

Tracking in Apps: Ist das legal?

Eine Übersicht über die mobile
Trackinglandschaft

FireShonks 2022





Malte (er/ihm)

Beisitzer Datenanfragen.de e. V.

- Doktorand am Institut für Anwendungssicherheit @ TUBS.
- Mag automatisierte Analysen sowie all things privacy.

malte@datenanfragen.de
[C7B5 0857 B713 F012](tel:+4970857713)

[@mal-tee:matrix.org](https://matrix.org/@mal-tee)
[@maltee@chaos.social](https://chaos.social/@maltee)



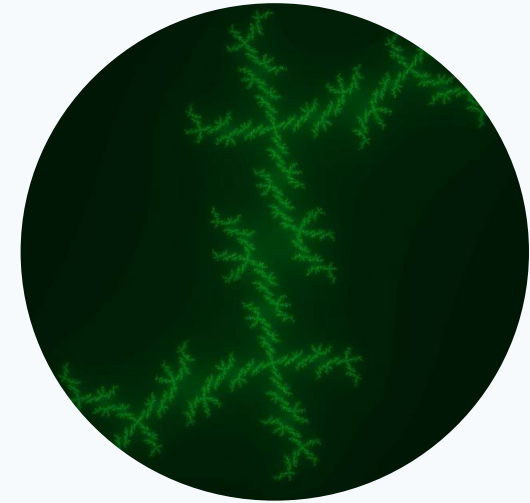
Benni (er/ihm)

Vorsitzender Datenanfragen.de e. V.

- Hat Informatik studiert.
- Mag neben Datenschutz auch IT-Sicherheit und all things FOSS. Aber hasst Computer.

benni@datenanfragen.de
[EB5C F074 AF13 81BD](tel:+4970857713)

[@benni:matrix.altpeter.me](https://matrix.org/@benni)
[@baltpeter@mastodon.social](https://mastodon.social/@baltpeter)



Lorenz (er/ihm)

Vorsitzender Datenanfragen.de e. V.

- Studiert Physik.
- Findet, dass konsequenter Datenschutz eine Systemtransformation fordern muss.

lorenz@datenanfragen.de
[DFAF 12BB 4C44 A6EF](tel:+4970857713)

[@zner0L:matrix.cccgoe.de](https://matrix.org/@zner0L)
[@zner0L@chaos.social](https://chaos.social/@zner0L)

**Wir sind vom Datenanfragen.de e. V.,
einem gemeinnützigen Verein, der
es sich zur Aufgabe gemacht hat,
Dir bei der Ausübung Deines
[Rechts auf Datenschutz](https://Datenanfragen.de) zu helfen.**

Tracking?

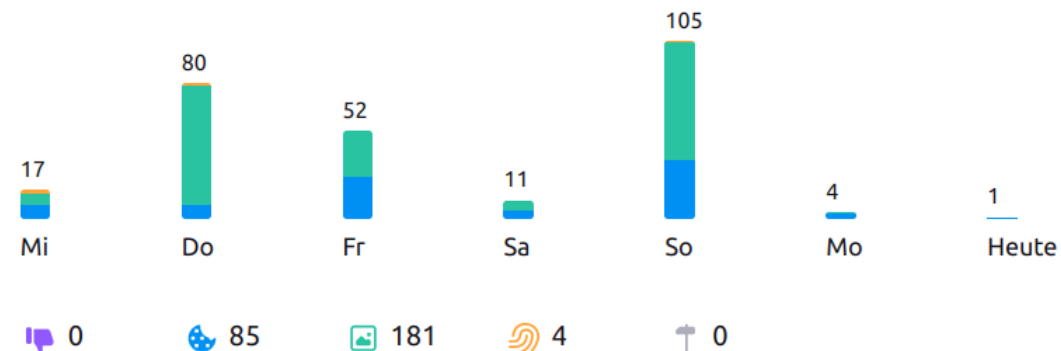
- Nutzungsverhalten und mehr wird an die Anbieterin des Dienstes oder Dritte geschickt.
- Warum?
 - Werbung, Telemetrie, Marktanalyse, Verkauf unserer Daten, ...
 - Aufzeichnung des Verhaltens für finanzielle Ziele
- Bringt Nutzer_innen wenig.
- Andere erfahren aber viel über uns!



Verbesserter Tracking-Schutz: Immer an

Firefox verhindert automatisch, dass Unternehmen heimlich Ihre Aktivitäten im Internet verfolgen.

Firefox blockierte 270 Skripte zur Aktivitätenverfolgung innerhalb der letzten Woche.



Social-Media-Tracker (Skripte zur Aktivitätenverfolgung durch soziale Netzwerke)

Auf anderen Websites eingebundene Elemente sozialer Netzwerke (z.B. zum Teilen von Inhalten) können Skripte enthalten, die verfolgen, was Sie online machen, angezeigt bekommen und sich anschauen. Dies ermöglicht den Unternehmen hinter den sozialen Netzwerken, mehr über Sie zu erfahren als allein durch die Inhalte, die Sie mit Ihrem Profil im sozialen Netzwerk teilen. [Weitere Informationen](#)

84.218 Skripte zur Aktivitätenverfolgung blockiert seit 21. Mai 2020.

Apps haben potentiell Zugriff auf viel **mehr Informationen** als der Browser (Sensoren, Kommunikation, Kontakte, ...).



Thank you for tracking with Deutsche Bahn.

DB Schnüffel-Navigator: Datenschutz juckt uns nicht.

#DBTracking
digitalcourage.de/db-tracking

Datenschutz-Labels

Bei iOS und Android müssen
Entwickler_innen selbst deklarieren,
welche Daten sie sammeln.

Der Entwickler, **Meta Platforms, Inc.**, hat darauf hingewiesen, dass die Datenschutzrichtlinien der App den unten stehenden Umgang mit Daten einschließen können. Weitere Informationen findest du in den [Datenschutzrichtlinien des Entwicklers](#).



Daten, die zum Tracking deiner Person verwendet werden

Die folgenden Daten werden möglicherweise verwendet, um dich über Apps und Websites anderer Unternehmen hinweg zu verfolgen:

-  Kontaktinformationen
-  Kennungen
-  Sonstige Daten



Mit dir verknüpfte Daten

Die folgenden Daten werden möglicherweise erfasst und mit deiner Identität verknüpft:

-  Gesundheit und Fitness
-  Gekaufte Artikel
-  Finanzinformationen
-  Standort
-  Kontaktinformationen
-  Kontakte
-  Benutzerinhalte
-  Suchverlauf
-  Browser-Verlauf
-  Kennungen
-  Nutzungsdaten
-  Vertrauliche Daten
-  Diagnose
-  Sonstige Daten

Die Datenschutzpraktiken können zum Beispiel je nach den von dir verwendeten Funktionen oder deinem Alter variieren. [Weitere Infos](#)

Informationen

Anbieter

Größe

Kategorie

<https://apps.apple.com/de/app/facebook/id284882215>

Simon Koch*, Malte Wessels, Benjamin Altpeter, Madita Olvermann, and Martin Johns

Keeping Privacy Labels Honest

Abstract: At the end of 2020, Apple introduced privacy nutritional labels, requiring app developers to state what data is collected by their apps and for what purpose. In this paper, we take an in-depth look at the privacy labels and how they relate to actual transmitted data.

First, we give an exploratory statistically evaluation of 11074 distinct apps across 22 categories and their corresponding privacy label or lack thereof. Our dataset shows that only some apps provide privacy labels, and a small number self-declare that they do not collect any data. Additionally, our statistical methods showcase the differences of the privacy labels across application categories.

We then select a subset of 1687 apps across 22 categories from the German App Store to conduct a no-touch traffic collection study. We analyse the traffic against a set of 18 honey-data points and a list of known advertisement and tracking domains. At least 276 of these apps violate their privacy label by transmitting data without declaration, showing that the privacy labels' correctness was not validated during the app approval process. In addition, we evaluate the apps' adherence to the GDPR

1 Introduction

Smartphones are ubiquitous [16], and ever more services rely on smartphone ownership, e.g., in the forms of banking apps or messaging application. Smartphones are carried everywhere and have become part of our day-to-day clothing. They carry data that provides deep insights into our private life, including our contacts, pictures, browsing behavior, and where we spend our time.

Contacts and contact interaction provide information about who is in our social network and possibly on the types of relationships between us [22, 43]. As most current smartphones include GPS and a myriad of other sensors, they observe and record where we go every day and for how long we stay [37, 47]. Finally, any tokens that are unique to a user can cross-identify a user across different data collectors. Combining identifying tokens with privacy-sensitive data presents a huge threat for the smartphone user's privacy.

Privacy is heavily contested. The EU introduced the GDPR law in 2016, and made it mandatory in 2018 [12]. This law requires that a user has to explicitly agree to *any personal data collection* in the context of an app



Nicht mit dir verknüpfte Daten

Die folgenden Daten, die zwar möglicherweise erfasst, aber nicht mit deiner Identität verknüpft werden, können für die folgenden Zwecke verwendet werden:

Analyse



Standort

Genauer Standort
Ungefäher Standort



Kennungen

Benutzer-ID



Nutzungsdaten

Produktinteraktion

App-Funktionalität



Kontaktinformationen

E-Mail-Adresse



Benutzerinhalte

Kundendienst



Diagnose

Crash-Daten
Leistungsdaten

16 % der betrachteten
Apps (1.687) übermittelten
Daten, die gar **nicht in ihrem
Label** angegeben waren.

Datensicherheit →

Was die Sicherheit angeht, solltest du nachvollziehen, wie Entwickler deine Daten erheben und weitergeben. Die Datenschutz- und Sicherheitspraktiken können je nach Verwendung, Region und Alter des Nutzers variieren. Diese Informationen wurden vom Entwickler zur Verfügung gestellt und können jederzeit von ihm geändert werden.

 Diese App kann die folgenden Datentypen an Dritte weitergeben
Standort, Personenbezogene Daten und 7 andere

 Diese App kann die folgenden Datentypen erheben
Standort, Personenbezogene Daten und 10 andere

 Daten werden bei der Übertragung verschlüsselt

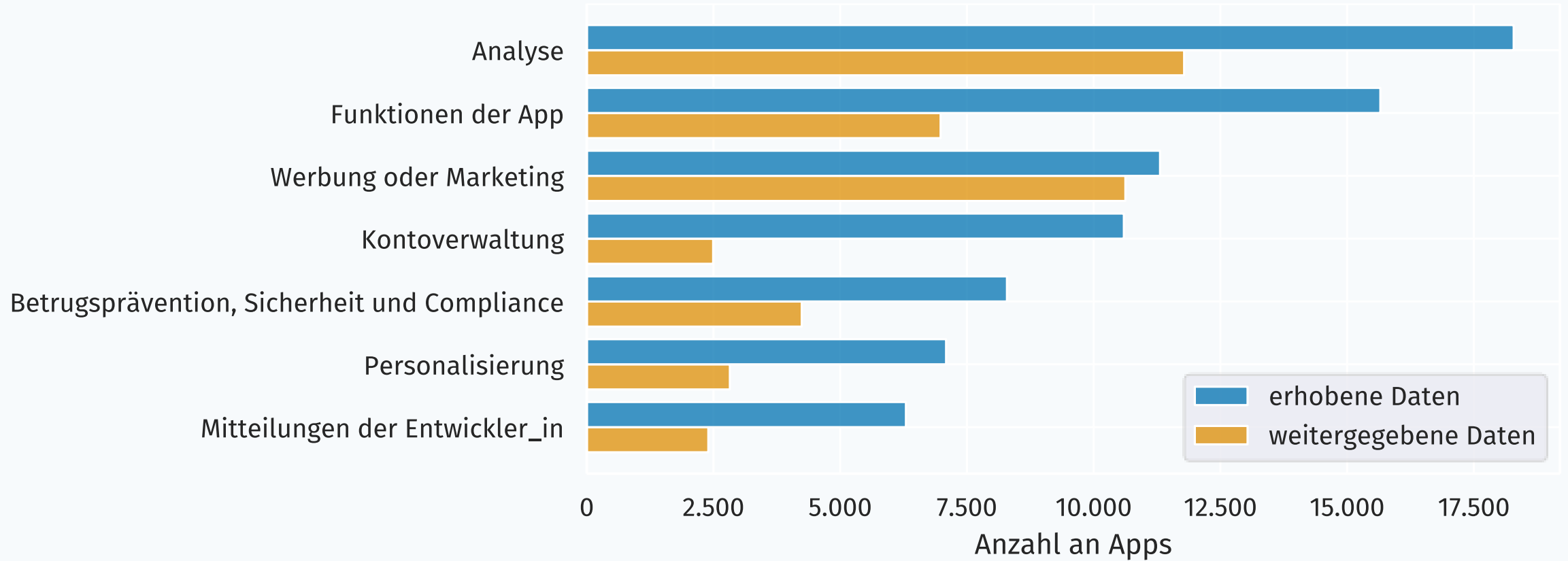
 Du kannst das Löschen der Daten beantragen

[Details ansehen](#)

Bewertungen und Rezensionen →

Bewertungen und Rezensionen sind verifiziert ⓘ

<https://play.google.com/store/apps/details?id=com.amazon.mShop.android.shopping&hl=de>



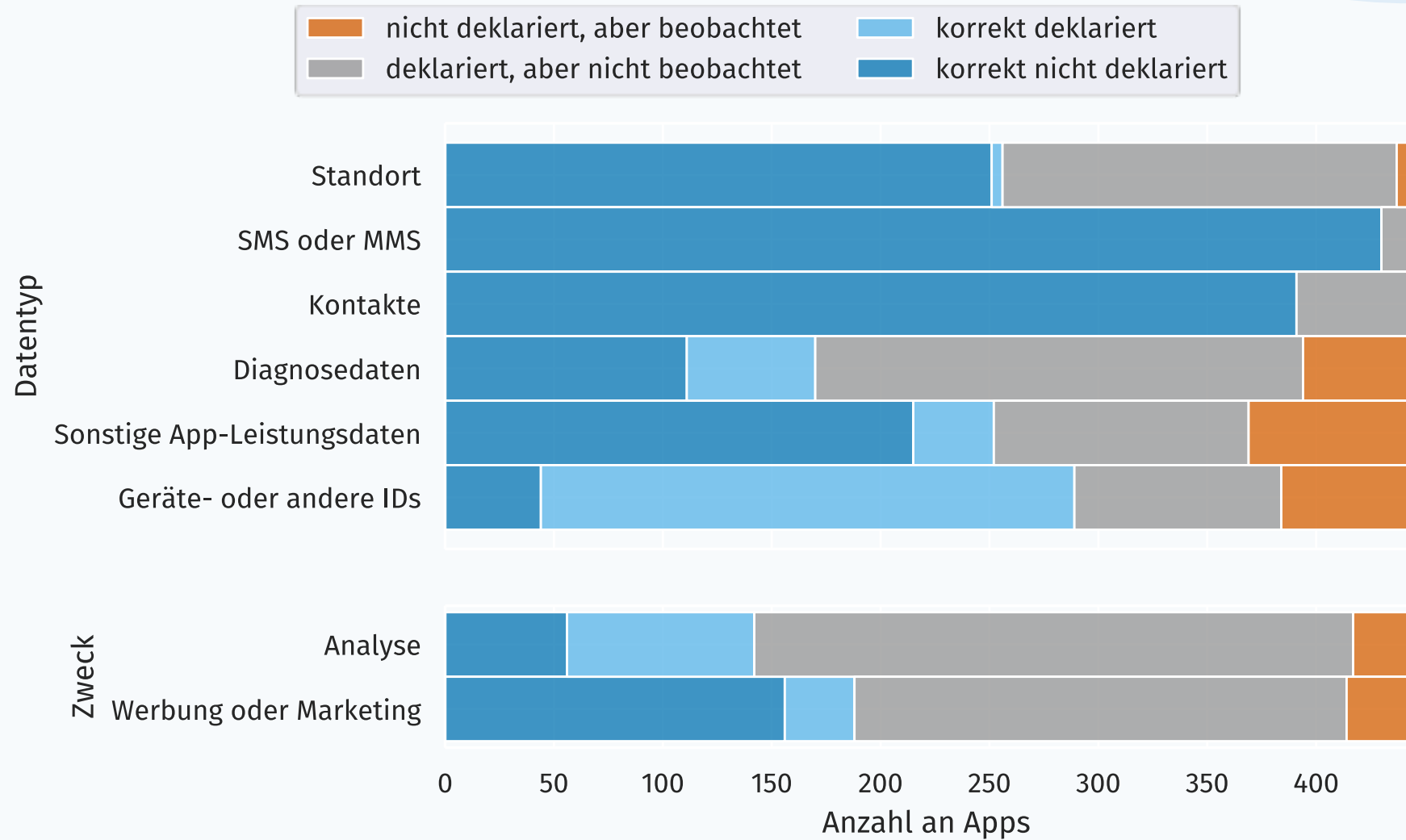
Anzahl an Apps, welche nach ihrem Label für die jeweiligen Zwecke Daten erheben und/oder weitergeben.

Beunruhigende Geständnisse

Bei der Analyse der Datensicherheits-Labels sind uns beunruhigend viele Apps aufgefallen, die deklarieren, dass sie hochsensible Daten wie Informationen über die sexuelle Orientierung, politische oder religiöse Überzeugungen und die Gesundheit ihrer Nutzer_innen zu Tracking- oder Werbezwecken sammeln oder sogar weitergeben. Und wie gesagt: Es handelt sich um Selbsterklärungen der Entwickler_innen, nicht um Behauptungen von uns oder Dritten. Die Entwickler_innen selbst scheinen kein Problem damit zu haben, diese unglaublich problematischen Verarbeitungen zuzugeben.

- [Facebook](#)  erhebt politische oder religiöse Überzeugungen, die sexuelle Orientierung und Gesundheitsdaten zu Analysezielen
- [Amazon Shopping](#)  erhebt und teilt Gesundheitsdaten für Analyseziele
- [Roblox](#)  erhebt die sexuelle Orientierung für Analyseziele und teilt sie für Analyse- und Werbe- oder Marketingziele
- [SoundCloud - Musik & Songs](#)  teilt die sexuelle Orientierung für Werbe- oder Marketingziele
- [My Little Pony: Magic Princess](#)  erhebt die sexuelle Orientierung für Analyse- und Werbe- oder Marketingziele und teilt sie für Werbe- oder Marketingziele
- [FarmVille 2: Country Escape](#)  erhebt die sexuelle Orientierung für Werbe- oder Marketingziele
- [9GAG: Funny GIF, Meme & Video](#)  erhebt die sexuelle Orientierung für Analyseziele
- [Zalando Lounge - Shopping Club](#)  erhebt und teilt die sexuelle Orientierung für Analyse- und Werbe- oder Marketingziele
- [momox: Bücher & mehr verkaufen](#)  erhebt und teilt die sexuelle Orientierung für Werbe- oder Marketingziele
- [nebenan.de - dein Nachbarschaftsnetzwerk](#)  erhebt die sexuelle Orientierung für Werbe- oder Marketingziele

Wir wissen nicht, ob alle Apps die Daten tatsächlich auf diese Weise verwenden, aber selbst wenn es sich



Auswertung der Richtigkeit der Datentypen und Zwecke in den analysierten Datensicherheits-Labels. Bedenke, dass wir nur definitiv sagen können, wenn Daten erhoben werden, aber nie bestätigen können, dass sie niemals erhoben werden.

Tatsächliche Übertragungen

Einige Beispiele von realem Tracking-Traffic, den wir beobachtet haben.

Stand:

März 2021 (Android), August 2021 (iOS)

Audible unter Android

POST <https://control.kochava.com/track/json>

```
"action": "install",
"kochava_device_id": "KA3731610548931t77133e5ade9f4[...]",
"sdk_protocol": "14",
"sdk_version": "AndroidTracker 3.7.3",
"nt_id": "d45c5-1-47dfae35-b398-40d2-a2e6-bd7bb40c88d0",
"data": {
  "screen_brightness": 0.4,
  "device_orientation": "portrait",
  "volume": 0.3333,
  "carrier_name": "Android",
  "adid": "827d8162-0e1c-48cd-892e-4abd3df95ba8",
  "device": "sdk_gphone_x86_64_arm64-google",
  "disp_h": 2560,
  "disp_w": 1440,
  "package": "com.audible.application",
  "installed_date": 1610548859,
  "os_version": "Android 11",
  "device_limit_tracking": false,
  "is_genuine": false,
  "screen_dpi": 560,
  "screen_inches": 5,
  "manufacturer": "Google",
  "product_name": "sdk_gphone_x86_64_arm64",
  "architecture": "x86_64",
  "battery_status": "not_charging",
  "battery_level": 77,
  "device_cores": 2,
  "locale": "en-US",
  "timezone": "Europe/Berlin",
  "bluetooth_name": "sdk_gphone_x86_64_arm64",
  "ui_mode": "Normal",
  "notifications_enabled": true,
  "background_location": false,
  "bms": 1610548366742,
  "network_conn_type": "wifi",
  "network_metered": false,
  "usertime": 1610548931,
  "uptime": 6.764,
  "state_active": true,
  "app_limit_tracking": false,
  "identity_link": {
    "marketingcloudvisitorid":
      "14340173368323804205870968500570471451"
  }
},
"sdk_id": "c456-s26905-",
"send_date": "2021-01-13T14:42:17.885Z"
```

Audible unter Android

POST <https://control.kochava.com/track/json>

```
"action": "install",
"kochava_device_id": "KA3731610548931t77133e5ade9f4[...]",
"sdk_protocol": "14",
"sdk_version": "AndroidTracker 3.7.3",
"nt_id": "d45c5-1-47dfae35-b398-40d2-a2e6-bd7bb40c88d0",
"data": {
  "screen_brightness": 0.4,
  "device_orientation": "portrait",
  "volume": 0.3333,
  "carrier_name": "Android",
  "adid": "827d8162-0e1c-48cd-892e-4abd3df95ba8",
  "device": "sdk_gphone_x86_64_arm64-google",
  "disp_h": 2560,
  "disp_w": 1440,
  "package": "com.audible.application",
  "installed_date": 1610548859,
  "os_version": "Android 11",
  "device_limit_tracking": false,
  "is_genuine": false,
  "screen_dpi": 560,
  "screen_inches": 5,
  "manufacturer": "Google",
  "product_name": "sdk_gphone_x86_64_arm64",
  "architecture": "x86_64",
  "battery_status": "not_charging",
  "battery_level": 77,
  "device_cores": 2,
  "locale": "en-US",
  "timezone": "Europe/Berlin",
  "bluetooth_name": "sdk_gphone_x86_64_arm64",
  "ui_mode": "Normal",
  "notifications_enabled": true,
  "background_location": false,
  "bms": 1610548366742,
  "network_conn_type": "wifi",
  "network_metered": false,
  "usertime": 1610548931,
  "uptime": 6.764,
  "state_active": true,
  "app_limit_tracking": false,
  "identity_link": {
    "marketingcloudvisitorid":
      "14340173368323804205870968500570471451"
  }
},
"sdk_id": "c456-s26905-",
"send_date": "2021-01-13T14:42:17.885Z"
```

Audible unter Android

POST https://control.kochava.com/track/json

```
"action": "install",
"kochava_device_id": "KA3731610548931t77133e5ade9f4[...]",
"sdk_protocol": "14",
"sdk_version": "AndroidTracker 3.7.3",
"nt_id": "d45c5-1-47dfae35-b398-40d2-a2e6-bd7bb40c88d0",
"data": {
  "screen_brightness": 0.4,
  "device_orientation": "portrait",
  "volume": 0.3333,
  "carrier_name": "Android",
  "adid": "827d8162-0e1c-48cd-892e-4abd3df95ba8",
  "device": "sdk_gphone_x86_64_arm64-google",
  "disp_h": 2560,
  "disp_w": 1440,
  "package": "com.audible.application",
  "installed_date": 1610548859,
  "os_version": "Android 11",
  "device_limit_tracking": false,
  "is_genuine": false,
  "screen_dpi": 560,
  "screen_inches": 5,
  "manufacturer": "Google",
  "product_name": "sdk_gphone_x86_64_arm64",
  "architecture": "x86_64",
  "battery_status": "not_charging",
  "battery_level": 77,
  "device_cores": 2,
  "locale": "en-US",
  "timezone": "Europe/Berlin",
  "bluetooth_name": "sdk_gphone_x86_64_arm64",
  "ui_mode": "Normal",
  "notifications_enabled": true,
  "background_location": false,
  "bms": 1610548366742,
  "network_conn_type": "wifi",
  "network_metered": false,
  "usertime": 1610548931,
  "uptime": 6.764,
  "state_active": true,
  "app_limit_tracking": false,
  "identity_link": {
    "marketingcloudvisitorid":
      "14340173368323804205870968500570471451"
  }
},
"sdk_id": "c456-s26905-",
"send_date": "2021-01-13T14:42:17.885Z"
```


Audible unter Android

POST https://control.kochava.com/track/json

```
"action": "install",
"kochava_device_id": "KA3731610548931t77133e5ade9f4[...]",
"sdk_protocol": "14",
"sdk_version": "AndroidTracker 3.7.3",
"nt_id": "d45c5-1-47dfae35-b398-40d2-a2e6-bd7bb40c88d0",
"data": {
  "screen_brightness": 0.4,
  "device_orientation": "portrait",
  "volume": 0.3333,
  "carrier_name": "Android",
  "adid": "827d8162-0e1c-48cd-892e-4abd3df95ba8",
  "device": "sdk_gphone_x86_64_arm64-google",
  "disp_h": 2560,
  "disp_w": 1440,
  "package": "com.audible.application",
  "installed_date": 1610548859,
  "os_version": "Android 11",
  "device_limit_tracking": false,
  "is_genuine": false,
  "screen_dpi": 560,
  "screen_inches": 5,
  "manufacturer": "Google",
  "product_name": "sdk_gphone_x86_64_arm64",
  "architecture": "x86_64",
  "battery_status": "not_charging",
  "battery_level": 77,
  "device_cores": 2,
  "locale": "en-US",
  "timezone": "Europe/Berlin",
  "bluetooth_name": "sdk_gphone_x86_64_arm64",
  "ui_mode": "Normal",
  "notifications_enabled": true,
  "background_location": false,
  "bms": 1610548366742,
  "network_conn_type": "wifi",
  "network_metered": false,
  "usertime": 1610548931,
  "uptime": 6.764,
  "state_active": true,
  "app_limit_tracking": false,
  "identity_link": {
    "marketingcloudvisitorid":
      "14340173368323804205870968500570471451"
  }
},
"sdk_id": "c456-s26905-",
"send_date": "2021-01-13T14:42:17.885Z"
```

Audible unter Android

POST https://control.kochava.com/track/json

```
"action": "install",
"kochava_device_id": "KA3731610548931t77133e5ade9f4[...]",
"sdk_protocol": "14",
"sdk_version": "AndroidTracker 3.7.3",
"nt_id": "d45c5-1-47dfae35-b398-40d2-a2e6-bd7bb40c88d0",
"data": {
  "screen_brightness": 0.4,
  "device_orientation": "portrait",
  "volume": 0.3333,
  "carrier_name": "Android",
  "adid": "827d8162-0e1c-48cd-892e-4abd3df95ba8",
  "device": "sdk_gphone_x86_64_arm64-google",
  "disp_h": 2560,
  "disp_w": 1440,
  "package": "com.audible.application",
  "installed_date": 1610548859,
  "os_version": "Android 11",
  "device_limit_tracking": false,
  "is_genuine": false,
  "screen_dpi": 560,
  "screen_inches": 5,
  "manufacturer": "Google",
  "product_name": "sdk_gphone_x86_64_arm64",
  "architecture": "x86_64",
  "battery_status": "not_charging",
  "battery_level": 77,
  "device_cores": 2,
  "locale": "en-US",
  "timezone": "Europe/Berlin",
  "bluetooth_name": "sdk_gphone_x86_64_arm64",
  "ui_mode": "Normal",
  "notifications_enabled": true,
  "background_location": false,
  "bms": 1610548366742,
  "network_conn_type": "wifi",
  "network_metered": false,
  "usertime": 1610548931,
  "uptime": 6.764,
  "state_active": true,
  "app_limit_tracking": false,
  "identity_link": {
    "marketingcloudvisitorid":
      "14340173368323804205870968500570471451"
  }
},
"sdk_id": "c456-s26905-",
"send_date": "2021-01-13T14:42:17.885Z"
```

Audible unter Android

POST https://control.kochava.com/track/json

```
"action": "install",
"kochava_device_id": "KA3731610548931t77133e5ade9f4[...]",
"sdk_protocol": "14",
"sdk_version": "AndroidTracker 3.7.3",
"nt_id": "d45c5-1-47dfae35-b398-40d2-a2e6-bd7bb40c88d0",
"data": {
  "screen_brightness": 0.4,
  "device_orientation": "portrait",
  "volume": 0.3333,
  "carrier_name": "Android",
  "adid": "827d8162-0e1c-48cd-892e-4abd3df95ba8",
  "device": "sdk_gphone_x86_64_arm64-google",
  "disp_h": 2560,
  "disp_w": 1440,
  "package": "com.audible.application",
  "installed_date": 1610548859,
  "os_version": "Android 11",
  "device_limit_tracking": false,
  "is_genuine": false,
  "screen_dpi": 560,
  "screen_inches": 5,
  "manufacturer": "Google",
  "product_name": "sdk_gphone_x86_64_arm64",
  "architecture": "x86_64",
```

```
"battery_status": "not_charging",
"battery_level": 77,
"device_cores": 2,
"locale": "en-US",
"timezone": "Europe/Berlin",
"blue_tooth_mac": "00:00:00:00:00:00",
"ui_mode": "normal",
"not_charging": true,
"background": true,
"bms": "normal",
"net_type": "wifi",
"net_ip": "192.168.1.1",
"used": true,
"uptime": 6.764,
"state_active": true,
"app_limit_tracking": false,
"identity_link": {
  "marketingcloudvisitorid":
    "14340173368323804205870968500570471451"
},
"sdid": "c456-s26905-",
"send_date": "2021-01-13T14:42:17.885Z"
```

Tracker verschiedener
Unternehmen verknüpfen
ihre IDs untereinander.

PayPal unter iOS

POST https://api-m.paypal.com/v1/mfsauth/proxy-auth/token

```
"app_id": "com.yourcompany.PPClient",
"app_guid": "8384FB18-571B-44F0-9809-40F040EB0961",
"source_app_version": "7.40.5",
"cloud_identifier":
  "a2a058f2-9367-4920-8190-bc504b4c90d9",
"local_identifier":
  "8b8cc6fa-aa04-4109-a27d-ae957c8db00d",
"linker_id": "71842c5e-88c0-45c7-a482-0a9cb9d71d58",
"risk_comp_session_id":
  "26afa6d4-1b33-483f-ba2e-169d431f75a2",
"dc_id": "b07f13e37dde7971d431b95a263a55f0",
"device_uptime": 807997862,
"locale_lang": "en",
"device_name": "R2G150Lv20",
"os_type": "iOS",
"os_version": "14.5.1",
"device_model": "iPhone10,4",
"is_rooted": true,
"is_emulator": false,
"TouchIDEnrolled": "false",
"PasscodeSet": "true",
"email_configured": true,
"sms_enabled": true,
"location_auth_status": "authorizedWhenInUse",

"total_storage_space": 127968497664,
"tz_name": "Europe/Berlin",
"conn_type": "wifi",
"ssid": "WLAN3.ALTPETER.ME",
"bssid": "34:81:c4:dc:36:1",
"ip_addresses": [
  "10.0.0.83",
  "fd31:4159::cf9:d932:11c3:bede",
  "fd31:4159::5998:c752:9f96:5e30",
  "fd31:4159::30a2:88d6:66c9:125f",
  "2003:dd:af1c:ab00:cc6:9a3a:7bf5:90d7",
  "2003:dd:af1c:ab00:69d6:4c4d:cabc:5168",
  "2003:dd:af1c:ab00:c81:68e1:2199:631",
  "fd31:4159::c9a3:68ec:ea3f:f085",
  "fe80::f631:960f:130f:5dc1",
  "fe80::87bf:b362:c6d3:616f"
],
"proxy_setting":
  "host=10.0.0.68,port=8080,type=kCFProxyTypeHTTPS",
"location": {
  "lng": 10.564191494436333,
  "lat": 52.23529052734375, "acc": 65
}
```

PayPal unter iOS

POST https://api-m.paypal.com/v1/mfsauth/proxy-auth/token

```
"app_id": "com.yourcompany.PPClient",
"app_guid": "8384FB18-571B-44F0-9809-40F040EB0961",
"source_app_version": "7.40.5",
"cloud_identifier":
  "a2a058f2-9367-4920-8190-bc504b4c90d9",
"local_identifier":
  "8b8cc6fa-aa04-4109-a27d-ae957c8db00d",
"linker_id": "71842c5e-88c0-45c7-a482-0a9cb9d71d58",
"risk_comp_session_id":
  "26afa6d4-1b33-483f-ba2e-169d431f75a2",
"dc_id": "b07f13e37dde7971d431b95a263a55f0",
"device_uptime": 807997862,
"locale_lang": "en",
"device_name": "R2G150Lv20",
"os_type": "iOS",
"os_version": "14.5.1",
"device_model": "iPhone10,4",
"is_rooted": true,
"is_emulator": false,
"TouchIDEnrolled": "false",
"PasscodeSet": "true",
"email_configured": true,
"sms_enabled": true,
"location_auth_status": "authorizedWhenInUse",
```

```
"total_storage_space": 127968497664,
"tz_name": "Europe/Berlin",
"conn_type": "wifi",
"ssid": "WLAN3.ALTPETER.ME",
"bssid": "34:81:c4:dc:36:1",
"ip_addresses": [
  "10.0.0.83",
  "fd31:4159::cf9:d932:11c3:bede",
  "fd31:4159::5998:c752:9f96:5e30",
  "fd31:4159::30a2:88d6:66c9:125f",
  "2003:dd:af1c:ab00:cc6:9a3a:7bf5:90d7",
  "2003:dd:af1c:ab00:69d6:4c4d:cabc:5168",
  "2003:dd:af1c:ab00:c81:68e1:2199:631",
  "fd31:4159::c9a3:68ec:ea3f:f085",
  "fe80::f631:960f:130f:5dc1",
  "fe80::87bf:b362:c6d3:616f"
],
"proxy_setting":
  "host=10.0.0.68,port=8080,type=kCFProxyTypeHTTPS",
"location": {
  "lng": 10.564191494436333,
  "lat": 52.23529052734375, "acc": 65
}
```

PayPal unter iOS

POST https://api-m.paypal.com/v1/mfsauth/proxy-auth/token

```
"app_id": "com.yourcompany.PPClient",
"app_guid": "8384FB18-571B-44F0-9809-40F040EB0961",
"source_app_version": "7.40.5",
"cloud_identifier":
  "a2a058f2-9367-4920-8190-bc504b4c90d9",
"local_identifier":
  "8b8cc6fa-aa04-4109-a27d-ae957c8db00d",
"linker_id": "71842c5e-88c0-45c7-a482-0a9cb9d71d58",
"risk_comp_session_id":
  "26afa6d4-1b33-483f-ba2e-169d431f75a2",
"dc_id": "b07f13e37dde7971d431b95a263a55f0",
"device_uptime": 807997862,
"locale_lang": "en",
"device_name": "R2G150Lv20",
"os_type": "iOS",
"os_version": "14.5.1",
"device_model": "iPhone10,4",
"is_rooted": true,
"is_emulator": false,
"TouchIDEnrolled": "false",
"PasscodeSet": "true",
"email_configured": true,
"sms_enabled": true,
"location_auth_status": "authorizedWhenInUse",
```

```
"total_storage_space": 127968497664,
"tz_name": "Europe/Berlin",
"conn_type": "wifi",
"ssid": "WLAN3.ALTPETER.ME",
"bssid": "34:81:c4:dc:36:1",
"ip_addresses": [
  "10.0.0.83",
  "fd31:4159::cf9:d932:11c3:bede",
  "fd31:4159::5998:c752:9f96:5e30",
  "fd31:4159::30a2:88d6:66c9:125f",
  "2003:dd:af1c:ab00:cc6:9a3a:7bf5:90d7",
  "2003:dd:af1c:ab00:69d6:4c4d:cabc:5168",
  "2003:dd:af1c:ab00:c81:68e1:2199:631",
  "fd31:4159::c9a3:68ec:ea3f:f085",
  "fe80::f631:960f:130f:5dc1",
  "fe80::87bf:b362:c6d3:616f"
],
"proxy_setting":
  "host=10.0.0.68,port=8080,type=kCFProxyTypeHTTPS",
"location": {
  "lng": 10.564191494436333,
  "lat": 52.23529052734375, "acc": 65
}
```

PayPal unter iOS

POST https://api-m.paypal.com/v1/mfsauth/proxy-auth/token

```
"app_id": "com.yourcompany.PPClient",
"app_guid": "8384FB18-571B-44F0-9809-40F040EB0961",
"source_app_version": "7.40.5",
"cloud_identifier":
  "a2a058f2-9367-4920-8190-bc504b4c90d9",
"local_identifier":
  "8b8cc6fa-aa04-4109-a27d-ae957c8db00d",
"linker_id": "71842c5e-88c0-45c7-a482-0a9cb9d71d58",
"risk_comp_session_id":
  "26afa6d4-1b33-483f-ba2e-169d431f75a2",
"dc_id": "b07f13e37dde7971d431b95a263a55f0",
"device_uptime": 807997862,
"locale_lang": "en",
"device_name": "R2G150Lv20",
"os_type": "iOS",
"os_version": "14.5.1",
"device_model": "iPhone10,4",
"is_rooted": true,
"is_emulator": false,
"TouchIDEnrolled": "false",
"PasscodeSet": "true",
"email_configured": true,
"sms_enabled": true,
"location_auth_status": "authorizedWhenInUse",
```

```
"total_storage_space": 127968497664,
"tz_name": "Europe/Berlin",
"conn_type": "wifi",
"ssid": "WLAN3.ALTPETER.ME",
"bssid": "34:81:c4:dc:36:1",
"ip_addresses": [
  "10.0.0.83",
  "fd31:4159::cf9:d932:11c3:bede",
  "fd31:4159::5998:c752:9f96:5e30",
  "fd31:4159::30a2:88d6:66c9:125f",
  "2003:dd:af1c:ab00:cc6:9a3a:7bf5:90d7",
  "2003:dd:af1c:ab00:69d6:4c4d:cabc:5168",
  "2003:dd:af1c:ab00:c81:68e1:2199:631",
  "fd31:4159::c9a3:68ec:ea3f:f085",
  "fe80::f631:960f:130f:5dc1",
  "fe80::87bf:b362:c6d3:616f"
],
"proxy_setting":
  "host=10.0.0.68,port=8080,type=kCFProxyTypeHTTPS",
"location": {
  "lng": 10.564191494436333,
  "lat": 52.23529052734375, "acc": 65
}
```

PayPal unter iOS

POST https://api-m.paypal.com/v1/mfsauth/proxy-auth/token

```
"app_id": "com.yourcompany.PPClient",
"app_guid": "8384FB18-571B-44F0-9809-40F040EB0961",
"source_app_version": "7.40.5",
"cloud_identifier":
  "a2a058f2-9367-4920-8190-bc504b4c90d9",
"local_identifier":
  "8b8cc6fa-aa04-4109-a27d-ae957c8db00d",
"linker_id": "71842c5e-88c0-45c7-a482-0a9cb9d71d58",
"risk_comp_session_id":
  "26afa6d4-1b33-483f-ba2e-169d431f75a2",
"dc_id": "b07f13e37dde7971d431b95a263a55f0",
"device_uptime": 807997862,
"locale_lang": "en",
"device_name": "R2G150Lv20",
"os_type": "iOS",
"os_version": "14.5.1",
"device_model": "iPhone10,4",
"is_rooted": true,
"is_emulator": false,
"TouchIDEnrolled": "false",
"PasscodeSet": "true",
"email_configured": true,
"sms_enabled": true,
"location_auth_status": "authorizedWhenInUse",

"total_storage_space": 127968497664,
"tz_name": "Europe/Berlin",
"conn_type": "wifi",
"ssid": "WLAN3.ALTPETER.ME",
"bssid": "34:81:c4:dc:36:1",
"ip_addresses": [
  "10.0.0.83",
  "fd31:4159::cf9:d932:11c3:bede",
  "fd31:4159::5998:c752:9f96:5e30",
  "fd31:4159::30a2:88d6:66c9:125f",
  "2003:dd:af1c:ab00:cc6:9a3a:7bf5:90d7",
  "2003:dd:af1c:ab00:69d6:4c4d:cabc:5168",
  "2003:dd:af1c:ab00:c81:68e1:2199:631",
  "fd31:4159::c9a3:68ec:ea3f:f085",
  "fe80::f631:960f:130f:5dc1",
  "fe80::87bf:b362:c6d3:616f"
],
"proxy_setting":
  "host=10.0.0.68,port=8080,type=kCFProxyTypeHTTPS",
"location": {
  "lng": 10.564191494436333,
  "lat": 52.23529052734375, "acc": 65
}
```


Bitmoji unter Android

POST <https://bitmoji.api.snapchat.com/api/analytics/wevents>

```
"events": [ {
  "category": "application",
  "action": "app_open",
  "avatarId": "0",
  "timestamp": 1610547947100,
  "label":
    "{\\"with_screen_read\\":false,\\"state\\":\\"cold\\"}",
  "appId": 1,
  "has_snapchat_installed": false,
  "session_id":
    "5ceba0d8-46c5-4992-8142-0edf3e994bbe",
  "experimentIds": [],
  "sequence_id": 0,
  "login_session_id":
    "4104bb10-1abc-4128-a828-18b9e7413dbd"
}, {
  "category": "performance",
  "action": "INSTALL_EXPERIMENT_PULL",
  "avatarId": "0",
  "timestamp": 1610547949712,
  "label": "{\\"latency\\":2628,\\"success\\":true}",
  "appId": 1,
  "has_snapchat_installed": false,
  "session_id":
    "5ceba0d8-46c5-4992-8142-0edf3e994bbe",
  "experimentIds": [274, 331, 392],
  "sequence_id": 1,
  "login_session_id":
    "4104bb10-1abc-4128-a828-18b9e7413dbd"
}, {
  "category": "welcome",
  "action": "page_view",
  "avatarId": "0",
  "timestamp": 1610547963550,
  "label":
    "{\\"referrer\\":\\"\\",\\"login_version\\":1}",
  "appId": 1,
  "has_snapchat_installed": false,
  "session_id":
    "5ceba0d8-46c5-4992-8142-0edf3e994bbe",
  "experimentIds": [274, 331, 392],
  "sequence_id": 2,
  "login_session_id":
    "4104bb10-1abc-4128-a828-18b9e7413dbd"
} ]
```

Bitmoji unter Android

POST https://bitmoji.api.snapchat.com/api/analytics/wevents

```
"events": [ {
  "category": "application",
  "action": "app_open",
  "avatarId": "0",
  "timestamp": 1610547947100,
  "label":
    "{\\"with_screen_read\\":false,\\"state\\":\\"cold\\"}",
  "appId": 1,
  "has_snapchat_installed": false,
  "session_id":
    "5ceba0d8-46c5-4992-8142-0edf3e994bbe",
  "experimentIds": [],
  "sequence_id": 0,
  "login_session_id":
    "4104bb10-1abc-4128-a828-18b9e7413dbd"
}, {
  "category": "performance",
  "action": "INSTALL_EXPERIMENT_PULL",
  "avatarId": "0",
  "timestamp": 1610547949712,
  "label": "{\\"latency\\":2628,\\"success\\":true}",
  "appId": 1,
  "has_snapchat_installed": false,
  "session_id":
    "5ceba0d8-46c5-4992-8142-0edf3e994bbe",
  "experimentIds": [274, 331, 392],
  "sequence_id": 1,
  "login_session_id":
    "4104bb10-1abc-4128-a828-18b9e7413dbd"
}, {
  "category": "welcome",
  "action": "page_view",
  "avatarId": "0",
  "timestamp": 1610547963550,
  "label":
    "{\\"referrer\\":\\"\\",\\"login_version\\":1}",
  "appId": 1,
  "has_snapchat_installed": false,
  "session_id":
    "5ceba0d8-46c5-4992-8142-0edf3e994bbe",
  "experimentIds": [274, 331, 392],
  "sequence_id": 2,
  "login_session_id":
    "4104bb10-1abc-4128-a828-18b9e7413dbd"
} ]
```

Bitmoji unter Android

POST <https://bitmoji.api.snapchat.com/api/analytics/wevents>

```
"events": [ {
  "category": "application",
  "action": "app_open",
  "avatarId": "0",
  "timestamp": 1610547947100,
  "label":
    "{\\"with_screen_read\\":false,\\"state\\":\\"cold\\"}",
  "appId": 1,
  "has_snapchat_installed": false,
  "session_id":
    "5ceba0d8-46c5-4992-8142-0edf3e994bbe",
  "experimentIds": [],
  "sequence_id": 0,
  "login_session_id":
    "4104bb10-1abc-4128-a828-18b9e7413dbd"
}, {
  "category": "performance",
  "action": "INSTALL_EXPERIMENT_PULL",
  "avatarId": "0",
  "timestamp": 1610547949712,
  "label": "{\\"latency\\":2628,\\"success\\":true}",
  "appId": 1,
  "has_snapchat_installed": false,
  "session_id":
    "5ceba0d8-46c5-4992-8142-0edf3e994bbe",
  "experimentIds": [274, 331, 392],
  "sequence_id": 1,
  "login_session_id":
    "4104bb10-1abc-4128-a828-18b9e7413dbd"
}, {
  "category": "welcome",
  "action": "page_view",
  "avatarId": "0",
  "timestamp": 1610547963550,
  "label":
    "{\\"referrer\\":\\"\\",\\"login_version\\":1}",
  "appId": 1,
  "has_snapchat_installed": false,
  "session_id":
    "5ceba0d8-46c5-4992-8142-0edf3e994bbe",
  "experimentIds": [274, 331, 392],
  "sequence_id": 2,
  "login_session_id":
    "4104bb10-1abc-4128-a828-18b9e7413dbd"
} ]
```

Bitmoji unter Android

POST <https://bitmoji.api.snapchat.com/api/analytics/wevents>

```
"events": [ {
  "category": "application",
  "action": "app_open",
  "avatarId": "0",
  "timestamp": 1610547947100,
  "label":
    "{\\"with_screen_read\\":false,\\"state\\":\\"cold\\"}",
  "appId": 1,
  "has_snapchat_installed": false,
  "session_id":
    "5ceba0d8-46c5-4992-8142-0edf3e994bbe",
  "experimentIds": [],
  "sequence_id": 0,
  "login_session_id":
    "4104bb10-1abc-4128-a828-18b9e7413dbd"
}, {
  "category": "performance",
  "action": "INSTALL_EXPERIMENT_PULL",
  "avatarId": "0",
  "timestamp": 1610547949712,
  "label": "{\\"latency\\":2628,\\"success\\":true}",
  "appId": 1,
  "has_snapchat_installed": false,
  "session_id":
    "5ceba0d8-46c5-4992-8142-0edf3e994bbe",
  "experimentIds": [274, 331, 392],
  "sequence_id": 1,
  "login_session_id":
    "4104bb10-1abc-4128-a828-18b9e7413dbd"
}, {
  "category": "welcome",
  "action": "page_view",
  "avatarId": "0",
  "timestamp": 1610547963550,
  "label":
    "{\\"referrer\\":\\"\\",\\"login_version\\":1}",
  "appId": 1,
  "has_snapchat_installed": false,
  "session_id":
    "5ceba0d8-46c5-4992-8142-0edf3e994bbe",
  "experimentIds": [274, 331, 392],
  "sequence_id": 2,
  "login_session_id":
    "4104bb10-1abc-4128-a828-18b9e7413dbd"
} ]
```

Indeed Job Search unter Android

POST `https://t.appsflyer.com/api/v4/androidevent`

`?buildnumber=4.10.3&app_id=com.indeed.android.jobsearch`

```
"af_timestamp": "1611209035694",
"appsflyerKey": "ExLocXqS6j9TGyNebHQHrG",
"operator": "T-Mobile",
"network": "MOBILE",
"timepassedsincelastlaunch": "-1",
"open_referrer": "android-app://android",
"af_v2": "e1089f09b150658adadbacd6f807c1947d072cb2",
"uid": "1611209035909-2664535545820779500",
"isGaidWithGps": "true",
"lang_code": "en",
"installDate": "2021-01-21_060319+0000",
"app_version_code": "63766",
"firstLaunchDate": "2021-01-21_060358+0000",
"ivc": false,
"model": "sdk_gphone_x86_64_arm64",
"lang": "English",
"brand": "google",
"batteryLevel": "77.0",
"deviceType": "userdebug",
"product": "sdk_gphone_x86_64_arm64",
"advertiserId":
  "827d8162-0e1c-48cd-892e-4abd3df95ba8",
"deviceData": {
  "sensors": [ {
    "sT": 1,
    "sVS": [0.7662141, 9.013549, 3.795387],
    "sN": "Goldfish 3-axis Accelerometer",
    "sV": "The Android Open Source Project",
    "sVE": [0.7662141, 9.013549, 3.795387]
  },
  {
    "sT": 2,
    "sVS": [-17.875, 24.125, -38.4375],
    "sN": "Goldfish 3-axis Magnetic field sensor",
    "sV": "The Android Open Source Project",
    "sVE": [-17.875, 24.125, -38.4375]
  },
  {
    "sT": 4,
    "sVS": [0, 0, 0],
    "sN": "Goldfish 3-axis Gyroscope",
    "sV": "The Android Open Source Project",
    "sVE": [0, 0, 0]
  }
] }
```

Indeed Job Search unter Android

POST `https://t.appsflyer.com/api/v4/androidevent`
`?buildnumber=4.10.3&app_id=com.indeed.android.jobsearch`

```
"af_timestamp": "1611209035694",
"appsflyerKey": "ExLocXqS6j9TGyNebHQHrG",
"operator": "T-Mobile",
"network": "MOBILE",
"timepassedsincelastlaunch": "-1",
"open_referrer": "android-app://android",
"af_v2": "e1089f09b150658adadbacd6f807c1947d072cb2",
"uid": "1611209035909-2664535545820779500",
"isGaidWithGps": "true",
"lang_code": "en",
"installDate": "2021-01-21_060319+0000",
"app_version_code": "63766",
"firstLaunchDate": "2021-01-21_060358+0000",
"ivc": false,
"model": "sdk_gphone_x86_64_arm64",
"lang": "English",
"brand": "google",
"batteryLevel": "77.0",
"deviceType": "userdebug",
"product": "sdk_gphone_x86_64_arm64",
"advertiserId":
  "827d8162-0e1c-48cd-892e-4abd3df95ba8",
```

```
"deviceData": {
  "sensors": [ {
    "sT": 1,
    "sVS": [0.7662141, 9.013549, 3.795387],
    "sN": "Goldfish 3-axis Accelerometer",
    "sV": "The Android Open Source Project",
    "sVE": [0.7662141, 9.013549, 3.795387]
  },
  {
    "sT": 2,
    "sVS": [-17.875, 24.125, -38.4375],
    "sN": "Goldfish 3-axis Magnetic field sensor",
    "sV": "The Android Open Source Project",
    "sVE": [-17.875, 24.125, -38.4375]
  },
  {
    "sT": 4,
    "sVS": [0, 0, 0],
    "sN": "Goldfish 3-axis Gyroscope",
    "sV": "The Android Open Source Project",
    "sVE": [0, 0, 0]
  }
] }
```

Indeed Job Search unter Android

POST `https://t.appsflyer.com/api/v4/androidevent`
`?buildnumber=4.10.3&app_id=com.indeed.android.jobsearch`

```
"af_timestamp": "1611209035694",
"appsflyerKey": "ExLocXqS6j9TGyNebHQHrG",
"operator": "T-Mobile",
"network": "MOBILE",
"timepassedsincelastlaunch": "-1",
"open_referrer": "android-app://android",
"af_v2": "e1089f09b150658adadbacd6f807c1947d072cb2",
"uid": "1611209035909-2664535545820779500",
"isGaidWithGps": "true",
"lang_code": "en",
"installDate": "2021-01-21_060319+0000",
"app_version_code": "63766",
"firstLaunchDate": "2021-01-21_060358+0000",
"ivc": false,
"model": "sdk_gphone_x86_64_arm64",
"lang": "English",
"brand": "google",
"batteryLevel": "77.0",
"deviceType": "userdebug",
"product": "sdk_gphone_x86_64_arm64",
"advertiserId":
  "827d8162-0e1c-48cd-892e-4abd3df95ba8",
```

```
"deviceData": {
  "sensors": [ {
    "sT": 1,
    "sVS": [0.7662141, 9.013549, 3.795387],
    "sN": "Goldfish 3-axis Accelerometer",
    "sV": "The Android Open Source Project",
    "sVE": [0.7662141, 9.013549, 3.795387]
  },
  {
    "sT": 2,
    "sVS": [-17.875, 24.125, -38.4375],
    "sN": "Goldfish 3-axis Magnetic field sensor",
    "sV": "The Android Open Source Project",
    "sVE": [-17.875, 24.125, -38.4375]
  },
  {
    "sT": 4,
    "sVS": [0, 0, 0],
    "sN": "Goldfish 3-axis Gyroscope",
    "sV": "The Android Open Source Project",
    "sVE": [0, 0, 0]
  }
] }
```

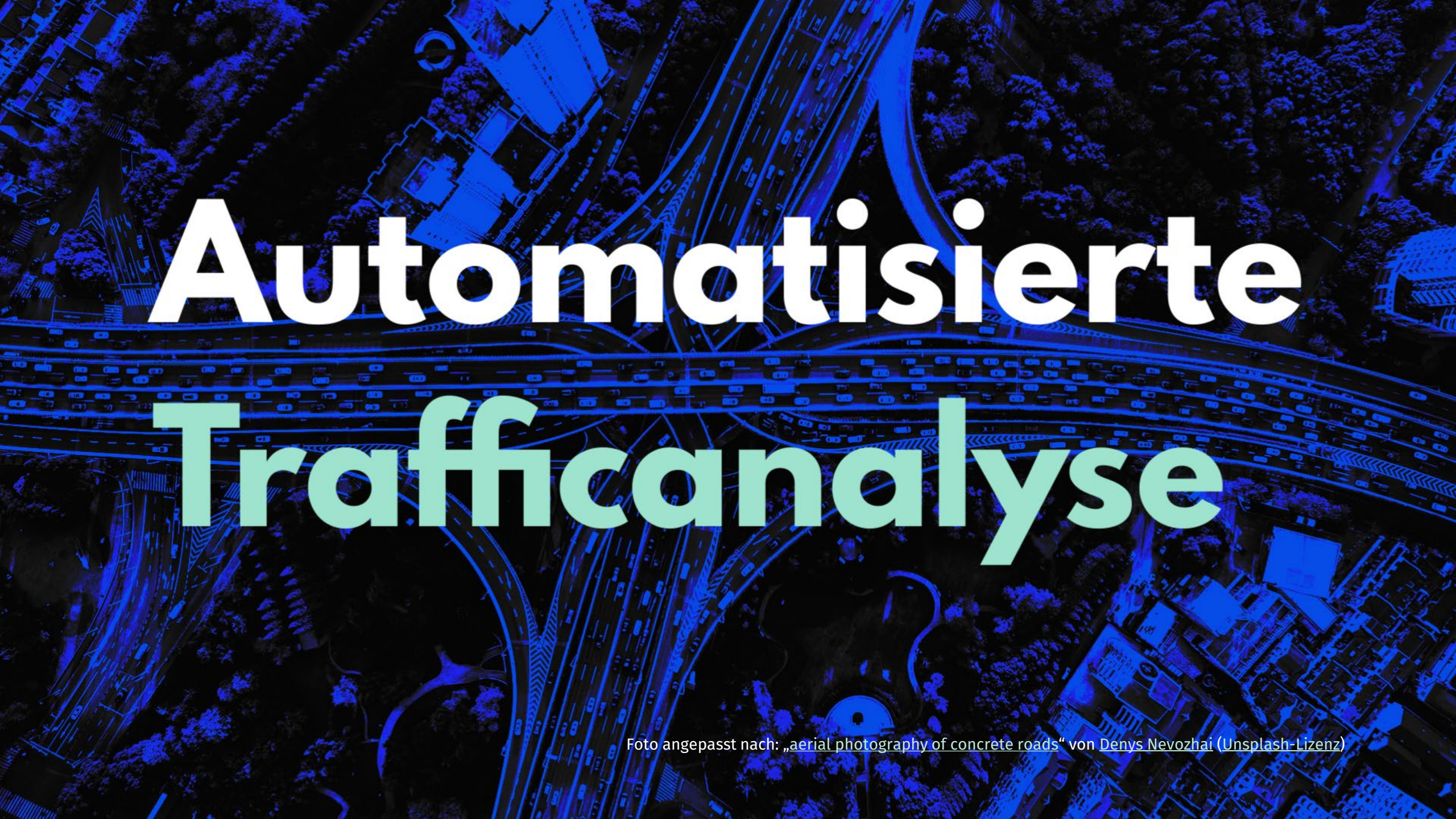
Poparazzi unter iOS

POST `https://poparazzi.com/api/contacts`

```
"data": [  
  {  
    "attributes": {  
      "is_profile_photo": true,  
      "last_name": "TBFFZbBYea",  
      "phone_numbers": ["+4915557543434"],  
      "full_name": "JGKfozntbF TBFFZbBYea",  
      "clean_name": "JGKfozntbF TBFFZbBYea",  
      "is_emoji": false,  
      "first_name": "JGKfozntbF"  
    },  
    "type": "contacts",  
    "id": "3A575DFF-C7FC-4F13-B40D-89D52F208C15:ABPerson"  
  },  
]  
]
```



Alle Kontakte aus
dem Adressbuch



Automatisierte Trafficanalyse

Foto angepasst nach: „aerial photography of concrete roads“ von [Denys Nevozhai](#) (Unsplash-Lizenz)

Setup unter Android

Android ist einfacher zu
instrumentieren. Fangen wir da an.

Analyseumgebung

- Android Emulator mit root

Analyseumgebung

- Android Emulator mit root
- Instrumentierung über adb, z. B.:
 - App installieren: `adb install-multiple -g <*.apk>`
 - App deinstallieren: `adb shell pm uninstall --user 0 <app_id>`
 - Zurücksetzen des Emulators: `adb emu avd snapshot load <name>`

Analyseumgebung

- Android Emulator mit root
- Instrumentierung über adb, z. B.:
 - App installieren: `adb install-multiple -g <*.apk>`
 - App deinstallieren: `adb shell pm uninstall --user 0 <app_id>`
 - Zurücksetzen des Emulators: `adb emu avd snapshot load <name>`
- Apps kriegen alle Berechtigungen.

Analyseumgebung

- Android Emulator mit root
- Instrumentierung über adb, z. B.:
 - App installieren: `adb install-multiple -g <*.apk>`
 - App deinstallieren: `adb shell pm uninstall --user 0 <app_id>`
 - Zurücksetzen des Emulators: `adb emu avd snapshot load <name>`
- Apps kriegen alle Berechtigungen.
- Machine in the Middle: mitmproxy

Analyseumgebung

- Android Emulator mit root
- Instrumentierung über adb, z. B.:
 - App installieren: `adb install-multiple -g <*.apk>`
 - App deinstallieren: `adb shell pm uninstall --user 0 <app_id>`
 - Zurücksetzen des Emulators: `adb emu avd snapshot load <name>`
- Apps kriegen alle Berechtigungen.
- Machine in the Middle: mitmproxy
- Umgehung von Certificate Pinning: objection & Frida

objection vs. Certificate Pinning

```
const sslCertificateChecker: SSLCertificateChecker =  
    Java.use("nl.xservices.plugins.SSLCertificateChecker");  
const SSLCertificateCheckerExecute =  
    sslCertificateChecker.execute;  
  
SSLCertificateCheckerExecute.overload(  
    "java.lang.String", "org.json.JSONArray",  
    "org.apache.cordova.CallbackContext").implementation =  
    function (str, jsonArray, callBackContext) {  
        callBackContext.success("CONNECTION_SECURE");  
        return true;  
    };
```

objection vs. Certificate Pinning

```
const sslCertificateChecker: SSLCertificateChecker =  
  Java.use("nl.xservices.plugins.SSLCertificateChecker");  
const SSLCertificateCheckerExecute =  
  sslCertificateChecker.execute;
```

```
SSLCertificateCheckerExecute.overload(  
  "java.lang.String", "org.json.JSONArray",  
  "org.apache.cordova.CallbackContext").implementation =  
  function (str, jsonArray, callBackContext) {  
    callBackContext.success("CONNECTION_SECURE");  
    return true;  
  };
```

objection vs. Certificate Pinning

```
const sslCertificateChecker: SSLCertificateChecker =  
  Java.use("nl.xservices.plugins.SSLCertificateChecker");  
const SSLCertificateCheckerExecute =  
  sslCertificateChecker.execute;
```

```
SSLCertificateCheckerExecute.overload(  
  "java.lang.String", "org.json.JSONArray",  
  "org.apache.cordova.CallbackContext").implementation =  
  function (str, jsonArray, callBackContext) {  
    callBackContext.success("CONNECTION_SECURE");  
    return true;  
  };
```

objection vs. Certificate Pinning

```
const sslCertificateChecker: SSLCertificateChecker =  
  Java.use("nl.xservices.plugins.SSLCertificateChecker");  
const SSLCertificateCheckerExecute =  
  sslCertificateChecker.execute;
```

```
SSLCertificateCheckerExecute.overload(  
  "java.lang.String", "org.json.JSONArray",  
  "org.apache.cordova.CallbackContext").implementation =  
  function (str, jsonArray, callBackContext) {  
    callBackContext.success("CONNECTION_SECURE");  
    return true;  
  };
```

mitmproxy zeichnet den gesamten
Traffic auf – einschließlich des
Hintergrundrauschens vom System
und anderen Apps.

Uhr-Widget

POST <https://ssl.google-analytics.com/batch>

```
"a": "1399991084",
"utc": ["Digital Widget", "Digital Widget",
"Digital Widget"],
"aip": ["1", "1", "1"],
"an": ["Clock", "Clock", "Clock"],
"tid": ["UA-61414137-1", "UA-61414137-1", "UA-
61414137-1"],
"utt": ["20", "4", "1"],
"t": ["timing", "timing", "timing"],
"_s": ["5", "6", "7"],
"av": ["6.2 (259367952)", "6.2 (259367952)", "6.2
(259367952)"],
"utv": ["Widget Data Fetch", "Widget Data Fetch",
"Widget Data Fetch"],
"v": ["1", "1", "1"],
"_v": ["ma18.5.89", "ma18.5.89", "ma18.5.89"],
"ul": ["en-us", "en-us", "en-us"],
"aid": ["com.google.android.deskclock",
"com.google.android.deskclock",
"com.google.android.deskclock"],
"cid": [
    "beb20edf-6c5c-4e13-93bb-5a788210cb72",
    "beb20edf-6c5c-4e13-93bb-5a788210cb72",
    "beb20edf-6c5c-4e13-93bb-5a788210cb72"
],
"sr": ["1440x2392", "1440x2392", "1440x2392"],
"ht": ["1610975551964", "1610975553497",
"1611663930874"],
"qt": ["688540681", "688539148", "161771"],
"_gmsv": ["201.8.17\\na=1399991084",
"201.8.17\\na=1399991084", "201.8.17"]
```

```
and not
    (requests.host = 'android.googleapis.com' and requests.path = '/auth/devicekey')
and not (requests.host ~~ '%.googleapis.com' and requests.path ~~ '/google.internal%')
and not
    (requests.host ~~ 'www.googleapis.com' and requests.path ~~ '/androidantiabuse/%')
and not (requests.host ~~ 'www.googleapis.com' and
    requests.path ~~ '/androidcheck/v1/attestations%')
and not (requests.host ~~ 'play.googleapis.com' and requests.path = '/log/batch')
and not (requests.host ~~ 'www.googleapis.com'
    and requests.path ~~ '/experimentsandconfigs/%')
and not requests.host = '172.217.19.74'
and not (requests.host ~~ 'firebaseinstallations.googleapis.com' and
    requests.path ~~ '/v1/projects/google.com%')
and not (requests.host ~~ 'firebaseinstallations.googleapis.com' and
    requests.path ~~ '/v1/projects/metal-dimension-646%')
and not (requests.host ~~ 'firebaseinstallations.googleapis.com' and
    requests.path ~~ '/v1/projects/zillatest-20296%')
and not (requests.host ~~ '%gvt1.com' and requests.path ~~ '/edgedl/%')
and not requests.host ~~ 'update.googleapis.com'
and not (requests.host ~~ 'www.gstatic.com' and requests.path ~~ '/android%')
and not (requests.host = 'www.google.com' and requests.path = '/loc/m/api')
and not (requests.host = 'ssl.gstatic.com' and requests.path ~ '/suggest-dev/yt')
and not (requests.host = 'android.googleapis.com' and requests.path = '/checkin')
and not (requests.host = 'www.gstatic.com' and requests.path ~ '/commerce/wallet')
and not (requests.host = 'app-measurement.com' and
    requests.path ~ '/config/app/1%3A357317899610%3Aandroid%3A4765c0ded882c665')
and not (requests.host = 'app-measurement.com' and
    requests.path ~ '/config/app/1%3A1086610230652%3Aandroid%3A131e4c3db28fca84')
```

```
and not (requests.host = 'app-measurement.com' and
```


🔗 Usage examples

Fetch app top charts

The following example fetches the current top 100 free apps across all categories for Germany:

```
import { fetchTopCharts } from 'parse-play';

(async () => {
  const topChart = await fetchTopCharts(
    { category: 'APPLICATION', chart: 'topselling_free', count: 100 },
    { country: 'DE', language: 'EN' }
  );

  console.log(topChart?.length); // 100
  console.log(topChart?.[0]?.app_id, topChart?.[0]?.name); // com.amazon.mShop.android.shopping Amazon Shopping
})();
```

You can also request multiple top charts at once. These will all be fetched in a single API request. Note that country and language apply to *all* requests in a batch.

This example fetches the top 5 free education apps, as well as the top 1000 paid adventure game apps, both for the UK:

```
const topCharts = await fetchTopCharts(
  [
    { category: 'EDUCATION', chart: 'topselling_free', count: 5 },
    { category: 'GAME_ADVENTURE', chart: 'topselling_paid', count: 1000 },
  ],
  { country: 'GB', language: 'EN' }
);
```

Apps herunterladen

- Es gibt viele Tools, die APKs herunterladen können.
- Die gehen aber leider auch gerne mal kaputt.
- Wir haben folgende genutzt:
 - [matlink/gplaycli](#)
 - [ClaudiuGeorgiu/PlaystoreDownloader](#)
 - [89z/googleplay](#) (nach Sperrungen zuletzt bei [rngh7r/googleplay](#))
 - [EFForg/apkeep](#)

Setup unter iOS

Um iOS zu instrumentieren, müssen wir erst einiges an Reverse-Engineering betreiben.



SSL Kill Switch 2 gegen
Certificate-Pinning



checkra1n als Jailbreak
(beschränkt auf iOS 14)

SSL Kill Switch 2 gegen
Certificate-Pinning



An Apps zu kommen ist schwerer

- Offizielle Tools:
 - Apple Configurator 2: kann nur bereits gekaufte Apps
 - App Store auf ARM-Mac: eingeschränkte Auswahl an Apps
 - Alte iTunes-Version: funktioniert, aber schwer zu automatisieren

An Apps zu kommen ist schwerer

- Offizielle Tools:
 - Apple Configurator 2: kann nur bereits gekaufte Apps
 - App Store auf ARM-Mac: eingeschränkte Auswahl an Apps
 - Alte iTunes-Version: funktioniert, aber schwer zu automatisieren
- Inoffizielle Tools:
 - iMazing: kann nur bereits gekaufte Apps
 - 3uTools: sieht vielversprechend aus

iPhone

iPad



corona-warn-app



Apple ID:

frank.walther.1978@iclou...

 Featured

 Apps

Recommended

Popular

Monthly Rank

Total Rank

 Games

Recommended

Popular

Monthly Rank

Total Rank

 No iDevice

Downloaded files will be
saved to PC

" corona-warn-app " related items were not found.

Q

Search

Highlight

Intercept

Path	Method	Status	Size	Time
 http://app.pcrs.3u.com/app_list.action	POST	200	2.8kb	909ms
 https://is3-ssl.mzstatic.com/image/thumb/Purple118/v4/86/4d/17/864d17a1-b688-4338-b876-d8f3ef79c56c/source/100x100bb.jpg	GET	200	7.6kb	1s
 https://is1-ssl.mzstatic.com/image/thumb/Purple124/v4/25/09/96/250996de-0d44-b65b-18fd-7fed8fff1183/source/100x100bb.jpg	GET	200	6.9kb	1s
 https://buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/authenticate	POST	200	3.7kb	2min
 http://app.pcrs.3u.com/stats_operate.action?objType=1&optType=1	POST	200	40b	679ms
 http://ios.pclog.3u.com/log/info/uploadLog.go?type=2	POST	200	771b	5s
 https://buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct	POST	200	11.1kb	2min
 https://buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownloadDone?Pod=22&songId=437818260&guid=50360D5F.8DD1C091.00000000.BA131198.4806E085.0EE93C0B.8AE9939D&download-id...	GET	302	0	4s
 https://p59-buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownloadDone?songId=437818260&guid=50360D5F.8DD1C091.00000000.BA131198.4806E085.0EE93C0B.8AE9939D&download-id=590...	GET	200	228b	4s
 http://ios.pclog.3u.com/log/info/uploadLog.go?type=3	POST	200	385b	307ms
 http://ios.pclog.3u.com/log/info/uploadLog.go?type=2	POST	200	937b	560ms

Path	Method	Status	Size	Time
 http://app.pcrs.3u.com/app_list.action	POST	200	2.8kb	909ms
 https://is3-ssl.mzstatic.com/image/thumb/Purple118/v4/86/4d/17/864d17a1-b688-4...	GET	200	7.6kb	1s
 https://is1-ssl.mzstatic.com/image/thumb/Purple124/v4/25/09/96/2509996de-0d44-b...	GET	200	6.9kb	1s
 https://buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/authenticate	POST	200	3.7kb	2min
 http://app.pcrs.3u.com/stats_operate.action?objType=1&optType=1	POST	200	40b	679ms
 http://ios.pclg.3u.com/log/info/uploadLog.go?type=2	POST	200	771b	5s
 https://buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct	POST	200	11.1kb	2min
 https://buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownloadD...	GET	302	0	4s
 https://p59-buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownlo...	GET	200	228b	4s
 http://ios.pclg.3u.com/log/info/uploadLog.go?type=3	POST	200	385b	307ms
 http://ios.pclg.3u.com/log/info/uploadLog.go?type=2	POST	200	937b	560ms

Request	Response	Details
POST https://buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct HTTP/1.1		
Host	buy.itunes.apple.com	
User-Agent	iTunes/11.4 (Windows; Microsoft Windows 7 x86 Ultimate Edition Service Pack 1 (Build 7601)) AppleWebKit/536.30.1	
Accept	*/*	
Cookie	ns-mzf-inst=104-14-443-52-240-9019-597195-59-st44; countryVerified=1; hsacctnt=1; mzf_in=597195; session-store-id=933443C4AC59F08CD0BC4688F05D8816; NSC_nagjobodf-bopo-qppm*0=ffffffff0944761c45525d5f4f58455e445a4a42378b; mz_mt0-20235749998=AnImEeO9CRmJkIVUspw1c8WHpG5kTDHJyLd+EvyH10j3Hfqo/zsYZ3n51b8oKEuhFx5afVXKezcnHADahDcGvP21sJgUg8xtcz+dHoryivpmVQM2+m2mV6ZSPR07NZ4PKJT9IQrcbv6bL5A6OS/2KxmxP8ipP5cnCGwF70xGBFIIAG1ZjG1zz+JiiDzvfTMjYJ9I8I=; X-Dsid=20235749998; itspod=59; mz_at0-20235749998=AwQAAAECAAGvQAAAAABgrlGk4w2EaacJH7Y638o4kjh+KnglHv0=; mz_at_ssl-20235749998=AwUAAAECAA GvQAAAAABgrlGkaLZyfjxplH7YlN1yZnwbVmzJvtA=; pldfltcdid=ec8960372f244c3db043866ab575bb91059; vrep=CO6U1LFLEgQIBRAAEgQICBAAEgQICHA AEgQIEBAAEgQIAHAAEgQIBxAAEgQIDxAAEgQIARAMEgQICRAAEgQIERAAEgQIAx AA E g Q I D R A A E g Q I B h A A E g Q I B B A A E g Q I C x A A E g Q I D h A A E g Q I D B A A ; wosid-lite=7WV4fPoxJJWF4bbfun8BF0	
X-Apple-Store-Front	143443-1,17	
Content-Type	application/x-apple-plist	
Cache-Control	no-cache	
Referer	http://itunes.apple.com/cn/app//id1225032527?mt=8	
Accept-Language	zh-cn, zh;q=0.5	
X-Apple-Tz	28800	
X-Token	AwIAAAECAAGvQAAAAABgrlGkf7sNCsrOrfwplAtNZOYjaKlZHyI=	
X-Dsid	20235749998	
Connection	Close	
Content-Length	1323	
<pre><?xml version="1.0" encoding="UTF-8"?> <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd"> <plist version="1.0"> <dict></pre>		

mitmproxy

StartOptionsFlow

Replay

Duplicate

Revert

Delete

Download

Export

Resume

Abort

Flow Modification

Export

Interception

Path	Method	Status	Size	Time
http://app.pcrs.3u.com/app_list.action	POST	200	2.8kb	909ms
https://is3-ssl.mzstatic.com/image/thumb/Purple118/v4/86/4d/17/864d17a1-b688-4...	GET	200	7.6kb	1s
https://is1-ssl.mzstatic.com/image/thumb/Purple124/v4/25/09/96/250996de-0d44-b...	GET	200	6.9kb	1s
https://buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/authenticate	POST	200	3.7kb	2min
http://app.pcrs.3u.com/stats_operate.action?objType=1&optType=1	POST	200	40b	679ms
http://ios.pcllog.3u.com/log/info/uploadLog.go?type=2	POST	200	771b	5s
https://buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct	POST	200	11.1kb	2min
https://buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownloadD...	GET	302	0	4s
https://p59-buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownlo...	GET	200	228b	4s
http://ios.pcllog.3u.com/log/info/uploadLog.go?type=3	POST	200	385b	307ms
http://ios.pcllog.3u.com/log/info/uploadLog.go?type=2	POST	200	937b	560ms

RequestResponseDetails

HTTP/1.1 200 OK

```
{
  "co": 20,
  "list": [
    {
      "appname": "Clash For Dawn-3D PVP MMORPG",
      "downloaded": "2",
      "icon": "https://is3-ssl.mzstatic.com/image/thumb/Purple118/v4/86/4d/17/864d17a1-b688-4...",
      "id": 4482,
      "isfull": 0,
      "itemid": "994842141",
      "longversion": "2.0.3",
      "md5": "",
      "minversion": "7.0",
      "path": "",
      "pkgatype": 1,
      "shortversion": "2.0.3",
      "sizebyte": "118799360",
      "slogan": "Clash For Dawn-3D PVP MMORPG - LEDO",
      "slogancolor": "#f0f0f0",
      "sort": 2,
      "sourceid": "com.wanmei.mini.dod.ios.ledo",
      "version": "2.0.3",
      "versionid": "0"
    },
    {
      "appname": "C-Date",
      "downloaded": "2",
      "icon": "https://is3-ssl.mzstatic.com/image/thumb/Purple115/v4/5b/b0/dd/5bb0dd36-303...",
      "id": 1775,
      "isfull": 0,
      "itemid": "1078584965",
      "longversion": "4",
      "md5": "",
      "minversion": "12.0"
    }
  ]
}
```

8080v6.0.2

Die einzig logische Lösung

```
def response(self, flow: http.HTTPFlow):
    if (flow.request.pretty_url == "http://app.p cres.3u.com/app_list.action"):
        i = int(flow.request.urlencoded_form.get("page")) - 1
        apps = self.apps[0+i*20:20+i*20]
        res_apps = [{
            "versionid": "0",
            "icon": f"https://via.placeholder.com/100?text={a['buyData']['bundle-id']}",
            "itemid": a['id'],
            "id": idx + i * 20,
            "slogancolor": "#f0f0f0",
            "appname": a['name'],
            "sourceid": a['buyData']['bundle-id'],
            "minversion": a['buyData']['minimum-os-version'],
            "sizebyte": a['buyData']['file-size'],
            "longversion": a['buyData']['minimum-os-version'],
            # [...]
        } for idx, a in enumerate(apps)]
        res = { "success": True, "type": 104, "list": res_apps, "co": 20 }
        flow.response.content = json.dumps(res).encode("utf-8")
```

Die einzig logische Lösung

```
def response(self, flow: http.HTTPFlow):  
    if (flow.request.pretty_url == "http://app.p cres.3u.com/app_list.action") :  
        i = int(flow.request.urlencoded_form.get("page")) - 1  
        apps = self.apps[0+i*20:20+i*20]  
        res_apps = [{  
            "versionid": "0",  
            "icon": f"https://via.placeholder.com/100?text={a['buyData']['bundle-id']}",  
            "itemid": a['id'],  
            "id": idx + i * 20,  
            "slogancolor": "#f0f0f0",  
            "appname": a['name'],  
            "sourceid": a['buyData']['bundle-id'],  
            "minversion": a['buyData']['minimum-os-version'],  
            "sizebyte": a['buyData']['file-size'],  
            "longversion": a['buyData']['minimum-os-version'],  
            # [...]  
        } for idx, a in enumerate(apps)]  
        res = { "success": True, "type": 104, "list": res_apps, "co": 20 }  
        flow.response.content = json.dumps(res).encode("utf-8")
```


Die einzig logische Lösung

```
def response(self, flow: http.HTTPFlow):
    if (flow.request.pretty url == "http://app.pcres.3u.com/app_list.action"):
        i = int(flow.request.urlencoded_form.get("page")) - 1
        apps = self.apps[0+i*20:20+i*20]
        res_apps = [{
            "versionid": "0",
            "icon": f"https://via.placeholder.com/100?text={a['buyData']['bundle-id']}",
            "itemid": a['id'],
            "id": idx + i * 20,
            "slogancolor": "#f0f0f0",
            "appname": a['name'],
            "sourceid": a['buyData']['bundle-id'],
            "minversion": a['buyData']['minimum-os-version'],
            "sizebyte": a['buyData']['file-size'],
            "longversion": a['buyData']['minimum-os-version'],
            # [...]
        } for idx, a in enumerate(apps)]
        res = { "success": True, "type": 104, "list": res_apps, "co": 20 }
        flow.response.content = json.dumps(res).encode("utf-8")
```

Die einzig logische Lösung

```
def response(self, flow: http.HTTPFlow):
    if (flow.request.pretty_url == "http://app.p cres.3u.com/app_list.action"):
        i = int(flow.request.urlencoded_form.get("page")) - 1
        apps = self.apps[0+i*20:20+i*20]
        res_apps = [{
            "versionid": "0",
            "icon": f"https://via.placeholder.com/100?text={a['buyData']['bundle-id']}",
            "itemid": a['id'],
            "id": idx + i * 20,
            "slogancolor": "#f0f0f0",
            "appname": a['name'],
            "sourceid": a['buyData']['bundle-id'],
            "minversion": a['buyData']['minimum-os-version'],
            "sizebyte": a['buyData']['file-size'],
            "longversion": a['buyData']['minimum-os-version'],
            # [...]
        } for idx, a in enumerate(apps)]
        res = { "success": True, "type": 104, "list": res_apps, "co": 20 }
        flow.response.content = json.dumps(res).encode("utf-8")
```

Die einzig logische Lösung

```
def response(self, flow: http.HTTPFlow):
    if (flow.request.pretty_url == "http://app.p cres.3u.com/app_list.action"):
        i = int(flow.request.urlencoded_form.get("page")) - 1
        apps = self.apps[0+i*20:20+i*20]
        res_apps = [{
            "versionid": "0",
            "icon": f"https://via.placeholder.com/100?text={a['buyData']['bundle-id']}",
            "itemid": a['id'],
            "id": idx + i * 20,
            "slogancolor": "#f0f0f0",
            "appname": a['name'],
            "sourceid": a['buyData']['bundle-id'],
            "minversion": a['buyData']['minimum-os-version'],
            "sizebyte": a['buyData']['file-size'],
            "longversion": a['buyData']['minimum-os-version'],
            # [...]
        } for idx, a in enumerate(apps)]
        res = { "success": True, "type": 104, "list": res_apps, "co": 20 }
        flow.response.content = json.dumps(res).encode("utf-8")
```

iPhone

iPad

< >

↺

Search app & games

🔍

Apple ID:

frank.walther.1978@iclou...

👑 Featured

📱 Apps

Recommended

Popular

Monthly Rank

Total Rank

🎮 Games

Recommended

Popular

Monthly Rank

Total Rank

🔌 No iDevice

Downloaded files will be saved to PC

Recommended

Choose category: ALL



1. luca app

1.0.0 | 27.68MB

1. luca app

Download



2. Google Arts & Culture

1.0.0 | 111.11MB

2. Google Arts & Culture

Download



3. Poparazzi

1.0.0 | 68.32MB

3. Poparazzi

Download



4. Darf ich das?

1.0.0 | 26.78MB

4. Darf ich das?

Download



5. CapCut

1.0.0 | 118.52MB

5. CapCut

Download



6. Like A Dino!

1.0.0 | 51.85MB

6. Like A Dino!

Download



7. Signal - Sicherer Messenger

1.0.0 | 164.76MB

7. Signal - Sicherer Messenger

Download



8. Google Maps - Transit & Essen

1.0.0 | 222.63MB

8. Google Maps - Transit & Essen

Download



9. PayPal

1.0.0 | 280.98MB

9. PayPal

Download



10. Instagram

1.0.0 | 167.3MB

10. Instagram

Download



11. TikTok

1.0.0 | 399.52MB

11. TikTok

Download



12. Klarna | Shop now. Pay later.

1.0.0 | 172.34MB

12. Klarna | Shop now. Pay later.

Download

☐ Close iTunes

V2.56

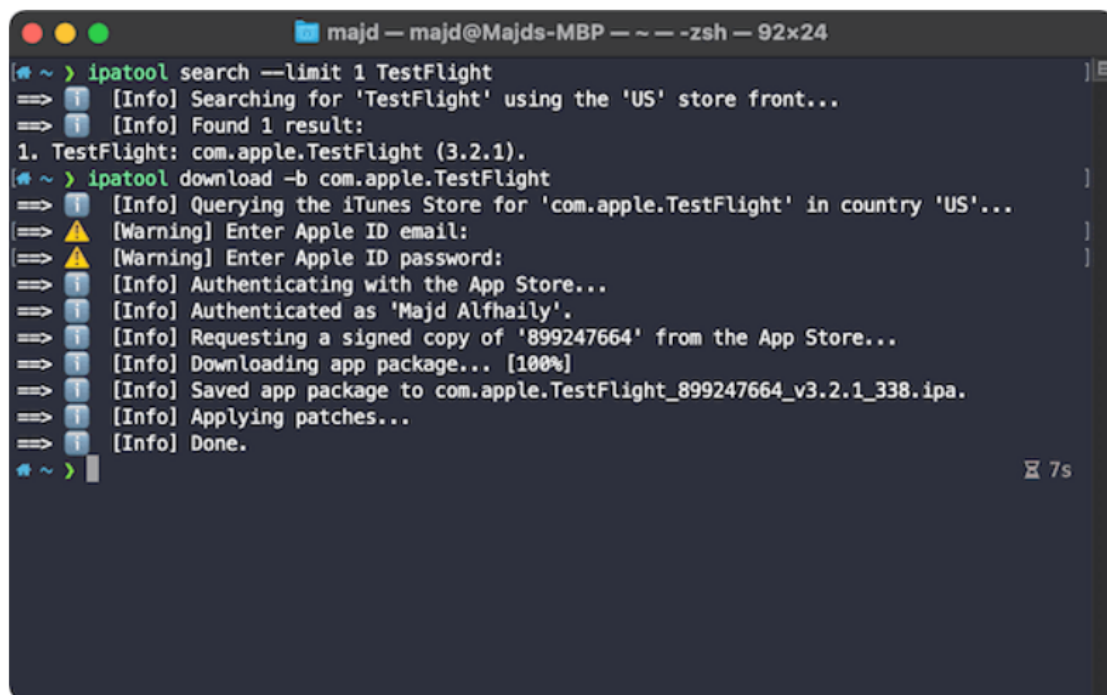
Feedback

Check Update

🔗 IPATool

Release **v2.0.0** License **MIT** Unit Tests **passing** Integration Tests **failing** Swift **5.5** macOS **10.15+**

`ipatool` is a command line tool that allows you to search for iOS apps on the [App Store](#) and download a copy of the app package, known as an *ipa* file.



```
majd — majd@Majds-MBP — — -zsh — 92x24
[~] > ipatool search --limit 1 TestFlight
=> [Info] Searching for 'TestFlight' using the 'US' store front...
=> [Info] Found 1 result:
1. TestFlight: com.apple.TestFlight (3.2.1).
[~] > ipatool download -b com.apple.TestFlight
=> [Info] Querying the iTunes Store for 'com.apple.TestFlight' in country 'US'...
=> [Warning] Enter Apple ID email:
=> [Warning] Enter Apple ID password:
=> [Info] Authenticating with the App Store...
=> [Info] Authenticated as 'Majd Alfhaily'.
=> [Info] Requesting a signed copy of '899247664' from the App Store...
=> [Info] Downloading app package... [100%]
=> [Info] Saved app package to com.apple.TestFlight_899247664_v3.2.1_338.ipa.
=> [Info] Applying patches...
=> [Info] Done.
[~] >
```

- [Requirements](#)
- [Installation](#)
 - [Manual](#)

Fixes #28: Add support for buying new apps #51

[New issue](#)

Merged majd merged 1 commit into `majd:main` from `baltpeter:b_buy-apps` on Mar 21

Conversation 1

Commits 1

Checks 6

Files changed 7

+239 -13



baltpeter commented on Mar 20 • edited

Contributor ...

Thank you very much for building and open-sourcing ipatool! I'm doing research on data protection in Android and iOS apps, so this is very helpful.

Previously, I was (ab)using [3uTools](#) for downloading IPAs but having to do that manually through a GUI was of course very cumbersome for the thousands of apps I need.

This PR adds support for downloading apps the used Apple ID doesn't already own (and thus [fixes #28](#)), a feature I need.

This is based on quite a lot of trial and error, and fighting with Apple's servers. I've looked at the network traffic of every program that can download IPAs that I could find. As you said, Apple Configurator 2 doesn't have the capability to buy new apps (same for tools based on that API, like iMazing). But older versions of iTunes could also download and buy apps (3u's mechanism is based on that, and I've also observed the same requests from the iOS App Store a year ago, though they seem to have changed that since...) through this endpoint:

```
https://buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct
```

Surprisingly, this endpoint also works with a Configurator user agent and corresponding auth cookies, though it behaves a little differently for that (for iTunes, it returns essentially the same information as the `volumeStoreDownloadProduct` endpoint, but for Configurator, it doesn't include the download URL in the response). Luckily, it seems like many of the parameters iTunes sets (including the dreaded `kbsync`) aren't actually necessary and can just be left out from the request.

I've tested this on two different Apple IDs, so hopefully it should work universally.



Fixes [majd#28](#): Add support for buying new apps

✓ 3fe990a

<https://github.com/majd/ipatool/pull/51>


```
user@users-iMac-Pro ~ % ipatool download --country de --email $user --password $password -a 284602850

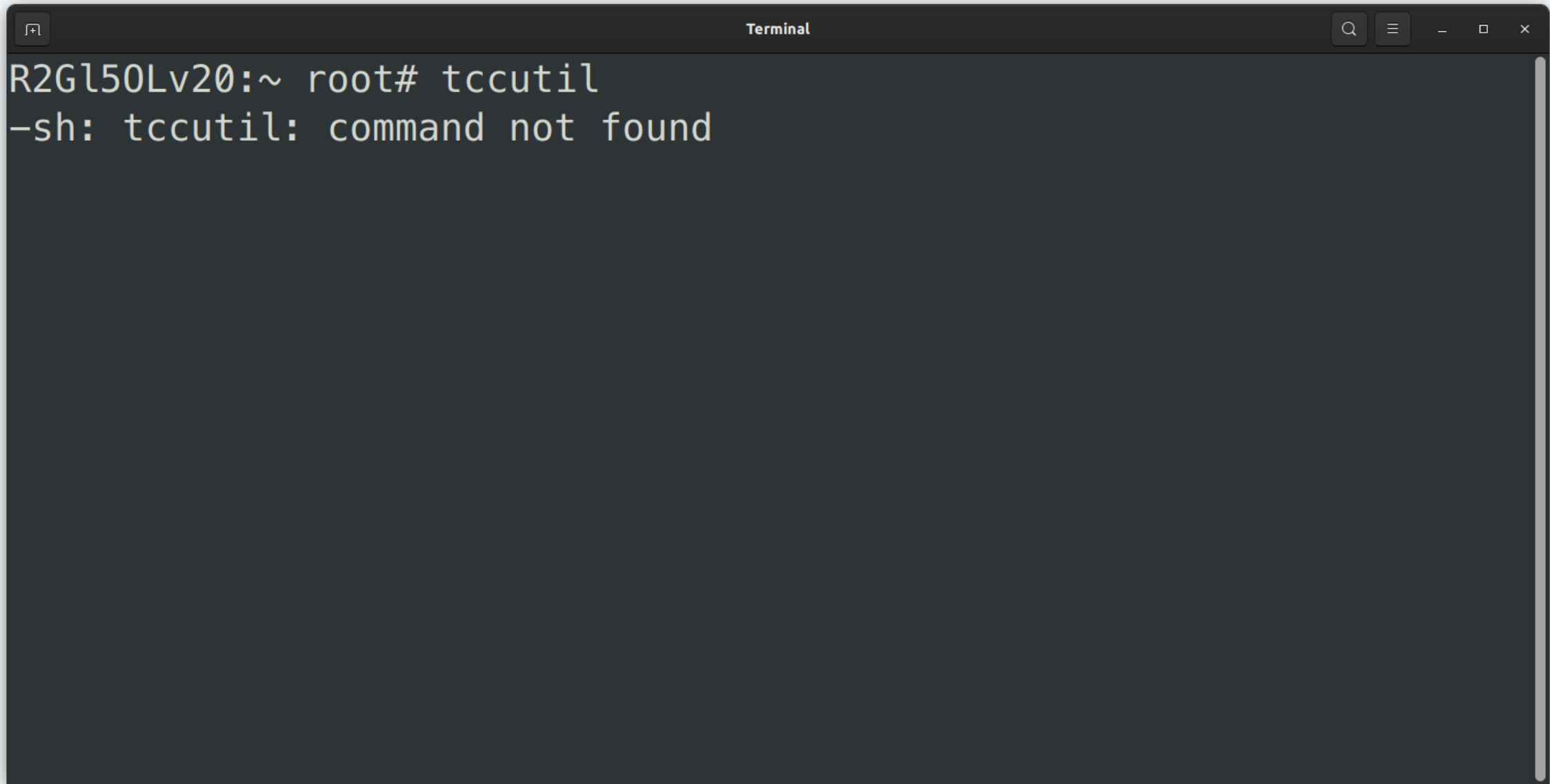
==> [i] [Info] Authenticating with the App Store...
==> [i] [Info] Authenticated as 'Vanessa Amsel'.
==> [i] [Info] Requesting a signed copy of '284602850' from the App Store...
==> [i] [Info] Downloading app package... [100%]
==> [i] [Info] Saved app package to 284602850.ipa.
==> [i] [Info] Applying patches...
==> [i] [Info] Done.
```

Instrumentierung

- Configurator 2 kann Apps verwalten:
 - Installieren: `cfgutil install-app "<file.ipa>"`
 - Deinstallieren: `cfgutil remove-app "<bundle_id>"`
- Unter Linux geht das mit `libimobiledevice`:
 - Installieren: `ideviceinstaller --install "<file.ipa>"`
 - Deinstallieren: `ideviceinstaller --uninstall "<bundle_id>"`

Instrumentierung

- Configurator 2 kann Apps verwalten:
 - Installieren: `cfgutil install-app "<file.ipa>"`
 - Deinstallieren: `cfgutil remove-app "<bundle_id>"`
- Unter Linux geht das mit `libimobiledevice`:
 - Installieren: `ideviceinstaller --install "<file.ipa>"`
 - Deinstallieren: `ideviceinstaller --uninstall "<bundle_id>"`
- Mit Activator können über SSH weitere Aktionen ausgeführt werden:
 - Home-Button drücken: `activator send libactivator.system.homebutton`
 - App starten: `activator send "<bundle_id>"`
 - Liste aller Aktionen: `activator listeners`

A terminal window with a dark background and a title bar labeled "Terminal". The title bar includes standard window controls (minimize, maximize, close) and a search icon. The terminal content shows a user prompt "R2Gl50Lv20:~ root#" followed by the command "tccutil". The output is "-sh: tccutil: command not found".

```
R2Gl50Lv20:~ root# tccutil
-sh: tccutil: command not found
```

```
Terminal
R2Gl50Lv20:~ root# tccutil
-sh: tccutil: command not found
R2Gl50Lv20:~ root# ps | grep tccd
 2253 ttys000      0:00.01 grep tccd
```

```
Terminal
R2Gl50Lv20:~ root# tccutil
-sh: tccutil: command not found
R2Gl50Lv20:~ root# ps | grep tccd
  2253 ttys000      0:00.01 grep tccd
R2Gl50Lv20:~ root# find / -name "TCC.db"
find: '/.fsevents': Operation not permitted
find: '/private/var/.fsevents': Operation not permitted
/private/var/mobile/Library/TCC/TCC.db
/private/var/root/Library/TCC/TCC.db
R2Gl50Lv20:~ root#
```



```
Terminal
R2Gl50Lv20:~ root# tccutil
-sh: tccutil: command not found
R2Gl50Lv20:~ root# ps | grep tccd
 2253 ttys000      0:00.01 grep tccd
R2Gl50Lv20:~ root# find / -name "TCC.db"
find: '/.fsevents': Operation not permitted
find: '/private/var/.fsevents': Operation not permitted
/private/var/mobile/Library/TCC/TCC.db
/private/var/root/Library/TCC/TCC.db
R2Gl50Lv20:~ root#
```

Table: access

Filter in any column

	service	client	client_type	auth_value	auth_reason	auth_version	csreq	policy_id	indirect_object_idenfier_type	indirect_object_idenfier	indirect_object_code_identity	flags	last_modified
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	kTCCServiceMotion	com.apple.Health	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620829599
2	kTCCServiceLiverpool	com.apple.Health	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991202
3	kTCCServiceUbiquity	com.apple.mobilesafari	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991211
4	kTCCServiceUbiquity	com.apple.iBooks	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991213
5	kTCCServiceUbiquity	com.apple.Passbook	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991213
6	kTCCServiceUbiquity	com.apple.MailCompositionService	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991213
7	kTCCServiceUbiquity	com.apple.mobilemail	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991213
8	kTCCServiceUbiquity	com.apple.DocumentsApp	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991214
9	kTCCServiceUbiquity	com.apple.shortcuts	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991214
10	kTCCServiceLiverpool	com.apple.shortcuts	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991272
11	kTCCServiceLiverpool	com.apple.stocks	0	2	5	1	NULL	NULL	NULL	UNUSED	NULL	0	1621001132
12	kTCCServiceWebKitIntelli...	org.mozilla.ios.Firefox	0	2	5	1	NULL	NULL	NULL	UNUSED	NULL	0	1621081431
13	kTCCServiceWebKitIntelli...	com.apple.mobilesafari	0	2	5	1	NULL	NULL	NULL	UNUSED	NULL	0	1621081877
14	kTCCServiceLiverpool	com.apple.upload-request-...	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1623176245
15	kTCCServiceLiverpool	com.apple.accessibility.Accessibility...	0	2	5	1	NULL	NULL	NULL	UNUSED	NULL	0	1623439707
16	kTCCServiceLiverpool	com.apple.security.cuttlefish	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1623440322

Table: access

Filter in any column

	service	client	client_type	auth_value	auth_reason	auth_version	csreq	policy_id	indirect_object_idenfier_type	indirect_object_idenfier	indirect_object_code_identity	flags	last_modified
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	kTCCServiceMotion	com.apple.Health	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620829599
2	kTCCServiceLiverpool	com.apple.Health	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991202
3	kTCCServiceUbiquity	com.apple.mobilesafari	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991211
4	kTCCServiceUbiquity	com.apple.iBooks	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991213
5	kTCCServiceUbiquity	com.apple.Passbook	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991213
6	kTCCServiceUbiquity	com.apple.MailCompositionService	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991213
7	kTCCServiceUbiquity	com.apple.mobilemail	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991213
8	kTCCServiceUbiquity	com.apple.DocumentsApp	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991214
9	kTCCServiceUbiquity	com.apple.shortcuts	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991214
10	kTCCServiceLiverpool	com.apple.shortcuts	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991272
11	kTCCServiceLiverpool	com.apple.stocks	0	2	5	1	NULL	NULL	NULL	UNUSED	NULL	0	1621001132
12	kTCCServiceWebKitIntelli..	org.mozilla.ios.Firefox	0	2	5	1	NULL	NULL	NULL	UNUSED	NULL	0	1621081431
13	kTCCServiceWebKitIntelli..	com.apple.mobilesafari	0	2	5	1	NULL	NULL	NULL	UNUSED	NULL	0	1621081877
14	kTCCServiceLiverpool	com.apple.upload-request-...	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1623176245
15	kTCCServiceLiverpool	com.apple.accessibility.Accessibility...	0	2	5	1	NULL	NULL	NULL	UNUSED	NULL	0	1623439707
16	kTCCServiceLiverpool	com.apple.security.cuttlefish	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1623440322

Table: access

Filter in any column

	service	client	client_type	auth_value	auth_reason	auth_version	csreq	policy_id	indirect_object_idenfier_type	indirect_object_idenfier	indirect_object_code_identity	flags	last_modified
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	kTCCServiceMotion	com.apple.Health	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620829599
2	kTCCServiceLiverpool	com.apple.Health	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991202
3	kTCCServiceUbiquity	com.apple.mobilesafari	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991211
4	kTCCServiceUbiquity	com.apple.iBooks	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991213
5	kTCCServiceUbiquity	com.apple.Passbook	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991213
6	kTCCServiceUbiquity	com.apple.MailCompositionService	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991213
7	kTCCServiceUbiquity	com.apple.mobilemail	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991213
8	kTCCServiceUbiquity	com.apple.DocumentsApp	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991214
9	kTCCServiceUbiquity	com.apple.shortcuts	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991214
10	kTCCServiceLiverpool	com.apple.shortcuts	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1620991272
11	kTCCServiceLiverpool	com.apple.stocks	0	2	5	1	NULL	NULL	NULL	UNUSED	NULL	0	1621001132
12	kTCCServiceWebKitIntelli...	org.mozilla.ios.Firefox	0	2	5	1	NULL	NULL	NULL	UNUSED	NULL	0	1621081431
13	kTCCServiceWebKitIntelli...	com.apple.mobilesafari	0	2	5	1	NULL	NULL	NULL	UNUSED	NULL	0	1621081877
14	kTCCServiceLiverpool	com.apple.upload-request-...	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1623176245
15	kTCCServiceLiverpool	com.apple.accessibility.Accessibility...	0	2	5	1	NULL	NULL	NULL	UNUSED	NULL	0	1623439707
16	kTCCServiceLiverpool	com.apple.security.cuttlefish	0	2	4	1	NULL	NULL	0	UNUSED	NULL	0	1623440322

Table: access

	service	client	client_type	auth_value	auth_reason	auth_version	direct_object_code_identity	flags	last_modified
	Filter	Filter	Filter	Filter	Filter	Filter		Fi...	Filter
1	kTCCServiceMotion	com.apple.Health		0	2	4		0	1620829599
2	kTCCServiceLiverpool	com.apple.Health		0	2	4		0	1620991202
3	kTCCServiceUbiquity	com.apple.mobilesafari		0	2	4		0	1620991211
4	kTCCServiceUbiquity	com.apple.iBooks		0	2	4		0	1620991213
5	kTCCServiceUbiquity	com.apple.Passbook		0	2	4		0	1620991213
6	kTCCServiceUbiquity	com.apple.MailCompositionService		0	2	4		0	1620991213
7	kTCCServiceUbiquity	com.apple.mobilemail		0	2	4		0	1620991213
8	kTCCServiceUbiquity	com.apple.DocumentsApp		0	2	4		0	1620991214
9	kTCCServiceUbiquity	com.apple.shortcuts		0	2	4		0	1620991214
10	kTCCServiceLiverpool	com.apple.shortcuts		0	2	4		0	1620991272
11	kTCCServiceLiverpool	com.apple.stocks		0	2	5	1 NULL NULL NULL	UNUSED	NULL 1621001132
12	kTCCServiceWebKitIntelli...	org.mozilla.ios.Firefox		0	2	5	1 NULL NULL NULL	UNUSED	NULL 1621081431
13	kTCCServiceWebKitIntelli...	com.apple.mobilesafari		0	2	5	1 NULL NULL NULL	UNUSED	NULL 1621081877
14	kTCCServiceLiverpool	com.apple.upload-request-...		0	2	4	1 NULL NULL 0	UNUSED	NULL 1623176245
15	kTCCServiceLiverpool	com.apple.accessibility.Accessibility...		0	2	5	1 NULL NULL NULL	UNUSED	NULL 1623439707
16	kTCCServiceLiverpool	com.apple.security.cuttlefish		0	2	4	1 NULL NULL 0	UNUSED	NULL 1623440322

auth_value == 0:
Berechtigung verweigert

auth_value == 2:
Berechtigung erteilt

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3 <plist version="1.0">
4 <dict>
5     <key>REQUEST_ACCESS_SERVICE_kTCCServiceSensorKitBedSensingWriting</key>
6     <string>Allow "%@" to Add Data for Research Purposes?</string>
7     <key>REQUEST_ACCESS_ALLOW_kTCCServiceGameCenterFriends</key>
8     <string>Allow</string>
9     <key>REQUEST_ACCESS_INFO_SUBSEQUENT_SERVICE_kTCCServiceExposureNotification</key>
10    <string>Only one region can notify you of possible exposure. Details associated with possible exposures—such as date, duration, and
Bluetooth signal strength—will be shared. These details help the app notify you of possible exposures.</string>
11    <key>REQUEST_ACCESS_INFO_SERVICE_kTCCServiceExposureNotification</key>
12    <string>Your iPhone can securely collect and share random IDs with nearby devices. The app can use these IDs to notify you if you
may have been exposed to COVID-19. The date, duration, and signal strength of an exposure will be shared with "%@".</string>
13    <key>REQUEST_LIMITED_AUTHORIZATION_BUTTON_TITLE_SERVICE_kTCCServicePrototype4Rights</key>
14    <string>Limited Proto4</string>
15    <key>REQUEST_ACCESS_DENY_kTCCServicePhotos</key>
16    <string>Don't Allow</string>
17    <key>REQUEST_ACCESS_SERVICE_kTCCServiceUserTracking</key>
18    <string>Allow "%@" to track your activity across other companies' apps and websites?</string>
19    <key>REQUEST_ACCESS_SERVICE_kTCCServiceReminders</key>
20    <string>"%@" Would Like to Access Your Reminders</string>
21    <key>REQUEST_ACCESS_SERVICE_kTCCServiceMediaLibrary</key>
22    <string>"%@" would like to access Apple Music, your music and video activity, and your media library</string>
23    <key>REQUEST_DEFAULT_PURPOSE_STRING_SERVICE_kTCCServiceBluetoothAlways</key>
24    <string>This will allow "%@" to find and connect to Bluetooth accessories. This app may also use Bluetooth to know when you're
nearby.</string>
25    <key>REQUEST_ACCESS_SERVICE_kTCCServiceFallDetection</key>
26    <string>Share Fall Detection Data With "%@"?</string>
27    <key>REQUEST_ACCESS_INFO_SERVICE_kTCCServiceFallDetection</key>
28    <string>If you choose to share, "%@" can receive data from Apple Watch if a fall is detected and follow up in case help is needed.</-
string>
29    <key>REQUEST_ACCESS_SERVICE_kTCCServiceGameCenterFriends</key>
30    <string>Allow "%@" to connect you with your Game Center friends?</string>
```



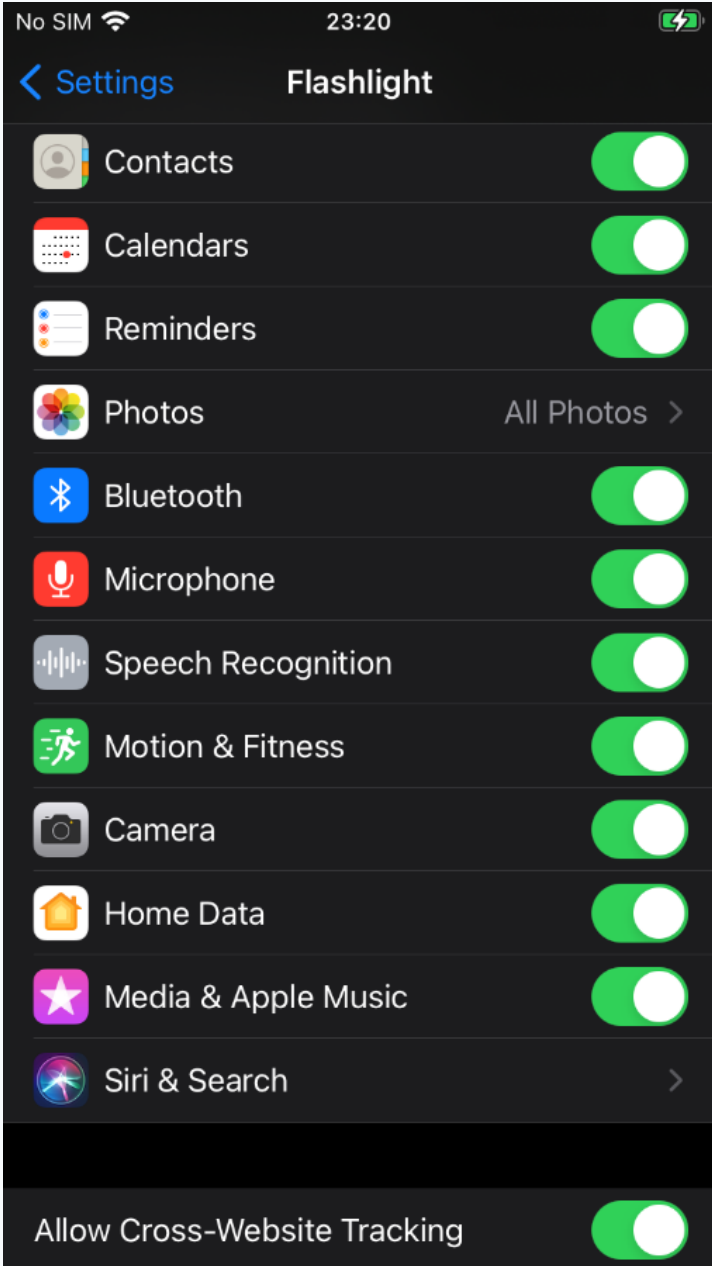
```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3 <plist version="1.0">
4 <dict>
5     <key>REQUEST_ACCESS_SERVICE_kTCCServiceSensorKitBedSensingWriting</key>
6     <string>Allow "%@" to Add Data for Research Purposes?</string>
7     <key>REQUEST_ACCESS_ALLOW_kTCCServiceGameCenterFriends</key>
8     <string>Allow</string>
9     <key>REQUEST_ACCESS_INFO_SUBSEQUENT_SERVICE_kTCCServiceExposureNotification</key>
10    <string>Only one region can notify you of possible exposure. Details associated with possible exposures—such as date, duration, and
Bluetooth signal strength—will be shared. These details help the app notify you of possible exposures.</string>
11    <key>REQUEST_ACCESS_INFO_SERVICE_kTCCServiceExposureNotification</key>
12    <string>Your iPhone can securely collect and share random IDs with nearby devices. The app can use these IDs to notify you if you
may have been exposed to COVID-19. The date, duration, and signal strength of an exposure will be shared with "%@".</string>
13    <key>REQUEST_LIMITED_AUTHORIZATION_BUTTON_TITLE_SERVICE_kTCCServicePrototype4Rights</key>
14    <string>Limited Proto4</string>
15    <key>REQUEST_ACCESS_DENY_kTCCServicePhotos</key>
16    <string>Don't Allow</string>
17    <key>REQUEST_ACCESS_SERVICE_kTCCServiceUserTracking</key>
18    <string>Allow "%@" to track your activity across other companies' apps and websites?</string>
19    <key>REQUEST_ACCESS_SERVICE_kTCCServiceReminders</key>
20    <string>"%" Would Like to Access Your Reminders</string>
21    <key>REQUEST_ACCESS_SERVICE_kTCCServiceMediaLibrary</key>
22    <string>"%" would like to access Apple Music, your music and video activity, and your media library</string>
23    <key>REQUEST_DEFAULT_PURPOSE_STRING_SERVICE_kTCCServiceBluetoothAlways</key>
24    <string>This will allow "%@" to find and connect to Bluetooth accessories. This app may also use Bluetooth to know when you're
nearby.</string>
25    <key>REQUEST_ACCESS_SERVICE_kTCCServiceFallDetection</key>
26    <string>Share Fall Detection Data With "%@"?</string>
27    <key>REQUEST_ACCESS_INFO_SERVICE_kTCCServiceFallDetection</key>
28    <string>If you choose to share, "%@" can receive data from Apple Watch if a fall is detected and follow up in case help is needed.</-
string>
29    <key>REQUEST_ACCESS_SERVICE_kTCCServiceGameCenterFriends</key>
30    <string>Allow "%@" to connect you with your Game Center friends?</string>
```



```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3 <plist version="1.0">
4 <dict>
5     <key>REQUEST_ACCESS_SERVICE_kTCCServiceSensorKitBedSensingWriting</key>
6     <string>Allow "%@" to Add Data for Research Purposes?</string>
7     <key>REQUEST_ACCESS_ALLOW_kTCCServiceGameCenterFriends</key>
8     <string>Allow</string>
9     <key>REQUEST_ACCESS_INFO_SUBSEQUENT_SERVICE_kTCCServiceExposureNotification</key>
10    <string>Only one region can notify you of possible exposure. Details associated with possible exposures—such as date, duration, and
Bluetooth signal strength—will be shared. These details help the app notify you of possible exposures.</string>
11    <key>REQUEST_ACCESS_INFO_SERVICE_kTCCServiceExposureNotification</key>
12    <string>Your iPhone can securely collect and share random IDs with nearby devices. The app can use these IDs to notify you if you
may have been exposed to COVID-19. The date, duration, and signal strength of an exposure will be shared with "%@".</string>
13    <key>REQUEST_LIMITED_AUTHORIZATION_BUTTON_TITLE_SERVICE_kTCCServicePrototype4Rights</key>
14    <string>Limited Proto4</string>
15    <key>REQUEST_ACCESS_DENY_kTCCServicePhotos</key>
16    <string>Don't Allow</string>
17    <key>REQUEST_ACCESS_SERVICE_kTCCServiceUserTracking</key>
18    <string>Allow "%@" to track your activity across other companies' apps and websites?</string>
19    <key>REQUEST_ACCESS_SERVICE_kTCCServiceReminders</key>
20    <string>"%@" Would Like to Access Your Reminders</string>
21    <key>REQUEST_ACCESS_SERVICE_kTCCServiceMediaLibrary</key>
22    <string>"%@" would like to access Apple Music, your music and video activity, and your media library</string>
23    <key>REQUEST_DEFAULT_PURPOSE_STRING_SERVICE_kTCCServiceBluetoothAlways</key>
24    <string>This will allow "%@" to find and connect to Bluetooth accessories. This app may also use Bluetooth to know when you're
nearby.</string>
25    <key>REQUEST_ACCESS_SERVICE_kTCCServiceFallDetection</key>
26    <string>Share Fall Detection Data With "%@"?</string>
27    <key>REQUEST_ACCESS_INFO_SERVICE_kTCCServiceFallDetection</key>
28    <string>If you choose to share, "%@" can receive data from Apple Watch if a fall is detected and follow up in case help is needed.</-
string>
29    <key>REQUEST_ACCESS_SERVICE_kTCCServiceGameCenterFriends</key>
30    <string>Allow "%@" to connect you with your Game Center friends?</string>
```

	service	Beschriftung in Einstellungen	Beschreibung
✓	kTCCServiceCalendar	Calendars	“Access Your Calendar”
✓	kTCCServiceAddressBook	Contacts	“Access Your Contacts”
✓	kTCCServiceReminders	Reminders	“Access Your Reminders”
✓	kTCCServicePhotos	Photos (All Photos)	“Access your photos”
✗	kTCCServicePhotosAdd	Photos (Add Photos Only)	“Add to your Photos”
✓	kTCCServiceMediaLibrary	Media & Apple Music	“Access Apple Music, your music and video activity, and your media library”
✓	kTCCServiceBluetoothAlways	Bluetooth	“Find and connect to Bluetooth accessories. This app may also use Bluetooth to know when you’re nearby.”
☐	kTCCServiceSpeechRecognition	Speech Recognition	“Access Speech Recognition”, “Speech data from this app will be sent to Apple to process your requests. This will also help Apple improve its speech recognition technology.”
✓	kTCCServiceMotion	Motion & Fitness	“Access Your Motion & Fitness Activity”
✗	kTCCServiceCamera	Camera	“Access the Camera”
✗	kTCCServiceMicrophone	Microphone	“Access the Microphone”
✓	kTCCServiceWillow	Home Data	“Access Your Home Data”

	service	Beschriftung in Einstellungen	Beschreibung
❑	kTCCServiceWebKitIntelligentTrackingPrevention	Allow Cross-Website Tracking	0 means do allow, 2 means don't allow
✓	kTCCServiceLiverpool	<i>kein sichtbarer Effekt</i>	maybe related to location access
✓	kTCCServiceUbiquity	<i>kein sichtbarer Effekt</i>	maybe related to iCloud
✗	kTCCServiceUserTracking	Allow Tracking	“Track your activity across other companies’ apps and websites”
❑	kTCCServiceSensorKitBedSensingWriting	<i>kein sichtbarer Effekt</i>	“Add Data for Research Purposes”, “Record bed sensing Sensor & Usage data”
❑	kTCCServiceGameCenterFriends	<i>kein sichtbarer Effekt</i>	“Connect you with your Game Center friends”
❑	kTCCServicePrototype3Rights	<i>kein sichtbarer Effekt</i>	“Authorization to Test Service Proto3Right”
❑	kTCCServicePrototype4Rights	<i>kein sichtbarer Effekt</i>	“Authorization to Test Service Proto4Right”
❑	kTCCServiceFallDetection	<i>kein sichtbarer Effekt</i>	“Receive data from Apple Watch if a fall is detected and follow up in case help is needed”
❑	kTCCServiceSiri	<i>kein sichtbarer Effekt</i>	“Some of your %@ data will be sent to Apple to process your requests.”
❑	kTCCServiceBluetoothPeripheral	<i>kein sichtbarer Effekt</i>	“Make data available to nearby Bluetooth devices even when you’re not using the app”
❑	kTCCServiceCalls	<i>kein sichtbarer Effekt</i>	“Receive VoIP Calls in the Background”
✓	kTCCServiceExposureNotification	Exposure Notifications	“Your iPhone can securely collect and share random IDs with nearby devices. The app can use these IDs to notify you if you may have been exposed to COVID-19. The date, duration, and signal strength of an exposure will be shared.”



Und die Standort-Berechtigung?

```
#!/bin/bash  
# Adapted after: https://stackoverflow.com/a/53875499 and  
https://stackoverflow.com/a/29548123  
NEEDLE="com.bryceco.GoMap"  
  
find / -name '*.db' -print0 | while IFS= read -r -d '' file; do  
    for X in $(sqlite3 $file .tables); do  
        sqlite3 $file "SELECT * FROM $X;" | grep >/dev/null $NEEDLE  
        && echo "Found in file '$file', table '$X'";  
    done  
done
```

Und die Standort-Berechtigung?

```
#!/bin/bash
```

```
# Adapted after: https://stackoverflow.com/a/53875499 and  
                https://stackoverflow.com/a/29548123
```

```
NEEDLE="com.bryceco.GoMap"
```

```
find / -name '*.db' -print0 | while IFS= read -r -d '' file; do  
    for X in $(sqlite3 $file .tables); do  
        sqlite3 $file "SELECT * FROM $X;" | grep >/dev/null $NEEDLE  
        && echo "Found in file '$file', table '$X'";  
    done  
done
```

Und die Standort-Berechtigung?

```
#!/bin/bash  
# Adapted after: https://stackoverflow.com/a/53875499 and  
                 https://stackoverflow.com/a/29548123  
NEEDLE="com.bryceco.GoMap"  
  
find / -name '*.db' -print0 | while IFS= read -r -d '' file; do  
    for X in $(sqlite3 $file .tables); do  
        sqlite3 $file "SELECT * FROM $X;" | grep >/dev/null $NEEDLE  
        && echo "Found in file '$file', table '$X'";  
    done  
done
```


Und die Standort-Berechtigung?

```
#!/bin/bash  
# Adapted after: https://stackoverflow.com/a/53875499 and  
                https://stackoverflow.com/a/29548123  
NEEDLE="com.bryceco.GoMap"  
  
find / -name '*.db' -print0 | while IFS= read -r -d '' file; do  
    for X in $(sqlite3 $file .tables); do  
        sqlite3 $file "SELECT * FROM $X;" | grep >/dev/null $NEEDLE  
        && echo "Found in file '$file', table '$X'";  
    done  
done
```

Found in file '/private/var/mobile/Library/Caches/com.apple.appstored/storeUser.db',
table '**launch_events**'

Found in file '/private/var/mobile/Library/Caches/com.apple.appstored/storeUser.db',
table '**purchase_history_apps**'

Found in file '/private/var/mobile/Library/Caches/com.apple.appstored/storeUser.db',
table '**current_apps_crossfire**'

Found in file '/private/var/mobile/Library/TCC/TCC.db', table '**access**'

Found in file '/private/var/mobile/Library/DuetExpertCenter/_ATXDataStore.db',
table '**anchorModelTrainingData**'

Found in file '/private/var/mobile/Library/DuetExpertCenter/_ATXDataStore.db',
table '**appInfo**'

Found in file '/private/var/mobile/Library/FrontBoard/applicationState.db',
table '**application_identifier_tab**'

Found in file '/private/var/mobile/Library/FrontBoard/applicationState.db',
table '**kvs_debug**'

Found in file '/private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db',
table '**ZOBJECT**'

Found in file '/private/var/Keychains/Analytics/trust_analytics.db', table '**hard_failures**'

```

139         else {
140             FR_Log(@"Failed to retrieve TCC information for %@", bundleId);
141         }
142         CFRelease(bundle);
143     }
144     else {
145         FR_Log(@"Cannot create bundle for %@.", bundle);
146     }
147 }
148 else {
149     FR_Log(@"Use list from caches.");
150 }
151 CLLocationAuthorizationStatus status = [CLLocationManager _authorizationStatusForBundleIdentifier:bundleId bundle:nil];
152 if (permissionList.count == 0 && (status == kCLLocationAuthorizationStatusNotDetermined || status == kCLLocationAuthorizationStatusRestricted)) {
153     FR_Log(@"No permissions requested! Do not show reset permission");
154     return originalShortcutItems;
155 }
156 FR_Log(@"Requested: %@; locationStatus: %d.", permissionList, status);
157
158 SBSApplicationShortcutItem *shortcutItem = [[objc_getClass("SBSApplicationShortcutItem") alloc] init];
159 shortcutItem.type = tweakIdentifier;
160 shortcutItem.localizedTitle = @"Reset permission";
161 shortcutItem.bundleIdentifierToLaunch = bundleId;
162
163 NSMutableArray *newShortcutItems = originalShortcutItems ? [originalShortcutItems mutableCopy] : [NSMutableArray arrayWithCapacity:1];
164 [newShortcutItems addObject:shortcutItem];
165 FR_Log(@"New shortcutItems: %@", newShortcutItems);
166 return newShortcutItems;
167 }
168

```

```

139         else {
140             FR_Log(@"Failed to retrieve TCC information for %@", bundleId);
141         }
142         CFRelease(bundle);
143     }
144     else {
145         FR_Log(@"Cannot create bundle for %@.", bundle);
146     }
147 }
148 else {
149     FR_Log(@"Use list from caches.");
150 }
151 CLAuthorizationStatus status = [CLLocationManager _authorizationStatusForBundleIdentifier:bundleId bundle:nil];
152 if (permissionList.count == 0 && (status == kCLAuthorizationStatusNotDetermined || status == kCLAuthorizationStatusRestricted)) {
153     FR_Log(@"No permissions requested! Do not show reset permission");
154     return originalShortcutItems;
155 }
156 FR_Log(@"Requested: %@; locationStatus: %d.", permissionList, status);
157
158 SBSApplicationShortcutItem *shortcutItem = [[objc_getClass("SBSApplicationShortcutItem") alloc] init];
159 shortcutItem.type = tweakIdentifier;
160 shortcutItem.localizedTitle = @"Reset permission";
161 shortcutItem.bundleIdentifierToLaunch = bundleId;
162
163 NSMutableArray *newShortcutItems = originalShortcutItems ? [originalShortcutItems mutableCopy] : [NSMutableArray arrayWithCapacity:1];
164 [newShortcutItems addObject:shortcutItem];
165 FR_Log(@"New shortcutItems: %@", newShortcutItems);
166 return newShortcutItems;
167 }
168

```

```
> frida -U Flashlight
```

```

  ____|
 | (  |
  > _|
 /_/_|_|
      Commands:
      help      -> Displays the help system
      object?   -> Display information about 'object'
      exit/quit -> Exit
      . . . .
      . . . .
      . . . .
      . . . .
      More info at https://frida.re/docs/home/

```

```

[iOS Device::Flashlight]-> function bundleURL(id) {
  var all_apps = ObjC.classes.LSApplicationWorkspace.defaultWorkspace().allInstalledApplications();
  for (var i = 0; i < all_apps.count(); i++) {
    var app = all_apps.objectAtIndex_(i);
    if (app.bundleIdentifier().toString() == id) return app.bundleURL();
  }
}

```

```

[iOS Device::Flashlight]-> var CFBundleCreate_addr = Module.findExportByName(null, "CFBundleCreate");
var CFBundleCreate = new NativeFunction(CFBundleCreate_addr, 'pointer', ['pointer', 'pointer']);
[iOS Device::Flashlight]-> var kCFAllocatorDefault = Module.findExportByName(null, "kCFAllocatorDefault");
[iOS Device::Flashlight]-> var b = bundleURL("com.7thg.flashlight");
[iOS Device::Flashlight]-> var bundle = CFBundleCreate(kCFAllocatorDefault, b);
[iOS Device::Flashlight]-> bundle

```

```
"0x121f07bf0"
```

```

[iOS Device::Flashlight]-> (new ObjC.Object(bundle)).toString()
"CFBundle 0x121f07bf0 </private/var/containers/Bundle/Application/917CDF6B-D1CE-4BF4-AD16-C8D69E3D5B0C/iPhone4Flashlight.app> (executable, loaded)"

```

```

[iOS Device::Flashlight]-> var TCCAccessCopyInformationForBundle_addr = Module.findExportByName("/System/Library/PrivateFrameworks/TCC.framework/TCC", "TCCAccessCopyInformationForBundle");

```

```

[iOS Device::Flashlight]-> var TCCAccessCopyInformationForBundle = new NativeFunction(TCCAccessCopyInformationForBundle_addr, "pointer", ["pointer"]);

```

```

[iOS Device::Flashlight]-> TCCAccessCopyInformationForBundle(bundle)

```

```
"0x0"
```

```

[iOS Device::Flashlight]->

```

```

[iOS Device::Flashlight]->

```

```

[iOS Device::Flashlight]-> ObjC.classes.CLLocationManager.setAuthorizationStatusByType_forBundleIdentifier_

```

```

  setAuthorizationPromptMapDisplayEnabled_
  setAuthorizationStatusByType_forBundleIdentifier_
  setAuthorizationStatusByType_forBundle_
  setAuthorizationStatusByType_withCorrectiveCompensation_forBundleIdentifier_
  setAuthorizationStatusByType_withCorrectiveCompensation_forBundle_
  setAuthorizationStatus_forBundleIdentifier_
  setAuthorizationStatus_forBundle_

```


~ master !4

> frida-trace -U -m "[CLLocationManager *]" Settings

Started tracing 236 functions. Press Ctrl+C to stop.

/* TID 0x103 */

```
7874 ms +[CLLocationManager allowableAuthorizationForLocationDictionary:0x2837c8460]
7875 ms +[CLLocationManager setEntityAuthorization:0x4 withCorrectiveCompensationType:0x0 forLocationDictionary:0x2837c8460]
7875 ms | +[CLLocationManager setAuthorizationStatusByType:0x3 withCorrectiveCompensation:0x0 forBundleIdentifier:0x2800a7030]
7894 ms +[CLLocationManager activeLocationServiceTypesForLocationDictionary:0x0]
7895 ms | +[CLLocationManager isEntityAuthorizedForLocationDictionary:0x0]
7895 ms | | +[CLLocationManager entityAuthorizationForLocationDictionary:0x0]
7895 ms +[CLLocationManager dateLocationLastUsedForLocationDictionary:0x0]
7906 ms +[CLLocationManager activeLocationServiceTypesForLocationDictionary:0x0]
7906 ms | +[CLLocationManager isEntityAuthorizedForLocationDictionary:0x0]
7906 ms | | +[CLLocationManager entityAuthorizationForLocationDictionary:0x0]
7906 ms +[CLLocationManager dateLocationLastUsedForLocationDictionary:0x0]
7908 ms +[CLLocationManager activeLocationServiceTypesForLocationDictionary:0x0]
7908 ms | +[CLLocationManager isEntityAuthorizedForLocationDictionary:0x0]
7908 ms | | +[CLLocationManager entityAuthorizationForLocationDictionary:0x0]
7908 ms +[CLLocationManager dateLocationLastUsedForLocationDictionary:0x0]
7910 ms +[CLLocationManager activeLocationServiceTypesForLocationDictionary:0x0]
7910 ms | +[CLLocationManager isEntityAuthorizedForLocationDictionary:0x0]
7910 ms | | +[CLLocationManager entityAuthorizationForLocationDictionary:0x0]
7910 ms +[CLLocationManager dateLocationLastUsedForLocationDictionary:0x0]
7911 ms +[CLLocationManager activeLocationServiceTypesForLocationDictionary:0x0]
7911 ms | +[CLLocationManager isEntityAuthorizedForLocationDictionary:0x0]
7911 ms | | +[CLLocationManager entityAuthorizationForLocationDictionary:0x0]
7911 ms +[CLLocationManager dateLocationLastUsedForLocationDictionary:0x0]
```

```
Terminal
~ master !4
> frida-trace -U -m "[CLLocationManager *]" Settings
Started tracing 236 functions. Press Ctrl+C to stop.
/* TID 0x103 */
7874 ms +[CLLocationManager allowableAuthorizationForLocationDictionary:0x2837c8460]
7875 ms +[CLLocationManager setEntityAuthorization:0x4 withCorrectiveCompensationType:0x0 forLocationDictionary:0x2837c8460]
7875 ms | +[CLLocationManager setAuthorizationStatusByType:0x3 withCorrectiveCompensation:0x0 forBundleIdentifier:0x2800a7030]
7894 ms +[CLLocationManager activeLocationServiceTypesForLocationDictionary:0x0]
7895 ms | +[CLLocationManager isEntityAuthorizedForLocationDictionary:0x0]
7895 ms | | +[CLLocationManager entityAuthorizationForLocationDictionary:0x0]
7895 ms +[CLLocationManager dateLocationLastUsedForLocationDictionary:0x0]
7906 ms +[CLLocationManager activeLocationServiceTypesForLocationDictionary:0x0]
7906 ms | +[CLLocationManager isEntityAuthorizedForLocationDictionary:0x0]
7906 ms | | +[CLLocationManager entityAuthorizationForLocationDictionary:0x0]
7906 ms +[CLLocationManager dateLocationLastUsedForLocationDictionary:0x0]
7908 ms +[CLLocationManager activeLocationServiceTypesForLocationDictionary:0x0]
7908 ms | +[CLLocationManager isEntityAuthorizedForLocationDictionary:0x0]
7908 ms | | +[CLLocationManager entityAuthorizationForLocationDictionary:0x0]
7908 ms +[CLLocationManager dateLocationLastUsedForLocationDictionary:0x0]
7910 ms +[CLLocationManager activeLocationServiceTypesForLocationDictionary:0x0]
7910 ms | +[CLLocationManager isEntityAuthorizedForLocationDictionary:0x0]
7910 ms | | +[CLLocationManager entityAuthorizationForLocationDictionary:0x0]
7910 ms +[CLLocationManager dateLocationLastUsedForLocationDictionary:0x0]
7911 ms +[CLLocationManager activeLocationServiceTypesForLocationDictionary:0x0]
7911 ms | +[CLLocationManager isEntityAuthorizedForLocationDictionary:0x0]
7911 ms | | +[CLLocationManager entityAuthorizationForLocationDictionary:0x0]
7911 ms +[CLLocationManager dateLocationLastUsedForLocationDictionary:0x0]
```


Standort-Berechtigung setzen

- Setzen mit Frida (im Kontext der Einstellungs-App):

```
ObjC.classes.CLLocationManager
    .setAuthorizationStatusByType_forBundleIdentifier_(
        <value>, "<bundle_id>"
    );
```

Standort-Berechtigung setzen

- Setzen mit Frida (im Kontext der Einstellungs-App):

```
ObjC.classes.CLLocationManager  
    .setAuthorizationStatusByType_forBundleIdentifier_  
        <value>, "<bundle_id>"  
    ) ;
```
- Mögliche Werte (durch Ausprobieren):
0: immer fragen, 2: nie, 3: immer, 4: während die App benutzt wird

Standort-Berechtigung setzen

- Setzen mit Frida (im Kontext der Einstellungs-App):

```
ObjC.classes.CLLocationManager
    .setAuthorizationStatusByType_forBundleIdentifier_(
        <value>, "<bundle_id>"
    );
```

- Mögliche Werte (durch Ausprobieren):

0: immer fragen, 2: nie, 3: immer, 4: während die App benutzt wird

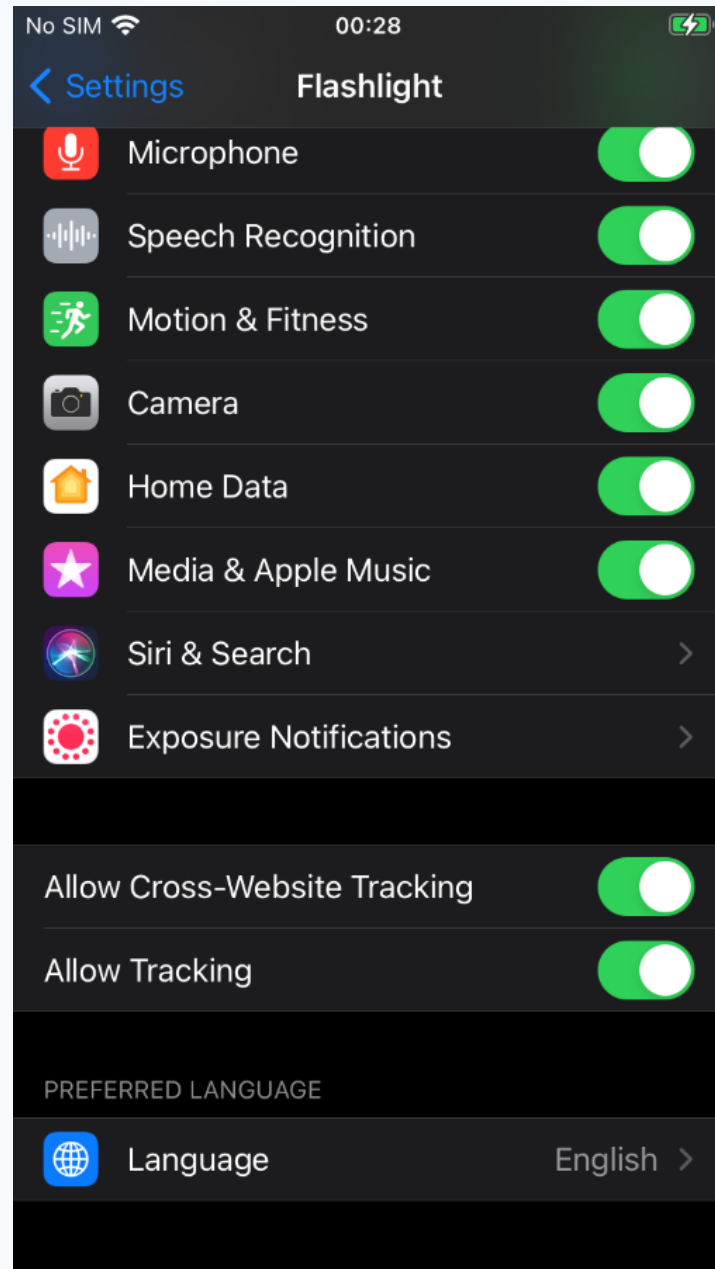
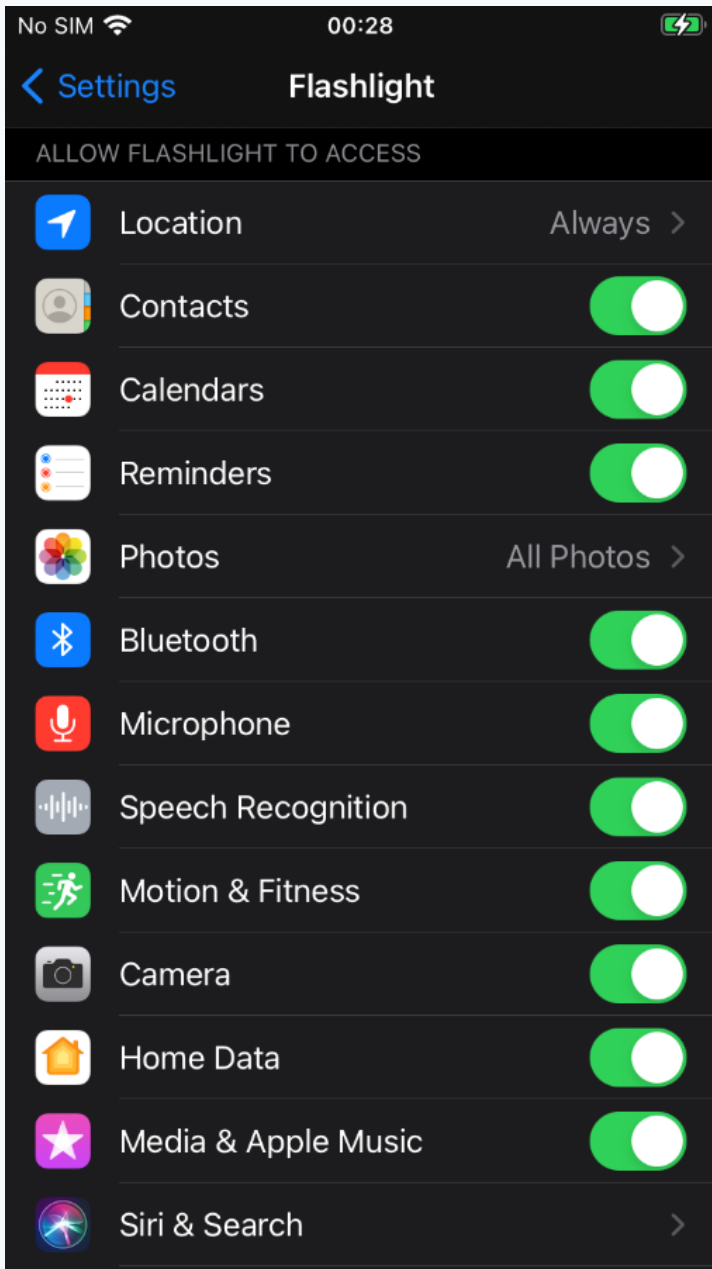
- Aktuellen Status überprüfen:

```
// Für die laufende App.
```

```
ObjC.classes.CLLocationManager.authorizationStatus();
```

```
// Für eine beliebige App.
```

```
ObjC.classes.CLLocationManager
    .authorizationStatusForBundleIdentifier_("<bundle_id>");
```



Zwischenablage

- Inhalt der Zwischenablage mit Frida setzen:

```
ObjC.classes.UIPasteboard.generalPasteboard()  
    .setString_("<string>");
```

Statistiken über Tracking-Aktivitäten

Mithilfe von automatisierten Analysen
können wir Aussagen über Tracking in
tausenden Apps treffen.

7. Results

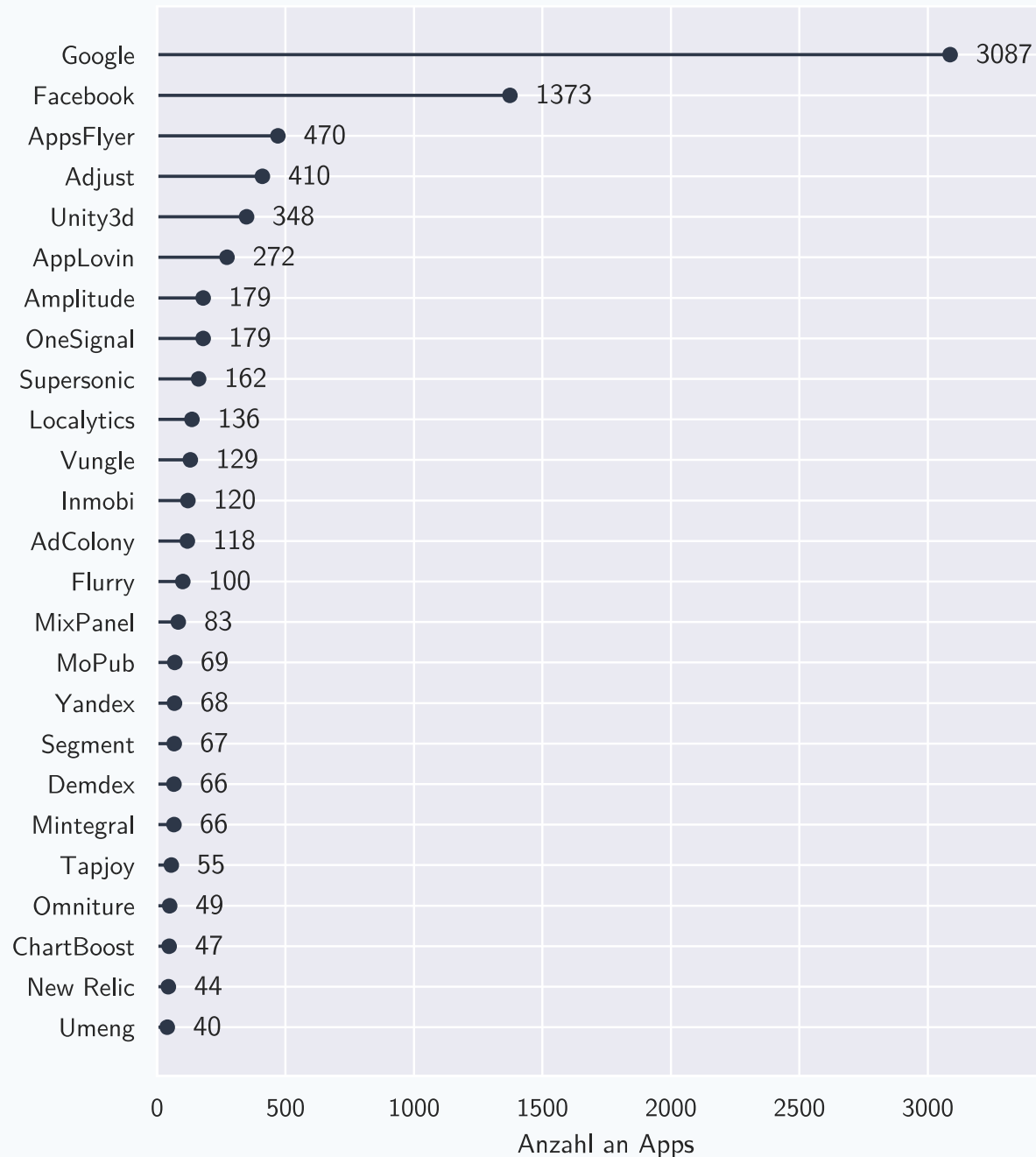
We successfully analysed 4,388 apps with 2,068 apps on Android and 2,320 apps on iOS, corresponding to 62.42 % and 93.51 % of the downloaded apps, respectively. On Android, the high number of apps we could not analyse is caused for the most part by problems with the certificate pinning bypass through objection. 1,049 of the Android apps failed to launch or quit immediately after being launched through objection. These apps were excluded from the analysis. We discuss this further in Section 8.2. On iOS, only 65 apps failed to launch and 18 apps could not be installed because they require a newer version of iOS than we can use. The remaining failures on both platforms were mostly due to Appium or Frida commands failing even after multiple retries.

In the interest of reproducibility, the processed data behind all graphs is available in our GitHub repository.

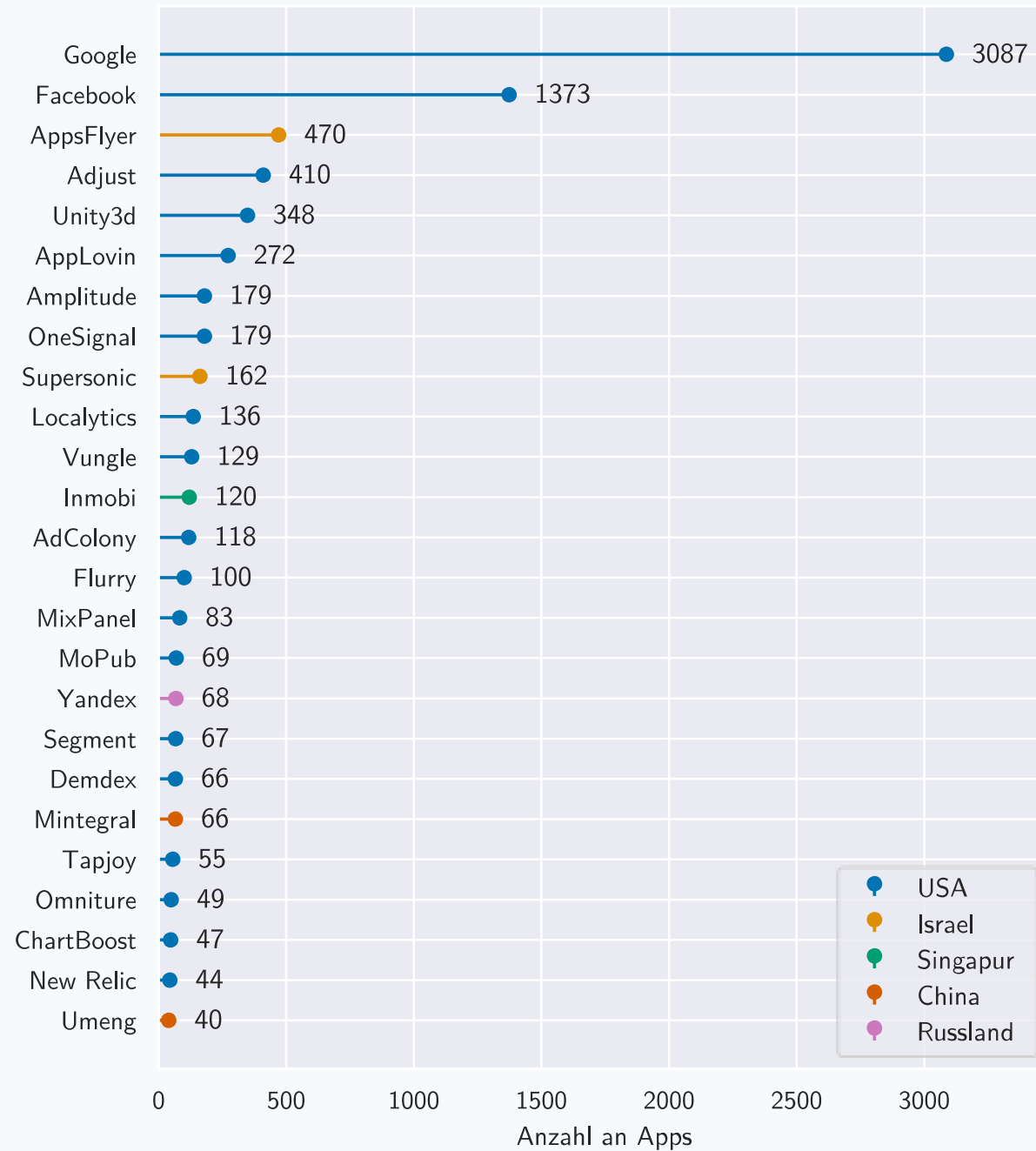
7.1. Network Traffic and Tracking

78 % der Apps haben
ohne jegliche Interaktion
mind. einen Tracker
kontaktiert.

Tracker (nach Exodus), an
welche die meisten von 4.388
beliebten Apps innerhalb einer
Minute nach Start und ohne
jegliche Interaktion Anfragen
geschickt haben.



Tracker (nach Exodus), an welche die meisten von 4.388 beliebten Apps innerhalb einer Minute nach Start und ohne jegliche Interaktion Anfragen geschickt haben, gefärbt nach Land der Hauptniederlassung.



33,3 % aller Anfragen
(ohne Interaktion)
gingen an **Trackingserver.**

Übertragene Daten erkennen

- Erster Ansatz: Textsuche nach vorher bekannten Werten (Werbe-IDs, Standort, Honey-Data, ...) im Traffic.
 - Das geht mit etwas Aufwand teils auch in enkodiertem Traffic (z. B. base64).

Übertragene Daten erkennen

- Erster Ansatz: Textsuche nach vorher bekannten Werten (Werbe-IDs, Standort, Honey-Data, ...) im Traffic.
 - Das geht mit etwas Aufwand teils auch in enkodiertem Traffic (z. B. [base64](#)).
- Probleme:
 - Funktioniert nur mit statischen, vorher bekannten Daten, die ausreichend eindeutig sind (nicht aber z. B. RAM-Auslastung, Akkustand, OS-Version).

Übertragene Daten erkennen

- Erster Ansatz: Textsuche nach vorher bekannten Werten (Werbe-IDs, Standort, Honey-Data, ...) im Traffic.
 - Das geht mit etwas Aufwand teils auch in enkodiertem Traffic (z. B. [base64](#)).
- Probleme:
 - Funktioniert nur mit statischen, vorher bekannten Daten, die ausreichend eindeutig sind (nicht aber z. B. RAM-Auslastung, Akkustand, OS-Version).
 - Trackingdaten sind häufig absurd verschachtelt und/oder obfuskiert.

POST [https://outcome-ssp.supersonicads.com/mediation
?adUnit=2&sessionId=742FF763-3F0F-4F06-8FA1-792415932910
&appKey=82d752b5](https://outcome-ssp.supersonicads.com/mediation?adUnit=2&sessionId=742FF763-3F0F-4F06-8FA1-792415932910&appKey=82d752b5)

H4sIAAAAAAAAAE+VYWY/bNhB+z68w/GypPEWqbz4LI9kk6G7zUhcCLVJeNtYBit5kG+x/L23dXqdpDhTJ9smW5uPMcO
aboTgfnolGYyu2ezUe/Twal4dCGV++u/VTJbWwOs8idacyW44nR6QUVpyAHzbZaLQZS3WnY3WVS7XfHN9vxvr1bZ6p
cII340mF+XNbi6w5qPZtok1pr1VZOhoX5IdSmbW8uS9ULT2++EVlygirZAtL4/gkB/XzzuSHYi1nL+tVkICQ486ZYn
/Y6eyNMj27zIc+RD7yTAsT1p6EqH7eHjK5V2tZr4jz1BepyHKrSj8VOx1bvVdlt7wohiZCHyBnBKA+5Lm6r8UcSubR
lrbSKq6vllc1YFoU+y42uozivChELUzEvuyEpdqlLmGtrwigMOiWZlaZTOxvVNlAXCqPsodBhHqB/y3T9r5VEOdZpu
IjMXqQdzrRLWKX2iudHVxoXiVJqapAQtrkSMg7ZawudbZrfWQErVYswB5egZVHViDw+GoKPRYiAmmIUQhBl/JsmPI6
VtcNAfMuD3k5TAMkPu/05FuXtLkwRitTA3LkyS6UA1d7210vVm9a0NZxRZkqkxA0Tumal5tx5/j7uauTM4cwgl3gKu
7++qbl1mLYk+vyhU61ncobI+K3zqlldixceal8tEzuviS46yM/SqutFvvlqfBPWn4/SkejD9VPRbNT6S5UYW+rvU86
4adIUqEKk99p2cb+quk456CdEWnqJPEjO6fWVDeRlkzz6YxDiGYepJh7ZLkMvemUhB7jc0JWjC8wxQMTQh4p3qv36r
XVqSsSkRaV2YCEgAEAMYasv/hw2mdrPQgABoQDb0tcoCFUshcNw9gLZCAFILGKJYkgZIBQShAbOKLeW9jk/lR1U1lG
mLKQk2ACXQ944QKWRW5bgGAY6TA0ADRGvIdxTnJMHwYqr/JtRHmAg5BN4Op+q0yEAaMM4+EjHCgkkFM2UAghGLoREI
YI7mOcnhCFjVFEAWcU99SSEFICQX8JDzjg6JFa2L2ZwPmtMHab56V1bgBycrXFE8gYbEy6egEMgwlamzy7zg8mVhGC
bi+EDnaHnWN9JYggGgSsh0Eu4ZzjRxg6QVM5z/d5dn/EUObYgF7oxOZJEgWIopCEznzmvNERpZQDQCaDLPdPvpulHA
Mud/yc5jXDkEtET7Q7nog6filcjZRN0x+Nuiq9eBg0kIfqz8PkUXnrzLmVxaqt388v73/sEGel34T935d+o2AqReFa
1rCtEh/7kH+nRf5NetaAEgD0t1QWrdq6d3wl/erd3xh3JpSPEvGVDLyQ0uvF8/N0Ah80ay6Q9aMLIXBEGib/2303aR
Dfklso/HLuIsJp8AS4W59yPwh3H/fLz2drTfP/U6PFGDH6FMhafYA9PbL+x98B31kvxZg8CXrWt4EfhJ6fPM5rth5/
/jiba6yMUlcqzZsLOQ5xcyW3f9VqlgeTO7puNj/NlNm3ZGsv4OtmlFBdwM+HR1HyLrprdwFD37EMJt01vZRvL82Xuq
nC1jZs7w1tvpghM/FeZLuD2DUFuHzpLZadtYNulbp70BzMV14wY07pjCy9kM6WHl8wzBcEBatpt66av3Uz1YgRlCQs
wDgBCU1AwBMbL44QPlZKrgI22cP42cPf7GKrK3QUAAA=

Recipe

From Base64

Alphabet

A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

Input

length: 1664
lines: 1

H4sIAAAAAAAAE+VYWY/bNhB+z68w/GypPEWqbz4LI9kk6G7zUhcCLVJeNtYBit5kG+x/L23dXqdpDhTJ9smW5uPMcOaboTgfno1GYyu2ezUe/Twa14dCGV++u/VtJbWw0s8idacyW44nR6QUVpyAHzbZaLQZS3WnY3WVS7XfHN9vxvr1bZ6pcII340mF+XNbi6w5qPZtok1pr1VZ0h0X5IdSmbW8uS9ULT2++EVlygirZAtL4/gkB/XzzuSHYi1nL+tVkICQ486ZYn

Output

time: 3ms
length: 1247
lines: 3

.....âXY.Û6.~Ï̃0ü1©<E^o>.#Û\$ènóR...-R^6Ö..bd.i./mÝ^§i..ÉöÉ.æãÏpæ.¡8...Fc+¶{5.ý<...B._¾»ðS%µ°:Ï̃"u§2[.'G▯.V...6Ûh´.Ku\$cu.Kµß.ßoÆúõm.©p.7ãI.ùs[.¬9̃̃öm¢MĩUY:..ä.R.µ¼¹/T-=¾øEeÊ.«d.Kãø\$.ðóÎä.b-g/ëU...ãÎ.b.Øéì.2=»Ï̃.>D>òL..Ö..̃~b.2¹WkỸ.óô.©Èr«J?.;.[½We·¼(.&B. g. >ä¹°^Ä.IFÑ.¶̃Ò*®̃.W5`Z.û.6°.â¼(D-LÃ¾ì.¥Ú¥.a.̃. Øè.fV.LìoTÛ@*.².A.z.ÿ-Ôö¼U.çY!â#1z.w:Ñ-b.Ú+..\\h^%I©^a@BÔdHÈ;e¬.u¶k}d..V,À.^..GV ðøj=. ".i.Q.A.òl.ò:V×.ó..y9L.\$>ïôä[.´¹0F+S.räÉ...W{Û}/VoZÐÖqE.*..4Né...qçøû¹«.3.Ø.]à*îpú!õ.bØ.èò.Nµ.Ê.#â·Î©ev,\\y©|´Lî¼\$,è#?J«..ûå©ð0Z~?JG£.Ö0E³Sé.Tao«¾0:á\$HR¡.ßiÛÆp^aé8ç ..iè\$ñ#;§ÖT7..Lóé.C.f.▯.{d¹.½é...ãsBV./0Å..B.)þ«÷êµÖ©+....Û.....1.¬çøpÚgk=.....oK\\ !T±·ÃØ.d . ±.%. d.PJ..8¢þ[ØäþTuSYF.²...`.].xá..En[.´2é04.4`¼.qNrL.f*̃òmDy...Màê~«L..£.ãá#.(\$.S6P.!.°.....îc.....QD.g.÷Ô..R.A..8àè.ZØ½.Àù.Øv.ç¥un.rrrµÄ.È.1L°z... Z.<>Î.&V..n/..v..c}%..¬.A.á.ãG.:AS9Î÷yv.ÄPæØ.^èÄæI...¢..Î|æ¼Ñ.¥..@&.,÷0¼....wü.æ5Ã.KD0´;...~¬..M;...°*½x.4..êÎÄäQyëÏ¹.A^a.ßÎ/i.i.igmß.ýß.~£`*EáZÖ°...û..§EþMzÖ...ô·T..Ú°w|%ýêÝß.w&...ñ..¼.ÒèÄóót..4k..õ£.!pD..ÿÛs·i.ß.»(ürî"Âið.,[.r?.w.÷ËÏgkMóÿS£Ä.1ú.ÈZ}.==²þçß.ßY/Ä.< zÖ.....<Îk¶..þ8.k¬.RW*Í..9.qs%·.Öj...;°n6?Í.Û·dk/àëf.P]ÄÏ.GQò.°kw.Cß±.&Ý5½.o/Í.°©ÂÖ61ïm¾...ñ^d».Ø5.,|é-..µ.n.°{Ð.ÌW^0cNé.,½.Î.._0Ï...«i·®.çu3....\$,À8. I@À../..>VJ®.6ÛÄøÛÄßib«.t...

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

length: 1664
lines: 1

+

📁

🔗

🗑️

🔧

Input

H4sIAAAAAAAAE+VYWY/bNhB+z68w/GypPEWqbz4LI9kk6G7zUhcCLVJeNtYBit5kG+x/L23dXqdpDhTJ9smW5uPMcOaboTgfno1GYyu2ezUe/Twa14dCGV++u/VtJbWw0s8idacyW44nR6QUVpyAHzbZaLQZS3WnY3WVS7XfHN9vxvr1bZ6pcII340mF+XNbi6w5qPZtok1pr1VZ0hOX5IdSmbW8uS9ULT2++EVlygirZAtL4/gkB/XzzuSHYi1nL+tVkiCQ486ZYn

Output

start: 51
end: 51
length: 0

time: 5ms
length: 5236
lines: 4

🗑️

📄

🔗

↶

🔧

```
{
  "table" : "super.dwh.mediation_events",
  "data" : "{\n  \"deviceModel\" : \"iPhone9,3\", \n  \"jb\" : \"true\", \n  \"firstSession\" : \"true\", \n  \"userIdType\" : \"userGenerated\", \n  \"mcc\" : 0, \n  \"groupIdBN\" : \"1409833\", \n  \"pluginVersion\" : \"7.1.12.2-r\", \n  \"att\" : 2, \n  \"bundleId\" : \"com.amanotes.magictiles\", \n  \"appVersion\" : \"9.021.102\", \n  \"appKey\" : \"82d752b5\", \n  \"deviceOEM\" : \"Apple\", \n  \"is_coppa\" : \"false\", \n  \"segmentId\" : \"20296\", \n  \"internalTestId\" : {\n\n  }, \n  \"pluginType\" : \"Unity\", \n  \"connectionType\" : \"wifi\", \n  \"gmtMinutesOffset\" : 120, \n  \"advertisingId\" : \"742FF763-3F0F-4F06-8FA1-792415932910\", \n  \"mnc\" : 0, \n  \"deviceOS\" : \"ios\", \n  \"osVersion\" : \"14.8\", \n  \"mobileCarrier\" : \"o2-de\", \n  \"advertisingIdType\" : \"IDFV\", \n  \"battery\" : 100, \n  \"icc\" : \"0\", \n  \"xCodeVersion\" : \"1321\", \n  \"groupIdRV\" : \"1453121\", \n  \"isLimitAdTrackingEnabled\" : \"true\", \n  \"idfV\" : \"742FF763-3F0F-4F06-8FA1-792415932910\", \n  \"InterstitialEvents\" : [\n    {\n      \"sessionDepth\" : 1, \n      \"connectionType\" : \"wifi\", \n      \"provider\" : \"Mediation\", \n      \"programmatic\" : 1, \n      \"eventSessionId\" : \"CAB8112B-1538-4EE9-AA49-78C44F78D353\", \n      \"adUnit\" : 2, \n      \"timestamp\" : 1649070013317, \n      \"auctionId\" : \"66030480-b406-11ec-b99c-6d6da04cecd4_1170455427\", \n      \"ext1\" : \"1UnityAds_3579846,1AppLovin_5380434,1UnityAds_5605678,1AppLovin_3178354,1AdMob_5863697,1Fyber_3075733,1Fyber_3075731,1UnityAds_5641857,1AppLovin_3111046,1AppLovin_5647243,1AppLovin_3075929,1AdMob_2508753,1UnityAds_4915410,1AppLovin_3868082,1AppLovin_5647241,1AppLovin,1Chartboost_3104731,1AppLovin_41771,1AdMob_3120730,2IronSource_2141845,1UnityAds_5638751,1AppLovin_2425667,1UnityAds_2164883,1AppLovin_2425665,2AdColony_2165717,2Liftoff_6252949,2InMobi_5558004,\"
    }, \n    {\n      \"firstSessionTimestamp\" : 1649070007838, \n      \"eventId\" : 2311, \n      \"genericParams\" : {\n        \"segmentId\" : \"20296\"
      }, \n      {\n        \"instanceType\" : 1, \n        \"connectionType\" : \"wifi\", \n        \"sessionDepth\" : 1, \n        \"provider\" : \"UnityAds\", \n        \"programmatic\" : 1, \n        \"providerAdapterVersion\" : \"4.3.18\", \n        \"adUnit\" : 2, \n        \"timestamp\" : 1649070013317, \n        \"auctionId\" : \"66030480-b406-11ec-b99c-6d6da04cecd4_1170455427\", \n        \"eventSessionId\" : \"CAB8112B-1538-4EE9-AA49-78C44F78D353\", \n        \"eventId\" : 2002, \n        \"spId\" : \"3579846\", \n        \"firstSessionTimestamp\" : 1649070007838, \n        \"auctionTrials\" : 1, \n        \"genericParams\" : {\n          \"segmentId\" : \"20296\"
        }, \n        {\n          \"providerSDKVersion\" : \"4.0.0\"
        }, \n        {\n          \"providerSDKVersion\" : \"10.3.7\", \n          \"connectionType\" : \"wifi\", \n          \"sessionDepth\" : 1, \n          \"provider\" : \"AppLovin\", \n          \"programmatic\" : 1, \n          \"providerAdapterVersion\" : \"4.3.29\", \n          \"
```


⊘ ||

▼

1

⊘ ||

⊘ ||

10

☒ Prevent eval

```
length: 1664
lines:    1
```

H4sIAAAAAAAAAE+VYWY/bNhB+z68w/GypPEWqbz4LI9kk6G7zUhCLVJeNtYBit5kG+x/L23dXqdpDhTJ9smW5uPMc0aboTgfn01GYyu2ezUe
/Twa14dCGV++u
/VTJbww0s8idacyW44nR6QUVpyAHzbZaLQZS3WnY3WVS7XFHN9vxvr1bZ6pcII340mF+XNbi6w5qPZtok1pr1VZ0h0X5IdSmbw8uS9ULT2++EVlygirZA
tL4/gkB/XzzuSHYi1nL+tvkICQ486ZYn

```
time: 3ms
length: 5178
lines: 1
```

```
{
  "deviceModel": "iPhone9,3",
  "jb": true,
  "firstSession": true,
  "userIdType": "userGenerated",
  "mcc": 0,
  "groupIdBN": "1409833",
  "pluginVersion": "7.1.12.2-r",
  "att": 2,
  "bundleId": "com.amanotes.magictiles",
  "appVersion": "9.021.102",
  "appKey": "82d752b5",
  "deviceOEM": "Apple",
  "is_coppa": false,
  "segmentId": "20296",
  "internalTestId": {
  },
  "pluginType": "Unity",
  "connectionType": "wifi",
  "gmtMinutesOffset": 120,
  "advertisingId": "742FF763-3F0F-4F06-8FA1-792415932910",
  "mnc": 0,
  "deviceOS": "ios",
  "osVersion": "14.8",
  "mobileCarrier": "o2-de",
  "advertisingIdType": "IDFV",
  "battery": 100,
  "icc": "0",
  "xCodeVersion": "1321",
  "groupIdRV": "1453121",
  "isLimitAdTrackingEnabled": true,
  "idfv": "742FF763-3F0F-4F06-8FA1-792415932910",
  "InterstitialEvents": [
    {
      "sessionDepth": 1,
      "connectionType": "wifi"
    }
  ],
  "provider": "Mediation",
  "programmatic": 1,
  "eventSessionId": "CAB8112B-1538-4EE9-AA49-78C44F78D353",
  "adUnit": 2,
  "timestamp": 1649070013317,
  "auctionId": "66030480-b406-11ec-b99c-6d6da04cecd4_1170455427",
  "ext1": "1UnityAds_3579846,1AppLovin_5380434,1UnityAds_5605678,1AppLovin_3178354,1AdMob_5863697,1Fyber_3075733,1Fyber_3075731,1UnityAds_5641857,1AppLovin_3111046,1AppLovin_5647243,1AppLovin_3075929,1AdMob_2508753,1UnityAds_4915410,1AppLovin_3868082,1AppLovin_5647241,1AppLovin,1Chartboost_3104731,1AppLovin_41771,1AdMob_3120730,2IronSource_2141845,1UnityAds_5638751,1AppLovin_2425667,1UnityAds_2164883,1AppLovin_2425665,2AdColony_2165717,2Liftoff_6252949,2InMobi_5558004,",
  "firstSessionTimestamp": 1649070007838,
  "eventId": 2311,
  "genericParams": {
    "segmentId": "20296"
  },
  "instanceType": 1,
  "connectionType": "wifi",
  "sessionDepth": 1,
  "provider": "UnityAds",
  "programmatic": 1,
  "providerAdapterVersion": "4.3.18",
  "adUnit": 2,
  "timestamp": 1649070013317,
  "auctionId": "66030480-b406-11ec-b99c-6d6da04cecd4_1170455427",
  "eventSessionId": "CAB8112B-1538-4EE9-AA49-78C44F78D353",
  "eventId": 2002,
  "spId": "3579846",
  "firstSessionTimestamp": 1649070007838,
  "auctionTrials": 1,
  "genericParams": {
    "segmentId": "20296"
  },
  "providerSDKVersion": "4.0.0",
  "providerSDKVersion": "10.3.7",
  "connectionType": "wifi",
  "sessionDepth": 1,
  "provider": "AppLovin",
  "programmatic": 1,
  "providerAdapterVersion": "4.3.29",
  "adUnit": 2,
  "timestamp": 1649070024856,
  "auctionId": "66030480-b406-11ec-b99c-6d6da04cecd4_1170455427",
  "eventSessionId": "CAB8112B-1538-4EE9-AA49-78C44F78D353"
}
```


⊘ ||

▼

☐

⊘ ||

⊘ ||

⊘ ||

⊘ ||

1


```
length: 1664
lines: 1
```

```
time: 10ms
length: 5169
lines: 141
```


K

7

in CyberChef anschauen

POST <https://graph.facebook.com/v12.0>

[illegible]



batch

\\n

☒ Prevent eval

```
length: 4151
lines: 1
```



```

{"batch":["[{"relative_url\":\"313732607382406
\\\\activities?access_token=313732607382406%7C7e5f1e2769be769bb6710ffbc14399c2&advertiser_id_collection_enabled=1&
anon_id=XZ0BAE1D89-562C-4B77-9D29-29E9E80F3051&application_tracking_enabled=1&custom_events=%5B%7B%22_eventName%22%3A
%22Backend_OK%22%2C%22_logTime%22%3A1650911380%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D

```



```
time: 1ms
length: 4107
lines: 1
```



```
%{"relative_url":"","access_token=313732607382406%7C7e5f1e2769be769bb6710ffbc14399c2&advertiser_id_collection_enabled=1&anon_id=XZ0BAE1D89-562C-4B77-9D29-29E9E80F3051&application_tracking_enabled=1&custom_events=%5B%7B%22_eventName%22%3A%22Backend_OK%22%2C%22_logTime%22%3A1650911380%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADReport_RequestError%22%2C%22_logTime%22%3A1650911382%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADReport_RequestStart%22%2C%22_logTime%22%3A1650911382%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADReport_RequestError%22%2C%22_logTime%22%3A1650911383%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADReport_RequestStart%22%2C%22_logTime%22%3A1650911383%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADReport_RequestError%22%2C%22_logTime%22%3A1650911383%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADReport_RequestError%22%2C%22_logTime%22%3A1650911383%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADStart_RequestError%22%2C%22_logTime%22%3A1650911384%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADStart_RequestStart%22%2C%22_logTime%22%3A1650911384%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADOpen_RequestStart%22%2C%22_logTime%22%3A1650911384%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADOpen_RequestError%22%2C%22_logTime%22%3A1650911384%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADStart_RequestError%22%2C%22_logTime%22%3A1650911384%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADStart_RequestStart%22%2C%22_logTime%22%3A1650911384%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADOpen_RequestStart%22%2C%22_logTime%22%3A1650911385%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADOpen_RequestError%22%2C%22_logTime%22%3A1650911385%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADOpen_RequestStart%22%2C%22_logTime%22%3A1650911387%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADOpen_RequestError%22%2C%22_logTime%22%3A1650911387%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADOpen_RequestStart%22%2C%22_logTime%22%3A1650911388%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADOpen_RequestError%22%2C%22_logTime%22%3A1650911388%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADStart_RequestSuccess%22%2C%22_logTime%22%3A1650911392%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADOpen_RequestSuccess%22%2C%22_logTime%22%3A1650911392
```



batch

\n



Prevent eval


```
length: 4151
lines: 1
```



```
{"batch":["[{"relative_url":"313732607382406
\\//activities?access_token=313732607382406%7C7e5f1e2769be769bb6710ffbc14399c2&advertiser_id_collection_enabled=1&
anon_id=XZ0BAE1D89-562C-4B77-9D29-29E9E80F3051&application_tracking_enabled=1&custom_events=%5B%7B%22_eventName%22%3A
%22Backend_OK%22%2C%22_logTime%22%3A1650911380%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D
```



```
time: 4ms
length: 4088
lines: 1
```

[illegible]



batch

\\n



Prevent eval

⊘ ||

```
*.relative_url
```

\\n



Prevent eval

```
length: 4151
lines: 1
```



```
{
  "batch": "[{"relative_url": "313732607382406
  \\\\/activities?access_token=313732607382406%7C7e5f1e2769be769bb6710ffbc14399c2&advertiser_id_collection_enabled=1&
  anon_id=XZ0BAE1D89-562C-4B77-9D29-29E9E80F3051&application_tracking_enabled=1&custom_events=%5B%7B%22_eventName%22%3A
  %22Backend_OK%22%2C%22_logTime%22%3A1650911380%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D
```



```
time: 1ms
length: 4020
lines: 2
```



```
"313732607382406/activities?access_token=313732607382406%7C7e5f1e2769be769bb6710ffbcb14399c2&
advertiser_id_collection_enabled=1&anon_id=XZ0BAE1D89-562C-4B77-9D29-29E9E80F3051&application_tracking_enabled=1&
custom_events=%5B%7B%22_eventName%22%3A%22Backend_OK%22%2C%22_logTime%22%3A1650911380%2C%22_valueToSum%22%3A1
%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADReport_RequestError%22%2C%22_logTime
%22%3A1650911382%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A
%22ADReport_RequestStart%22%2C%22_logTime%22%3A1650911382%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A
%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADReport_RequestError%22%2C%22_logTime%22%3A1650911383
%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A
%22ADReport_RequestStart%22%2C%22_logTime%22%3A1650911383%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A
%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADReport_RequestError%22%2C%22_logTime%22%3A1650911383
%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADStart_RequestError
%22%2C%22_logTime%22%3A1650911384%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B
%22_eventName%22%3A%22ADStart_RequestStart%22%2C%22_logTime%22%3A1650911384%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A
%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADOpen_RequestStart%22%2C%22_logTime%22%3A1650911384
%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADOpen_RequestError
%22%2C%22_logTime%22%3A1650911384%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B
%22_eventName%22%3A%22ADStart_RequestError%22%2C%22_logTime%22%3A1650911384%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A
%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADStart_RequestStart%22%2C%22_logTime%22%3A1650911384
%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADOpen_RequestStart
%22%2C%22_logTime%22%3A1650911385%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B
%22_eventName%22%3A%22ADOpen_RequestError%22%2C%22_logTime%22%3A1650911385%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A
%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADOpen_RequestStart%22%2C%22_logTime%22%3A1650911387
%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADOpen_RequestError
%22%2C%22_logTime%22%3A1650911387%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B
%22_eventName%22%3A%22ADOpen_RequestStart%22%2C%22_logTime%22%3A1650911388%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A
%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADOpen_RequestError%22%2C%22_logTime%22%3A1650911388
%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A
%22ADStart_RequestSuccess%22%2C%22_logTime%22%3A1650911392%2C%22_valueToSum%22%3A1%2C%22_ui%22%3A
%22UINavigationController%22%7D%2C%7B%22_eventName%22%3A%22ADOpen_RequestSuccess%22%2C%22_logTime%22%3A1650911392
```



batch

\\n



Prevent eval


```
*.relative_url
```

\\n



Prevent eval

⊘ ||

5



1000



&



Allow dot notation?



Allow comma arrays?


```
length: 4151
  lines: 1
```



Output

```
time: 10ms
length: 3461
lines: 24
```



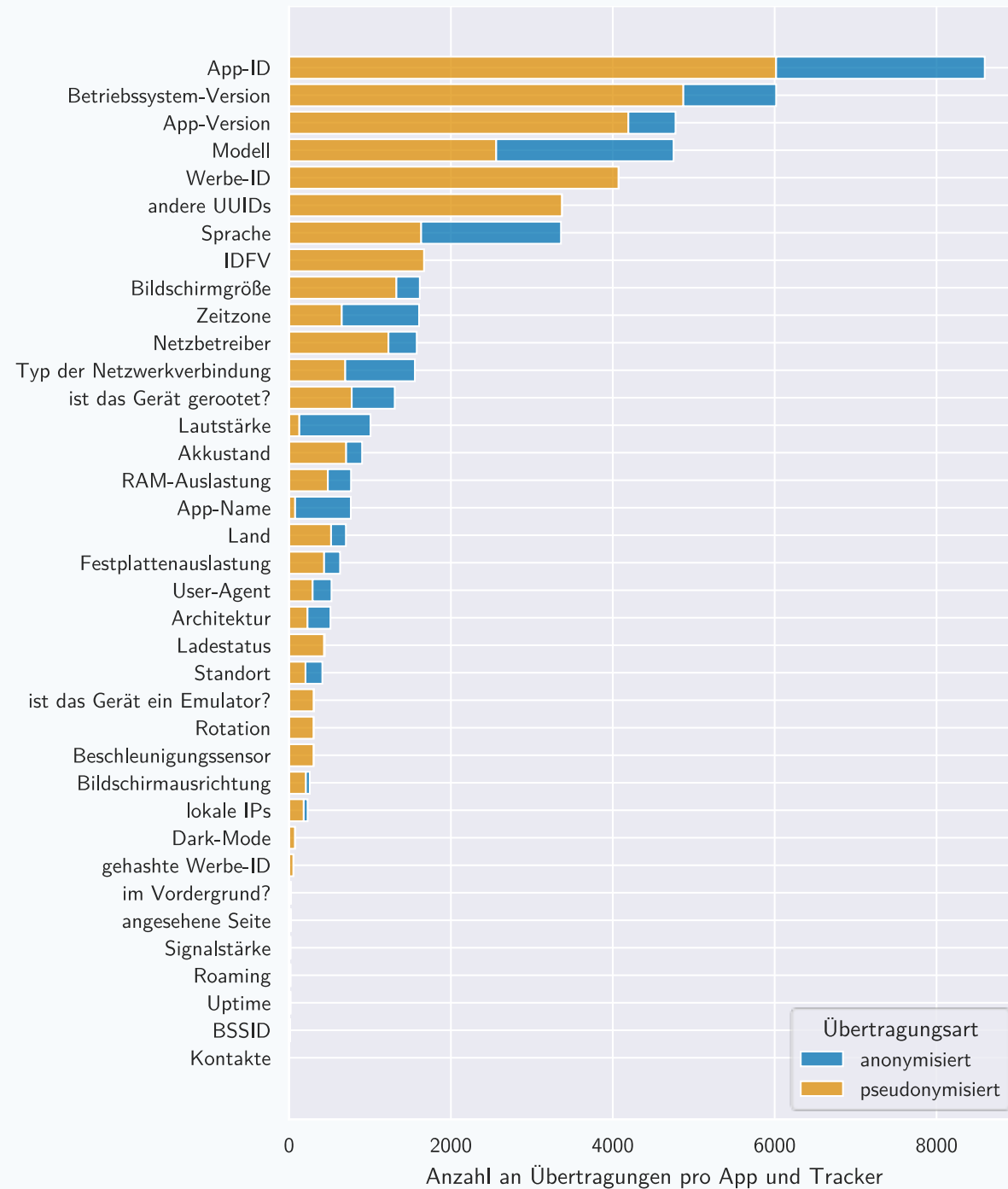
```
{
  "313732607382406/activities?access_token: "313732607382406|7e5f1e2769be769bb6710ffbc14399c2",
  advertiser_id_collection_enabled: "1",
  anon_id: "XZ0BAE1D89-562C-4B77-9D29-29E9E80F3051",
  application_tracking_enabled: "1",
  custom_events: "[{\\"_eventName\\":\\"Backend_OK\\",\\"_logTime\\":1650911380,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"},{\\"_eventName\\":\\"ADReport_RequestError\\",\\"_logTime\\":1650911382,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"},{\\"_eventName\\":\\"ADReport_RequestStart\\",\\"_logTime\\":1650911382,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"},{\\"_eventName\\":\\"ADReport_RequestError\\",\\"_logTime\\":1650911383,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"},{\\"_eventName\\":\\"ADReport_RequestStart\\",\\"_logTime\\":1650911383,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"},{\\"_eventName\\":\\"ADReport_RequestError\\",\\"_logTime\\":1650911383,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"},{\\"_eventName\\":\\"ADStart_RequestError\\",\\"_logTime\\":1650911384,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"},{\\"_eventName\\":\\"ADStart_RequestStart\\",\\"_logTime\\":1650911384,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"},{\\"_eventName\\":\\"ADOpen_RequestStart\\",\\"_logTime\\":1650911384,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"},{\\"_eventName\\":\\"ADOpen_RequestError\\",\\"_logTime\\":1650911384,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"},{\\"_eventName\\":\\"ADStart_RequestError\\",\\"_logTime\\":1650911384,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"},{\\"_eventName\\":\\"ADStart_RequestStart\\",\\"_logTime\\":1650911384,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"},{\\"_eventName\\":\\"ADOpen_RequestStart\\",\\"_logTime\\":1650911385,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"},{\\"_eventName\\":\\"ADOpen_RequestError\\",\\"_logTime\\":1650911385,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"},{\\"_eventName\\":\\"ADOpen_RequestStart\\",\\"_logTime\\":1650911387,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"},{\\"_eventName\\":\\"ADOpen_RequestError\\",\\"_logTime\\":1650911387,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"},{\\"_eventName\\":\\"ADOpen_RequestStart\\",\\"_logTime\\":1650911388,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"},{\\"_eventName\\":\\"ADOpen_RequestError\\",\\"_logTime\\":1650911388,\\"_valueToSum\\":1,\\"_ui\\":\\"UINavigationController\\"}]"
}
```

in CyberChef anschauen

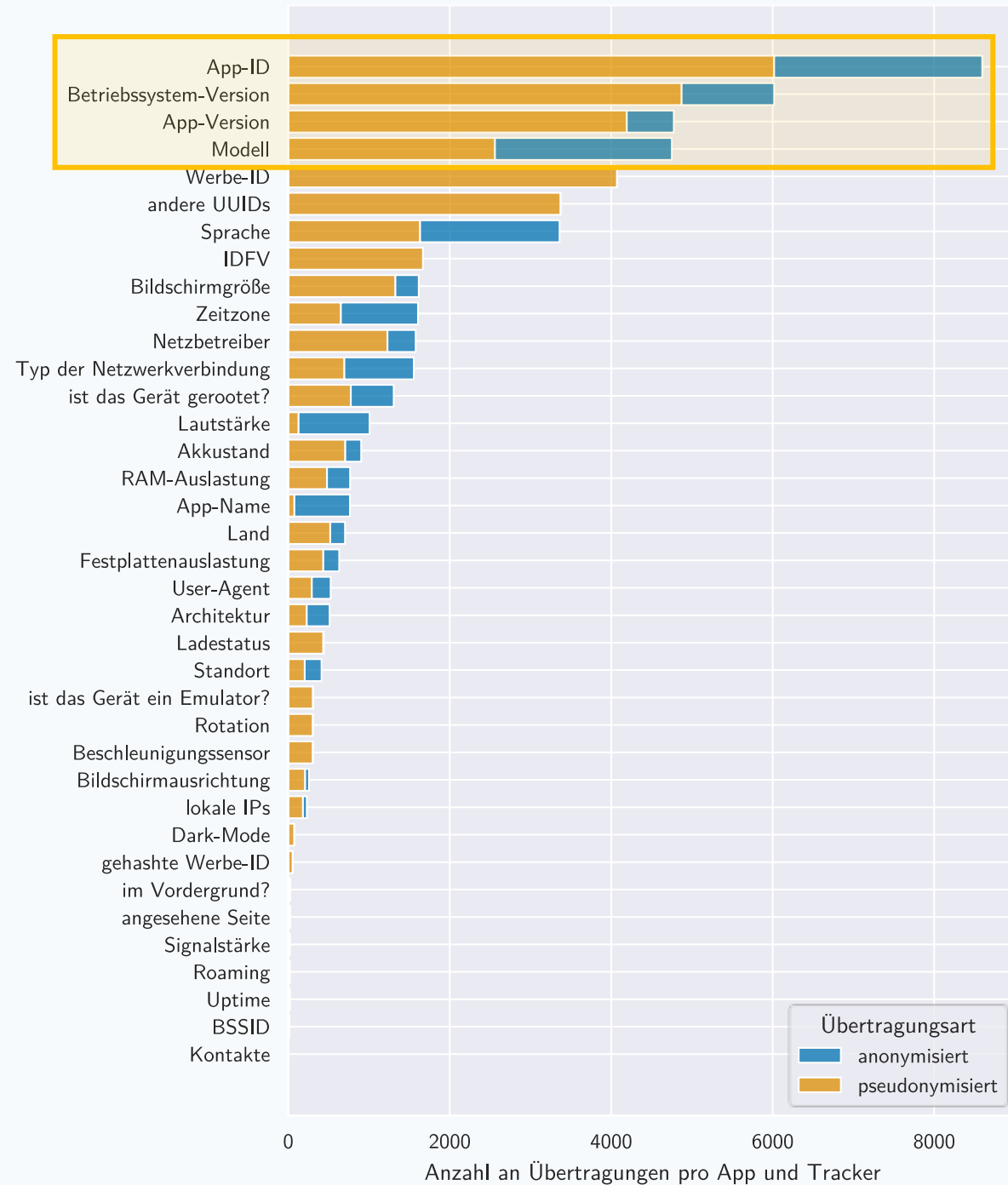
Anzahl	Endpunkt
4098	https://digitalassetlinks.googleapis.com/google.digitalassetlinks.v1.AssetLinks/Check
3015	https://app-measurement.com/a
2154	https://googleads.g.doubleclick.net/mads/gma
1836	https://csi.gstatic.com/csi
1643	https://csi.gstatic.com/csi
1543	https://googleads.g.doubleclick.net/pagead/interaction/
1214	https://googleads.g.doubleclick.net/favicon.ico
1212	https://fcmtoken.googleapis.com/register
1087	https://googleads.g.doubleclick.net/getconfig/pubsetting
1069	https://fonts.googleapis.com/css
1028	https://firebaselogging-pa.googleapis.com/v1/firelog/legacy/batchlog
1024	https://prod-ms.applovin.com/1.0/event/lerr
987	https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.js
986	https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.appcache
953	https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js
845	https://logs.ironsrc.mobi/logs
783	https://pagead2.googlesyndication.com/pagead/gen_204
753	https://www.facebook.com/adnw_sync2
719	https://www.googletagservices.com/activeview/js/current/lidar.js
675	https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html

26 Adapter für spezifische
Endpunkte reichen, um **10 %** des
gesamten Traffics abzudecken.

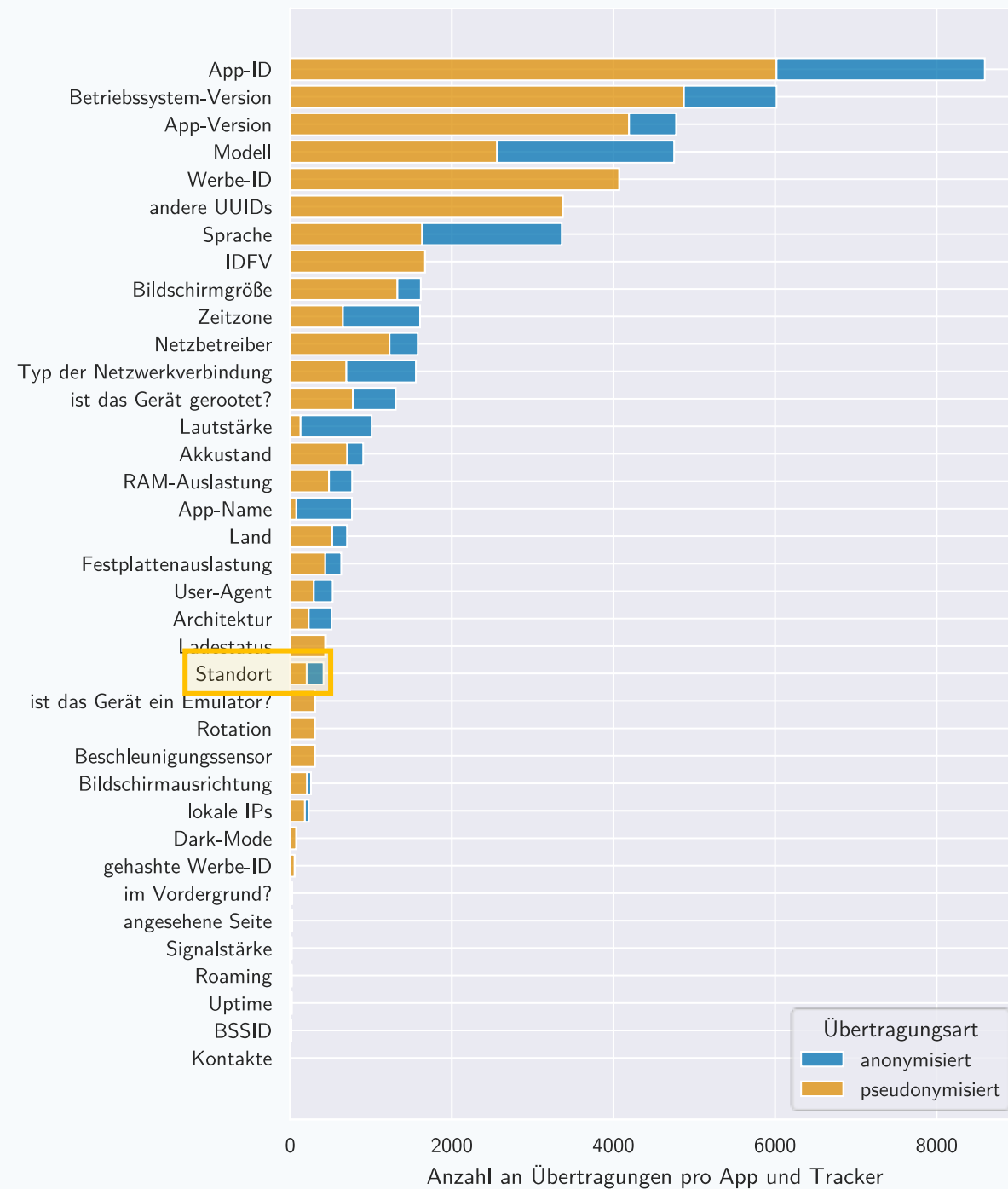
Anzahl an Übertragungen der beobachteten Datentypen pro App und Tracker, vor irgendeiner Interaktion.



Anzahl an Übertragungen der beobachteten Datentypen pro App und Tracker, vor irgendeiner Interaktion.



Anzahl an Übertragungen der beobachteten Datentypen pro App und Tracker, vor irgendeiner Interaktion.



The background image shows a person's hand pointing at a map pinned to a blue surface. The map features various locations like 'Santo Domingo' and 'San Pedro de Macoris'. A large white text overlay reads 'Maßnahmen gegen Tracking'.

Maßnahmen gegen Tracking

Foto angepasst nach: „person working on blue and white paper on board“ von Alvaro Reyes (Unsplash-Lizenz)

[illegible]



exodus

Die Datenschutz-Audit-Plattform
für Android-Anwendungen

Einen Bericht suchen

Name der Anwendung

Sie können nach einer Anwendung mit ihrem Namen, Handle oder ihrer Google Play-URL suchen

z. B.: *Meteo France* oder *fr.meteo* oder *https://play.google.com/store/apps/details?id=fr.meteo*

Sie können die Anwendung nicht finden? Suchen Sie sie unter [Google Play](#).

Los geht's!

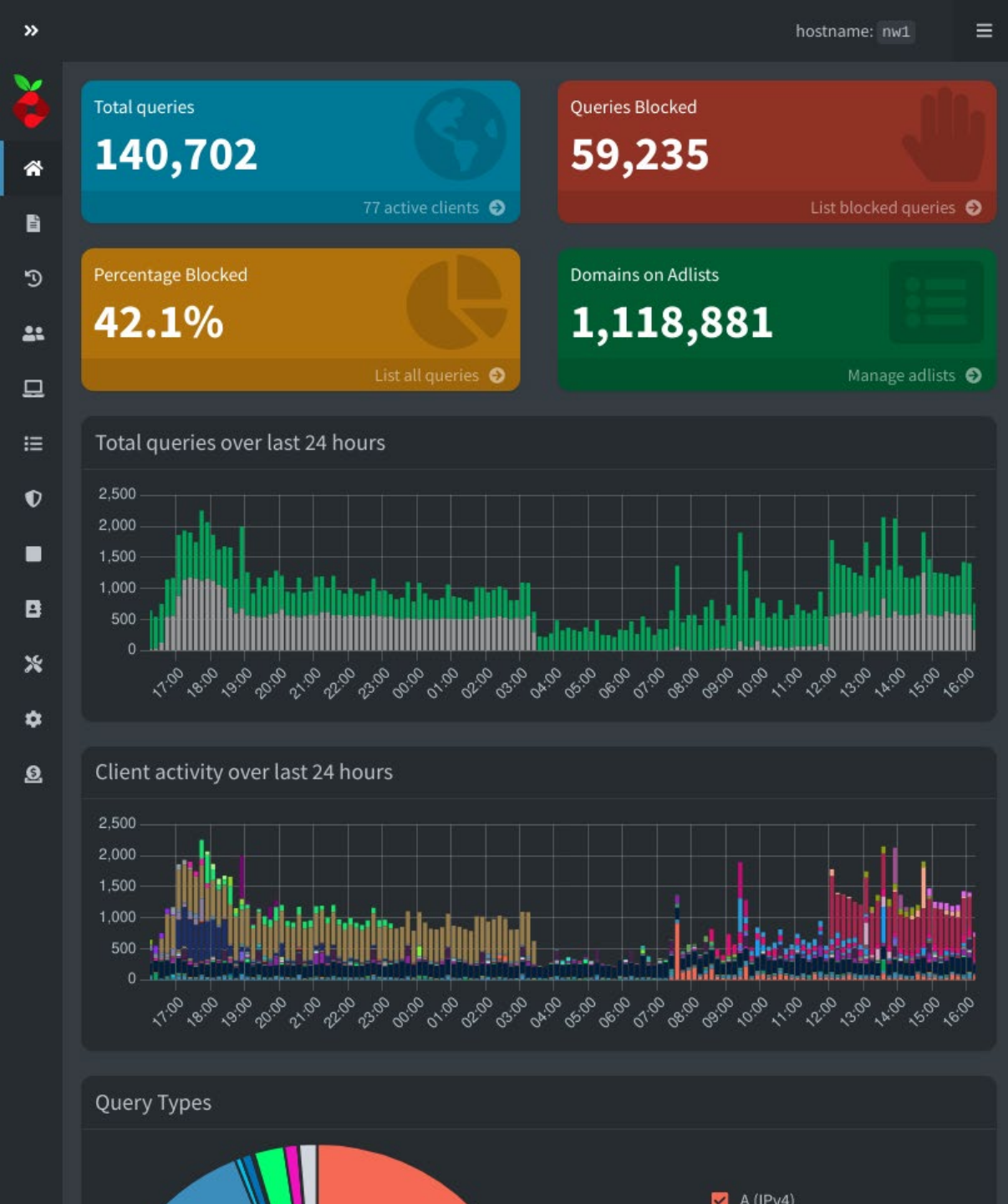
Suchen Sie nach einer Anwendung, die wir noch nicht kennen?

Eine neue Analyse durchführen

exodus analysiert Android-Anwendungen, um **eingebettete Tracker aufzulisten**.

Mithilfe von **exodus**
kannst Du herausfinden,
welche Tracker eine
Android-App einbindet.

> <https://reports.exodus-privacy.eu.org/de>



Pi-hole blockiert
Anfragen an Tracking-
Server (und Werbung)
auf der DNS-Ebene.

➤ <https://pi-hole.net/>

Rechtliche Handhabe

Die DSGVO stellt hohe Anforderungen an Tracking und erlaubt uns, gegen illegales Tracking vorzugehen.

Wann gilt die DSGVO? (Art. 2 DSGVO)

Die DSGVO gilt für die *Verarbeitung* von *personenbezogenen Daten*.

Wann gilt die DSGVO? (Art. 2 DSGVO)

Die DSGVO gilt für die *Verarbeitung von personenbezogenen Daten*.

- *personenbezogene Daten*: „**alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen**;

“ (Art. 4 Nr. 1 DSGVO)

Wann gilt die DSGVO? (Art. 2 DSGVO)

Die DSGVO gilt für die *Verarbeitung* von *personenbezogenen Daten*.

- *personenbezogene Daten*: „**alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen**; [also eine], die direkt oder indirekt, insbesondere mittels Zuordnung zu einer [...] einer **Kennnummer**, [...] identifiziert werden kann“ (Art. 4 Nr. 1 DSGVO)

Wann gilt die DSGVO? (Art. 2 DSGVO)

Die DSGVO gilt für die *Verarbeitung* von *personenbezogenen Daten*.

- *personenbezogene Daten*: „**alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen**; [also eine], die direkt oder indirekt, insbesondere mittels Zuordnung zu einer [...] einer **Kennnummer**, [...] identifiziert werden kann“ (Art. 4 Nr. 1 DSGVO)
- *Verarbeitung*: „**jede[r] [...] Vorgang [...] im Zusammenhang mit personenbezogenen Daten**

“ (Art. 4 Nr. 2 DSGVO)

Wann gilt die DSGVO? (Art. 2 DSGVO)

Die DSGVO gilt für die *Verarbeitung* von *personenbezogenen Daten*.

- *personenbezogene Daten*: „**alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen**; [also eine], die direkt oder indirekt, insbesondere mittels Zuordnung zu einer [...] einer **Kennnummer**, [...] identifiziert werden kann“ (Art. 4 Nr. 1 DSGVO)
- *Verarbeitung*: „**jede[r] [...] Vorgang [...] im Zusammenhang mit personenbezogenen Daten** wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das **Auslesen**, das Abfragen, die Verwendung, die **Offenlegung durch Übermittlung**, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“ (Art. 4 Nr. 2 DSGVO)

Wo gilt die DSGVO? (Art. 3 DSGVO)

- Die DSGVO gilt für alle Unternehmen in der EU.

Wo gilt die DSGVO? (Art. 3 DSGVO)

- Die DSGVO gilt für alle Unternehmen in der EU.
- Aber auch für Unternehmen außerhalb der EU, falls Du in der EU bist und
 - das Unternehmen Dir gezielt Waren oder Dienstleistungen anbietet; oder
 - Dein Verhalten beobachtet (-> Tracking).

➤ <https://www.datenanfragen.de/blog/dsgvo-raeumlicher-anwendungsbereich/>

Rechtsgrundlagen

Jede Verarbeitung braucht eine Rechtsgrundlage (Art. 6 Abs. 1 DSGVO):

- (a) Die betroffene Person hat ihre **Einwilligung** [...] gegeben;
- (b) die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, [...] erforderlich [...];
- (c) die Verarbeitung ist zur Erfüllung einer **rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;
- (d) die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- (e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die [...] in Ausübung **öffentlicher Gewalt** erfolgt, die dem Verantwortlichen übertragen wurde;
- (f) die Verarbeitung ist zur Wahrung der **berechtigten Interessen** des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person [...] überwiegen [...].

Rechtsgrundlagen für Tracking

Jede Verarbeitung braucht eine Rechtsgrundlage (Art. 6 Abs. 1 DSGVO):

- (a) Die betroffene Person hat ihre **Einwilligung** [...] gegeben;
- (b) die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, [...] erforderlich [...];
- ~~(c) die Verarbeitung ist zur Erfüllung einer **rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;~~
- ~~(d) die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen;~~
- ~~(e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die [...] in Ausübung **öffentlicher Gewalt** erfolgt, die dem Verantwortlichen übertragen wurde;~~
- (f) die Verarbeitung ist zur Wahrung der **berechtigten Interessen** des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person [...] überwiegen [...].

Für Tracking ist in aller Regel
eine Einwilligung die einzig
mögliche Rechtsgrundlage.

vgl. EDPB, Datenschutzkonferenz, LfDI BaWü

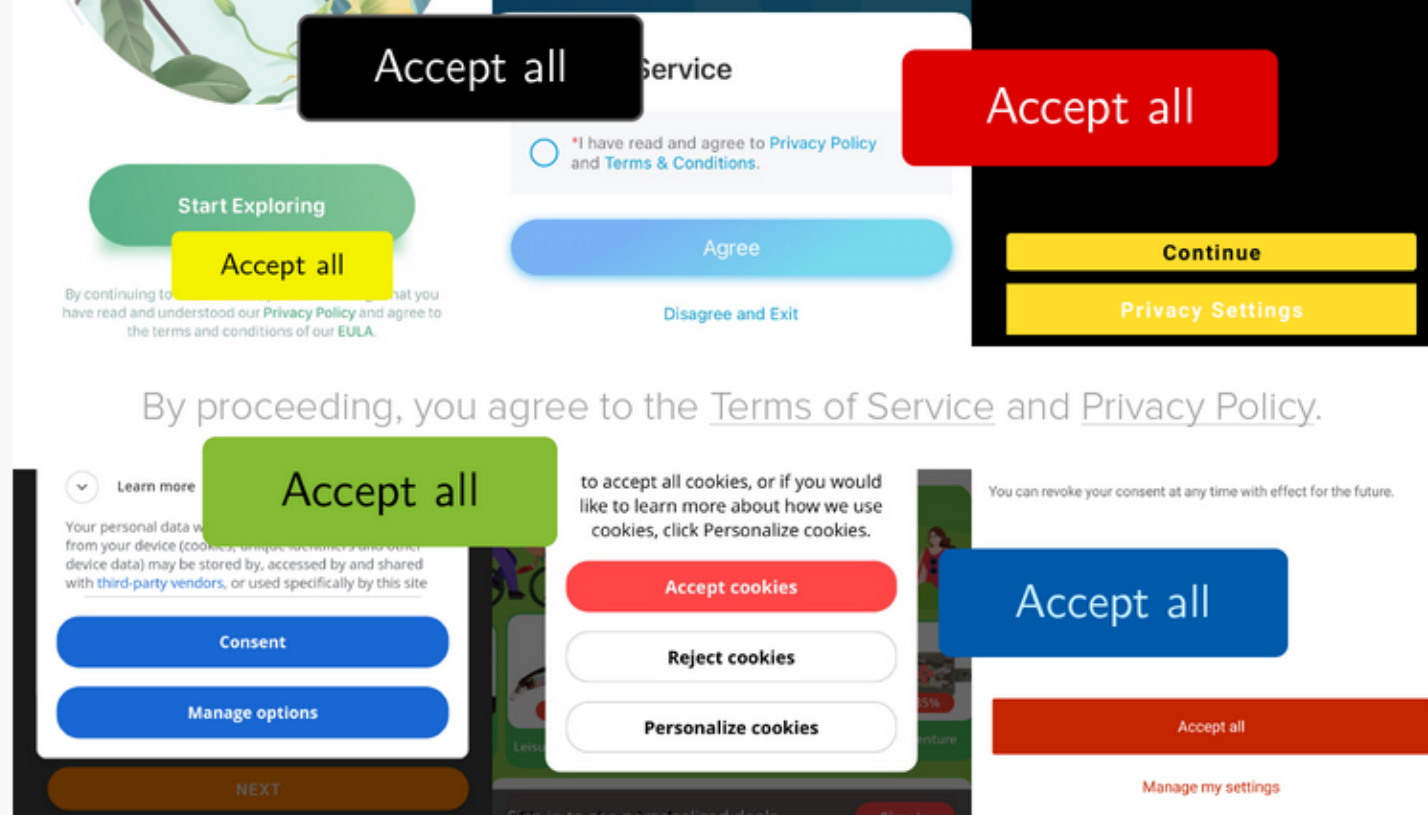
ePrivacy-Richtlinie

Art. 5 Abs. 3 ePrivacy-Richtlinie geht noch weiter und erfasst alle auf Gerät gespeicherten Informationen:

„Die Mitgliedstaaten stellen sicher, dass die **Speicherung von Informationen** oder der **Zugriff auf Informationen, die [...] im Endgerät [...] gespeichert sind, nur gestattet** ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen [...] seine **Einwilligung gegeben hat**. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.“

Wirksame Einwilligungen

Die Anforderungen an Einwilligungen sind hoch. Ein paar Beispiele, die keine wirksame Einwilligung einholen können.



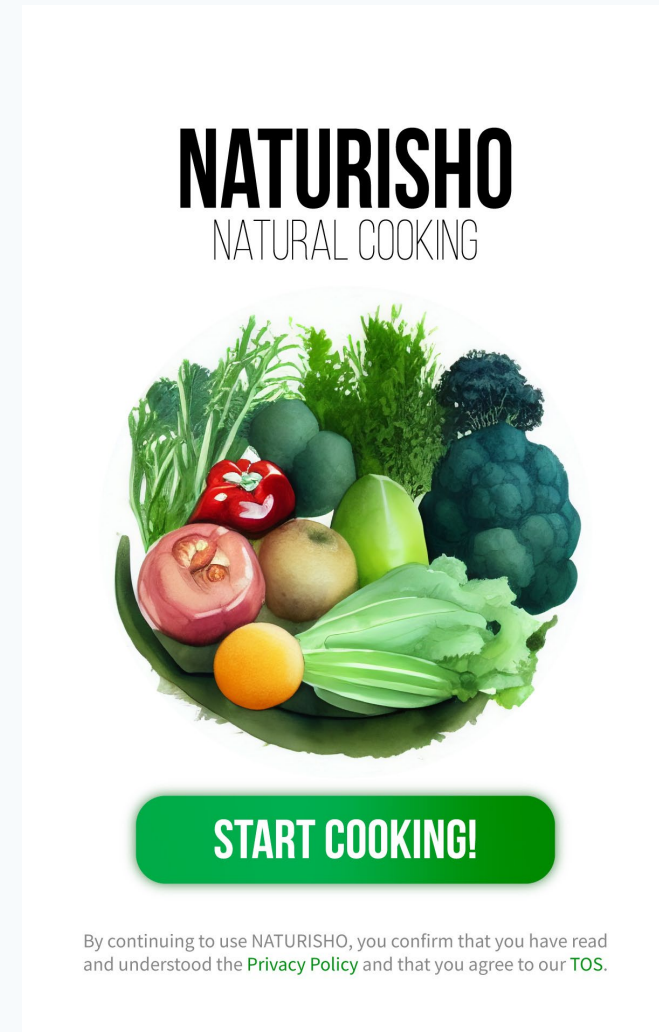
Legal requirements for tracking and consent dialogs under the GDPR and ePrivacy directive

Published: 2022-09-20T16:54

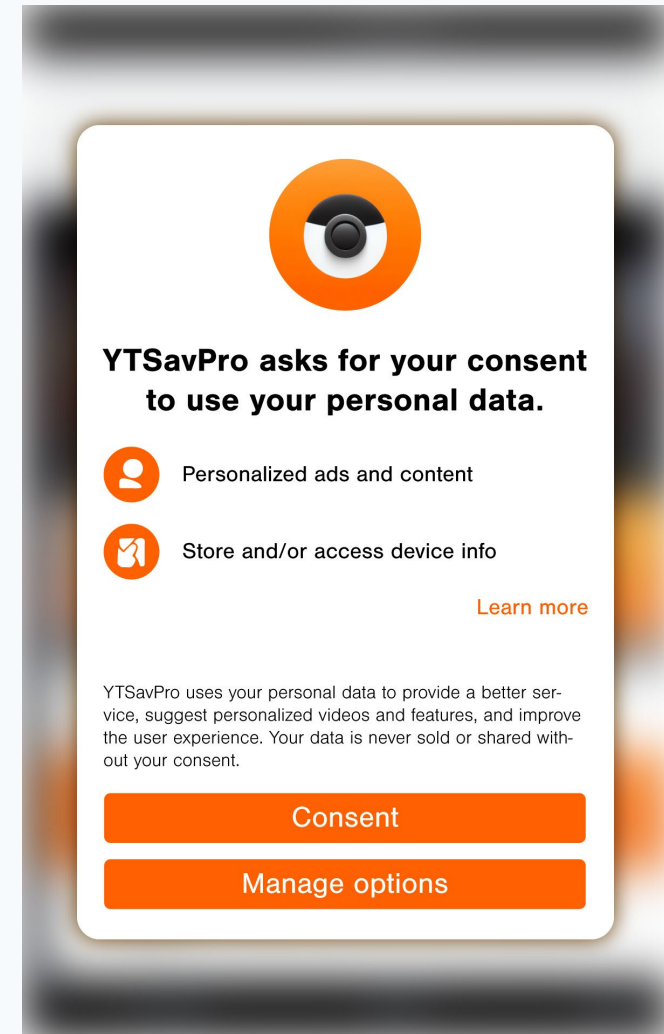
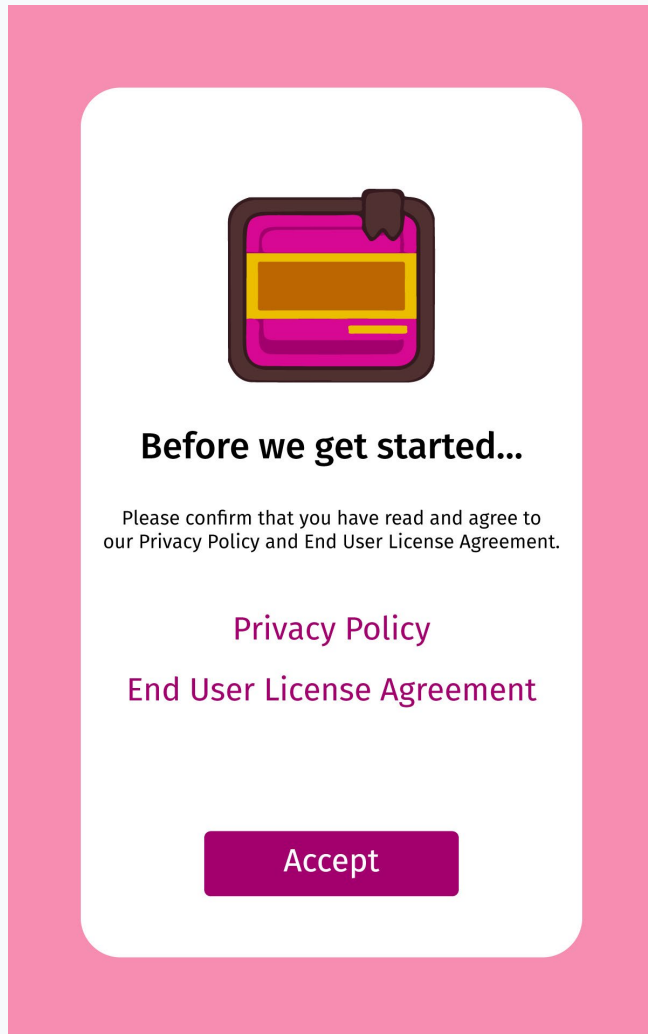
Consent and cookie notices seem ubiquitous both on the web and on mobile. They are an effort by publishers to comply with data protection legislation like the *General Data Protection Regulation* (GDPR), an EU regulation that went into force in 2018 and mandates strict legal guidelines for processing personal data. The flood of consent dialogs is often wrongly



Eindeutige Handlung



Ablehnung nicht schwerer



Eindeutige Buttons

We value your privacy.

Welcome to our newspaper app! As a user, you can expect to stay up-to-date on the latest news and current events with ease. Our app is designed to bring you the most relevant and important stories from around the world, covering a wide range of topics including politics, business, entertainment, sports, and more.

In order to provide you with a personalized and enjoyable experience, we may collect certain information about your interests and reading habits. This data helps us to curate a customized news feed for you, ensuring that you are presented with the stories that are most likely to be of interest to you. For example, if you frequently read articles about politics and current events, you may see more articles about those topics in your feed. We may also use your personal data to improve the overall functionality and user experience of the app, such as by identifying and fixing technical issues or enhancing the layout and design.

In addition to our curated news feed, our app also offers a range of other features to help you stay informed. You can customize your notification settings to receive alerts about breaking news or topics that you care about. You can also save articles to read later or share them with

Okay.

Manage my choices.



Your Privacy is Our Top Priority!

Our app allows you to easily refill your prescriptions and have them delivered right to your door. We collect information about your *pre-scription history* and medication needs to process orders efficiently and provide *personalized recommendations*.

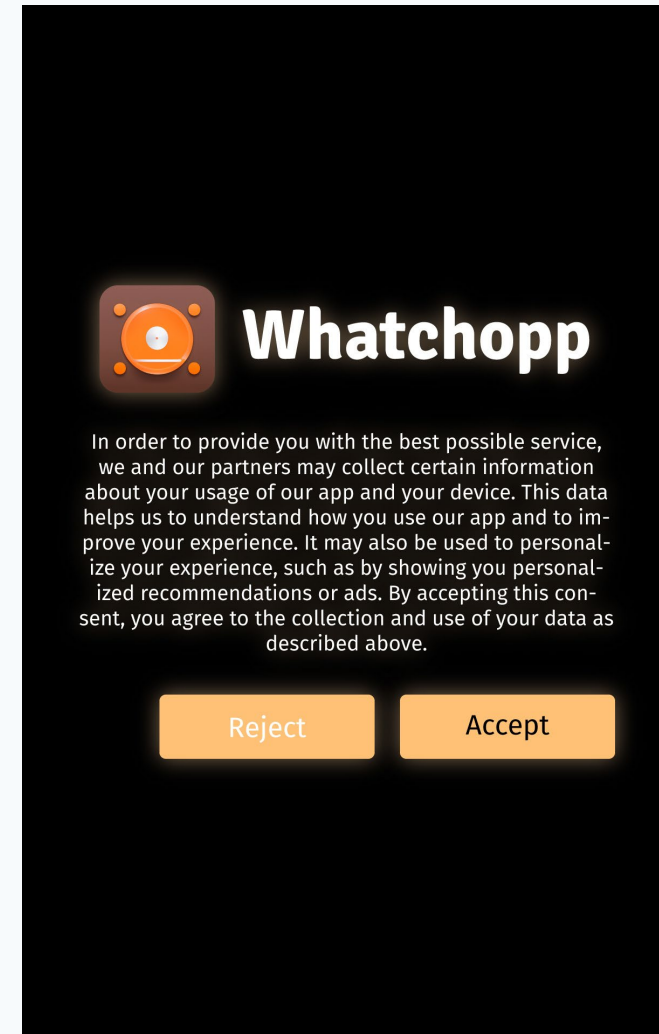
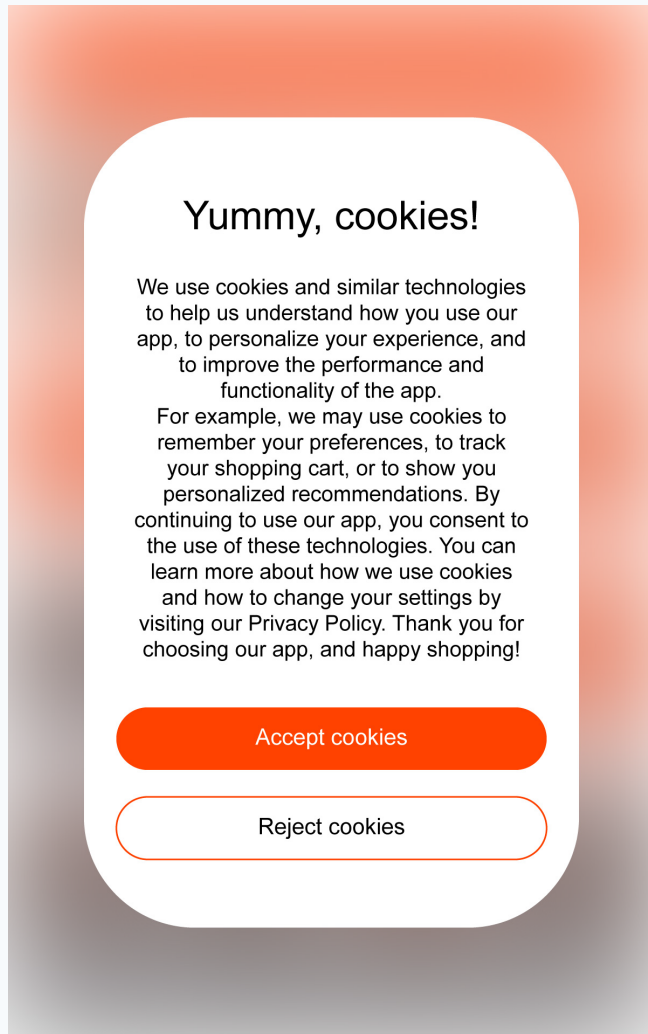
We understand that the privacy and security of your personal and health information is important, and we are committed to protecting it. Your information is kept secure and confidential, and we will never sell or share it without your explicit consent.

You can always revoke your consent later if you change your mind. Thank you for choosing us!

Accept all

Manage my settings

„Akzeptieren“ nicht hervorheben



„Akzeptieren“ nicht hervorheben

ChatEase

Your privacy is in your hands

In order to provide you with the best possible service, we may collect certain information about your usage of the app. This data helps us to improve the performance and functionality of the app, such as by identifying and fixing technical issues or enhancing the user experience. We may also use this information to personalize your experience within the app, such as by suggesting friends or features that we think you might be interested in.

We understand that the protection and privacy of your personal information is important, and we take great care to ensure that your data is kept secure. Your messages and conversations are encrypted to protect against unauthorized access, and we will never sell or share your personal information with third parties without your explicit consent. Thank you for choosing our app, and we hope that you enjoy staying connected with us.

Accept all

Reject all

[Terms of Use](#)

[Skip](#)

Welcome to FitMizo!



Transform your body and mind!

I accept the terms of service and privacy policy.

Accept

Einwilligung nicht verpflichtend



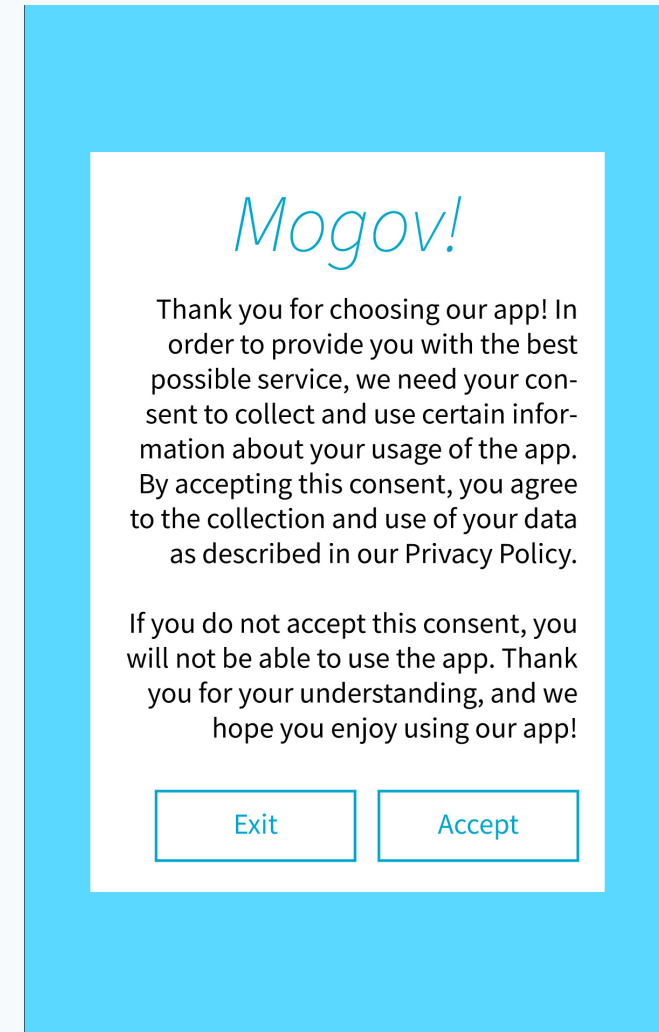
The image shows a dark blue background with abstract geometric shapes. The word "toppnotch" is written in a bold, white, sans-serif font. Below it, there is a white rounded rectangle containing the text "Privacy Consent". To the left of the text is a checked checkbox. The text continues: "I agree to the [privacy policy](#) and want to use the toppnotch app." At the bottom, there are two links: "Agree" and "Disagree and Exit", both in blue text.

toppnotch

Privacy Consent

☒ I agree to the [privacy policy](#) and want to use the toppnotch app.

[Agree](#) [Disagree and Exit](#)



The image shows a light blue background. In the center, there is a white rounded rectangle. At the top, the word "Mogov!" is written in a blue, cursive font. Below it, there is a paragraph of text: "Thank you for choosing our app! In order to provide you with the best possible service, we need your consent to collect and use certain information about your usage of the app. By accepting this consent, you agree to the collection and use of your data as described in our Privacy Policy." Below this, there is another paragraph: "If you do not accept this consent, you will not be able to use the app. Thank you for your understanding, and we hope you enjoy using our app!" At the bottom, there are two buttons: "Exit" and "Accept", both in blue text.

Mogov!

Thank you for choosing our app! In order to provide you with the best possible service, we need your consent to collect and use certain information about your usage of the app. By accepting this consent, you agree to the collection and use of your data as described in our Privacy Policy.

If you do not accept this consent, you will not be able to use the app. Thank you for your understanding, and we hope you enjoy using our app!

[Exit](#) [Accept](#)

Wenn eine App auch nur
gegen ein einziges dieser
Kriterien verstößt, entsteht
keine gültige Einwilligung.

Das Tracking erfolgt dann ohne
Rechtsgrundlage und ist illegal.

Analyse von Einwilligungsdialogen

Wir wollen **automatisiert überprüfen**,
wie üblich Einwilligungsdialoge sind und
ob Apps sich an die Anforderungen
halten.

Inspector

Console

Debugger

Network

Style Editor

Performance

Memory

Storage

Accessibility

Application

Filter Output

Errors

Warnings

Logs

Info

Debug

CSS

XHR

Requests

>> _tcfapi('getTCData', 2, (data) => console.log(data))

▼ Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "cmpuishown", cmpStatus: "loaded", listenerId: undefined, tcString: "CPZJTs0PZJTs0AcABBENCPCgAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAA.YAAAD_gAAAA", isServiceSpecific: true, useNonStandardStacks: false, ... } instrument.ts:124:32

cmpId: 28

cmpStatus: "loaded"

cmpVersion: 1

eventStatus: "cmpuishown"

gdprApplies: true

isServiceSpecific: true

listenerId: undefined

▶ outOfBand: Object { allowedVendors: {}, disclosedVendors: {} }

▶ publisher: Object { consents: {}, legitimateInterests: {...}, customPurpose: {...}, ... }

publisherCC: "US"

▼ purpose: Object { consents: {}, legitimateInterests: {...} }

▶ consents: Object { }

▶ legitimateInterests: Object { 1: false, 2: true, 3: true, ... }

▶ <prototype>: Object { ... }

purposeOneTreatment: false

specialFeatureOptins: Object { }

tcString: "CPZJTs0PZJTs0AcABBENCPCgAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAA.YAAAD_gAAAA"

tcfPolicyVersion: 2

useNonStandardStacks: false

▼ vendor: Object { consents: {}, legitimateInterests: {...} }

▶ consents: Object { }

▶ legitimateInterests: Object { 1: false, 2: false, 3: false, ... }

▶ <prototype>: Object { ... }

>>

Top

Inspector

Console

Debugger

Network

Style Editor

Performance

Memory

Storage

Accessibility

Application

Filter Output

Errors

Warnings

Logs

Info

Debug

CSS

XHR

Requests

>

_tcfapi('getTCData', 2, (data) => console.log(data))

▼

Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "cmpuishown", cmpStatus: "loaded", listenerId: undefined, tcString: "CPZJTs0PZJTs0AcABBENCPCgAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAA.YAAAD_gAAAA", isServiceSpecific: true, useNonStandardStacks: false, ... }

instrument.ts:124:32

cmpId: 28

cmpStatus: "loaded"

cmpVersion: 1

eventStatus: "cmpuishown"

gdprApplies: true

isServiceSpecific: true

listenerId: undefined

▶ outOfBand: Object { allowedVendors: {}, disclosedVendors: {} }

▶ publisher: Object { consents: {}, legitimateInterests: {...}, customPurpose: {...}, ... }

publisherCC: "US"

▼ purpose: Object { consents: {}, legitimateInterests: {...} }

▶ consents: Object { }

▶ legitimateInterests: Object { 1: false, 2: true, 3: true, ... }

▶ <prototype>: Object { ... }

purposeOneTreatment: false

▶ specialFeatureOptins: Object { }

tcString: "CPZJTs0PZJTs0AcABBENCPCgAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAA.YAAAD_gAAAA"

tcfPolicyVersion: 2

useNonStandardStacks: false

▼ vendor: Object { consents: {}, legitimateInterests: {...} }

▶ consents: Object { }

▶ legitimateInterests: Object { 1: false, 2: false, 3: false, ... }

▶ <prototype>: Object { ... }

>>

Top

Inspector

Console

Debugger

Network

Style Editor

Performance

Memory

Storage

Accessibility

Application

Filter Output

Errors

Warnings

Logs

Info

Debug

CSS

XHR

Requests

>> _tcfapi('getTCData', 2, (data) => console.log(data))

▼ Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "cmpuishown", cmpStatus: "loaded", listenerId: undefined, tcString: "CPZJTts0PZJTts0AcABBENCPCgAAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAAA.YAAAD_gAAAAA", isServiceSpecific: true, useNonStandardStacks: false, ... }

cmpId: 28

cmpStatus: "loaded"

cmpVersion: 1

eventStatus: "cmpuishown"

gdprApplies: true

isServiceSpecific: true

listenerId: undefined

▶ outOfBand: Object { allowedVendors: {}, disclosedVendors: {} }

▶ publisher: Object { consents: {}, legitimateInterests: {...}, customPurpose: {...}, ... }

publisherCC: "US"

▼ purpose: Object { consents: {}, legitimateInterests: {...} }

▶ consents: Object { }

▶ legitimateInterests: Object { 1: false, 2: true, 3: true, ... }

▶ <prototype>: Object { ... }

purposeOneTreatment: false

▶ specialFeatureOptins: Object { }

tcString: "CPZJTts0PZJTts0AcABBENCPCgAAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAAA.YAAAD_gAAAAA"

tcfPolicyVersion: 2

useNonStandardStacks: false

▼ vendor: Object { consents: {}, legitimateInterests: {...} }

▶ consents: Object { }

▶ legitimateInterests: Object { 1: false, 2: false, 3: false, ... }

▶ <prototype>: Object { ... }

>>

Top

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter Output Errors Warnings Logs Info Debug CSS XHR Requests

```
>> _tcfapi('getTCData', 2, (data) => console.log(data))
```

Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "cmpuishown", cmpStatus: "loaded", listenerId: undefined, tcString: "CPZJTts0PZJTts0AcABBENCPCgAAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAAA.YAAAD_gAAAAA", isServiceSpecific: true, useNonStandardStacks: false, ... }

instrument.ts:124:32

cmpId: 28

OneTrust

cmpStatus: "loaded"
cmpVersion: 1
eventStatus: "cmpuishown"
gdprApplies: true
isServiceSpecific: true
listenerId: undefined
outOfBand: Object { allowedVendors: {}, disclosedVendors: {} }
publisher: Object { consents: {}, legitimateInterests: {...}, customPurpose: {...}, ... }
publisherCC: "US"
purpose: Object { consents: {}, legitimateInterests: {...} }
 consents: Object { }
 legitimateInterests: Object { 1: false, 2: true, 3: true, ... }
 <prototype>: Object { ... }
purposeOneTreatment: false
specialFeatureOptins: Object { }
tcString: "CPZJTts0PZJTts0AcABBENCPCgAAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAAA.YAAAD_gAAAAA"
tcfPolicyVersion: 2
useNonStandardStacks: false
vendor: Object { consents: {}, legitimateInterests: {...} }
 consents: Object { }
 legitimateInterests: Object { 1: false, 2: false, 3: false, ... }
 <prototype>: Object { ... }

>> Top

Inspector

Console

Debugger

Network

Style Editor

Performance

Memory

Storage

Accessibility

Application

Filter Output

Errors

Warnings

Logs

Info

Debug

CSS

XHR

Requests

>> _tcfapi('getTCData', 2, (data) => console.log(data))

▼ Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "cmpuishown", cmpStatus: "loaded", listenerId: undefined, tcString: "CPZJTs0PZJTs0AcABBENCPCgAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAA.YAAAD_gAAAA", isServiceSpecific: true, useNonStandardStacks: false, ... } instrument.ts:124:32

cmpId: 28

cmpStatus: "loaded"

cmpVersion: 1

eventStatus: "cmpuishown"

gdprApplies: true

isServiceSpecific: true

listenerId: undefined

▶ outOfBand: Object { allowedVendors: {}, disclosedVendors: {} }

▶ publisher: Object { consents: {}, legitimateInterests: {...}, customPurpose: {...}, ... }

publisherCC: "US"

▼ purpose: Object { consents: {}, legitimateInterests: {...} }

▶ consents: Object { }

▶ legitimateInterests: Object { 1: false, 2: true, 3: true, ... }

▶ <prototype>: Object { ... }

purposeOneTreatment: false

▶ specialFeatureOptins: Object { }

tcString: "CPZJTs0PZJTs0AcABBENCPCgAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAA.YAAAD_gAAAA"

tcfPolicyVersion: 2

useNonStandardStacks: false

▼ vendor: Object { consents: {}, legitimateInterests: {...} }

▶ consents: Object { }

▶ legitimateInterests: Object { 1: false, 2: false, 3: false, ... }

▶ <prototype>: Object { ... }

>>

Top

Inspector

Console

Debugger

Network

Style Editor

Performance

Memory

Storage

Accessibility

Application

Filter Output

Errors

Warnings

Logs

Info

Debug

CSS

XHR

Requests

>> _tcfapi('getTCData', 2, (data) => console.log(data))

▼ Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "cmpuishown", cmpStatus: "loaded", listenerId: undefined, tcString: "CPZJTs0PZJTs0AcABBENCPCgAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAAA.YAAAD_gAAAAA", isServiceSpecific: true, useNonStandardStacks: false, ... } instrument.ts:124:32

cmpId: 28

cmpStatus: "loaded"

cmpVersion: 1

eventStatus: "cmpuishown"

gdprApplies: true

isServiceSpecific: true

listenerId: undefined

▶ outOfBand: Object { allowedVendors: {}, disclosedVendors: {} }

▶ publisher: Object { consents: {}, legitimateInterests: {...}, customPurpose: {...}, ... }

publisherCC: "US"

▼ purpose: Object { consents: {}, legitimateInterests: {...} }

▶ consents: Object { }

▶ legitimateInterests: Object { 1: false, 2: true, 3: true, ... }

▶ <prototype>: Object { ... }

purposeOneTreatment: false

▶ specialFeatureOptins: Object { }

tcString: "CPZJTs0PZJTs0AcABBENCPCgAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAAA.YAAAD_gAAAAA"

tcfPolicyVersion: 2

useNonStandardStacks: false

▼ vendor: Object { consents: {}, legitimateInterests: {...} }

▶ consents: Object { }

▶ legitimateInterests: Object { 1: false, 2: false, 3: false, ... }

▶ <prototype>: Object { ... }

>>

Top

Inspector

Console

Debugger

Network

Style Editor

Performance

Memory

Storage

Accessibility

Application

Filter Output

Errors

Warnings

Logs

Info

Debug

CSS

XHR

Requests

>> _tcfapi('getTCData', 2, (data) => console.log(data))

▼ Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "cmpuishown", cmpStatus: "loaded", listenerId: undefined, tcString: "CPZJTs0PZJTs0AcABBENCPCgAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAA.YAAAD_gAAAA", isServiceSpecific: true, useNonStandardStacks: false, ... } instrument.ts:124:32

cmpId: 28

cmpStatus: "loaded"

cmpVersion: 1

eventStatus: "cmpuishown"

gdprApplies: true

isServiceSpecific: true

listenerId: undefined

▶ outOfBand: Object { allowedVendors: {}, disclosedVendors: {} }

▶ publisher: Object { consents: {}, legitimateInterests: {...}, customPurpose: {...}, ... }

publisherCC: "US"

▶ purpose: Object { consents: {}, legitimateInterests: {...} }

▶ consents: Object { }

▶ legitimateInterests: Object { 1: false, 2: true, 3: true, ... }

▶ prototype: Object { ... }

purposeOneTreatment: false

specialFeatureOptins: Object { }

tcString: "CPZJTs0PZJTs0AcABBENCPCgAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAA.YAAAD_gAAAA"

tcfPolicyVersion: 2

useNonStandardStacks: false

▼ vendor: Object { consents: {}, legitimateInterests: {...} }

▶ consents: Object { }

▶ legitimateInterests: Object { 1: false, 2: false, 3: false, ... }

▶ prototype: Object { ... }

>>

Top ↕

Inspector

Console

Debugger

Network

Style Editor

Performance

Memory

Storage

Accessibility

Application

Filter Output

Errors

Warnings

Logs

Info

Debug

CSS

XHR

Requests

>> __tcfapi('getTCData', 2, (data) => console.log(data))

▼ Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "useractioncomplete", cmpStatus: "loaded", listenerId: undefined, tcString: "CPZJTs0PZJTs0AcABBENCPCkAP_AA...instrument.ts:124:32

useNonStandardStacks: false, ... }

cmpId: 28

cmpStatus: "loaded"

cmpVersion: 1

eventStatus: "useractioncomplete"

gdprApplies: true

isServiceSpecific: true

listenerId: undefined

outOfBand: Object { allowedVendors: {}, disclosedVendors: {} }

publisher: Object { consents: {...}, legitimateInterests: {...}, customPurpose: {...}, ... }

publisherCC: "US"

▼ purpose: Object { consents: {...}, legitimateInterests: {...} }

▶ consents: Object { 1: true, 2: true, 3: true, ... }

▶ legitimateInterests: Object { 1: false, 2: true, 3: true, ... }

▶ <prototype>: Object { ... }

purposeOneTreatment: false

▶ specialFeatureOptins: Object { 1: false, 2: true }

tcString: "CPZJTs0PZJTs0AcABBENCPCkAP_AA...f_gAD_gAAAAA"

tcfPolicyVersion: 2

useNonStandardStacks: false

▼ vendor: Object { consents: {...}, legitimateInterests: {...} }

▶ consents: Object { 1: false, 2: false, 3: false, ... }

▶ legitimateInterests: Object { 1: false, 2: false, 3: false, ... }

>>

Top

Inspector

Console

Debugger

Network

Style Editor

Performance

Memory

Storage

Accessibility

Application

Filter Output

Errors

Warnings

Logs

Info

Debug

CSS

XHR

Requests

>> __tcfapi('getTCData', 2, (data) => console.log(data))

▼ Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "useractioncomplete", cmpStatus: "loaded", listenerId: undefined, tcString: "CPZJTs0PZJTs0AcABBENCPCkAP_AAHAACiQImwFwAKgAYABKAESAJoAnABuAIQATsArMBXgFfALqAYEA0wBxADqAH6AP4AhgBG0C8wGMgMsgiICJoGWQDgAKgAyACIAH4AhABFgCjAF1AMCAcQA6gC8wGCAMsAA.f_gAD_gAAAAA", isServiceSpecific: true, useNonStandardStacks: false, ... } instrument.ts:124:32

cmpId: 28

cmpStatus: "loaded"

cmpVersion: 1

eventStatus: "useractioncomplete"

gdprApplies: true

isServiceSpecific: true

listenerId: undefined

outOfBand: Object { allowedVendors: {}, disclosedVendors: {} }

publisher: Object { consents: {...}, legitimateInterests: {...}, customPurpose: {...}, ... }

publisherCC: "US"

▼ purpose: Object { consents: {...}, legitimateInterests: {...} }

consents: Object { 1: true, 2: true, 3: true, ... }

legitimateInterests: Object { 1: false, 2: true, 3: true, ... }

<prototype>: Object { ... }

purposeOneTreatment: false

specialFeatureOptins: Object { 1: false, 2: true }

tcString: "CPZJTs0PZJTs0AcABBENCPCkAP_AAHAACiQImwFwAKgAYABKAESAJoAnABuAIQATsArMBXgFfALqAYEA0wBxADqAH6AP4AhgBG0C8wGMgMsgiICJoGWQDgAKgAyACIAH4AhABFgCjAF1AMCAcQA6gC8wGCAMsAA.f_gAD_gAAAAA"

tcfPolicyVersion: 2

useNonStandardStacks: false

▼ vendor: Object { consents: {...}, legitimateInterests: {...} }

consents: Object { 1: false, 2: false, 3: false, ... }

legitimateInterests: Object { 1: false, 2: false, 3: false, ... }

>>

Top

Inspector

Console

Debugger

Network

Style Editor

Performance

Memory

Storage

Accessibility

Application

Filter Output

Errors

Warnings

Logs

Info

Debug

CSS

XHR

Requests

>> __tcfapi('getTCData', 2, (data) => console.log(data))

▼ Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "useractioncomplete", cmpStatus: "loaded", listenerId: undefined, tcString: "CPZJTs0PZJTs0AcABBENCPCkAP_AAHAACiQImwFwAKgAYABkAESAJ0AnABuAIQATsArMBXgFfALqAYEA0wBxADqAH6AP4AhgBG0C8wGMgMsiICJoGWQDgAKgAyACIAH4AhABFgCjAF1AMCAcQA6gC8wGCAMsAA.f_gAD_gAAAAA", isServiceSpecific: true, useNonStandardStacks: false, ... } instrument.ts:124:32

cmpId: 28

cmpStatus: "loaded"

cmpVersion: 1

eventStatus: "useractioncomplete"

gdprApplies: true

isServiceSpecific: true

listenerId: undefined

▶ outOfBand: Object { allowedVendors: {}, disclosedVendors: {} }

▶ publisher: Object { consents: {...}, legitimateInterests: {...}, customPurpose: {...}, ... }

publisherCC: "IIS"

▶ purpose: Object { consents: {...}, legitimateInterests: {...} }

▶ consents: Object { 1: true, 2: true, 3: true, ... }

▶ legitimateInterests: Object { 1: false, 2: true, 3: true, ... }

▶ <prototype>: Object { ... }

purposeOneTreatment: false

▶ specialFeatureOptins: Object { 1: false, 2: true }

tcString: "CPZJTs0PZJTs0AcABBENCPCkAP_AAHAACiQImwFwAKgAYABkAESAJ0AnABuAIQATsArMBXgFfALqAYEA0wBxADqAH6AP4AhgBG0C8wGMgMsiICJoGWQDgAKgAyACIAH4AhABFgCjAF1AMCAcQA6gC8wGCAMsAA.f_gAD_gAAAAA"

tcfPolicyVersion: 2

useNonStandardStacks: false

▶ vendor: Object { consents: {...}, legitimateInterests: {...} }

▶ consents: Object { 1: false, 2: false, 3: false, ... }

▶ legitimateInterests: Object { 1: false, 2: false, 3: false, ... }

>>

Top

Funktioniert das auch für Apps?

- Es gibt den TCF-Standard auch für Apps.

Funktioniert das auch für Apps?

- Es gibt den TCF-Standard auch für Apps.
- Experiment mit 823 Android-Apps:
 - 21,99 % haben irgendein Einwilligungselement angezeigt.
 - 2,55 % haben TCF-Einstellungen gesetzt.

Funktioniert das auch für Apps?

- Es gibt den TCF-Standard auch für Apps.
- Experiment mit 823 Android-Apps:
 - 21,99 % haben irgendein Einwilligungselement angezeigt.
 - 2,55 % haben TCF-Einstellungen gesetzt.
- Wie wäre es mit Adaptern für spezifische CMPs?
 - Sehr grobes Experiment zur Nutzung bekannter CMPs: 2,8 % bei iOS, 7,15 % bei Android (obere Schranke).

Was jetzt?

- Stattdessen setzen wir auf text-basierte Erkennung üblicher Elemente in Einwilligungsdialogen.

Was jetzt?

- Stattdessen setzen wir auf text-basierte Erkennung üblicher Elemente in Einwilligungsdialogen.
- Dazu Regexes, die übliche Formulierungen erkennen, bspw.:
`/ (benutz | verwend | nutz | brauch | benötig | hab | setz
| sammel | frag) [^.]{0,25} (Cookie | Zustimmung
| Einwilligung | Einverständnis | Tracking) /`

Was jetzt?

- Stattdessen setzen wir auf text-basierte Erkennung üblicher Elemente in Einwilligungsdialogen.
- Dazu Regexes, die übliche Formulierungen erkennen, bspw.:
`/ (benutz | verwend | nutz | brauch | benötig | hab | setz
| sammel | frag) [^.]{0,25} (Cookie | Zustimmung
| Einwilligung | Einverständnis | Tracking) /`
- Zusätzliche Mechanismen, um False-Positives zu vermeiden, u. a. Punktesystem für übliche Schlagworte.

Einwilligungselemente

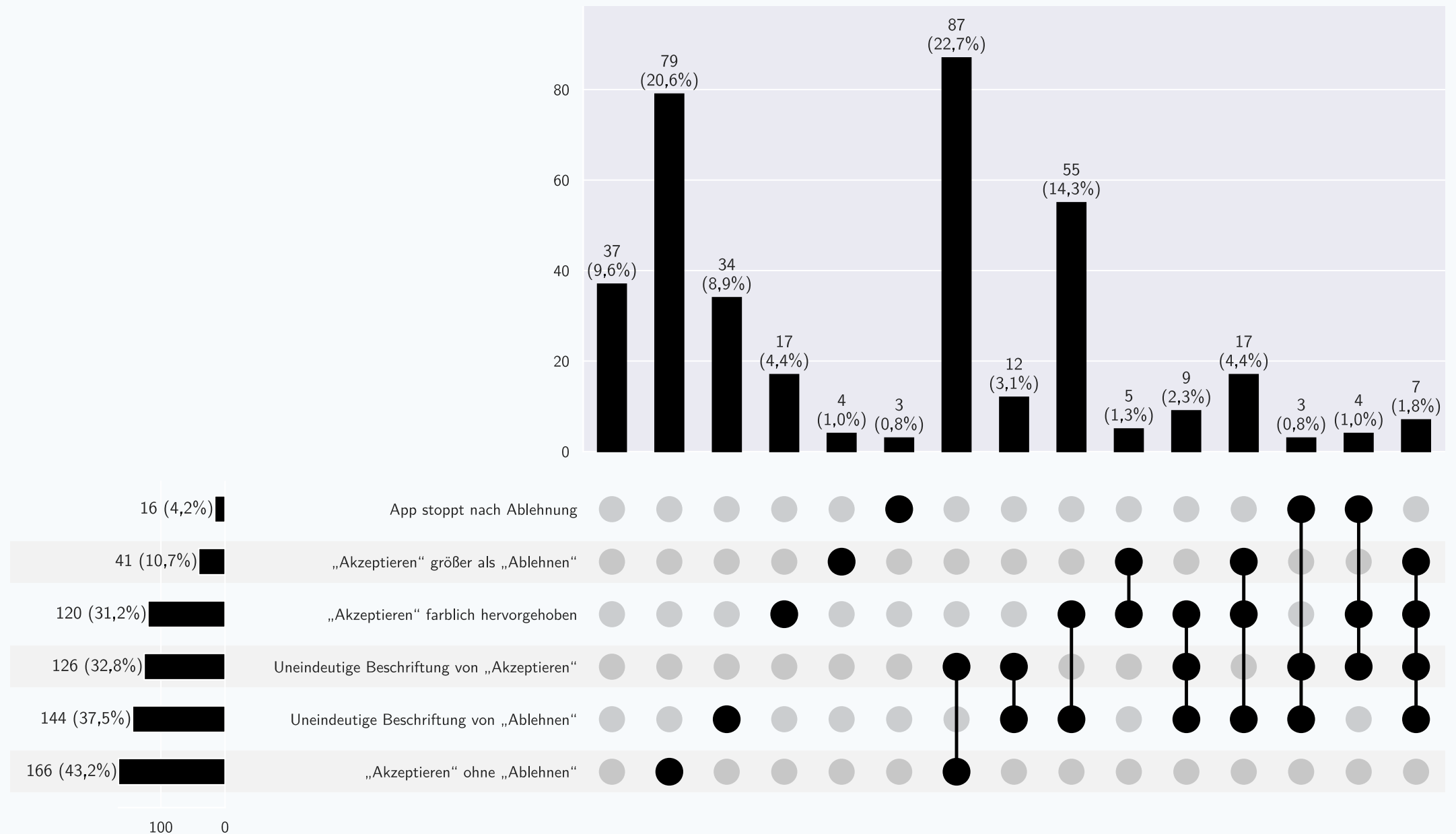
- Wir unterscheiden zwischen:
 - **Link:** App verlinkt nur Datenschutzerklärung, z. B. im Menü/Footer.
 - **Hinweis:** App weist auf Verarbeitung hin, gibt aber keine Wahl.
 - **Dialog:** App weist auf Verarbeitung hin und fragt aktiv Einwilligung ab.

Einwilligungselemente

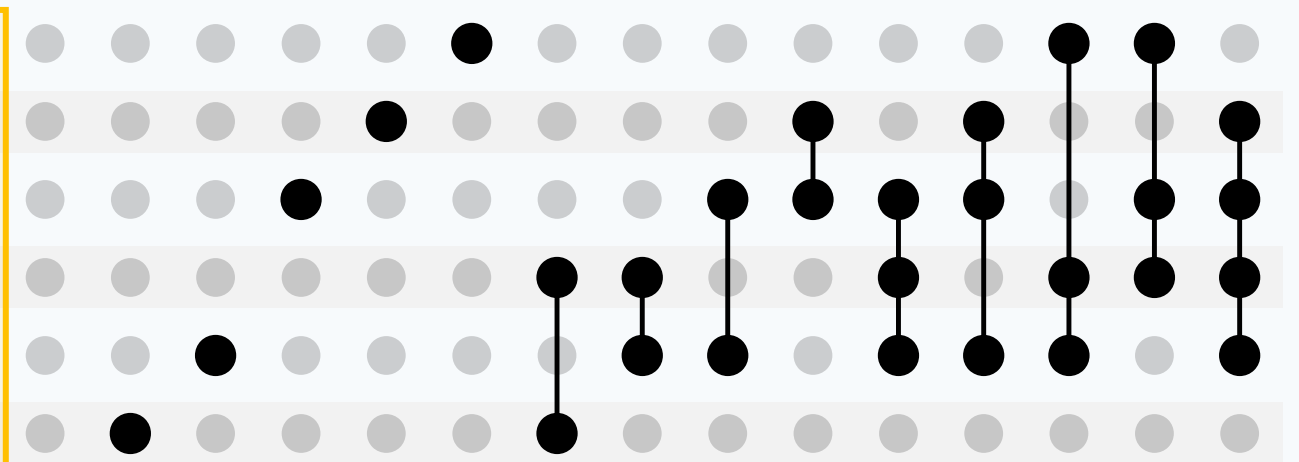
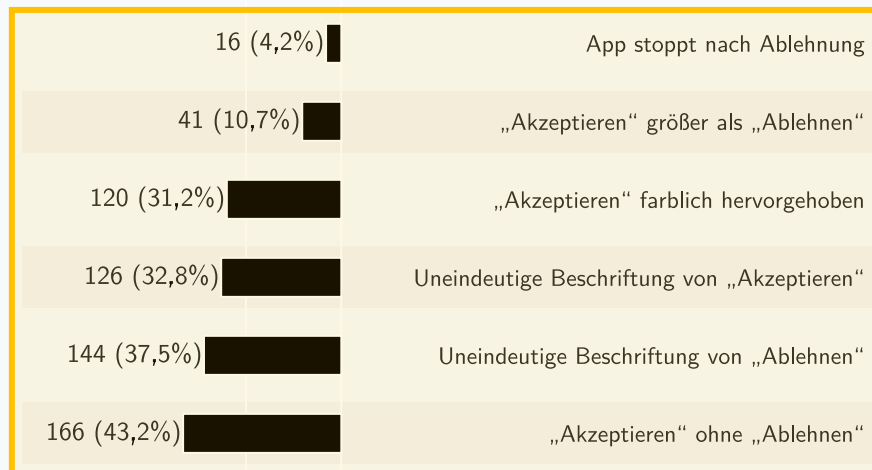
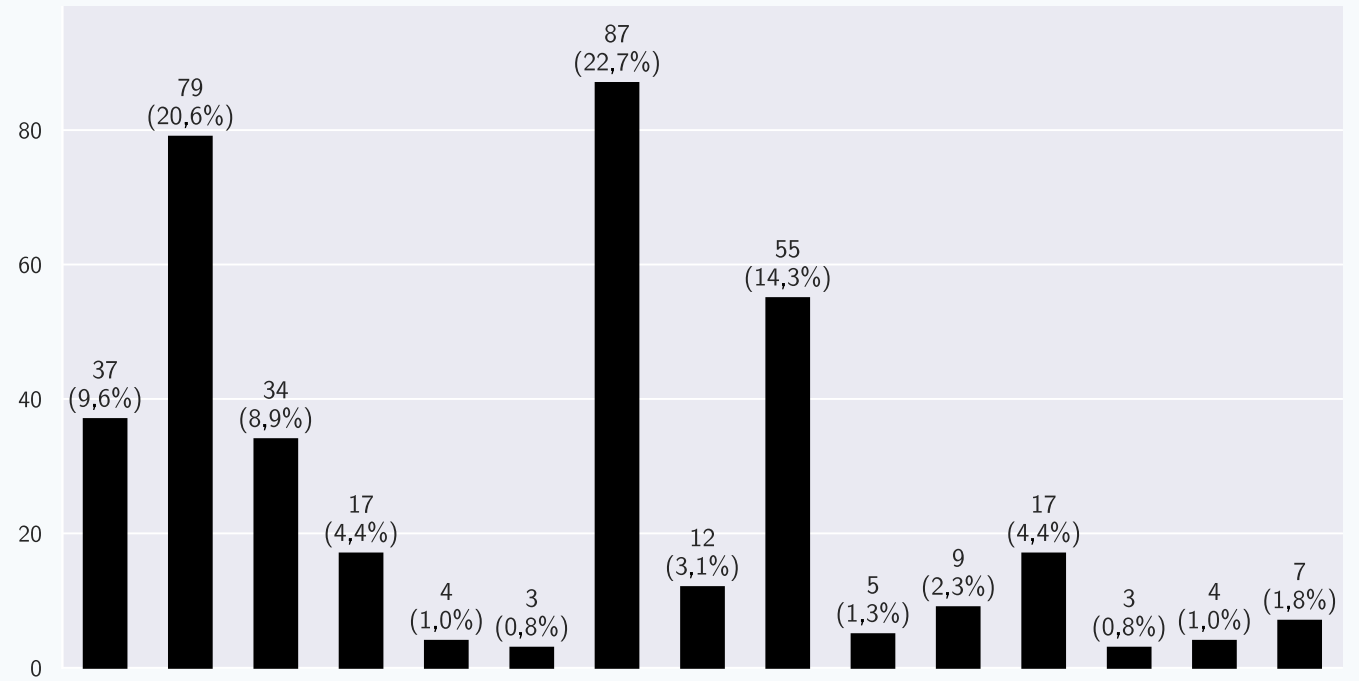
- Wir unterscheiden zwischen:
 - **Link:** App verlinkt nur Datenschutzerklärung, z. B. im Menü/Footer.
 - **Hinweis:** App weist auf Verarbeitung hin, gibt aber keine Wahl.
 - **Dialog:** App weist auf Verarbeitung hin und fragt aktiv Einwilligung ab.

Klassifizierung	Anzahl auf Android	Anzahl auf iOS	Anzahl insgesamt
Dialog	149 (7,21 %)	235 (10,13 %)	384 (8,75 %)
Hinweis	108 (5,22 %)	87 (3,75 %)	195 (4,44 %)
Link	103 (4,98 %)	103 (4,44 %)	206 (4,69 %)
nichts	1.708 (82,59 %)	1.895 (81,68 %)	3.603 (82,11 %)

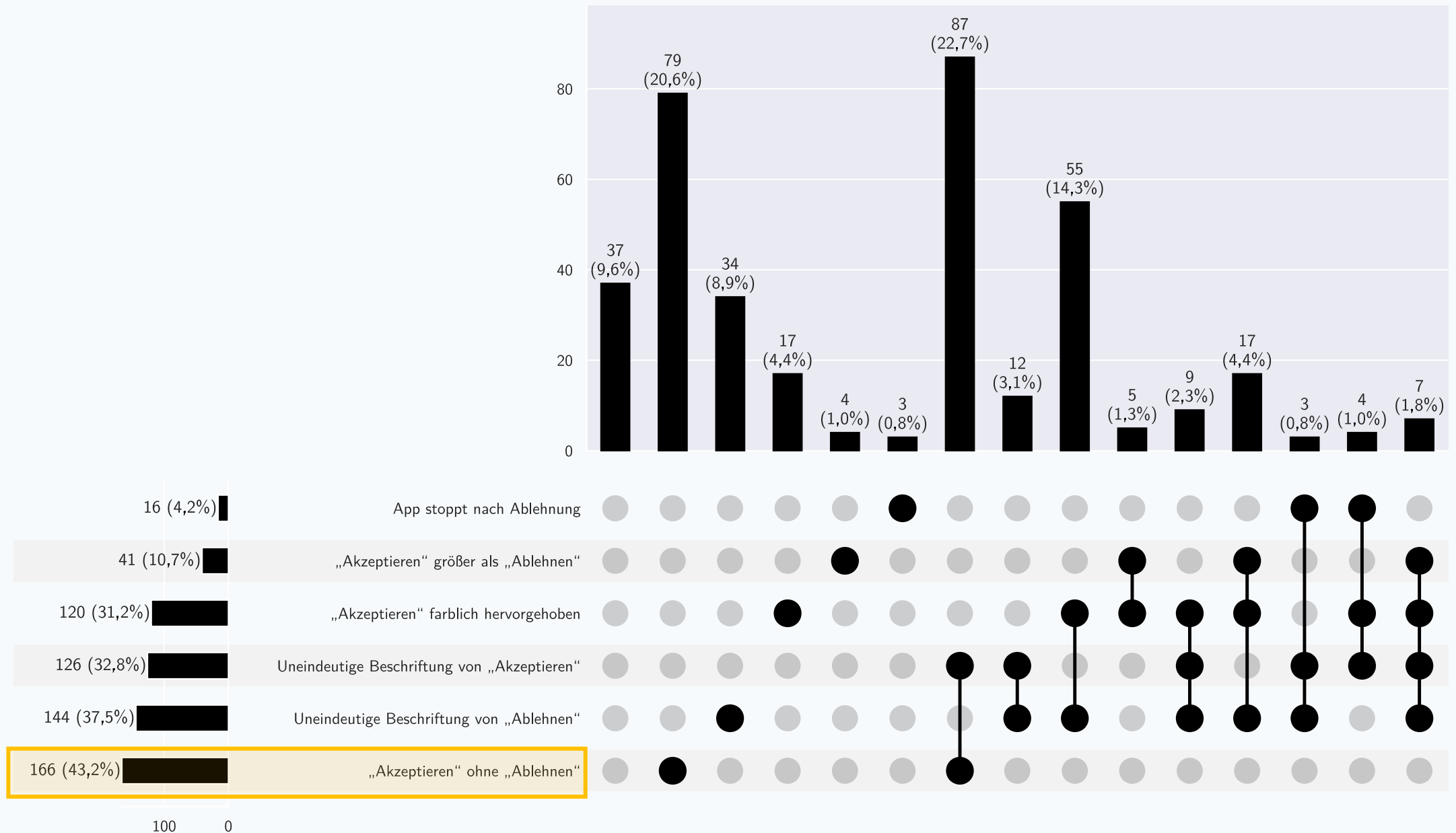
**> 90 % der
Einwilligungsdialoge
nutzten mind. ein
Dark Pattern.**



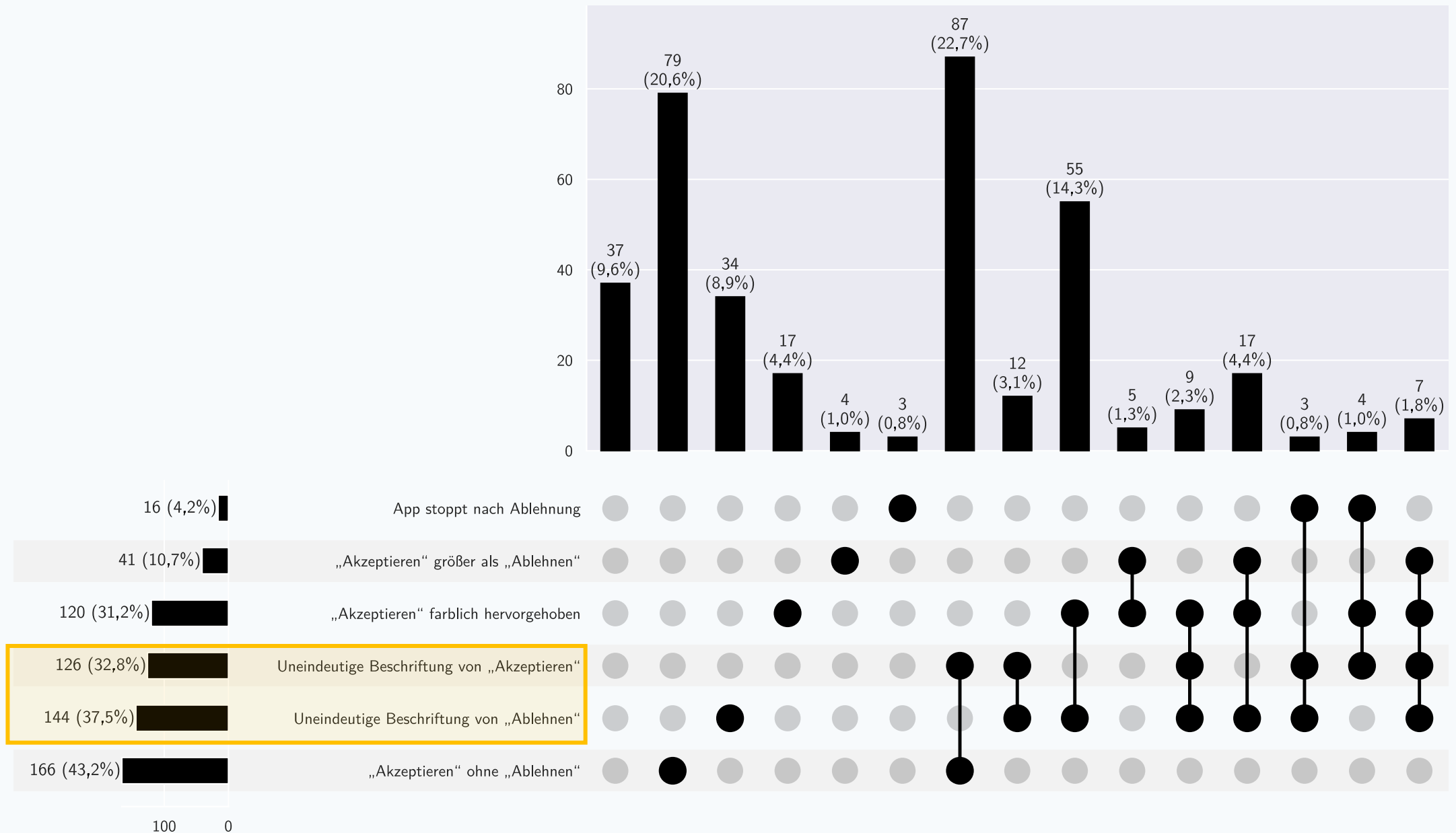
UpSet-Plot der unterschiedlichen Kombinationen von Dark Patterns, die wir in Einwilligungsdialogen erkannt haben. **Teilmengen mit weniger als drei Elementen sind im Plot ausgelassen.** Nicht alle Kombinationen sind möglich.



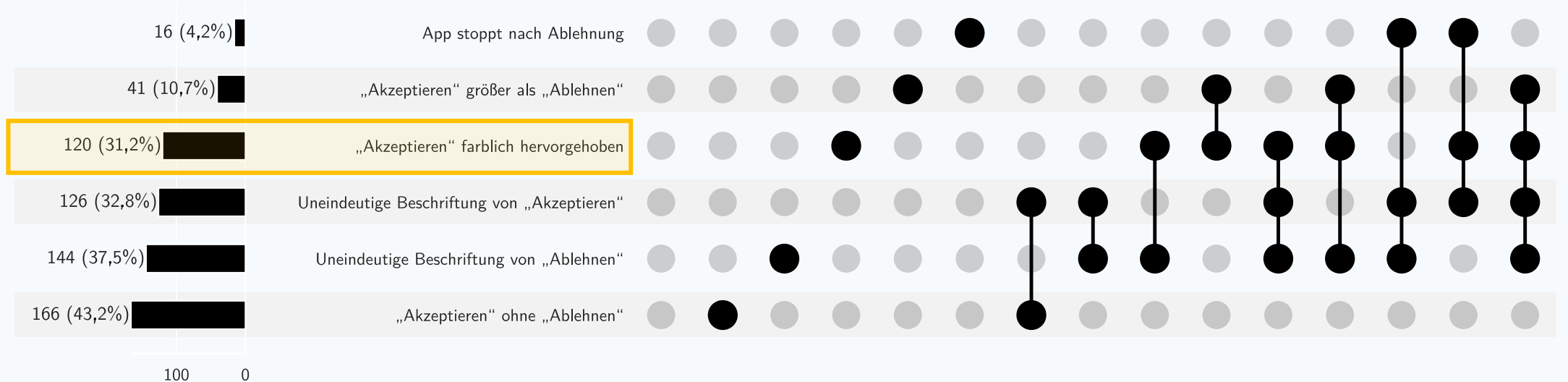
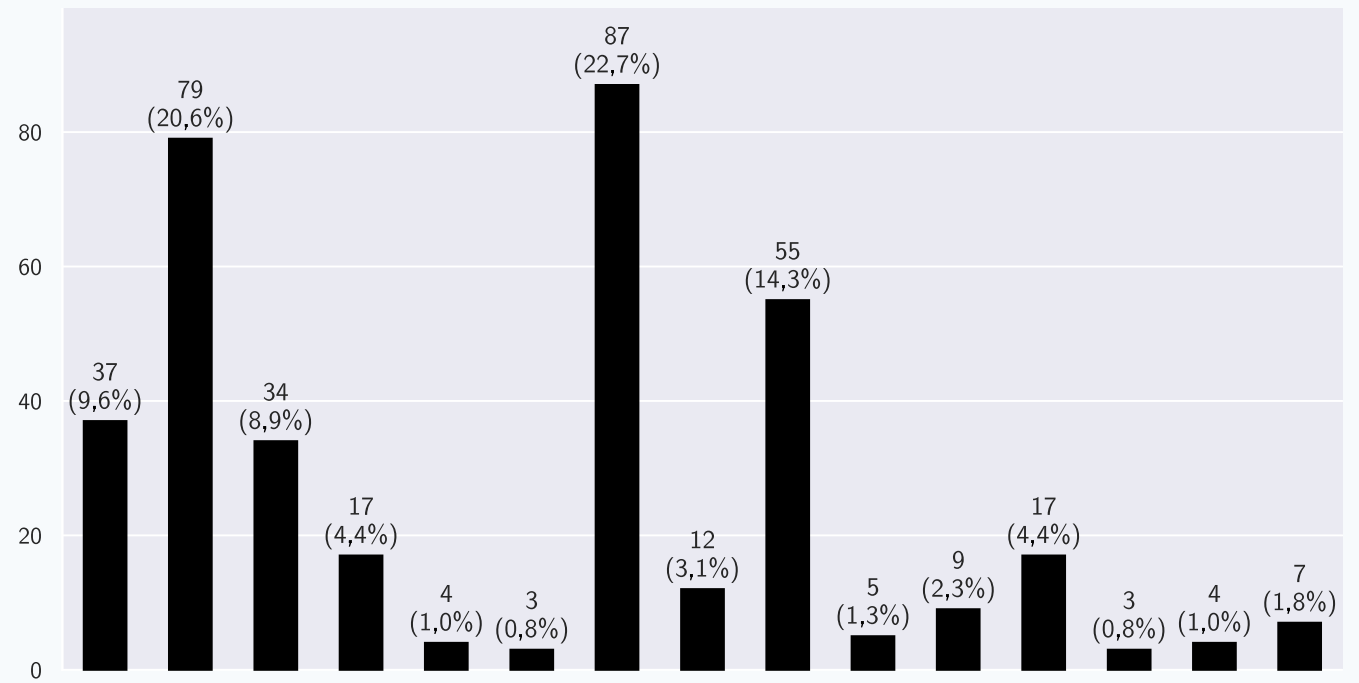
UpSet-Plot der unterschiedlichen Kombinationen von Dark Patterns, die wir in Einwilligungsdialogen erkannt haben. **Teilmengen mit weniger als drei Elementen sind im Plot ausgelassen.** Nicht alle Kombinationen sind möglich.



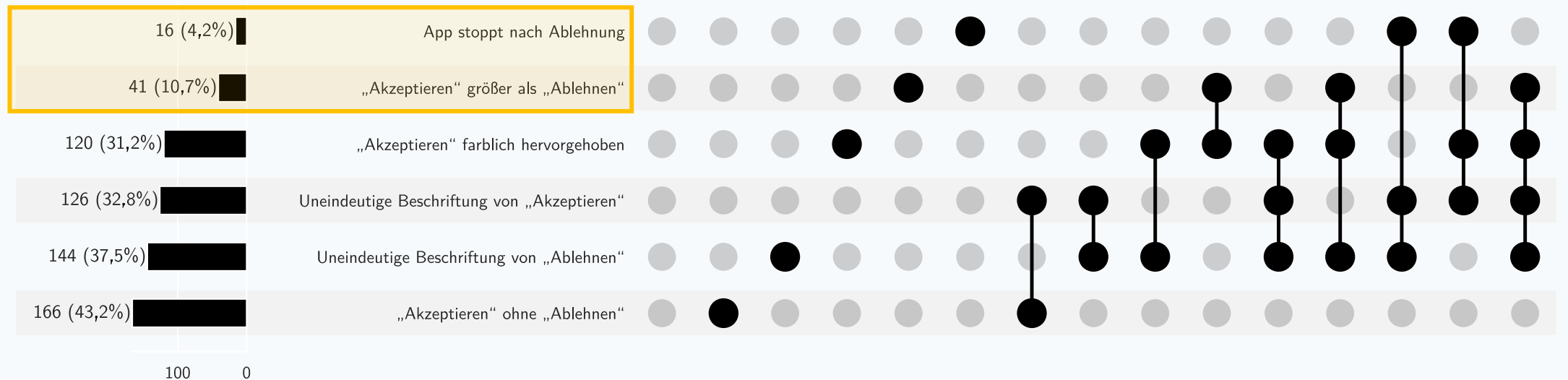
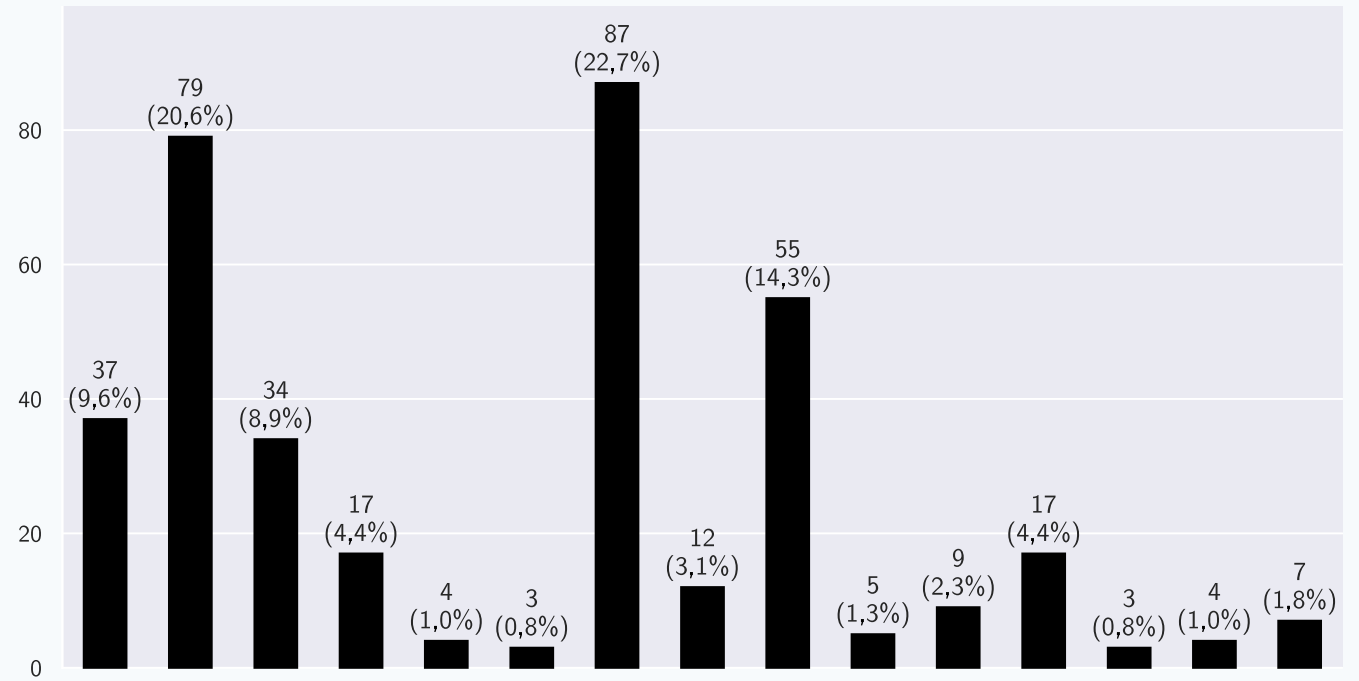
UpSet-Plot der unterschiedlichen Kombinationen von Dark Patterns, die wir in Einwilligungsdialogen erkannt haben. **Teilmengen mit weniger als drei Elementen sind im Plot ausgelassen.** Nicht alle Kombinationen sind möglich.



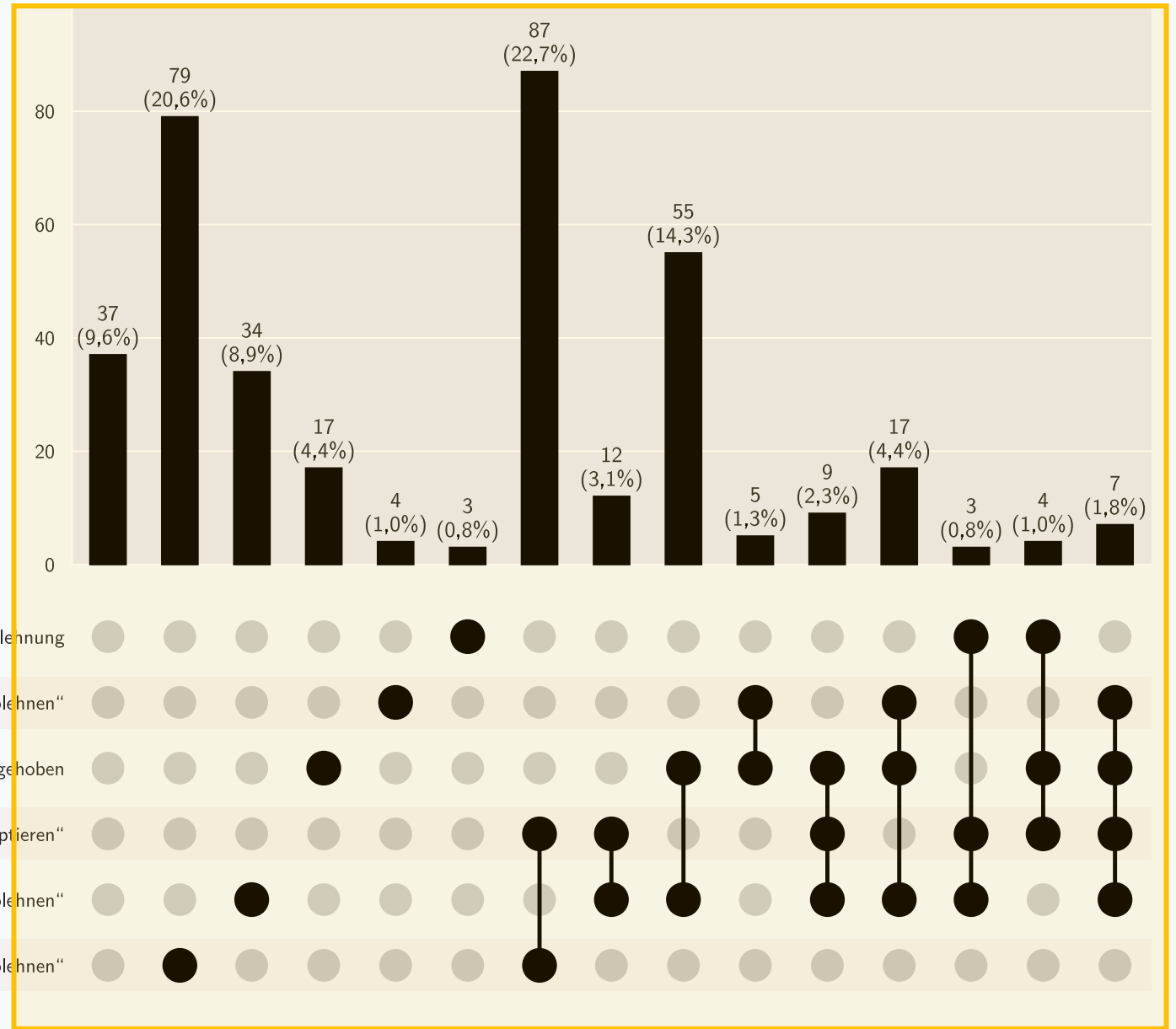
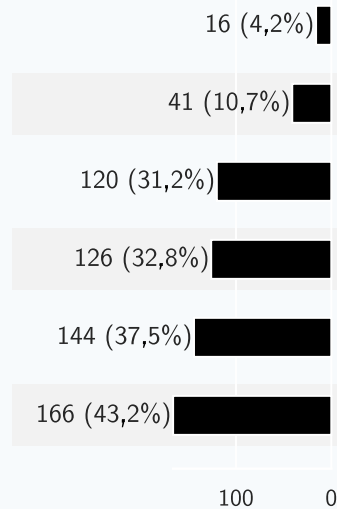
UpSet-Plot der unterschiedlichen Kombinationen von Dark Patterns, die wir in Einwilligungsdialogen erkannt haben. **Teilmengen mit weniger als drei Elementen sind im Plot ausgelassen.** Nicht alle Kombinationen sind möglich.



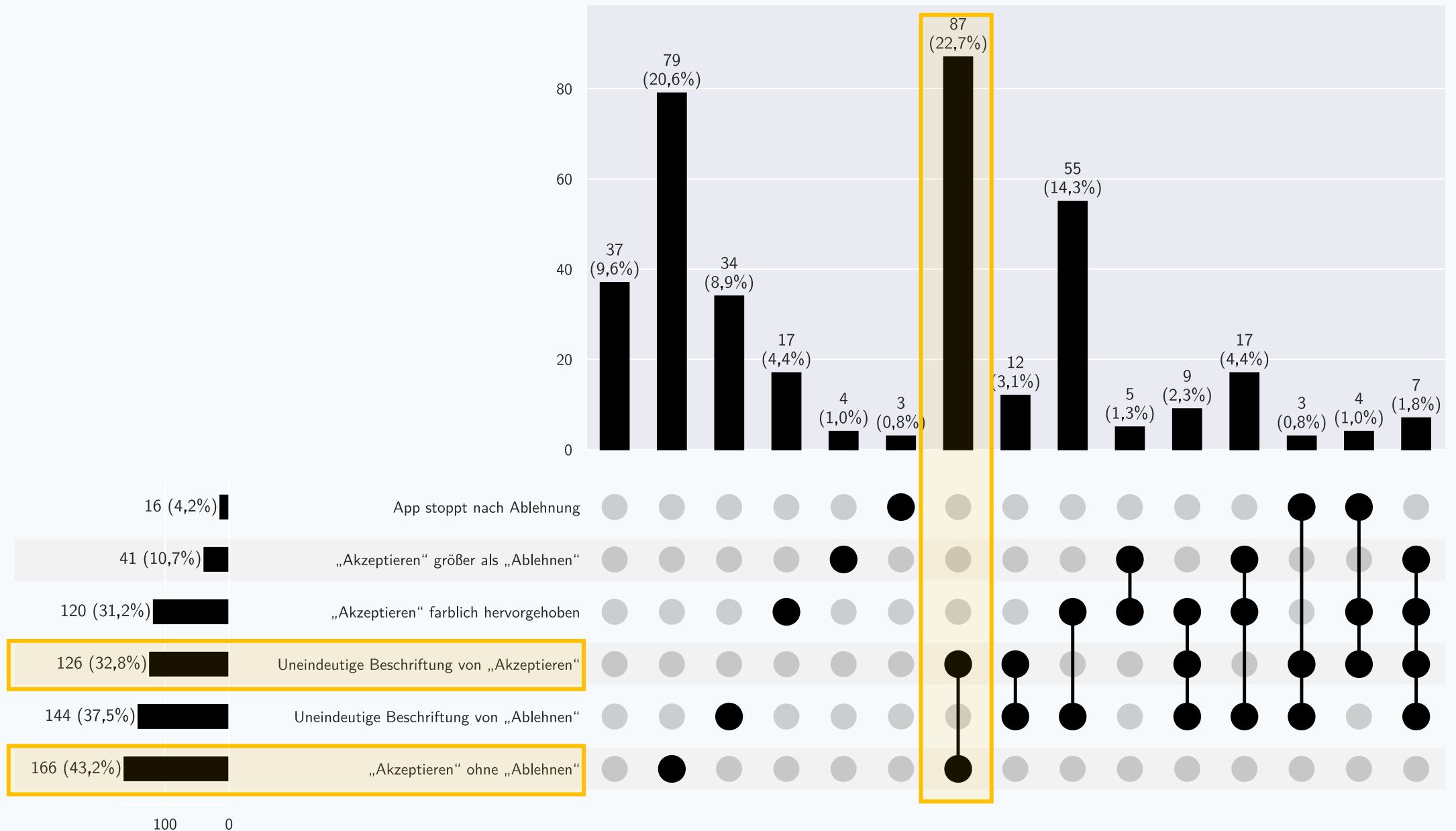
UpSet-Plot der unterschiedlichen Kombinationen von Dark Patterns, die wir in Einwilligungsdialogen erkannt haben. **Teilmengen mit weniger als drei Elementen sind im Plot ausgelassen.** Nicht alle Kombinationen sind möglich.



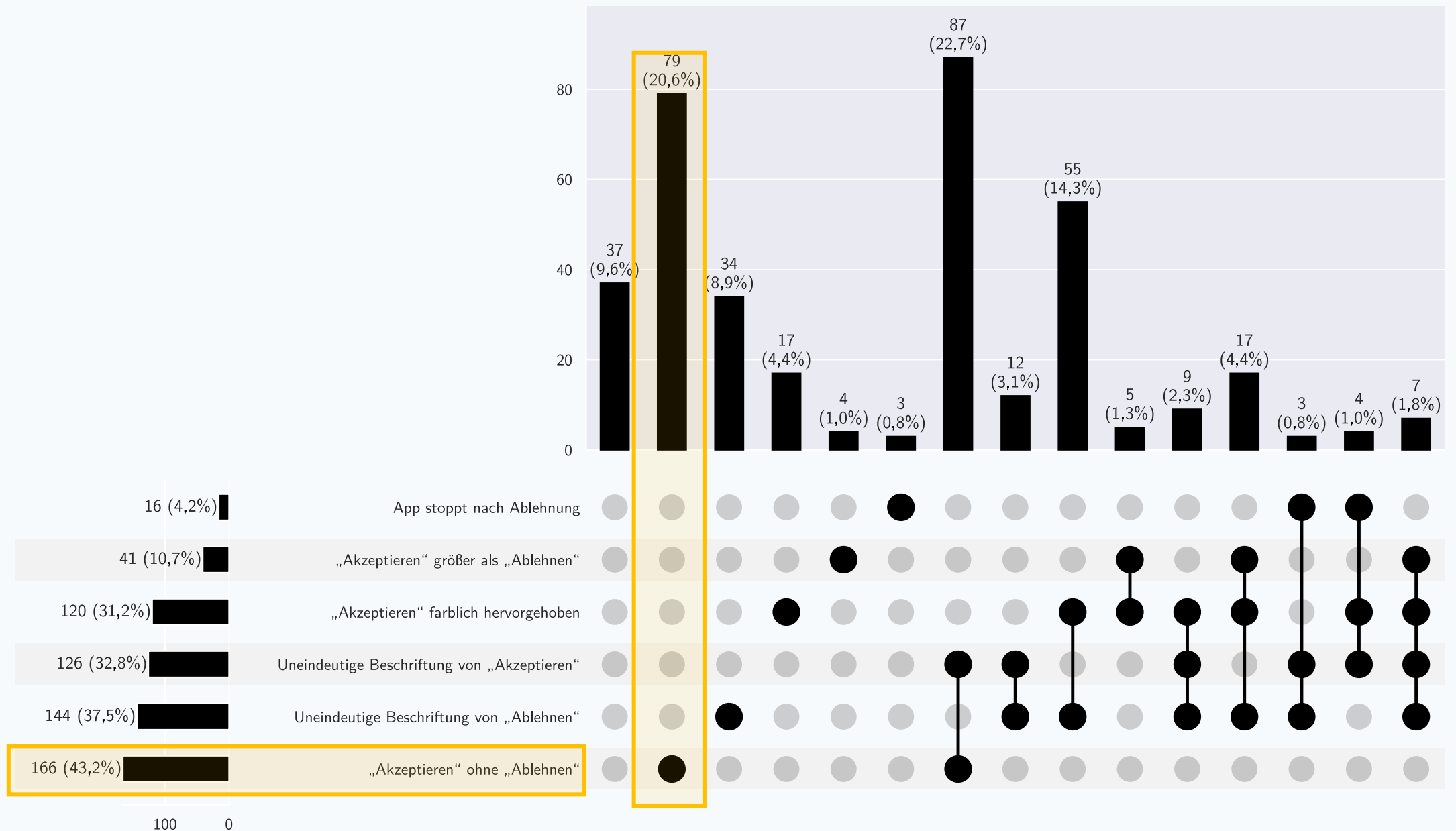
UpSet-Plot der unterschiedlichen Kombinationen von Dark Patterns, die wir in Einwilligungsdialogen erkannt haben. **Teilmengen mit weniger als drei Elementen sind im Plot ausgelassen.** Nicht alle Kombinationen sind möglich.



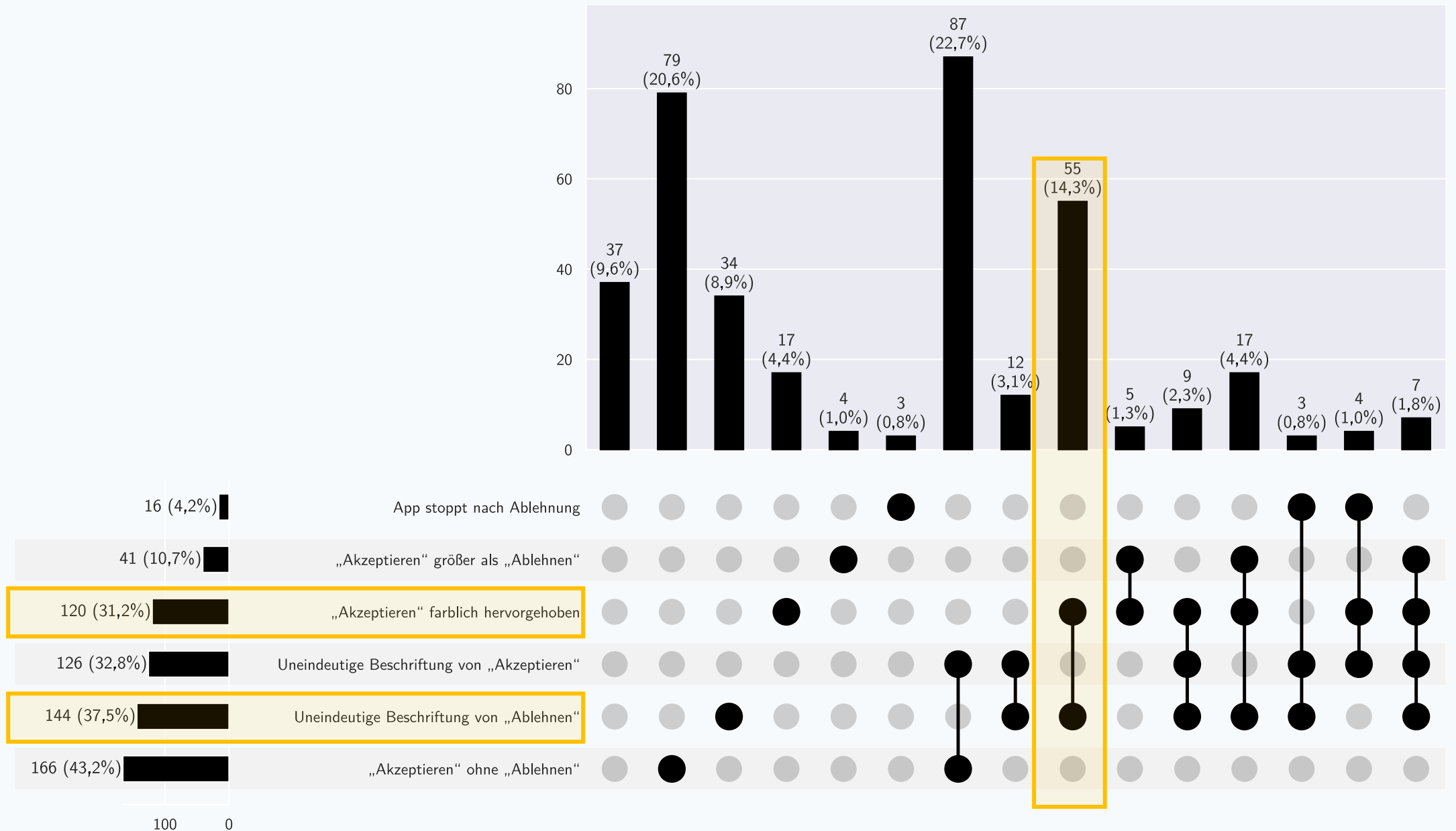
UpSet-Plot der unterschiedlichen Kombinationen von Dark Patterns, die wir in Einwilligungsdialogen erkannt haben. **Teilmengen mit weniger als drei Elementen sind im Plot ausgelassen.** Nicht alle Kombinationen sind möglich.



UpSet-Plot der unterschiedlichen Kombinationen von Dark Patterns, die wir in Einwilligungsdialogen erkannt haben. **Teilmengen mit weniger als drei Elementen sind im Plot ausgelassen.** Nicht alle Kombinationen sind möglich.



UpSet-Plot der unterschiedlichen Kombinationen von Dark Patterns, die wir in Einwilligungsdialogen erkannt haben. **Teilmengen mit weniger als drei Elementen sind im Plot ausgelassen.** Nicht alle Kombinationen sind möglich.



UpSet-Plot der unterschiedlichen Kombinationen von Dark Patterns, die wir in Einwilligungsdialogen erkannt haben. **Teilmengen mit weniger als drei Elementen sind im Plot ausgelassen.** Nicht alle Kombinationen sind möglich.

Recht auf Beschwerde



Wenn Du meinst, dass eine App Tracking illegal verwendet, kannst Du Dich **kostenlos** bei einer Aufsichtsbehörde beschweren.

Die Aufsichtsbehörden haben **Kontrollbefugnisse** und dürfen Unternehmen konkrete Verarbeitungen **verbieten** oder sogar **Bußgelder** verhängen.

Workshop „Wie viel Energie verbraucht mein Handy, um mich zu überwachen?“ – Bits & Bäume 2022

Veranstaltungsdatum

2022-10-02 um 10:00

Veranstaltungsort

Technische Universität Berlin

Straße des 17. Juni 135, 10623 Berlin, Deutschland

Dauer

90m

Viele Apps auf Smartphones sind unentwegt damit befasst, unser Verhalten zu analysieren und sonstwohin zu senden. Das verbraucht einen nicht unerheblichen Anteil des mobilen Energiebudgets. Doch wie hoch ist der Anteil genau? Sollten wir diese Handy-Aktivitäten zum Schutz der Umwelt abstellen? Und wie ist das zu machen?

Zu diesen wichtigen Fragen steuern wir im Workshop die Datenschutzperspektive bei. Wir erklären, wie man mithilfe der DSGVO Auskunft über Tracking erhalten und sich dagegen wehren kann.

[Workshop im Konferenz-Programm](#) 

Vortragsfolien:

- [Einleitung](#)
- [Gruppe 1 und 2: Stromverbrauch-messende Apps, Wie erfolgt die Ausspähung genau?](#)
- [Gruppe 3: Mobiles Tracking aus Datenschutzsicht](#)

Beschwerde gegen Otto (GmbH & Co KG)

**BESCHWERDE NACH DSGVO UND
TTDSG**

erhoben von

[Redacted Name]

(Beschwerdeführer, im Folgenden: „ich“)

gegen

Otto (GmbH & Co KG), Werner-Otto-Straße 1-7, 22179 Hamburg, Deutschland
(Beschwerdegegnerin, im Folgenden: „Verantwortliche“)

wegen

> <https://static.dacdn.de/docs/tracking-beschwerde-otto.pdf>

Das ist viel zu schwer.
Unser nächstes Projekt:
automatisierte Beschwerden
gegen Tracking in Apps.

Wir werden aus unserem
Forschungscode gut
dokumentierte **Tools und**
Bibliotheken machen.

Bleibt in Kontakt mit uns

- Wir trötenmastodonnern:
[@DatenanfragenDE@mastodon.social](https://mastodon.social/@DatenanfragenDE)
- Längere Artikel gibt es im Blog (auch per RSS):
<https://www.datenanfragen.de/blog/>
- Wir sind bei Matrix:
[#datenanfragen:matrix.altpeter.me](https://matrix.altpeter.me/#datenanfragen:matrix.altpeter.me)
- Wir freuen uns immer über helfende Hände:
<https://www.datenanfragen.de/mitmachen/>

Das war's.

Die Folien gibt es zum Runterladen auf unserer Seite:

www.datenanfragen.de/verein/event/fireshonks-tracking-2022/

Die Folien sind als CC BY 4.0 lizenziert.

Lizenzen externer Assets: www.datenanfragen.de/open-source