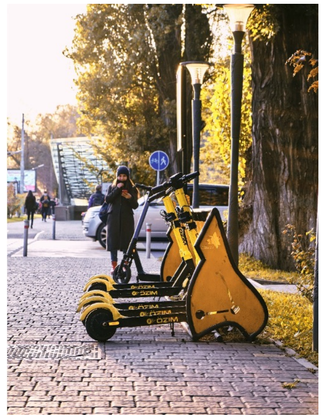
An Investigative Study on the Privacy Implications of Mobile E-scooter Rental Apps

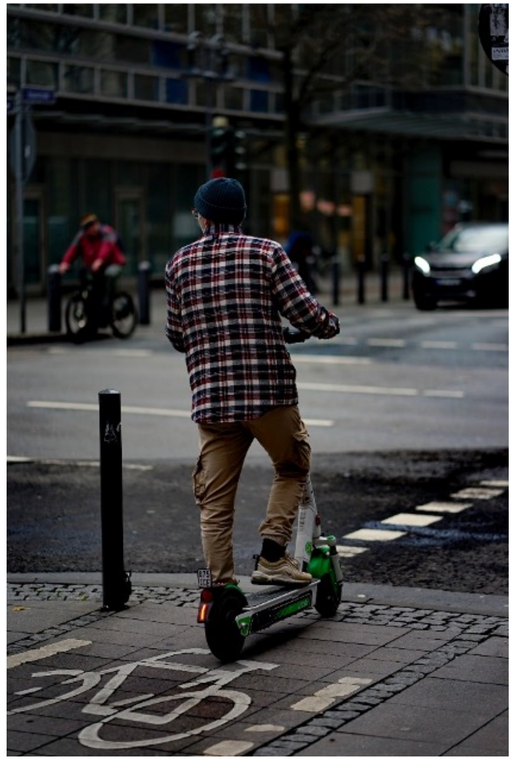
Nisha Vinayaga Sureshkanth, Raveen Wijewickrama, Anindya Maiti, Murtuza Jadliwala

Micromobility

Exploring transportation rental options in urban communities

- Battery- or people-powered.
- Docked or dockless.
- Seated or standing models:
  - E-scooters.
  - E-bikes.
  - E-skateboards.
  - Hoverboards.
  - Other micromobility.



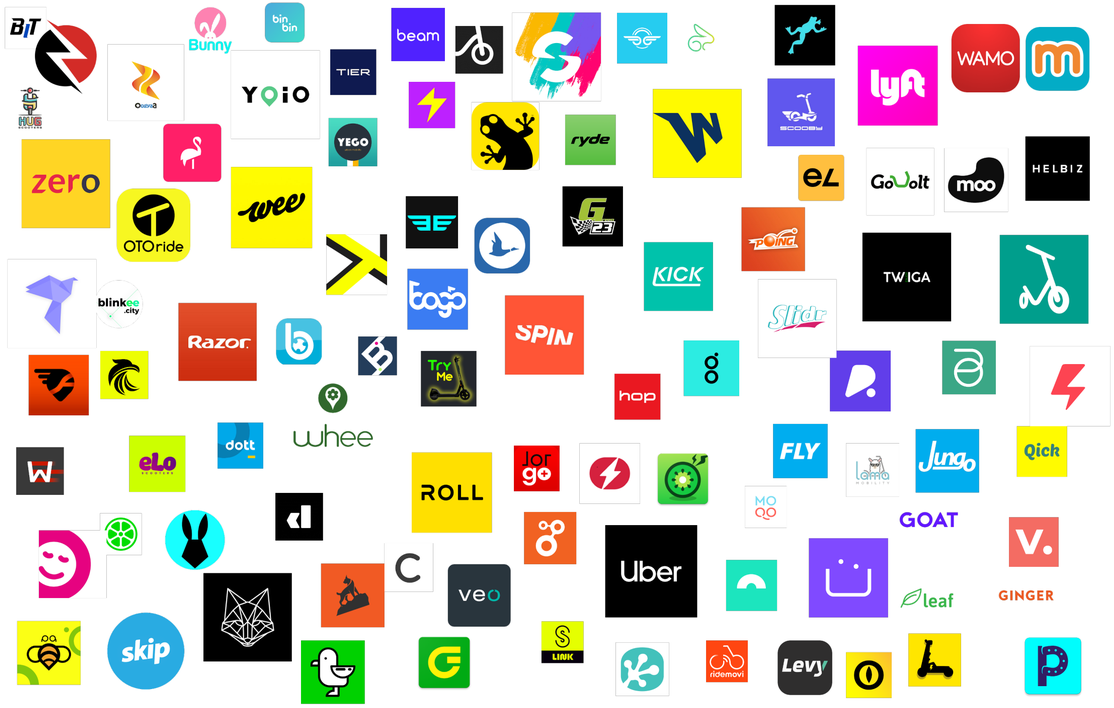


* E-scooter usage comparatively higher (>100M trips) in the U.S.

E-scooter Rental Providers

Peeking into the world of e-scooter rental service providers

- Concept introduced in 2017*.
- Over 100 unique service providers across the globe.
- Operations in multiple cities and/or countries.
- Outsource or develop their own service app and APIs; versions may vary across regions.

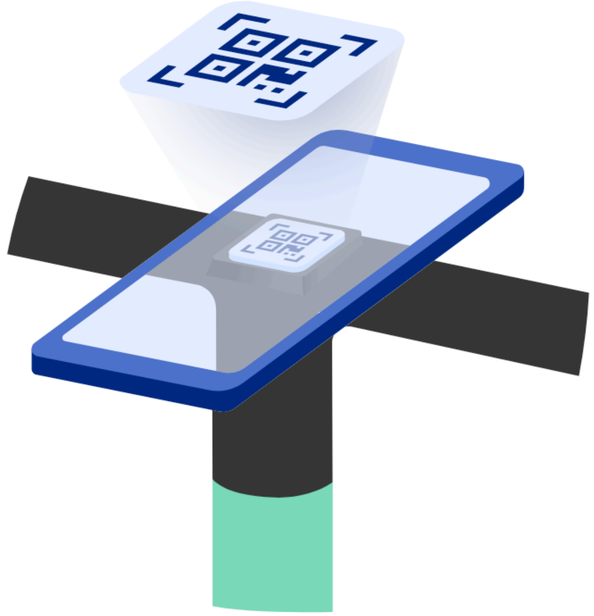


* Based on when the initial e-scooter rental service apps were available for the general public.

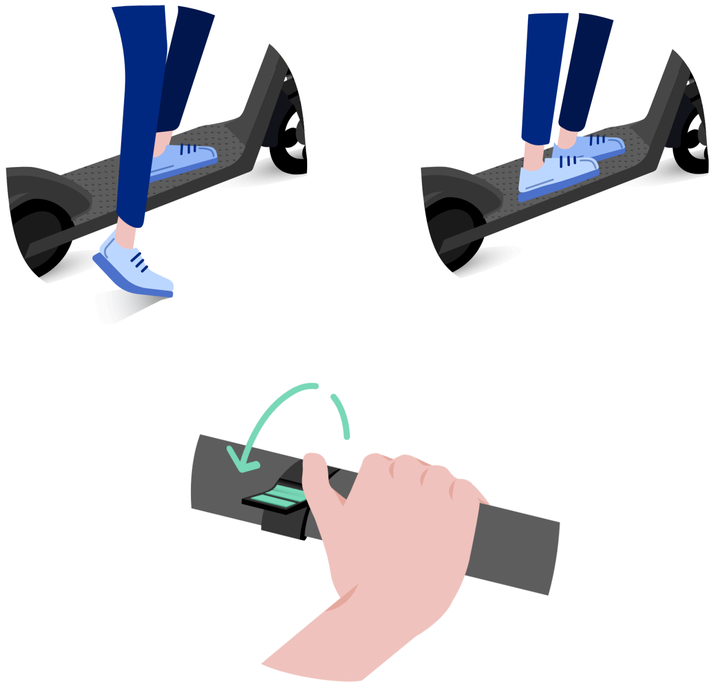
Electric Scooters (E-Scooters)

Renting and using a standing e-scooter using rental service apps

Initial Step: Scan QR code



Credit: https://tier-eu.freshdesk.com



Viola!

E-scooter Service Ecosystem

Identifying potential data leakage scenarios

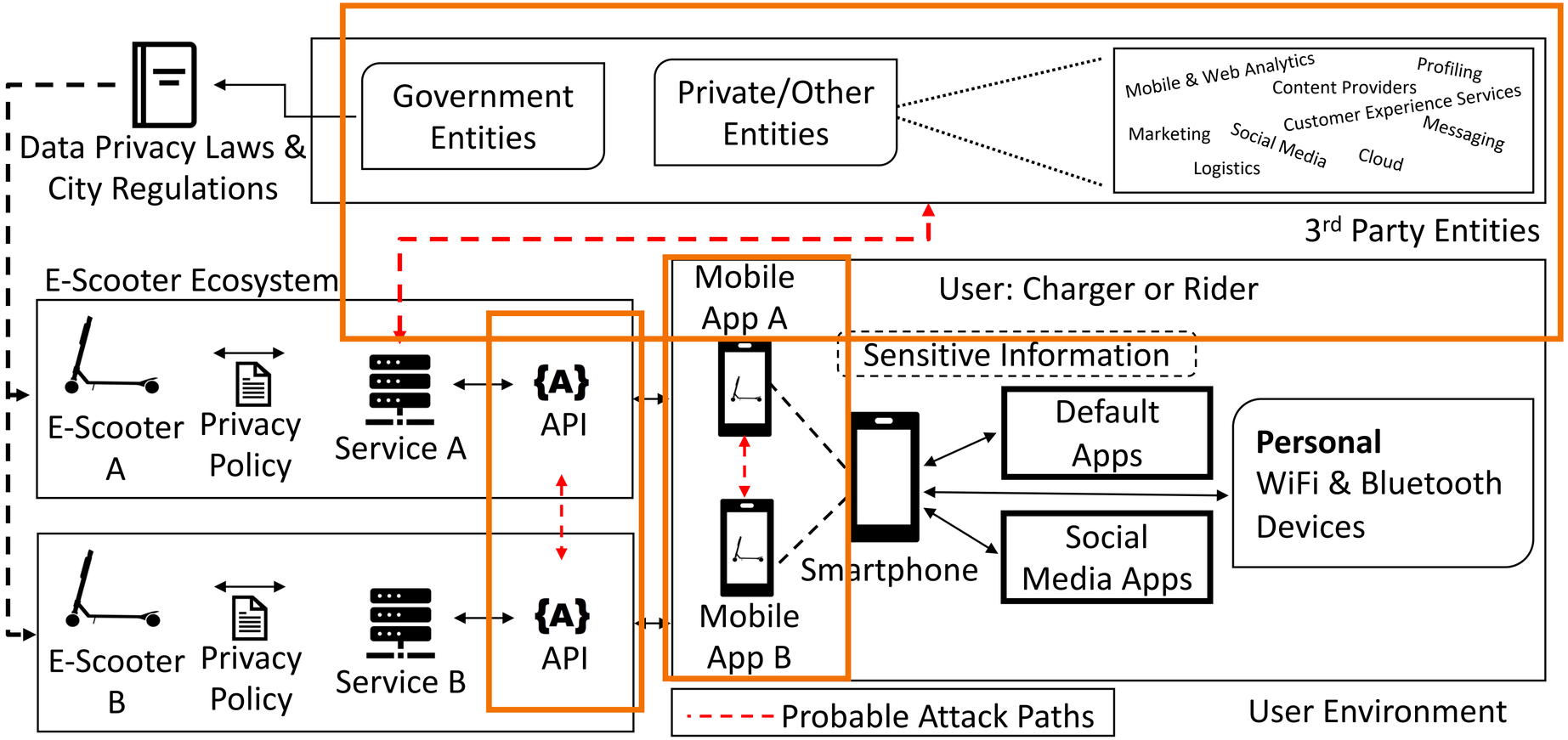


Figure highlighting the components of a typical e-scooter rental service ecosystem.

Related Work

Surveying what has been covered in the literature

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

* Ample literature on sensitive data leakage identification, app and privacy policy analysis overall but ***none extensively focus on practices in e-scooter rental service apps***.

Research Objectives

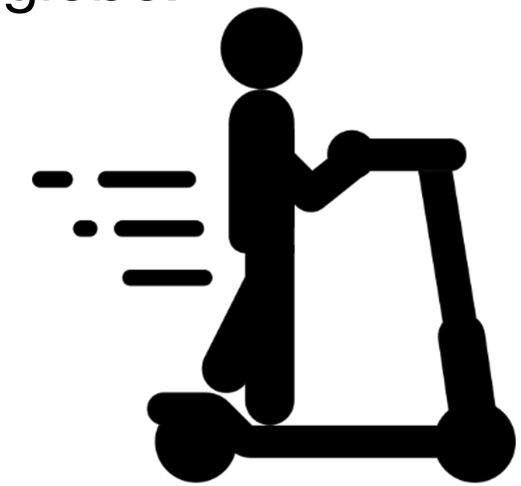
Investigating e-scooter rental services' potential to risk user privacy

- **RO1**: Analyzing service providers' **data**-related (access, collection, storage) practices in their mobile apps.
- **RO2**: Analyzing service providers’ data sharing practices with **third-parties**.
- **RO3**: Analyzing the coverage, accessibility and terminology similarity in service provider supplied **privacy policy** documents.
- **RO4**: Identifying **historical perspectives** and **trends** through a chronological analysis of different versions of individual apps.

Analysis Datasets

Shortlisting apps associated with e-scooter rental services

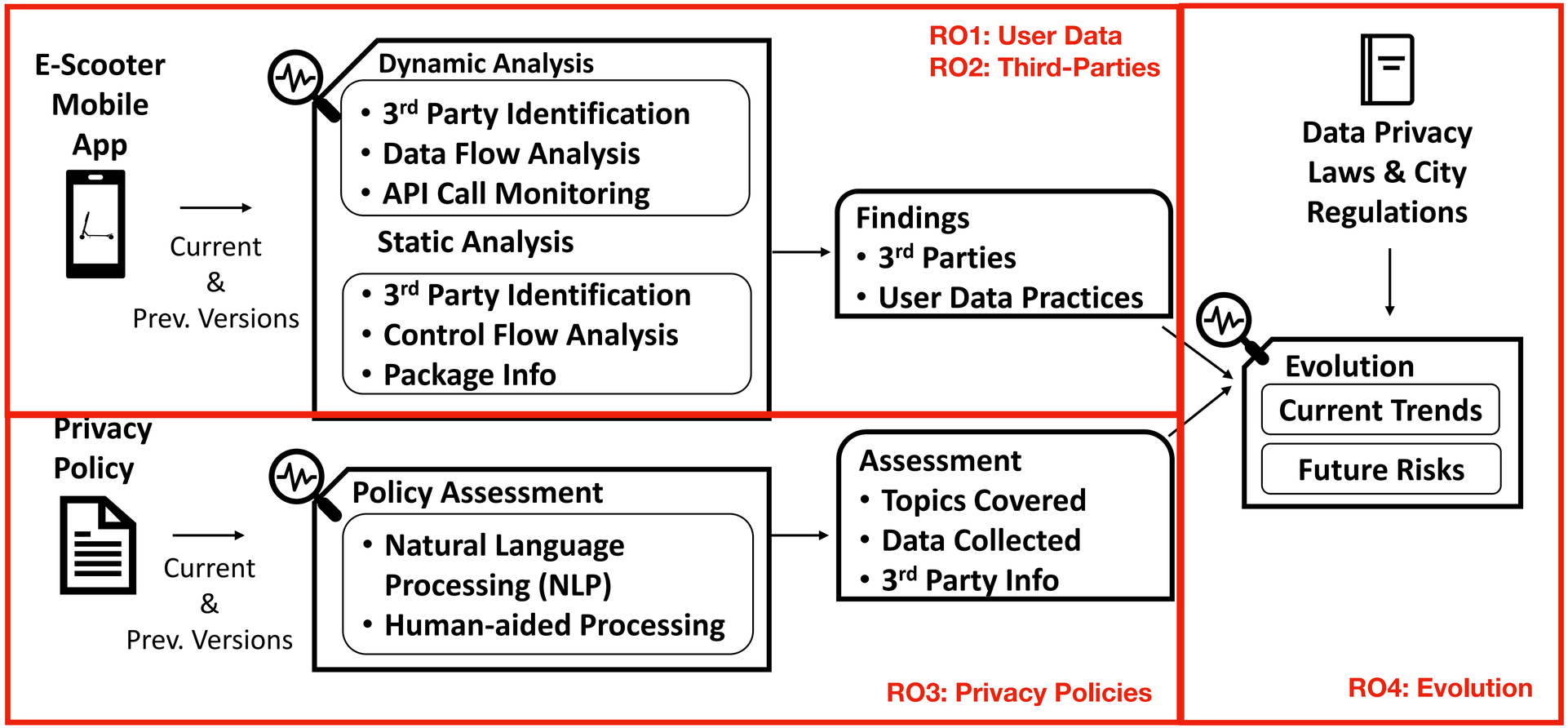
- Android apps with English language support across the globe.
- **1079** app versions (**102** rental services) until mid-2021:
  - *Older* (**RO4***): AndroZoo.
  - *Latest* (**RO1-3***): Google Play.
- Grouping based on download count:
  - *Most* popular (>100K), *moderately* popular and *least* popular (<10K).



* The number of unique rental service components analyzed varied across ROs depending on the app, version or policy document availability/compatibility to the analysis toolset.

Analysis Methodology

Outlining the rental service app and policy analysis pipeline and outcomes



Analysis Platforms

Summarizing the tools, environment and devices in the analysis

- 64-bit desktop computers
  - Windows 10 and Ubuntu.
- Android OS v9.0, 6.0 and 5.0
  - Moto X4, G7 Play.
  - Android Emulators.
- *Intensive* human-aided analysis.

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

Findings: RO1 - User Data

Outlining user data accessible to e-scooter rental service apps

- **Location** data — precise or relative, single or multiple sources.
  - GPS, Cellular network, Wi-Fi, Bluetooth data.
- **Identity** data - physical or virtual, required or optional, direct or indirect.
  - Identity documents, Demographic, Social media data, etc,.
- **Device** data - about device or about data stored in device.
  - IMEI, Files, Folders and Photos, Other device identifiers, and app data.

Findings: RO1 - User Data

Exploring how frequently data is being collected by service apps

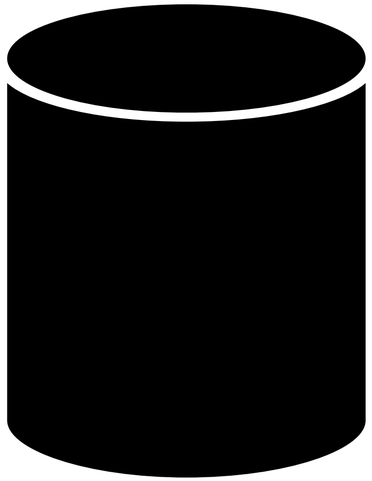
- **Location** data: On-demand or as frequently as every 15-20 minutes when app is in use, during ride-related process or in background.
- **Identity** data: At least once either during sign-up or occasionally after infrequent use or trigger events.
- **Device** data: At least once when the app is in use or not with varying access frequency as frequent as at least thrice in a day's span.

- Approximately one-fifths of service apps collected and/or shared location data and/or device identifiers even when the app was not in use.

Findings: RO1 - User Data

Identifying data storage practices related to e-scooter service apps

- Nearly 70% of the services analyzed required both read and write access to external storage.
- Almost three-fourths had information related to the user, device or service in cleartext format, or were exposed to other apps.
  - Most vulnerabilities associated with how third-party libraries handled accessed data.
  - For instance, raw device identifiers or unique identifiers generated by the either the core or third-party codebase.



Findings: RO2 - Third-Parties

Identifying third-party entities based on library presence

- Identified via AndroGuard and LibRadar++ during static analysis.
- **Re-tagged** manually based on available tags from Exodus Privacy and LibRadar mappings.
- Most ***prevalent*** third-party libraries: *Adjust, Braze, OneSignal, Branch, Google Ads,* and *Facebook libraries (Login, Places)*.

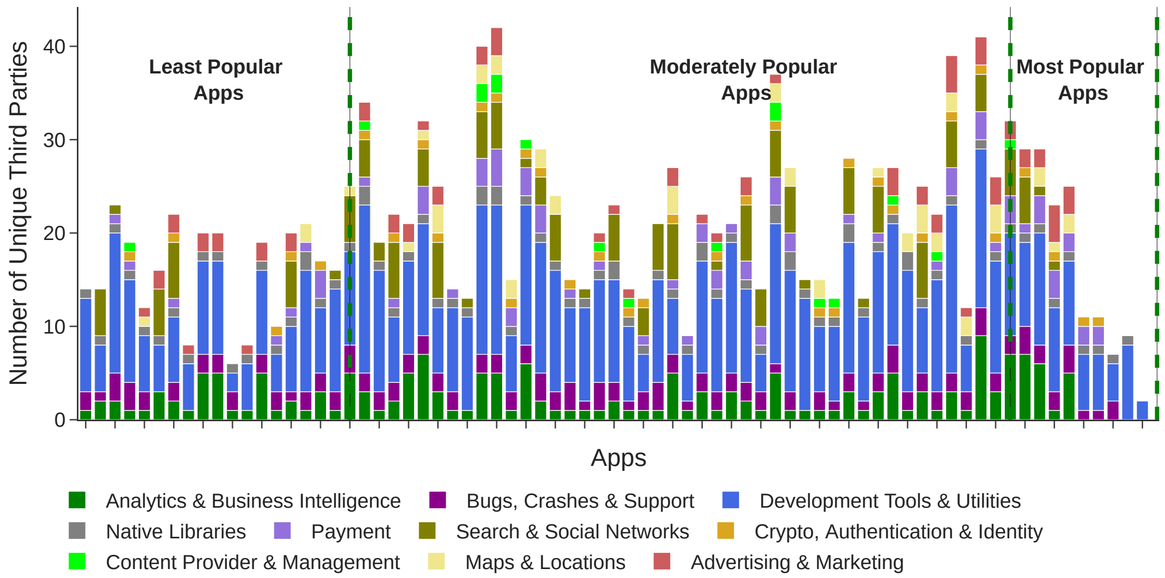


Figure providing statistics of different third-party SDKs associated with each of the investigated e-scooter rental service apps.

Findings: RO2 - Third-Parties

Identifying third-party entities based on contacted domains

- Identified during runtime analysis with chosen toolset.
- **Tagged** based on whotracks.me database entries.
- Most frequently ***accessed*** domains: *Google CrashLytics, Firebase Analytics, Branch, and Facebook Analytics*.
- Most frequently ***sent*** data: **device** -related data (raw/combined).

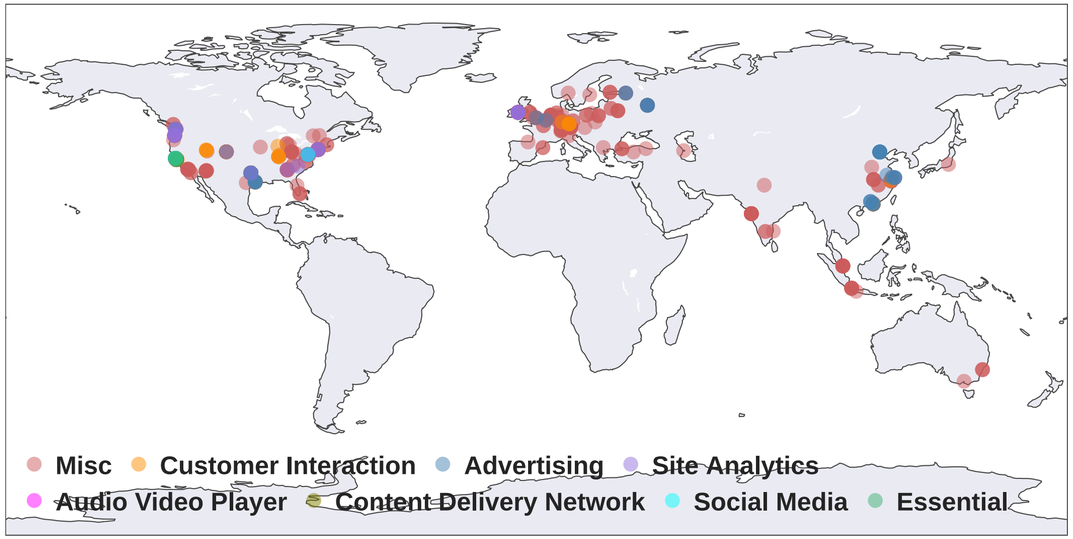


Figure denoting the approximate location of third-party Internet domains used by popular e-scooter rental apps. Location approximated based on their server IP address at the time of analysis.

Findings: RO3 - Privacy Policies

Identifying the information present in rental apps' privacy policies

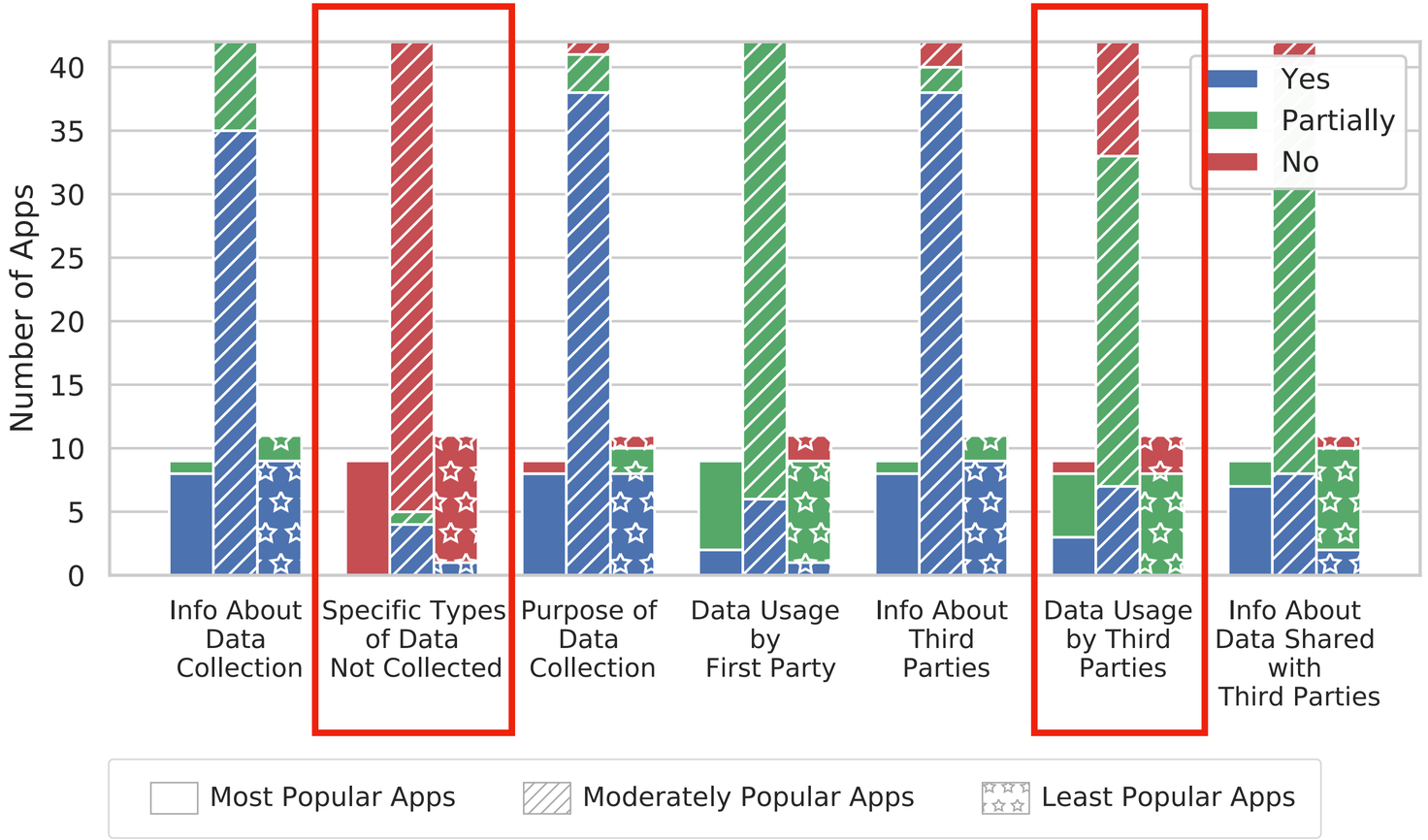


Figure highlighting the number of privacy policies that provide any (**generic or specific**) information related to their e-scooter rental services' user data handling policies.

Findings: RO3 - Privacy Policies

Informing users about third-parties and their data practices

Incident management	Photos of injuries (optional) Medical reports and records (optional)	Directly from you.	Affiliates. Partners. Trusted external service providers and data processors. Regulators and law enforcement agencies.	Necessary for our **legitimate interest** (to respond to customer communications, to investigate incidents and to maintain our brand and reputation) Necessary to protect **vital interests** of data subject Establishment or defence of **legal claims**

Figure previewing privacy policy content detailing what type of data is collected and with whom it may be shared along with their purpose.

Findings: RO3 - Privacy Policies

Analyzing how similar privacy policies are in the rental service domain

- Content overlap in more than two-thirds of services.
  - Collected data types.
  - Third-party information.
  - Statements regarding data handling and usage.
- Significant policy content overlap in related services.
  - Bird and Circ policies had 99.8% overlap.

Figure showcasing common words across privacy policies. Bigger and bolder the font, the more times it occurred across different service policy documents.

Findings: RO3 - Privacy Policies

Analyzing how readable privacy policies are to different populace

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%

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

- Based on the Dale-Chall Index, intended for readability with respect to a fourth grader (or a user with limited technical comprehension), majority of the policies did not fall within the recommended score range.

Findings: RO3 - Privacy Policies

Delving into the setbacks of identifying privacy policy violations

- Generic description of the type of data being collected about users and/or shared with third-parties:
  - "*personal data*", "*information about you*".
- Less than one-tenths of services specify they "*do not collect*" specific information.
- Majority of the services do not provide information about the *frequency, type and density* of data collected and shared with third-parties.

○ At least one version of twelve e-scooter rental apps was capable of collecting and/or sharing information not specifically disclosed in their privacy policy document.

Findings: RO4 - Evolution

Analyzing app version and policy updates

- More than nine-tenths of the *new app versions* released after GDPR introduction.
- Nearly half of the *new app versions* released around CCPA introduction.
- Highest number of *privacy policy revisions* in the eight-month period prior to GDPR went into effect in EU.

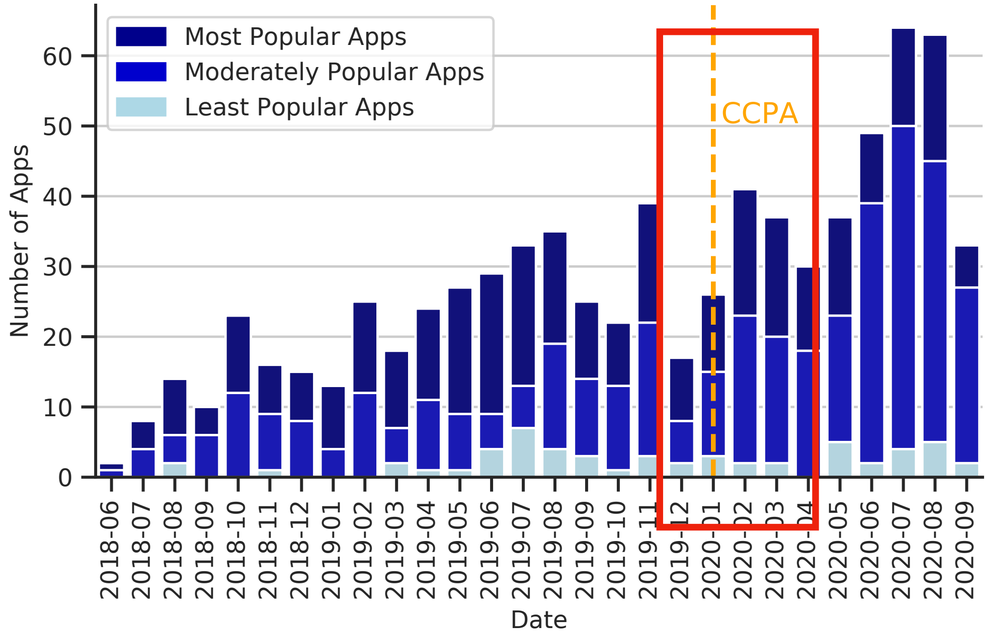


Figure highlighting the privacy policy changes of different e-scooter rental service app versions over time based on available privacy policies.

Findings: RO4 - Evolution

Analyzing app vulnerabilities

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%

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

- More than 85% of the rental service apps had third-party libraries associated with insufficient/weak cryptographic primitive usage and/or insecure data storage vulnerabilities.

Findings: RO4 - Evolution

Informing users about data-related provisions

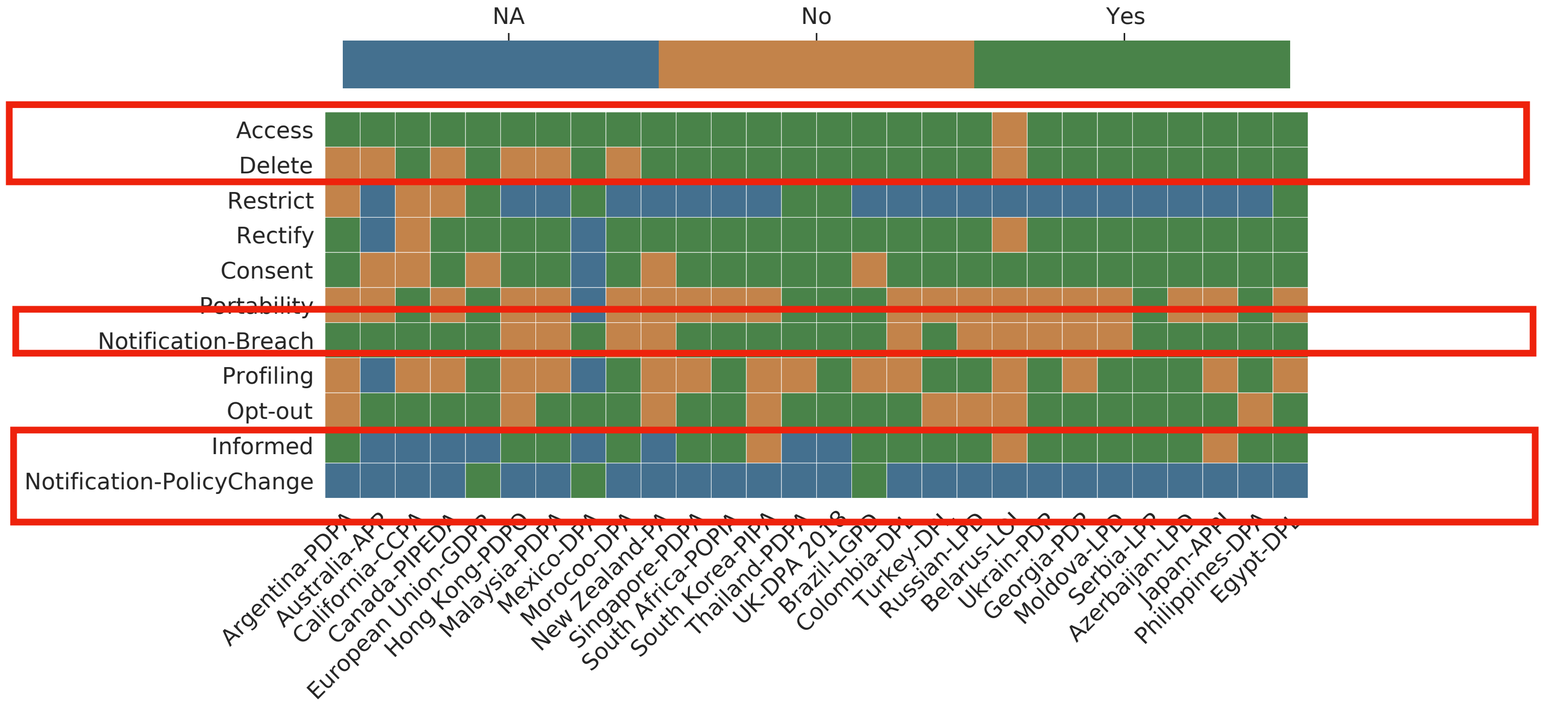


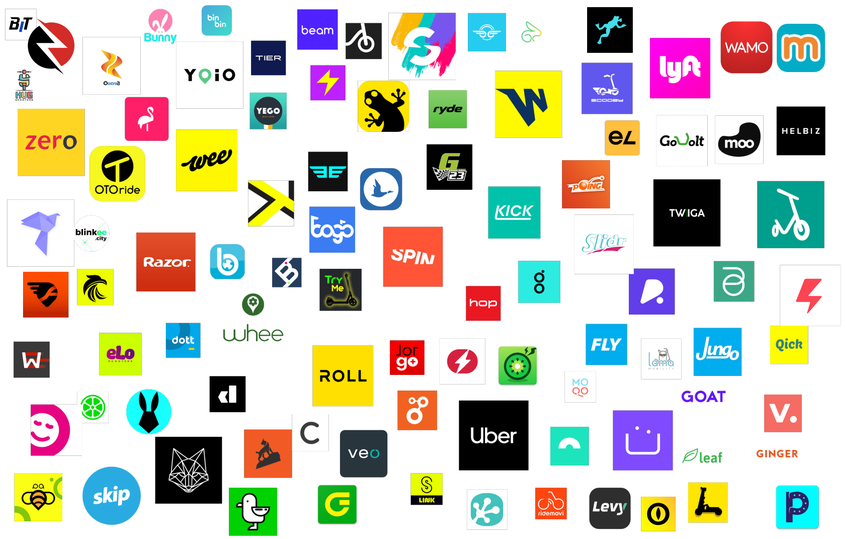
Figure providing user data related provisions found in different data privacy laws and regulations. NA cells indicate that the provision was not explicitly mentioned in the corresponding document.

- Only 32% of services explicitly mention about notifying users about any policy or data practice changes.
- Nearly three-fourths of services explicitly mention about allowing users to access or delete their data.

Privacy Implications

Summarizing entities affected by e-scooter rental service usage

- Affected users:
  - Loyal/frequent riders.
  - Users of multiple rental service providers.
  - Users who do not restrict app background access.
- Affected data:
  - Data collected from earlier versions.
  - Data leakage across service apps.
  - Seemingly non-sensitive data accumulated over time.



Conclusion

Wrapping up

- *Comprehensively* studied Android e-scooter rental apps and their privacy policies.
- *Investigated* the data collection and handling processes practiced by providers and associated third-parties.
- *Analyzed* how e-scooter rental services evolved over time to reflect their privacy policies and local regulations.

- Overall, choosing to be users of e-scooter rental services may put them at risk to privacy leakage scenarios pertaining to identity, possession or environment inference.

Questions?