. Unfortunately, the cached content was unavailable for a majority of the apps (52%), which forced us to limit our analysis to a smaller subset of apps in the appset, as discussed later in Sections 6 and 7.

To gain an insight on how e-scooter service provider popularity/reputation impacts its operation and conduct (vis-à-vis user privacy), we compile three subsets of apps based on their number of downloads on the Google Play Store. We refer to the subset of apps in our appset with over 100k downloads on the Google Play store as the *Most Popular Apps*, apps with downloads between 10-100k as *Moderately Popular Apps*, and apps with less than 10k downloads as *Least Popular Apps*. We also approximate the risk factor (or inversely, the trustworthiness) of apps in the appset by averaging the individual *Common Vulnerability Scoring System (CVSS)* values pertaining to a subset of routinely exploited vulnerabilities, both extracted from our chosen toolset (Refer to Tables 1 and 2 and Figure 8 in the Appendix). We then categorize apps with an average CVSS score above 7.0 as *High Risk Services*, while those with average CVSS scores within 4.0 - 6.9 as *Medium Risk Services*.

3.2 APK Analysis

Our investigation comprises of a three-phased process (Figure 2) involving an analysis of the app binaries (or APKs) first, followed by an analysis of app privacy policies and concluding with a behavioral analysis of the evolution of these apps and privacy policies over time. In the first phase of this analysis pipeline (Figure 2), designed to accomplish research objectives RO1 and RO2, we investigate the (user) perceived and actual runtime behavior of app packages, in order to further understand and characterize their user data collection practices. Leveraging on traditional *static* and *dynamic* analysis tools and techniques (Table 1), we identify and categorize data items that the e-scooter rental apps access or could potentially access during their execution.

Static Analysis. For static code analysis, we attempt to decode the APK packages and decipher its behavior using the popular MobSF framework [7]. The MobSF framework was chosen for this task because it supports static analysis on apps based on Android API Level 28 and below, with additional capabilities of detecting a wide spectrum of API-related vulnerabilities. From the bytecode files disassembled using MobSF, we process associated data pools such as *classes*, *fields*, *strings* and *prototypes*. *AndroGuard*, a part of the MobSF framework, is a mobile application analysis tool that has been widely used by other research efforts for malware analysis in the literature [2]. AndroGuard already has pre-defined mappings between the items in the identified data pools and the corresponding API classes/methods, which we utilize for our analysis. To augment and optimize the control flow analysis and to identify user data points not included in the MobSF framework, we use its standalone version along with other tools in (refer to Table 1 in the Appendix) in tandem with automated analysis. By extracting app-requested permissions using the MobSF framework, we determine the nature and type of resources requested by each e-scooter rental app in our appset. With the results from this analysis, we visually identify code segments, and ultimately API call-related data points to further scrutinize during dynamic analysis (discussed next).

Dynamic Analysis. To capture an app's functional behavior, we monitor the network traffic (HTTP/S) during runtime while manually interacting with the app. To identify and verify the app's behavior in the older API levels (25-), we rely on the dynamic analysis component of MobSF framework, Drozer [45] and AppMon [64]) for emulated environments (supported by these tools) in addition to the real device environments that are rooted. During the analysis, the API calls, permission requests, file system changes, resource utilization and network data flows were automatically monitored by these tools (or manually configured to be monitored), all while manually interacting with the GUI elements for each app and environments mentioned in Section 3.2. For completeness purposes, we monitor the high-level data shared (to remote servers) by a subset of apps directly on the non-rooted smartphones using the public version of Lumen Privacy Monitor [68] that supports only device-related identifiers. Further, we use the data obtained from the aforementioned tools to manually scrutinize the data flows and identify the context in which the accessed data is used, and to whom and how frequently it is being sharing with, including identifying and characterizing the entities (first or third-parties) with whom the apps share data.

Third-party Identification. We identify individual third-parties from the decompiled APKs via three different approaches. First, we use the MobSF framework that relies on the Exodus tracker database [37] to identify the third-parties found in the apps. We also manually supplement the list of third-parties detected by the MobSF framework by identifying the presence of additional third-party libraries (SDKs) based on information available in Android-related package repositories (Mvn repository and Android Studio package manager), and using LibRadar++ [87]. We also identify third-parties from network packets captured via network traffic monitoring tools (refer to Table 1 in the Appendix) and then filter packets based on known tracker signatures obtained from the Exodus privacy tracker list (used by MobSF) and the `whotrack.me` database [9]. Later, the source-sink locations (domain names or IP addresses) from these filtered packets are identified and associated to the corresponding third-parties.

Analysis Platforms. The dynamic analysis tasks were done on Android OS 9.0, 6.0 and 5.0 platforms by appropriately alternating between (i) an emulated Android environment, and (ii) a real Android instance running on an actual smartphone (Moto X4 and

G7 Play), whereas the remaining analysis tasks were completed on 64-bit desktop computers (running Windows 10 and Ubuntu). During static analysis, we noticed apps that are possibly capable of detecting the execution environment, and modify their behavior accordingly. For this reason, we additionally chose to study the data being accessed, collected and shared by the apps during runtime on a rooted and a non-rooted phone using the publicly available tools mentioned in Table 1 (the data extracted from this analysis were subjected to the limitations of these tools in the corresponding runtime environments). Though the chosen tools collected and processed the data automatically, the UI interactions were performed manually, mimicking realistic scenarios for each app.

3.3 Privacy Policy Analysis

To accomplish research objective RO3, we analyze the privacy policies using semi-automated text processing techniques to extract actionable information from them to evaluate the quality of their content. We use Polisis [49] to extract the required information for most of the privacy policies in our dataset, and utilized the same features/attributes used by Polisis to manually identify policies that Polisis failed to process. For *coverage* analysis, we examine the privacy policies for key topics pertaining to both first-party and third-party data collection, its purpose, and usage information. For *accessibility*, we use standard readability metrics such as Flesch Readability Ease [43], Gunning Fog Index [21], and Coleman-Liau Index [79] (refer to Table 3 in the Appendix for a complete list). For *similarity* analysis, we identify identical components across the policy documents of different apps using the Term Frequency-Inverse Document Frequency (TF-IDF) NLP model based on cosine similarity scores. We further analyze the policy documents to determine if any third-party services were specified (within the document) as being involved in any kind of data handling along with the types of data shared or handled by them. We also characterize privacy-related information from the privacy policy documents manually and analyze if the real behavior of the apps are congruent with their policy statements. This manual task, although non-trivial and time consuming, is required because: (i) not all policy documents contained the specifics of data (as expected by the tools) that are collected by their corresponding apps (i.e., they contained generic terminology), and are required to use the relevant publicly available tools, and (ii) not all publicly-available policy and conformance analysis tools consider app usage, device and network data within their analysis framework, thus limiting their scope.

3.4 Service Evolution

To accomplish objective RO4, we examine how e-scooter rental apps and their privacy policies have evolved over time. Although it is intuitive to consider only recent apps to analyze current e-scooter rental provider data access trends within a region, we believe that it is equally important to study and consider how different providers and their app releases behaved (in terms of user data collection). Especially during their infancy stages to predict future e-scooter rental data access trends. To this end, we assess content trends in different versions of privacy policies for the same app, and how these different policies correlate with external factors, such as new data privacy laws, over time. In addition to repeating the prior analysis of apps and privacy policy documents (RO1-RO3) for multiple versions of the same app (introduced over a period of time), we also analyze auxiliary information such as when and how frequently apps and privacy policies were updated/revised.

4 RO1: FINDINGS ON USER DATA

In this section, we present our findings related to user data that is accessible, and potentially collected, by e-scooter rental service apps, and how it can directly or indirectly affect users' privacy.

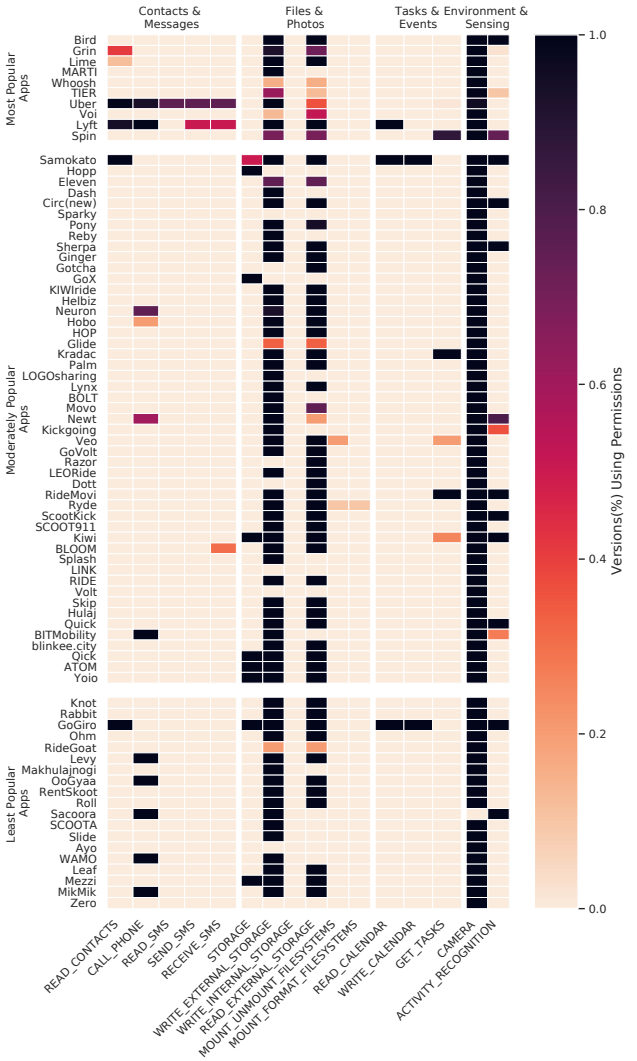

Figure 3: A subset of apps and their requested permissions. Each cell value corresponds to the percentage (fraction) of an e-scooter service app versions using the permission. On average, apps overall requested at least three dangerous permissions and accessed user data methods associated with eight of the requested permissions during runtime.

4.1 Location and Relative Positioning Privacy.

Location data/permissions is essential to the operation of an e-scooter rental app, and thus all apps in our analysis did collect and handle users' location information (validated using both static and dynamic analyses). However, certain aspects of location and other relative positioning data collection, specifically the method of data collection and whether data was collected when users are not renting an e-scooter, can affect user privacy at varying degrees, and can be a cause of concern for users. From our analysis, we found that all apps in our appset access, and potentially accumulate over time, either accurate location or relative positioning information using multiple channels, that include a combination of GPS, cellular network, Wi-Fi and Bluetooth data. We also observed that 18% of apps collected location data even when the app was not in use. Moreover, the frequency of location data collection varied significantly among these apps from on-demand access as needed to frequent access as short as every 15-20 minutes. This can be considered as inappropriate app behavior as users (using Android 9 OS or below) may not want to be tracked outside of their e-scooter usage location(s) and it is likely that, many users may be unaware of this background location tracking behavior. Travel and commutes made using rented e-scooters are naturally known to the service provider. However, a service provider can potentially extend its inferences well beyond that, using auxiliary and contextual information. For instance, e-scooters are often used as a last-mile transportation solution for commutes and travels [62]. As a result, user's workplace and/or residence can potentially be inferred by the service provider, especially when location data related to recurring travels and commutes have been collected by the service provider over a period of time [19].

4.2 Identity Privacy.

Among the identity related information collected by apps in the appset, all apps collected at least one type of financial data, and two-thirds of the apps collected at least one combination of uniquely identifiable set of demographic data. As almost all of these information must be manually typed and submitted by the user (implying explicit consent of the user), we disregard how and when these data are collected. Interestingly, popular apps such as Uber and Lyft also requested `READ_PROFILE` permission in some of its earlier versions which gave them access to any user information that is stored in users' contact cards. Nevertheless, to limit the discussion on the privacy impact after potentially identifiable information is collected by service providers, we conduct analyses of identifiable data privacy loss with respect to the characteristics of the service providers that cause it. Specifically, we further analyze the trade-off between data sensitivity vs. service provider reputation (or popularity) in e-scooter rental apps.

Among the different types of data (refer to Table 5 in the Appendix) collected by e-scooter apps, we observe that roughly 30% of the (most and moderately) popular apps collected demographic and social data related to the user in at least one version. The combination of such data has been proved to be sensitive as it poses a high risk of (re-)identification [75]. On the other hand, only 17% of least popular apps collected demographic and social data related to the user in at least one version. Based on these observations, we postulate that service providers may be leveraging on the fact that users tend to be be more willing to trust a popular service provider with more sensitive data about themselves. Conversely, service providers tend to collect fewer sensitive user data types when they are not very popular and maybe perceived as less trustworthy.

4.3 Phone Data Privacy.

Mobile platforms such as smartphones contain a trove of other personal data that are not essential for the functionality of an e-scooter rental service app. Yet, many apps ask for, and utilize, permissions to such data residing on users' smartphones. In Figure 3, we outline some of the most privacy sensitive permissions requested by e-scooter rental apps. Data showcased in this figure accounts for all version numbers of each app which may have added or dropped particular permission requests. While in most cases, data accessed with the help of these permissions are used for e-scooter operation or authentication purposes, there is potential for this data being misused to infer sensitive information. Now, let us discuss a few of these significant permissions in a bit more detail by grouping them into categories based on the type of data they impact.

Contacts and Messaging. Users' phone contacts (such as phone numbers and emails of friends, family, colleagues, and acquaintances) and messages are not only private to them, but also for their contacts. Moreover, those contacts may not be e-scooter riders themselves and may not be willing to share any personal information with e-scooter service providers. This is not a new problem, as we have seen several instances in the past where these permissions have been misused [39]. The biggest distinction and privacy concern we want to highlight here is that not all e-scooter rentals services functionally require access to these permissions in order to operate their service. Yet, we found that 20% of the e-scooter rental apps we analyzed are asking for these permissions for sharing or receiving promotional content. (`READ_CONTACTS`, `WRITE_CONTACTS`, `CALL_PHONE`, `READ_SMS`, `SEND_SMS`, and `RECEIVE_SMS`).

Files and Photos. Files and photos on a smartphone, either generated by the user or another app, often contain sensitive information related to the user. Except for a few specific use-cases (such as information related to the underlying APIs), e-scooter rentals services should not functionally require access to files and photos. Yet, a significant number of e-scooter rental apps required permissions to read from and write to the mobile platform's external memory storage, which could potentially store sensitive files and images. For instance, 11% required access to `STORAGE`, 86% to `WRITE_EXTERNAL_STORAGE`, and 70% to `READ_EXTERNAL_STORAGE`. During runtime, we noticed files generated by nearly three-fourths of the apps contained information related to the user, device or service in cleartext format, or were exposed to other apps. On closer inspection, a significant fraction of these storage requests pertained to third party SDKs which saved its configuration files and accessed other files in the residing directory. We did not find any significant difference between more popular and less popular apps for these permissions.

Environment and Sensing. Several sensors present on a smartphone can be used to infer users' context, environment and activities. Almost all of the unique apps we investigated required and utilized the `android.permisson.CAMERA` permission in at least one

version, which can be directly used to capture visuals of the user and/or their surroundings. This can be partially attributed to the fact that apps (in the past) accessed the camera to scan QR codes to initiate e-scooter rides and to check if they are parked in a safe place after the ride [10, 55]. Nearly 14% of the analyzed apps asked for and used the `ACTIVITY_RECOGNITION` permission which leverages Google's API [5] to infer users' current activity in a broader sense. We did not find any significant difference between more popular and less popular apps for these permissions. Nonetheless, all apps also have access to sensors that do not require any explicit user permissions such as accelerometer, gyroscope, and ambient light sensor, which can be used to infer sensitive information such as keystrokes [57], speech [61], and geo-location [48].

Tasks and Events. Lastly, we also analyzed how many apps were using the `READ_CALENDAR`, `WRITE_CALENDAR`, `GET_TASKS`, and `REORDER_TASKS` permissions. A user's calendar and tasks may contain personal information, which should not be required by an e-scooter rental service provider. We determined that 12% of the apps that were analyzed require access to at least one of these permissions. Only `WRITE_CALENDAR` has a legitimate use-case wherein apps can add pre-booked rides to a user's calendar. Surprisingly, we discovered that such a feature/service is not offered by 73% of the apps despite asking for the `WRITE_CALENDAR` permission. After carefully studying all the functionalities of these apps, we still could not determine a legitimate use for this permission. We did not find any significant difference between more popular and less popular apps for these permissions. These findings once again demonstrate the problem of permission over-provisioning by e-scooter service providers and their mobile apps, and personal/sensitive data that could be potentially collected because of it.

5 RO2 FINDINGS: THIRD-PARTIES

Service providers often share the user data they collect with external entities, also referred by us as *third-parties*. The purpose for sharing user data may include integration with external services (such as social networking and media services) and monetization (such as through targeted marketing/advertisement practices). In this section, we present results of our analysis of the data sharing behavior of e-scooter rental apps with third-parties, together with a characterization of these third-parties and the data being shared with them.

Prevalence of Third-Parties. From an end-user perspective, a third-party in an e-scooter rental ecosystem is any entity that is not affiliated with (or owned by) the e-scooter service provider and that utilizes the user data collected by the provider's app. We use static and dynamic analyses to detect third-party libraries and Internet domains (presumably, for data uploading) within each e-scooter rental app's code and execution flow, as detailed in Section 3. Based on this analysis, we observe that more than 90% of the apps are employing one or more third-parties for a variety of purposes, detailed later in this section.

We observe that many of the third-parties detected using our static and dynamic analyses are associated with a variety of Internet-based services, beyond the e-scooter rental ecosystem. From the network data analysis, we observe that the most frequently utilized third-party domains from within the e-scooter rental apps belong

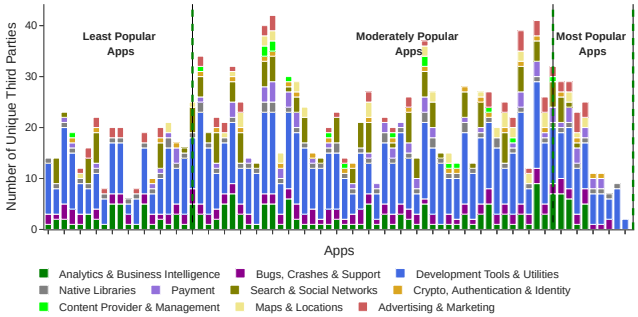

Figure 4: Statistics of different third-party SDKs associated with each of the investigated e-scooter rental service apps.

to *Google CrashLytics* and *Firebase Analytics*, both of which are data-analytics service providers and often integrated across different categories of Android apps during the application development process. Nonetheless, Google should be considered as a third-party in the e-scooter rental ecosystem as it is not a micromobility service provider. Additionally, we notice other popular third-parties such as Branch, and Facebook Analytics, are highly utilized within the e-scooter rental apps as well.

Similarly, the most prevalent statically identified third-party SDKs were related to Adjust, Braze, OneSignal, Branch, Google Ads, and Facebook libraries (Login, Places) indicating a significant presence in the e-scooter service ecosystem. Section 5 shows the number of third-party libraries used by e-scooter rental apps. Overall, the mean and median number of third-parties used by e-scooter rental apps are 8.2 ($\sigma = 5.8$) and 7, respectively. This includes apps such as Spin and Lyft that used as many as 12 or more third-parties to three apps that did not use any third-parties at all. In summary, third-parties are very prevalent within the analyzed e-scooter rental apps, and this motivates us to conduct further analysis on these third-parties.

Are End-users Appropriately Informed? A critical aspect of ethically, and legally, sharing users' data with third-parties is to obtain informed consent from them beforehand (typically, at service initiation). Next, we analyze if e-scooter rental apps are informing their customers about any third-parties with whom their data may be potentially shared with. We accomplish this by means of an in-depth analysis of their privacy policies. As shown in Figure 10 (in the Appendix), a majority of the most and moderately popular (95%) and least popular (67%) apps do inform users about the involvement of third-parties, at least at a high-level. Among them, only 33% of the most popular apps and 16% of moderately popular apps provide additional details on the third-parties, such as the type of service offered and type of data processed by them. The least popular apps only provided generic information on the type of third-parties (e.g., cloud providers) to which data may be shared without specifying their names. Only one-thirds of the least popular apps (in contrast to 12% of the most popular apps and 18% of the moderately popular apps) summarize or provide direct access to the privacy policies of the third-parties involved. Approximately 77% of the most popular apps (in contrast to 18% each of moderately and least popular apps) provide additional details on the data being

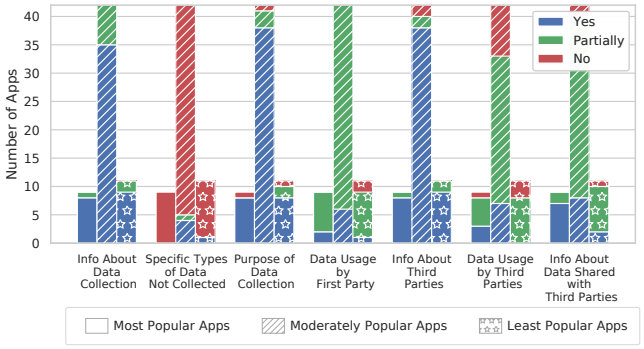

Figure 5: Number of privacy policies that provide any (generic or specific) information related to their e-scooter rental services' user data handling policies.

shared with third-parties, such as device, network, location, and demographics. In summary, most e-scooter rental apps informed users in some form, of their interaction with third-parties, but we conjecture that a lack of full transparency in terms of their data-sharing relationship with third-parties may be either due to a sinister motive (concerning their own usage of users' private data) or due to a lack of understanding of how third-parties may use their customers' data.

6 RO3 FINDINGS: PRIVACY POLICIES

Privacy policies are legal documents that state user data collection, handling, and processing practices of the service providers. Typically, end-users are expected to read and agree to the terms of a service provider's privacy policy prior to obtaining services from that provider. Pertaining to e-scooter services, the rental apps link to a privacy policy which either appears internally within the application or is accessible externally through a redirection (via browser) to a website. Nearly 39% of apps that we investigated in our study did not have their privacy policy in English, which we translated using Google Translate [6] prior to using them with English-based analysis tools. We also found that six apps which hosted their privacy policy externally redirected to an expired or non-existent page, which are therefore not part of the following analyses.

Coverage. One of the most important characteristics of a privacy policy document is how comprehensively it covers the different user data collection, handling, and processing practices by the service providers. As shown in Figure 5, we examine the privacy policy documents for seven key topics of coverage that we believe are essential for end-users to make an informed decision on whether to use a service or not. About 77% of the analyzed privacy policies mention collecting data about the users, but only 46% of them provide details on why the data is collected. For instance, from our analysis, 26% of the analyzed apps utilize user data to track them on other websites and 62% utilize the information for other purposes, mainly for different types of analytics. We already discussed how well users are informed on third-party data sharing in Section 5, which is also a critical component of a privacy policy document. In summary, 72% of the apps covered all the seven topics at least briefly, indicating that these apps are more likely furnishing enough information for concerned end-users to make a decision about their privacy.

Similarity. Privacy policies can potentially be copied and reused between rental e-scooter service providers. This practice is often observed between service providers with a common parent company (a.k.a. platform providers in the e-scooter rental ecosystem) or when service providers employ the same developer for their apps. We use privacy policy similarity analysis to identify such instances, which may not be evident otherwise. Nearly 65% of privacy policy documents had at least 75% overlap in content with at least another service provider's policy document. As a case in point, we noted 99.8% overlap in privacy policy documents of Circ and Bird, and further investigation revealed that both of them are owned by the same parent company (Bird). We also noticed the terms *personal data* and *information about you* are most widely used across different service providers' policies (Figure 14 in Appendix). Also, 72% of the privacy policies mention collecting a similar set of personal data from the users, and the top most commonly collected data are identity, location, and device related information such as device model, OS version and name.

Conformance. A violation occurs when an app does not conform with its privacy policies. Overall, we observe that e-scooter rental service apps defined policies that were either very comprehensive or very generic (missing fine-grained details on the information collected), which made it difficult to automate the detection of violations. For example, nearly three-fourths of the policies mention that they collect "personal information" for service usage, which could potentially point to identity, device, or network data depending on the user's interpretation and description context. In fact, less than 7% of policy documents use very clear notions like "does not collect" in their verbiage. Therefore, we manually verify the data practices *based on our interpretation of usage and personal data that included information about physical environment and usage preferences*. We found that at least one version of 12 e-scooter rental apps is capable of collecting and/or sharing information not specifically disclosed in their privacy policy document. However, it is subjective whether they can be considered violations due to their generic policy verbiage, thus highlighting the difficulty in determining if an app violates their own privacy policies or not. These observations on the usage of generic and/or ambiguous phrases emphasize the prevalence of escape clauses that may allow (the e-scooter services) autonomy over the (frequency, type and density of) data collected and shared with third-parties. Nonetheless, we find that the privacy policies of currently operational service apps conform to their local regulations by disclosing the bare minimum information regarding the user's data rights.

7 RO4 FINDINGS: EVOLUTION TRENDS

A service provider's utilization of the user data collected through its app can evolve or mature over time, and such changes in app behavior can impact user privacy. Some factors that play a critical role in the evolution of e-scooter rental services' app behavior are: (i) enactment of new privacy laws, (ii) risk-aversion (to legal issues) due to service provider growth and rise in popularity, and (iii) integration of additional features requiring more user data and access

to third-parties (and associated libraries). Next, we investigate how e-scooter rental app behavior has (temporally) evolved, especially in relation to some of the major privacy laws enacted around the world. We also analyze how app behavior has evolved in relation to app popularity (i.e., evolutionary differences between popular and least popular apps).

Background. For the sake of simplicity, we limit the scope of our evolutionary analyses to e-scooter rental apps in the *.com* Play Store (most of which are also archived in the AndroZoo database [13]). Figure 7 (in Appendix) shows that the apps we analyze are geographically well-distributed, operating in diverse privacy regulations/jurisdictions. This helps our analyses by representing how various service providers have evolved in different times periods. In Figure 7 (in Appendix), we also depict some of the most significant data privacy laws and regulations enacted in different countries since 2016 (a year prior to when rental e-scooter services first emerged). In addition to this, a timeline of app revision counts is also plotted in Figure 12 (in the Appendix). Two of the most significant data privacy laws out of these are the GDPR (of Europe) and CCPA (of California), which impact 37 and 10 service providers in our appset, respectively. Among the app revisions, we observed that approximately 94% and 46% of the new app version releases occurred after the release of GDPR and CCPA, respectively. This shows that data privacy regulations of the operating jurisdictions played a critical role in the functional and policy evolution of the e-scooter rental apps.

Data Collection Permissions. Across the evolution timeline, we observed the number of permissions requested or accessed by a majority of the most popular apps, excluding Uber and Lyft, increased by at least two (Figure 6), but remained the same for least popular apps. We noticed sensor and network data permissions introduced in almost all newer app versions and categories, indicating that initial e-scooter rental services may have been less connected (Internet or network dependent) but reliant on QR code and Bluetooth-based rentals, and later upgraded to fully Internet-connected e-scooters in order to simplify user interactions and to thwart hardware theft/abuse. After CCPA was enforced (blue vertical line in Figure 6), we observe that the change in data permissions requested or accessed by a majority of the popular apps in their respective operating regions was not significant (remained same or increased by at most 1). This implies that the services that operated in these countries and jurisdictions were prepared, with respect to the user data that was being collected and related data permissions, for the introduction (and enforcement) of relevant privacy laws.

App Vulnerabilities. Vulnerabilities in source code or protocols used by apps can endanger user data towards theft and/or misuse. As seen in Table 2 in the Appendix, more than three-fourths of the e-scooter rental service apps had one or more flaws that could be exploited by potential adversarial entities to obtain sensitive information. In our chronological analysis of moderately and least popular apps, we observed information exposure risks grew over time, which correlate with the increasing presence of third-party libraries and how they handled data in future versions. We also noted a few high risk vulnerabilities that were introduced but were often quickly resolved in at least 10% of the most popular apps, which could be attributed to either previously unknown vulnerabilities or vulnerabilities that were initially missed by quality assurance in

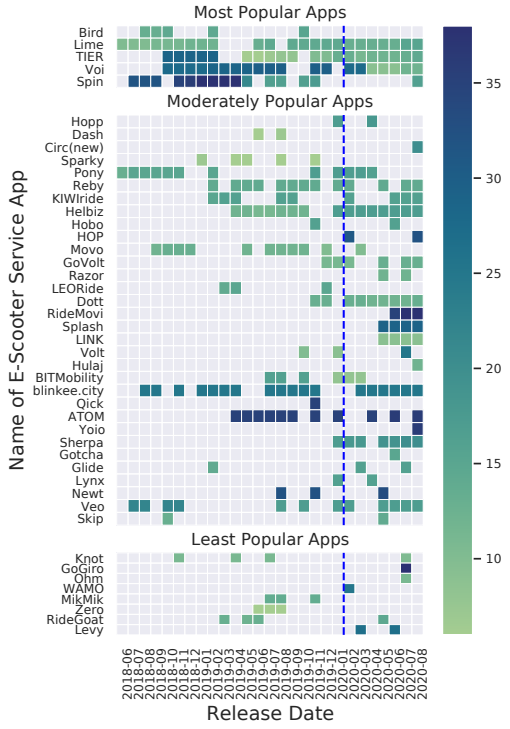

Figure 6: Number of permissions used by different e-scooter service apps over time. CCPA enforcements is represented by the vertical blue line. Services with more than 30 missing app versions were excluded.

the app's development lifecycle. Code injection vulnerabilities have prevailed across a significant portion of the apps throughout the years, both prior to and post GDPR and CCPA enaction. Overall, majority of the associated flaws were not fixed in subsequent app releases, indicating that rental services may not be prioritizing on app security.

Privacy Policies. We observed two notable time periods when privacy policy revisions were conducted by a significant number of e-scooter apps (January-2019 to March-2019 and January-2020 to March-2020, as shown in Figure 11 in the Appendix). We can correlate one of them to a 8-month period just before GDPR went into effect in the European Union on May-2018, and the second one to around the same time period CCPA went into effect in California on January-2020. Upon closer inspection we find that the newer versions of apps include additional topics such as user related rights (found in Figure 13 in the Appendix) in their privacy policy, in-line with the requirements of the GPDR and CCPA data privacy regulations.

Informing Users About App Evolution. Whenever service providers update their user data policy, it is important to inform existing users about these changes. We discovered that less than 32% of the analyzed privacy policies stated that the service provider will notify existing users of changes, while it remains unknown for the other 68% of the service providers. Moreover, seven service providers claim to store user data for 10 or more years, unless

requested for deletion. Also, nearly 76% of services allow the user to access and delete their data, but only 2% of them offer direct web forms for users to control their data. If an app policy changes in a way that users no longer wish to use the app or store their data with the app, such a data deletion service will be useful to users for deleting their data.

8 RELATED WORK

While in this paper we primarily focus on a privacy-centric analysis of e-scooter (micromobility) service providers and apps, here we provide a brief overview of other relevant research efforts in the literature. Due to the large number of related research efforts in these directions, and the space limitation here, we only describe some key research works below. An exhaustive list of other related research efforts, which has been appropriately categorized, is outlined in Table 4 in the Appendix.

Android Application Analysis. Akin to traditional program analysis, two types of techniques are primarily employed for Android app analysis: (i) static analysis, and (ii) dynamic analysis. *Static analysis* examines an application's source code and the underlying program logic [23, 46], while *dynamic analysis* examines an application's runtime behavior from the information and control flows during its execution [35, 63]. While early works in the literature have employed either one of these techniques to study the security and privacy risks associated with Android apps, it has been shown that employing both of these techniques in a complementary fashion improves the overall effectiveness and accuracy of the targeted analysis [91].

Privacy Policy Analysis. Related works on privacy policy analysis have focused on analyzing large classes of mobile apps in the wild to verify the availability/existence and adoption of valid privacy policies [36, 82]. Additionally, other works in this direction have focused on evaluating privacy policies for linguistic and human-comprehension attributes, namely, readability, tone and quality of the policy content [30, 74, 80]. A closely related work in this direction is *Polisis* [49], a state-of-the-art NLP based privacy policy analysis framework. Polisis provides a salient summary of the analyzed application's data handling practices and important user-centric linguistic attributes of its privacy policy. There are also several works that conducted privacy analysis within specific application categories, such as health apps [51, 54], dating apps [53, 60, 65], parental control apps [42] and financial apps [29, 33]. While works also attempt to identify various forms of sensitive data leaks and privacy policy discrepancies within these application categories, prior works focused on micromobility and transportation applications have been limited. For instance, in a closely related effort Achara et al. [11] analyzed an application in the public transportation domain, and observed several discrepancies between the provided privacy policy and the actual application behavior related to data sharing with third-parties. More recently, Petersen [66] studied the invasive data collection practices of e-scooter companies such as Bird, Lime and Spin. However, their work was limited to a high-level analysis based only on policy and terms-of-service documents, and not a comprehensive application-level analysis as conducted in this paper.

9 LIMITATIONS

One of the most challenging task of our study was the collection of all older versions of the apps in the appset. While we utilized AndroZoo for its comprehensive app database, we could not find any analogous databases of apps published outside of the US English edition of Google Play Store, nor for iOS apps. Additionally, our policy dataset was restricted to the availability of older policy versions in public archives. This lack of policy document content, combined with generic/ambiguous policy verbiage, limited our data practice analysis with respect to their privacy policies for older app versions. Our static and dynamic analysis was limited by the selected tools' functionality and the selected apps' built-in mechanisms to thwart debugging and reverse engineering. Additionally, dynamic analysis was not feasible or relevant for several apps in our appset, especially for the older versions of apps that required users to update to the latest versions, and domains that changed over time. Furthermore, there may be other associated user data types and third-parties whose identification is beyond the scope of existing tools and would require time-consuming, strenuous manual efforts. Due to generic policy text, our data categories, and the analysis scope, we could not adopt existing behavior conformance tools directly without any modifications. Additionally, the possibility of apps' (modified) behavior when installed and run from a different country than it was intended for, and the relatively small number of the e-scooter providers (less than 1% of unique apps considered in our appset) operating at our location (during 2019-2021) hindered collecting data while operating the e-scooter and obtaining generalized insights for the corresponding apps operating in other regions.

10 CONCLUSION

We conducted a comprehensive analysis of Android e-scooter rental applications and service provider privacy policies in order to gain an insight into the data collection and handling processes practiced by providers, their relationship with third-party entities regarding sharing and exchange of sensitive user data, and how these processes evolved over time to reflect their privacy policies and local regulations. To this end, we utilized state-of-the-art static and dynamic analysis tools and techniques to carry out an in-depth examination of the various user data and resources that are accessible to these applications. We also identified the third-parties (Internet domains and SDKs) associated with the rental apps, and characterized the data shared by service providers along with the privacy policies defined by these apps (and service providers). Lastly, we studied how the data collection and sharing behavior and the privacy policies of these apps have evolved over time. The results presented in this paper are intended to increase awareness among consumers vis-à-vis the data they (explicitly or implicitly) share with service providers in return for the received e-scooter rental service, and at the same time to evoke more accountability and transparency from service providers towards their efforts and processes on protecting consumer privacy.

ACKNOWLEDGMENTS

Research reported in this publication was supported by the US NSF under award numbers 1943351 and 2016717.

REFERENCES

[1] AppCensus. https://search.appcensus.io, 2020. [Online; accessed 20-August-2020].

[2] Androguard. https://github.com/androguard/androguard, 2021. [Online; accessed 15-June-2021].

[3] Ghidra Software Reverse Engineering Framework. https://github.com/NationalSecurityAgency/ghidra, 2021. [Online; accessed 10-July-2021].

[4] Google Play. https://play.google.com/store/apps, 2021. [Online; accessed 22-June-2021].

[5] Google Play Services Activity Recognition. https://developers.google.com/android/reference/com/google/android/gms/location/ActivityRecognition, 2021. [Online; accessed 18-May-2021].

[6] Google Translate. https://translate.google.com, 2021. [Online; accessed 24-June-2021].

[7] Mobile Security Framework (MobSF). https://github.com/MobSF/Mobile-Security-Framework-MobSF, 2021. [Online; accessed 15-June-2021].

[8] VirtualAPK. https://github.com/didi/VirtualAPK, 2021. [Online; accessed 26-June-2021].

[9] WhoTracks.me - Bringing Transparency to Online Tracking. https://developer.android.com/studio, 2021. [Online; accessed 20-June-2021].

[10] Lime 2nd Street. New Parked Or Not Feature Lets Riders Rate Proper Scooter Parking. https://www.li.me/second-street/parked-or-not-feature-riders-rate-scooter-parking, 2018. [Online; accessed 11-June-2021].

[11] Jagdish Prasad Achara, James-Douglass Lefruit, Vincent Roca, and Claude Castelluccia. Detecting privacy leaks in the ratp app: How we proceeded and what we found. *Journal of Computer Virology and Hacking Techniques*, 10(4):229–238, 2014.

[12] Suzan Ali, Mounir Elgharabawy, Quentin Duchaussoy, Mohammad Mannan, and Amr Youssef. Betrayed by the guardian: Security and privacy risks of parental control solutions. In *Annual Computer Security Applications Conference*, pages 69–83, 2020.

[13] Kevin Allix, Tegawendé F Bissyandé, Jacques Klein, and Yves Le Traon. Androzoo: Collecting millions of android apps for the research community. In *2016 IEEE/ACM 13th Working Conference on Mining Software Repositories (MSR)*, pages 468–471. IEEE, 2016.

[14] Jonathan Anderson. Lix and rix: Variations on a little-known readability index. *Journal of Reading*, 26(6):490–496, 1983.

[15] Benjamin Andow, Samin Yaseer Mahmud, Justin Whitaker, William Enck, Bradley Reaves, Kapil Singh, and Serge Egelman. Actions speak louder than words: Entity-sensitive privacy policy and data flow analysis with policheck. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 985–1002, 2020.

[16] The Internet Archive. Digital library of Free And Borrowable Books, Movies, Music And Wayback Machine. https://archive.org, 2021. [Online; accessed 25-June-2021].

[17] Austin Transportation Department (ATD). Shared Mobility Services. https://austintexas.gov/sharedmobility, 2020. [Online; accessed 11-May-2021].

[18] Mariam Bachiri, Ali Idri, José Luis Fernández-Alemán, and Ambrosio Toval. Evaluating the privacy policies of mobile personal health records for pregnancy monitoring. *Journal of medical systems*, 42(8):144, 2018.

[19] Benjamin Baron and Mirco Musolesi. Where you go matters: A study on the privacy implications of continuous location tracking. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 4(4):1–32, 2020.

[20] Benjamin Bichsel, Veselin Raychev, Petar Tsankov, and Martin Vechev. Statistical deobfuscation of android applications. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 343–355, 2016.

[21] Judith Bogert. In defense of the fog index. *The Bulletin of the Association for Business Communication*, 48(2):9–12, 1985.

[22] BoxerCycles. Scooter Share Companies in the US. https://boxercycles.com/scooter-share-companies, 2020. [Online; accessed 11-May-2021].

[23] Dan Boxler and Kristen R Walcott. Static taint analysis tools to detect information flows. In *Proceedings of the International Conference on Software Engineering Research and Practice (SERP)*, pages 46–52. The Steering Committee of The World Congress in Computer Science, 2018.

[24] Paolo Calciati, Konstantin Kuznetsov, Alessandra Gorla, and Andreas Zeller. Automatically granted permissions in android apps: An empirical study on their prevalence and on the potential threats for privacy. In *Proceedings of the 17th International Conference on Mining Software Repositories*, pages 114–124, 2020.

[25] John Caylor, Thoman Stict, and J Patrick Ford. The forcast readability formula. *Literacy Discussion. International Institute for Adult Literacy: UNESCO*, 67:68, 1973.

[26] Cheng Chang, Huaxin Li, Yichi Zhang, Suguo Du, Hui Cao, and Haojin Zhu. Automated and personalized privacy policy extraction under gdpr consideration. In *International Conference on Wireless Algorithms, Systems, and Applications*, pages 43–54. Springer, 2019.

[27] Christina Charitou, Dimitrios G Kogias, Spyros E Polykalas, Charalampos Z Patrikakis, and Ioana Cristina Cotoi. Use of apps for crime reporting and the eu general data protection regulation. In *Societal implications of community-oriented policing and technology*, pages 55–61. Springer, Cham, 2018.

[28] Hai-Hon Chen. How to use readability formulas to access and select english reading materials. *Journal of Educational Media & Library Sciences*, 50(2), 2012.

[29] Sen Chen, Ting Su, Lingling Fan, Guozhu Meng, Minhui Xue, Yang Liu, and Lihua Xu. Are mobile banking apps secure? what can be improved? In *Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, pages 797–802. ACM, 2018.

[30] Hui Na Chua, Anthony Herbland, Siew Fan Wong, and Younghoon Chang. Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics*, 34(4):157–170, 2017.

[31] Regina R Clewlow. The Micro-Mobility Revolution: The Introduction and Adoption of Electric Scooters in the United States. https://medium.com/populus-ai/the-micro-mobility-revolution-95e396db3754, 2018. [Online; accessed 11-May-2021].

[32] Caitlin D Cottrill. Maas surveillance: Privacy considerations in mobility as a service. *Transportation Research Part A: Policy and Practice*, 131:50–57, 2020.

[33] Hesham Darvish and Mohammad Husain. Security analysis of mobile money applications on android. In *2018 IEEE International Conference on Big Data (Big Data)*, pages 3072–3078. IEEE, 2018.

[34] Android Developers. Android Studio. https://developer.android.com/studio, 2021. [Online; accessed 16-June-2021].

[35] William Enck, Peter Gilbert, Seungyeop Han, Vasant Tendulkar, Byung-Gon Chun, Landon P Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N Sheth. Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones. *ACM Transactions on Computer Systems (TOCS)*, 32(2):1–29, 2014.

[36] Mojtaba Eskandari, Bruno Kessler, Maqsood Ahmad, Anderson Santana de Oliveira, and Bruno Crispo. Analyzing remote server locations for personal data transfers in mobile apps. *Proceedings on Privacy Enhancing Technologies*, 2017(1):118–131, 2017.

[37] Exodus-Privacy. Exodus. https://github.com/Exodus-Privacy/exodus, 2021. [Online; accessed 11-June-2021].

[38] Benjamin Fabian, Tatiana Ermakova, and Tino Lentz. Large-scale readability analysis of privacy policies. In *Proceedings of the international conference on web intelligence*, pages 18–25, 2017.

[39] Zheran Fang, Weili Han, and Yingjiu Li. Permission based android security: Issues and countermeasures. *computers & security*, 43:205–218, 2014.

[40] Kassem Fawaz and Kang G Shin. Location privacy protection for smartphone users. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 239–250, 2014.

[41] Álvaro Feal, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, and Alessandra Gorla. Angel or devil? a privacy study of mobile parental control apps. *Proceedings of Privacy Enhancing Technologies (PoPETS)*, 2020, 2020.

[42] Álvaro Feal Fajardo. *Study on privacy of parental control mobile applications*. PhD thesis, ETSI Informatica, 2017.

[43] R Flesch. A new readability yardstick. In *Journal of Applied Psychology*, 1948.

[44] Geoffrey A Fowler. One of the first contact-tracing apps violates its own privacy policy. https://www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/, 2020. [Online; accessed 11-May-2021].

[45] FSecureLABS. Drozer: The Leading Security Assessment Framework for Android. https://github.com/FSecureLABS/drozer, 2021. [Online; accessed 14-June-2021].

[46] Clint Gibler, Jonathan Crussell, Jeremy Erickson, and Hao Chen. Androidleaks: automatically detecting potential privacy leaks in android applications on a large scale. In *International Conference on Trust and Trustworthy Computing*, pages 291–307. Springer, 2012.

[47] Stefan Gössling. Integrating e-scooters in urban transportation: Problems, policies, and the prospect of system change. *Transportation Research Part D: Transport and Environment*, 79:102230, 2020.

[48] Jun Han, Emmanuel Owusu, Le T Nguyen, Adrian Perrig, and Joy Zhang. Accomplice: Location inference using accelerometers on smartphones. In *2012 Fourth International Conference on Communication Systems and Networks (COMSNETS 2012)*, pages 1–9. IEEE, 2012.

[49] Hamza Harkous, Kassem Fawaz, Rémi Lebret, Florian Schaub, Kang G Shin, and Karl Aberer. Polisis: Automated analysis and presentation of privacy policies using deep learning. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 531–548, 2018.

[50] Brenda Lynn Hoke. Comparison of recreational reading books levels using the fry readability graph and the flesch-kincaid grade level. 1999.

[51] Anett Hoppe, Jenny Knackmuß, Maik Morgenstern, and Reiner Creutzburg. Privacy issues in mobile health applications-assessment of current android health apps. *Electronic Imaging*, 2017(6):76–83, 2017.

[52] Qiwei Jia, Lu Zhou, Huaxin Li, Ruoxu Yang, Suguo Du, and Haojin Zhu. Who leaks my privacy: Towards automatic and association detection with gdpr compliance. In *International Conference on Wireless Algorithms, Systems, and Applications*, pages 137–148. Springer, 2019.

[53] Kuyju Kim, Taeyun Kim, Seungjin Lee, Soolin Kim, and Hyoungshick Kim. When harry met tinder: Security analysis of dating apps on android. In *Nordic Conference*

on Secure IT Systems, pages 454–467. Springer, 2018.
[54] Jenny Knackmuss, Eric Clausing, and Reiner Creutzburg. Investigation of security relevant aspects of android ehealthapps: permissions, storage properties and data transmission. *Electronic Imaging*, 2017(6):65–75, 2017.
[55] Lime. Electric Scooter Sharing. https://www.li.me/electric-scooter, 2020. [Online; accessed 19-June-2021].
[56] Andreas Löcken, Pascal Brunner, and Ronald Kates. Impact of hand signals on safety: Two controlled studies with novice e-scooter riders. In *12th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, pages 132–140, 2020.
[57] Anindya Maiti, Oscar Armbruster, Murtuza Jadliwala, and Jibo He. Smartwatch-based keystroke inference attacks and context-aware protection mechanisms. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, pages 795–806, 2016.
[58] Anindya Maiti, Nisha Vinayaga-Sureshkanth, Murtuza Jadliwala, Raveen Wijewickrama, and Greg P Griffin. Impact of e-scooters on pedestrian safety: A field study using pedestrian crowd-sensing. *arXiv preprint arXiv:1908.05846*, 2019.
[59] Peder Lind Mangset. Analysis of mobile application's compliance with the general data protection regulation (gdpr). Master's thesis, NTNU, 2018.
[60] Nicholas Mata, Nicole Beebe, and Kim-Kwang Raymond Choo. Are your neighbors swingers or kinksters? feeld app forensic analysis. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 1433–1439. IEEE, 2018.
[61] Yan Michalevsky, Dan Boneh, and Gabi Nakibly. Gyrophone: Recognizing speech from gyroscope signals. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 1053–1067, 2014.
[62] National Association of City Transportation Officials. Shared Micromobility in the U.S.: 2019. https://nacto.org/shared-micromobility-2019, 2019. [Online; accessed 11-May-2021].
[63] Achilleas Papageorgiou, Michael Strigkos, Eugenia Politou, Efthimios Alepis, Agusti Solanas, and Constantinos Patsakis. Security and privacy analysis of mobile health applications: the alarming state of practice. *IEEE Access*, 6:9390–9403, 2018.
[64] Nishant Das Patnaik. AppMon. https://github.com/dpnishant/appmon, 2021. [Online; accessed 23-June-2021].
[65] Constantinos Patsakis, Athanasios Zigomitros, and Agusti Solanas. Analysis of privacy and security exposure in mobile dating applications. In *International Conference on Mobile, Secure and Programmable Networking*, pages 151–162. Springer, 2015.
[66] Andrew Boyles Petersen. Scoot over smart devices: The invisible costs of rental scooters. *Surveillance & Society*, 17(1/2):191–197, 2019.
[67] CMU PrivacyGrade. Grading The Privacy Of Smartphone Apps. http://privacygrade.org/, 2015. [Online; accessed 11-May-2021].
[68] Haystack Project. Lumen Privacy Monitor. https://www.icsi.berkeley.edu/icsi/projects/networking/haystack, 2021. [Online; accessed 22-June-2021].
[69] Lina Qiu, Yingying Wang, and Julia Rubin. Analyzing the analyzers: Flowdroid/iccta, amandroid, and droidsafe. In *Proceedings of the 27th ACM SIGSOFT International Symposium on Software Testing and Analysis*, pages 176–186, 2018.
[70] Zhengyang Qu, Vaibhav Rastogi, Xinyi Zhang, Yan Chen, Tiantian Zhu, and Zhong Chen. Autocog: Measuring the description-to-permission fidelity in android applications. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 1354–1365, 2014.
[71] Joel Reardon, Álvaro Feal, Primal Wijesekera, Amit Elazari Bar On, Narseo Vallina-Rodriguez, and Serge Egelman. 50 ways to leak your data: An exploration of apps' circumvention of the android permissions system. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 603–620, 2019.
[72] Research and Markets. Micromobility Telematics Market Research Report: By Service Type, Offering, Technology, Sharing Type - Global Industry Trends Analysis and Revenue Forecast to 2030. https://www.researchandmarkets.com/reports/5331633/micromobility-telematics-market-research-report, 2020. [Online; accessed 10-June-2020].
[73] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. "won't somebody think of the children?" examining coppa compliance at scale. *Proceedings on Privacy Enhancing Technologies*, 2018(3):63–83, 2018.
[74] Julie M Robillard, Tanya L Feng, Arlo B Sporn, Jen-Ai Lai, Cody Lo, Monica Ta, and Roland Nadler. Availability, readability, and content of privacy policies and terms of agreements of mental health apps. *Internet Interventions*, 17:100243, 2019.
[75] Luc Rocher, Meenatchi Sundaram Muthu, and Yves-Alexandre de Montjoye. The observatory of anonymity: An interactive tool to understand re-identification risks in 89 countries. In *Companion Proceedings of the Web Conference 2021*, pages 687–689, 2021.
[76] Manuel Rudolph, Denis Feth, and Svenja Polst. Why users ignore privacy policies–a survey and intention model for explaining user privacy behavior. In *International Conference on Human-Computer Interaction*, pages 587–598. Springer, 2018.
[77] RJ Senter and Edgar A Smith. Automated readability index. Technical report, University of Cincinnati, Ohio, 1967.
[78] Hossain Shahriar, Md Arabin Talukder, and Md Saiful Islam. An exploratory analysis of mobile security tools. In *KSU Proceedings on Cybersecurity Education, Research and Practice. 4*, 2019.
[79] Randi Shedlosky-Shoemaker, Amy Curry Sturm, Muniba Saleem, and Kimberly M. Kelly. Tools for assessing readability and quality of health-related web sites. *Journal of Genetic Counseling*, 18(1):49–59, 2009.
[80] Ravi Inder Singh, Manasa Sumeeth, and James Miller. Evaluating the readability of privacy policies in mobile environments. *International Journal of Mobile Human Computer Interaction (IJMHCI)*, 3(1):55–78, 2011.
[81] Rocky Slavin, Xiaoyin Wang, Mitra Bokaei Hosseini, James Hester, Ram Krishnan, Jaspreet Bhatia, Travis D Breaux, and Jianwei Niu. Toward a framework for detecting privacy policy violations in android application code. In *Proceedings of the 38th International Conference on Software Engineering*, pages 25–36, 2016.
[82] Peter Story, Sebastian Zimmeck, and Norman Sadeh. Which apps have privacy policies? In *Annual Privacy Forum*, pages 3–23. Springer, 2018.
[83] Xiaoyu Sun, Li Li, Tegawendé F Bissyandé, Jacques Klein, Damien Octeau, and John Grundy. Taming reflection: An essential step toward whole-program analysis of android apps. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 30(3):1–36, 2021.
[84] Junwei Tang, Ruixuan Li, Hongmu Han, Heng Zhang, and Xiwu Gu. Detecting permission over-claim of android applications with static and semantic analysis approach. In *2017 IEEE Trustcom/BigDataSE/ICESS*, pages 706–713. IEEE, 2017.
[85] Sylvaine Tuncer and Barry Brown. E-scooters on the ground: Lessons for redesigning urban micro-mobility. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2020.
[86] Narseo Vallina-Rodriguez. Illuminating the third party mobile ecosystem with the lumen privacy monitor. 2017.
[87] Haoyu Wang, Zhe Liu, Jingyue Liang, Narseo Vallina-Rodriguez, Yao Guo, Li Li, Juan Tapiador, Jingcun Cao, and Guoai Xu. Beyond google play: A large-scale comparative study of chinese android app markets. In *Proceedings of the Internet Measurement Conference 2018*, pages 293–307, 2018.
[88] Robert T Williams. A table for rapid determination of revised dale-chall readability scores. *The Reading Teacher*, 26(2):158–165, 1972.
[89] Hong Yang, Qingyu Ma, Zhenyu Wang, Qing Cai, Kun Xie, and Di Yang. Safety of micro-mobility: analysis of e-scooter crashes by mining news reports. *Accident Analysis & Prevention*, 143:105608, 2020.
[90] Xueling Zhang, Xiaoyin Wang, Rocky Slavin, Travis Breaux, and Jianwei Niu. How does misconfiguration of analytic services compromise mobile privacy? ICSE '20, page 1572–1583, New York, NY, USA, 2020. Association for Computing Machinery.
[91] Zipeng Zhang and Xinyu Feng. Androidleaker: A hybrid checker for collusive leak in android applications. In *International Symposium on Dependable Software Engineering: Theories, Tools, and Applications*, pages 164–180. Springer, 2017.
[92] Sebastian Zimmeck, Peter Story, Daniel Smullen, Abhilasha Ravichander, Ziqi Wang, Joel Reidenberg, N Cameron Russell, and Norman Sadeh. Maps: Scaling privacy compliance analysis to a million apps. *Proceedings on Privacy Enhancing Technologies*, 2019(3):66–86, 2019.

APPENDIX

Table 1: List of Open Source Android Application Analysis Frameworks and Tools Used. *S denotes Static (Source-code); D denotes Dynamic; O denotes Other Analysis Tools.

Name	Version	Technique	Occurrence	Mode	Main role or Features
MobSF [7]	3.0.5, 3.2.6	S, D	Asynchronous	Computer	Reverse Engineering
Android Studio [34]	4	S, D	Real-time	Computer	Debugging
Polisis [49]	-	P, O	Asynchronous	Online	Policy Analysis
DeGuard [20]	-	O	Asynchronous	Online	De-obfuscation
VirtualAPK [8]	0.9.8	O	Real-time	On-device	Real-time data flow monitor
Lumen Monitor [86]		D	Real-time	On-device	API Tier Visualization
AppMon [64]	0.5	S, D, O	Real-time	Computer	Sniffing and Tracing
Ghidra [3]	9.1.2	S	Real-time	Computer	Deassembly
Drozer [45]	2.4.4	D	Real-time	Computer	Inter-app Interactions
LibRadar++ [87]	-	S	Asynchronous	Computer	Third party Library Identification

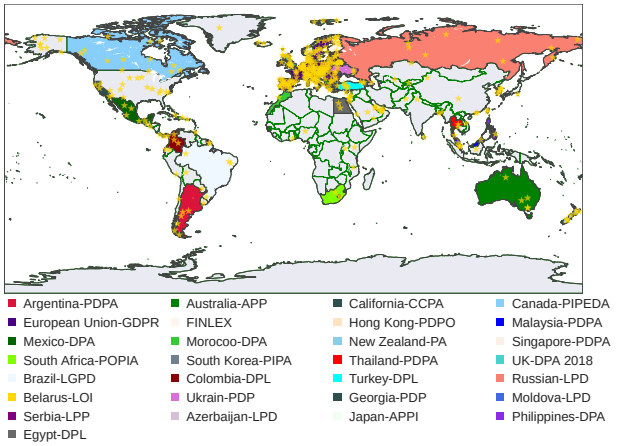

Figure 7: E-scooter rental service operating countries and data privacy laws. Yellow stars represent e-scooter rental companies.

Table 2: List of Common Weakness Enumerations (CWEs) associated with one or more vulnerabilities observed in core and/or third-party component(s) codebase across services.

Description	Presence (Most-Least Popular)
CWE-200 Information Exposure	100%, 76%, 42%
CWE-250 Execution with Unnecessary Privileges	<1%, - , <1%
CWE-276 Incorrect Default Permissions	100%, 90%, 100%
CWE-295 Improper Certificate Validation	45%, 18%, -
CWE-312 Cleartext Storage of Sensitive Information	100%, 90%, 75%
CWE-327 Use of Broken or Risky Cryptographic Algorithm	100%, 84%, 67%
CWE-330 Use of Insufficiently Random Values	100%, 88%, 83%
CWE-532 Insertion of Sensitive Information to Log File	100%, 90%, 100%
CWE-749 Exposed Dangerous Method or Function	91%, 45%, 33%
CWE-780 Use of RSA Algorithm without OAEP	<1%, <1%, -
CWE-89 Improper Neutralization of Special Elements in SQL Queries	100%, 82%, 67%
CWE-919 Weaknesses in Mobile Applications	55%, 31%, 17%

Summary: More than 85% of the rental service apps had third-party libraries associated with insufficient or weak cryptographic primitive usage or insecure data storage vulnerabilities. At least 10% of most popular e-scooter rental apps fixed a few vulnerabilities related to CWE-200, 295, 749 in future release versions.

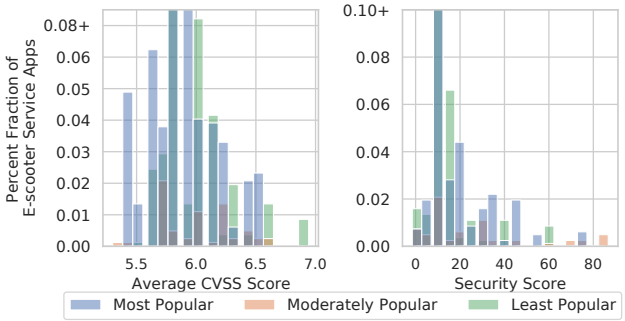

Figure 8: Statistics of average CVSS scores and security scores generated by the MobSF framework in most and least popular service apps.

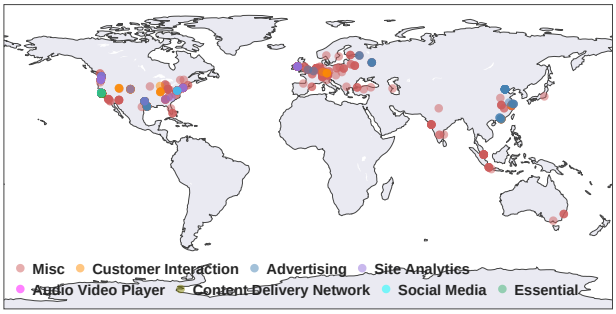

Figure 9: Approximate location of third-party Internet domains used by popular e-scooter rental apps. Location approximated based on their server IP address at the time of analysis.

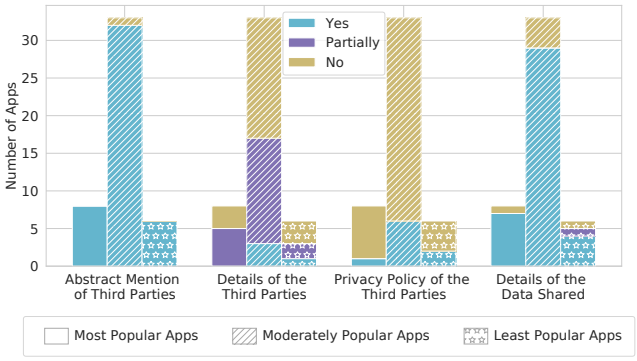

Figure 10: Number of apps that discuss about third-parties and data sharing.

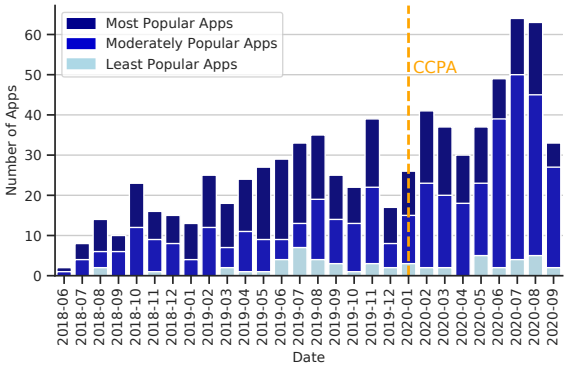

Figure 11: Privacy policy changes of different e-scooter rental service app versions over time based on available privacy policies.

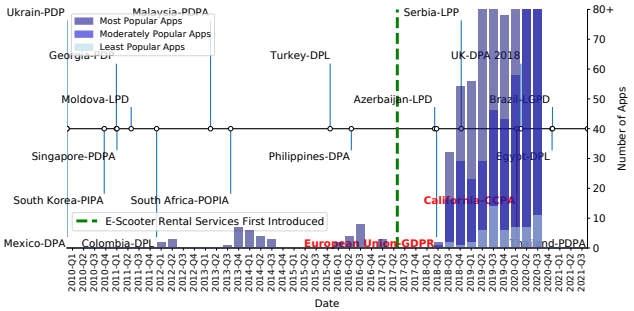

Figure 12: E-scooter service app updates in chronological order vs the regional privacy law updates.

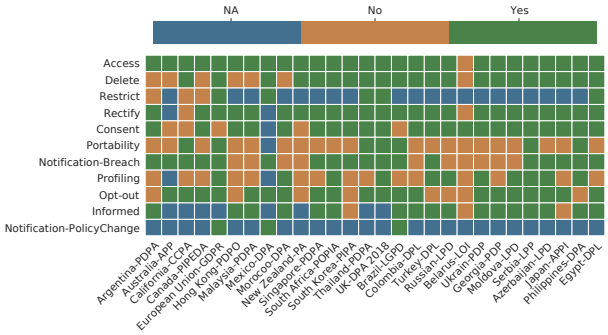

Figure 13: User data related provisions found in different data privacy laws and regulations. *NA* cells indicate that the provision was not explicitly mentioned in the corresponding document.

Figure 14: Commonly used words in both default and translated privacy policies of e-scooter rental apps.

A CLASSIFICATION OF THIRD-PARTIES

We conducted an in-depth investigation of the potential use (or misuse) of users' data by third-parties by characterizing their primary business model and service provided by them. While characterizing third-parties, we utilize different classifications for the third-party libraries and for the third-party domains. For libraries associated with the apps, which were statically identified, we manually compile and reassign categories for each library inspired from the existing databases [37, 87]. Section 5 shows the distribution of libraries found among all the e-scooter service apps. A significant portion of libraries found are development aids, for example, custom GUI components and frameworks. Most interestingly, analytics and business intelligence libraries are present in at least 95% of the apps, with the sub-categories of advertising and marketing related libraries found in nearly half of the e-scooter service apps.

Table 3: Summary of readability metrics used to assess policy content. * denotes score range or grade level recommended for an average adult or general public.

Readability Metric	Target Usage	Recommended*	Policies Not Within Range (Most-Least Popular)
Flesch Reading Ease [43]	General Usage	70-80 or above	53%, 84%, 90%
Gunning Fog Index [21]	Business Literature	8-10 or below	47%, 88%, 90%
Linsear Write [28]	Technical Writing	70-80 or above	53%, 86%, 90%
Automated Readability Index [77]	Technical Writing	8-10 or below	42%, 84%, 90%
Lix Readability [14]	Non-English Text	35-45 or below	42%, 84%, 90%
FORCAST Grade Level [25]	Technical Manuals	8-10 or below	53%, 88%, 90%
Flesch-Kincaid Grade [50]	General Usage	8-10 or below	37%,38, 70%
Coleman-Liau Index [79]	Education	8-10 or below	47%, 84%, 90%
Rix Readability [14]	Non-English Text	8-10 or below	0%, <1%, 0%
New Dale-Chall Score [88]	Student Materials	8-10 or below	47%, 86%, 90%

For third-party web servers or domains that were identified from network data flows during runtime, we base our analysis on the `whotracks.me` [9] database which characterizes business and service model of online service providers based on the technologies employed by them and service provided to end users (if any). About 23.6% of the observed third-parties are primarily in the *Site Analytics* category, which means they collect and analyze data related to usage and performance of the e-scooter rental apps. Around 26.9% are primarily in the *Advertising* category, wherein the third-parties provide advertising or advertising-related services such as data collection, behavioral analysis or re-targeting. About 2.25% can be primarily categorized in the *Customer Interaction* category, wherein the third-parties' main offered service is to enable chat, email messaging, customer support, and other interaction tools. Around 2.2% are primarily categorized as *Essential* that includes tag managers, privacy notices, and technologies that are critical to the functionality of the e-scooter rental apps. Approximately 45% of the entries (IP addresses, domains with WHOIS privacy protection) are not found in the `whotracks.me` database, thus making it difficult to categorize and determine the trustworthiness of these less prominent third-parties that are likely to evade scrutiny by the community.

Finally, we identify where the third-party servers, to which apps are communicating with, are located to study whether apps send data to a region within or outside of its operating region, and to obtain a high-level view of where the collected data may be physically stored or processed. Figure 9 shows the geographical location of these third-parties, approximated based on their server IP address (excludes third-parties detected solely based on the presence of their libraries via static analysis). We observe that most of the third-party services are hosted in the US (69%), followed by Europe (16%) and East Asia (8%). We also observe that a majority of *Site Analytics* services are hosted in North America, whereas *Advertising* services are predominantly hosted in Europe and East Asia.

Table 4: Related Works. * indicates that some of the apps in the analysis dataset were e-scooter service apps. AA denotes Android Apps, and PP denotes Privacy Policy in the analysis scope.

Analysis Scope	Related Work	Related Works' Focus
AA: Overall	Qiu et al. [69], Zhang et al. [91], Sun et al. [83]	Benchmark or randomly selected apps
	Shariar et al. [78]	Malware apps from a 3rd party market place
AA: Sensitive Data Leaks, Permissions and Privacy Risks	Lin et al. [67], Reardon et al. [71], Andow et al. [15], Xueling et al. [90]	Popular apps belonging to various categories
	Reyes et al. [1, 73], Calciati et al. [24]	Randomly selected apps*
	Knackmuss et al. [54], Hoppe et al. [51]	Health apps
	Patsakis et al. [65], Kim et al. [53], Mata et al. [60], Mata et al. [60]	Dating apps
	Darvish et al. [33], Chen et al. [29]	Financial apps
	Feal et al. [42], Ali et al. [12], Feal et al. [41]	Parental control apps
PP: Content Availability and Validity, Readability and Quality	Eskandari et al. [36], Story et al. [82], Harkous et al. [49]	Regionally popular apps or random apps
	Robillard et al. [74], Singh et al. [80]	Health apps or popular generic apps.
PP: Behavior and Regulation Conformance	Slavin et al. [81], Chua et al. [30], Mangset et al. [59], Chang et al. [26], Charitou et al. [27], Jia et al. [52], Bachiri et al. [18], Achara et al. [11], Petersen[66], Zimmeck et al. [92]	Popular apps from Google Play
	Bachiri et al. [18]	Pregnancy monitoring apps
	Achara et al. [11]	A transport app
	Petersen [66]	3 E-scooter rental service apps
	Fowler [44]	Contact Tracing apps
	Cottrill [32]	Mobility as a Service apps

Table 5: High-level data types associated with e-scooter services. At least one version of the unique services either had the potential to access or had accessed, collected or shared one or more of the data types in the sub-categories.

Data Type Sub-category	Possible Inference Attributes
Data Related To The Person or Individual Using the E-scooter Service	
Unique identifiers	Identity, Environment
Contact information	
Demographic information	
Visual identifiers and similar data	
Data Related To The App, Smartphone, or Environment of the Person or Individual Using the E-scooter Service	
Persistent and non-persistent device identifiers	Device, Environment
Other device and e-scooter app usage data	
Physical/virtual, precise/approximate location data	
Other data related to hardware/software of other devices (nearby/in same network)	
Data Related To The Social Accounts & Other Activities of the Person or Individual Using the E-scooter Service	
Social media information	Identity, Device, Environment
Other account(s) information (Raw/De-identified)	
Health and biometric Data	
On-device (physical/virtual) interactions & activities	
Off-device (virtual) interactions & activities	

B ACCESSIBILITY

Language readability refers to the characteristics of the policy content that allows it to be easily read and understood by average end-users, with varying levels of language proficiency. We compute readability scores using several different readability metrics from the literature, as outlined in Table 3. We notice 95% of the privacy policies fared well on the Rix scale indicating that the sentences used in the document can be understood by an 8th-grade level student. However, based on the Dale-Chall Index, intended for readability with respect to a fourth grader (or a user with limited technical comprehension), 97% of the policies did not fall within the recommended score range. The latter trend is due to the higher percentage of difficult words in the policy content, which the metric computation relies on unlike the former metric which is based on the word length. Surprisingly, we did not find any significant differences between the privacy policy readability scores of most and least popular e-scooter rental apps. About 93% of the privacy policies were offered in two or more languages, with a mean and median of 3.07 and 2, respectively. As intuitive, we observed that the number of supported language is generally higher when a service provider operates in multiple countries. About 94% of the privacy policies are available as downloadable webpages, which we use to conduct web accessibility measurement tests. Nearly one-half of the policy hosting webpages passed the WCAG 2.1 (at least Level A) and section 508 compliance standards. In summary, accessibility of the analyzed privacy policies can widely vary in terms of multilingual support, but readability and document design aspects are more homologous across the analyzed privacy policies.