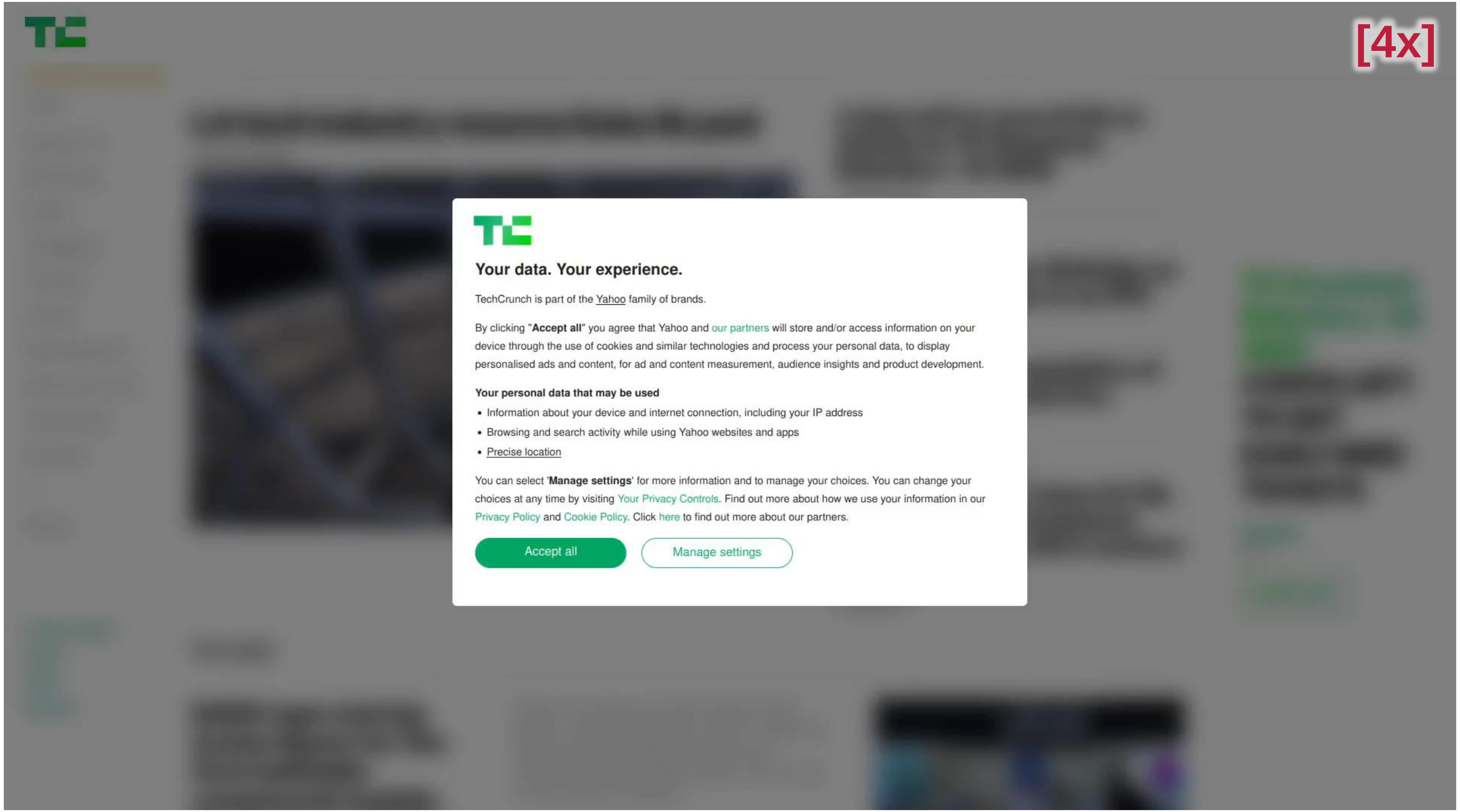
Technische Universität Braunschweig

IAS INSTITUTE FOR APPLICATION SECURITY

Informed consent?
A study of “consent dialogs” on Android and iOS

Benjamin Altpeter, 2022-05-19



[4x]

Your data. Your experience.

TechCrunch is part of the Yahoo family of brands.

By clicking "**Accept all**" you agree that Yahoo and our partners will store and/or access information on your device through the use of cookies and similar technologies and process your personal data, to display personalised ads and content, for ad and content measurement, audience insights and product development.

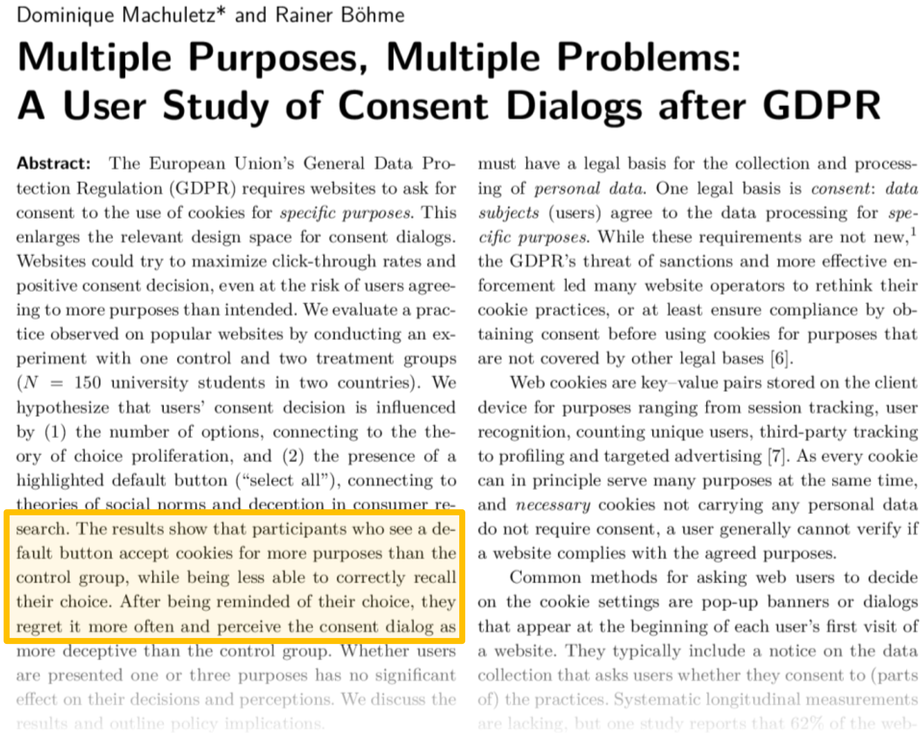
Your personal data that may be used

- Information about your device and internet connection, including your IP address
- Browsing and search activity while using Yahoo websites and apps
- Precise location

You can select '**Manage settings**' for more information and to manage your choices. You can change your choices at any time by visiting Your Privacy Controls. Find out more about how we use your information in our Privacy Policy and Cookie Policy. Click here to find out more about our partners.

https://techcrunch.com

More than just annoying



Dominique Machuletz* and Rainer Böhme

Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR

Abstract: The European Union's General Data Protection Regulation (GDPR) requires websites to ask for consent to the use of cookies for *specific purposes*. This enlarges the relevant design space for consent dialogs. Websites could try to maximize click-through rates and positive consent decision, even at the risk of users agreeing to more purposes than intended. We evaluate a practice observed on popular websites by conducting an experiment with one control and two treatment groups ($N = 150$ university students in two countries). We hypothesize that users' consent decision is influenced by (1) the number of options, connecting to the theory of choice proliferation, and (2) the presence of a highlighted default button ("select all"), connecting to theories of social norms and deception in consumer research. The results show that participants who see a default button accept cookies for more purposes than the control group, while being less able to correctly recall their choice. After being reminded of their choice, they regret it more often and perceive the consent dialog as more deceptive than the control group. Whether users are presented one or three purposes has no significant effect on their decisions and perceptions. We discuss the results and outline policy implications.

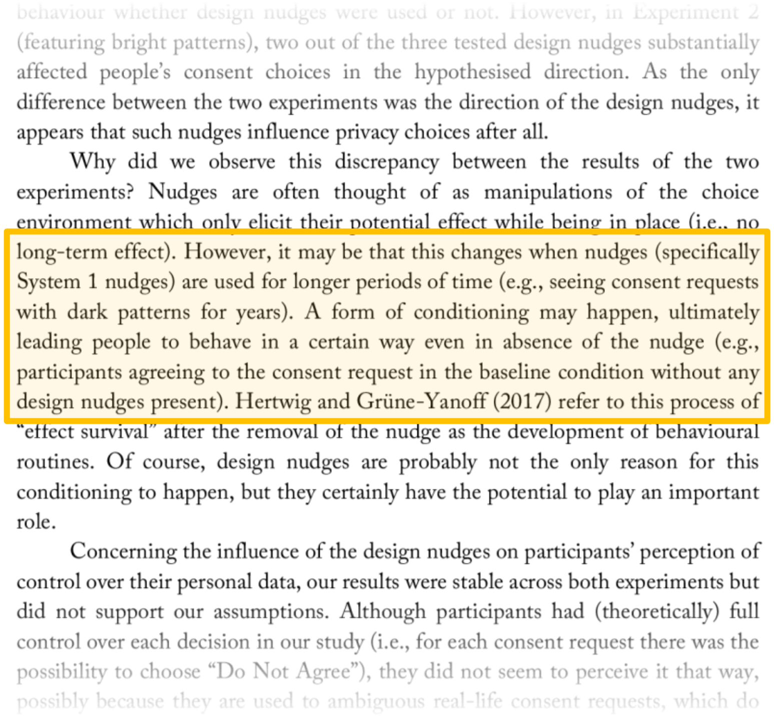
must have a legal basis for the collection and processing of *personal data*. One legal basis is *consent*: *data subjects* (users) agree to the data processing for *specific purposes*. While these requirements are not new,[1] the GDPR's threat of sanctions and more effective enforcement led many website operators to rethink their cookie practices, or at least ensure compliance by obtaining consent before using cookies for purposes that are not covered by other legal bases [6].

Web cookies are key–value pairs stored on the client device for purposes ranging from session tracking, user recognition, counting unique users, third-party tracking to profiling and targeted advertising [7]. As every cookie can in principle serve many purposes at the same time, and *necessary* cookies not carrying any personal data do not require consent, a user generally cannot verify if a website complies with the agreed purposes.

Common methods for asking web users to decide on the cookie settings are pop-up banners or dialogs that appear at the beginning of each user's first visit of a website. They typically include a notice on the data collection that asks users whether they consent to (parts of) the practices. Systematic longitudinal measurements are lacking, but one study reports that 62% of the web-

D. Machuletz and R. Böhme, "Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR," 10.2478/popets-2020-0037.

More than just annoying



behaviour whether design nudges were used or not. However, in Experiment 2 (featuring bright patterns), two out of the three tested design nudges substantially affected people's consent choices in the hypothesised direction. As the only difference between the two experiments was the direction of the design nudges, it appears that such nudges influence privacy choices after all.

Why did we observe this discrepancy between the results of the two experiments? Nudges are often thought of as manipulations of the choice environment which only elicit their potential effect while being in place (i.e., no long-term effect). However, it may be that this changes when nudges (specifically System 1 nudges) are used for longer periods of time (e.g., seeing consent requests with dark patterns for years). A form of conditioning may happen, ultimately leading people to behave in a certain way even in absence of the nudge (e.g., participants agreeing to the consent request in the baseline condition without any design nudges present). Hertwig and Grüne-Yanoff (2017) refer to this process of "effect survival" after the removal of the nudge as the development of behavioural routines. Of course, design nudges are probably not the only reason for this conditioning to happen, but they certainly have the potential to play an important role.

Concerning the influence of the design nudges on participants' perception of control over their personal data, our results were stable across both experiments but did not support our assumptions. Although participants had (theoretically) full control over each decision in our study (i.e., for each consent request there was the possibility to choose "Do Not Agree"), they did not seem to perceive it that way, possibly because they are used to ambiguous real-life consent requests, which do

P. Graßl, H. Schraffenberger, F. Z. Borgesius, and M. Buijzen, "Dark and Bright Patterns in Cookie Consent Requests," 10.33621/jdsr.v3i1.54.

Image: Sebastian Pichler (Unsplash license)

Legal situation

General Data Protection Regulation (GDPR)

- Concerns itself with the *processing* of *personal data* (Art. 2(1) GDPR).

General Data Protection Regulation (GDPR)

- Concerns itself with the *processing* of *personal data* (Art. 2(1) GDPR).
- Both terms defined in Art. 4 GDPR:
  - **personal data**: “any information relating to an identified or identifiable natural person […]”
  - **processing**: “any operation […] performed on personal data […]”

General Data Protection Regulation (GDPR)

- Concerns itself with the *processing* of *personal data* (Art. 2(1) GDPR).
- Both terms defined in Art. 4 GDPR:
  - **personal data**: “any information relating to an identified or identifiable natural person […]”
  - **processing**: “any operation […] performed on personal data […]”

- Explicitly very broad terms, in essence any data that can somehow be connected to a person (including pseudonymously!) and that a company deals with in some way is covered by the GDPR.

Legal bases

- Processing personal data is only legal if (Art. 6(1) GDPR):

(a) “the data subject has given **consent** […]”;

(b) “processing is necessary for the **performance of a contract** to which the data subject is party […]”;

(c) “processing is necessary for compliance with a **legal obligation** [of] the controller […]”;

(d) “processing is necessary in order to **protect the vital interests** of the data subject or of another natural person”;

(e) “processing is necessary for the performance of a task carried out in the public interest or in the exercise of **official authority** vested in the controller”;

(f) “processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child”.

Legal bases

- Processing personal data is only legal if (Art. 6(1) GDPR):

(a) “the data subject has given **consent** […]”;

(b) “processing is necessary for the **performance of a contract** to which the data subject is party […]”;

(c) “processing is necessary for compliance with a **legal obligation** [of] the controller […]”;

(d) “processing is necessary in order to **protect the vital interests** of the data subject or of another natural person”;

(e) “processing is necessary for the performance of a task carried out in the public interest or in the exercise of **official authority** vested in the controller”;

(f) “processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child”.

Legal basis for tracking

- Processing personal data is only legal if (Art. 6(1) GDPR):
  (a) “the data subject has given **consent** […]”;
  (b) “processing is necessary for the **performance of a contract** to which the data subject is party […]”;
  ~~(c) “processing is necessary for compliance with a **legal obligation** [of] the controller […]”;~~
  (d) “processing is necessary in order to **protect the vital interests** of the data subject or of another natural person”;
  (e) “processing is necessary for the performance of a task carried out in the public interest or in the exercise of **official authority** vested in the controller”;
  (f) “processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child”.

Legal basis for tracking

- Processing personal data is only legal if (Art. 6(1) GDPR):

(a) "the data subject has given **consent** […]";

(b) "processing is necessary for the **performance of a contract** to which the data subject is party […]";

~~(c) "processing is necessary for compliance with a **legal obligation** [of] the controller […]";~~

~~(d) "processing is necessary in order to **protect the vital interests** of the data subject or of another natural person";~~

(e) "processing is necessary for the performance of a task carried out in the public interest or in the exercise of **official authority** vested in the controller";

(f) "processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".

Legal basis for tracking

- Processing personal data is only legal if (Art. 6(1) GDPR):

(a) “the data subject has given **consent** […]”;

(b) “processing is necessary for the **performance of a contract** to which the data subject is party […]”;

~~(c) “processing is necessary for compliance with a **legal obligation** [of] the controller […]”;~~

~~(d) “processing is necessary in order to **protect the vital interests** of the data subject or of another natural person”;~~

~~(e) “processing is necessary for the performance of a task carried out in the public interest or in the exercise of **official authority** vested in the controller”;~~

(f) “processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child”.

Legal basis for tracking

- Processing personal data is only legal if (Art. 6(1) GDPR):

  (a) “the data subject has given **consent** […]”;

  ~~(b) “processing is necessary for the **performance of a contract** to which the data subject is party […]”;~~

  ~~(c) “processing is necessary for compliance with a **legal obligation** [of] the controller […]”;~~

  ~~(d) “processing is necessary in order to **protect the vital interests** of the data subject or of another natural person”;~~

  ~~(e) “processing is necessary for the performance of a task carried out in the public interest or in the exercise of **official authority** vested in the controller”;~~

  ~~(f) “processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child”.~~

ePrivacy Directive (“the cookie law”)

- Art. 5(3) ePD applies to all data accessed from a device:

  “Member States shall ensure that the **storing of information**, or the **gaining of access to information** already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her **consent**, having been provided with clear and comprehensive information […]. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.”

ePrivacy Directive (“the cookie law”)

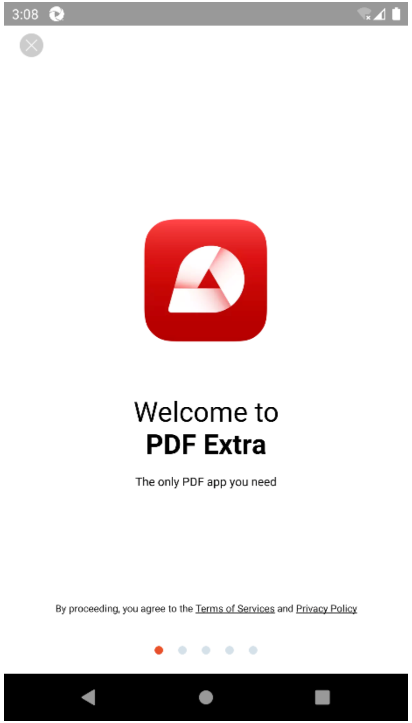
- No legal basis other than consent:

  “Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information […]. This shall not prevent any technical storage or access for the **sole purpose of carrying out the transmission of a communication** over an electronic communications network, or as **strictly necessary** in order for the provider of an information society service **explicitly requested** by the subscriber or user to provide the service.”

Image: Glenn Carstens-Peters (Unsplash license)

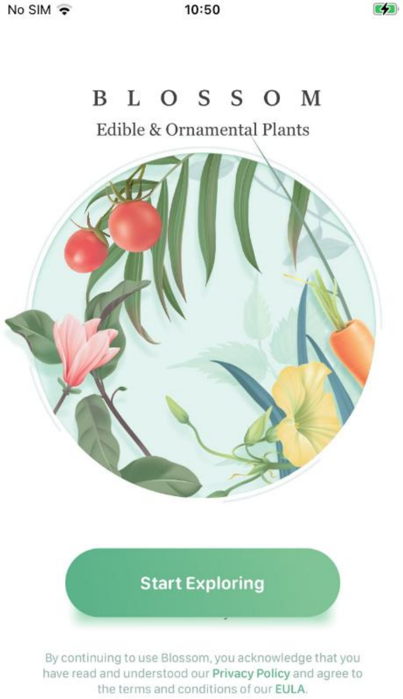
Consent dialog criteria

Clear affirmative action



By proceeding, you agree to the Terms of Services and Privacy Policy

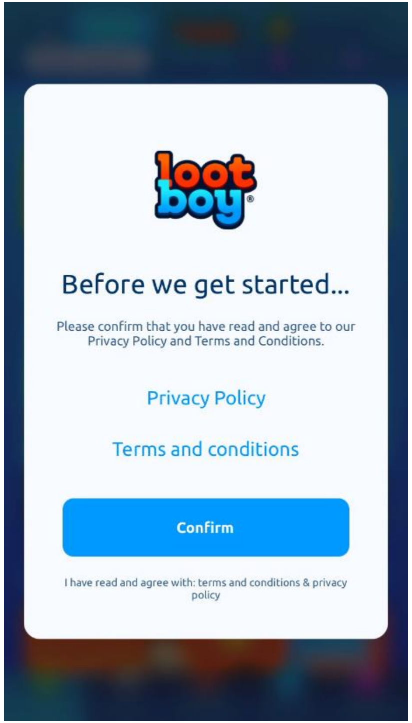
PDF Extra - Scan, Edit & Sign (Android)



By continuing to use Blossom, you acknowledge that you have read and understood our Privacy Policy and agree to the terms and conditions of our EULA.

Blossom - Plant Care Guide (iOS)

Refusing is as easy as accepting



Before we get started...

Please confirm that you have read and agree to our Privacy Policy and Terms and Conditions.

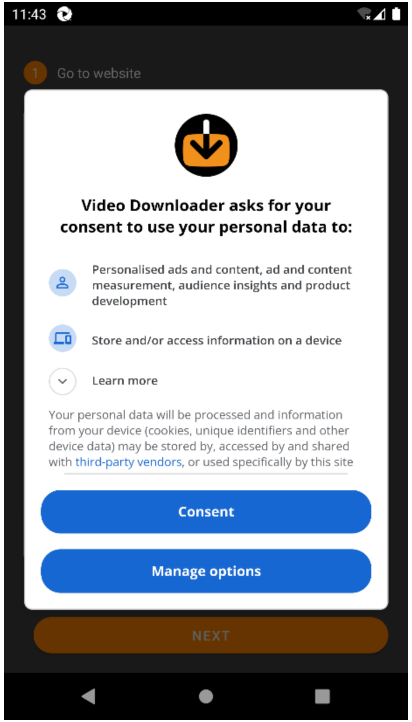
Privacy Policy

Terms and conditions

Confirm

I have read and agree with: terms and conditions & privacy policy

LootBoy - Grab your loot! (iOS)



Video Downloader asks for your consent to use your personal data to:

- Personalised ads and content, ad and content measurement, audience insights and product development
- Store and/or access information on a device
- Learn more

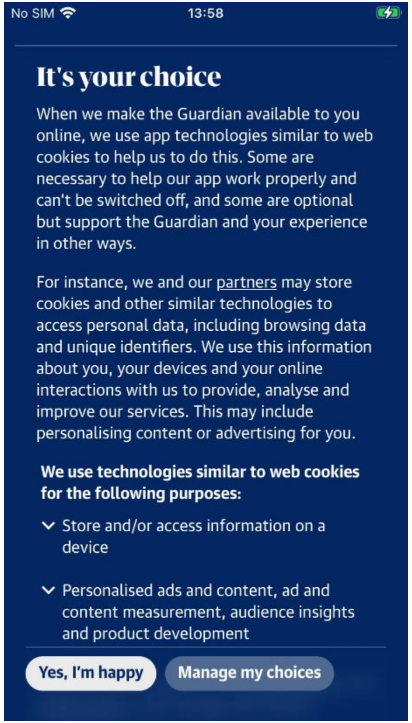
Your personal data will be processed and information from your device (cookies, unique identifiers and other device data) may be stored by, accessed by and shared with third-party vendors, or used specifically by this site

Consent

Manage options

Video Downloader & Video Saver (Android)

Unambiguous button labels



It's your choice

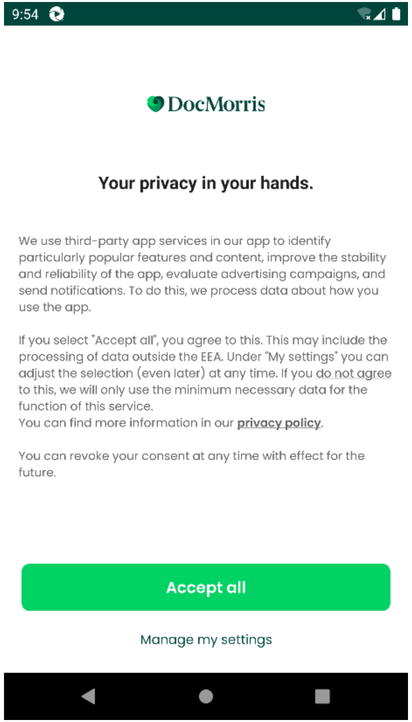
When we make the Guardian available to you online, we use app technologies similar to web cookies to help us to do this. Some are necessary to help our app work properly and can't be switched off, and some are optional but support the Guardian and your experience in other ways.

For instance, we and our partners may store cookies and other similar technologies to access personal data, including browsing data and unique identifiers. We use this information about you, your devices and your online interactions with us to provide, analyse and improve our services. This may include personalising content or advertising for you.

We use technologies similar to web cookies for the following purposes:

- Store and/or access information on a device
- Personalised ads and content, ad and content measurement, audience insights and product development

The Guardian: Breaking News (iOS)



Your privacy in your hands.

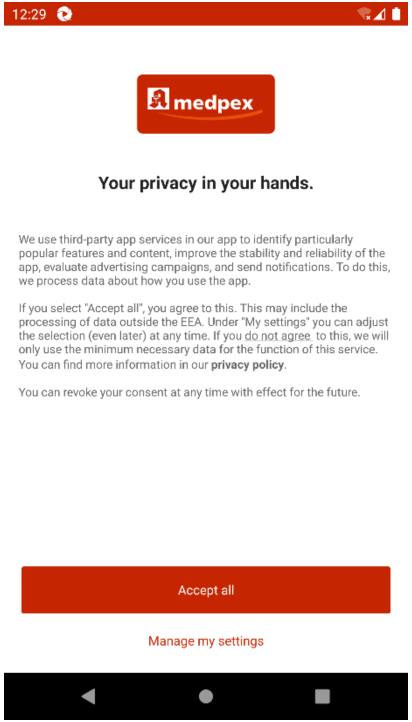
We use third-party app services in our app to identify particularly popular features and content, improve the stability and reliability of the app, evaluate advertising campaigns, and send notifications. To do this, we process data about how you use the app.

If you select "Accept all", you agree to this. This may include the processing of data outside the EEA. Under "My settings" you can adjust the selection (even later) at any time. If you do not agree to this, we will only use the minimum necessary data for the function of this service.
You can find more information in our privacy policy.

You can revoke your consent at any time with effect for the future.

DocMorris (Android)

“Accept” button not highlighted by size



12:29

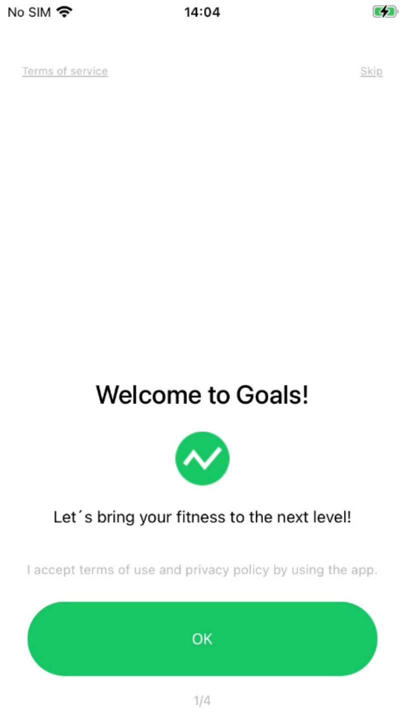
Your privacy in your hands.

We use third-party app services in our app to identify particularly popular features and content, improve the stability and reliability of the app, evaluate advertising campaigns, and send notifications. To do this, we process data about how you use the app.

If you select "Accept all", you agree to this. This may include the processing of data outside the EEA. Under "My settings" you can adjust the selection (even later) at any time. If you do not agree to this, we will only use the minimum necessary data for the function of this service. You can find more information in our **privacy policy**.

You can revoke your consent at any time with effect for the future.

medpex: Online Apotheke (Android)



No SIM 14:04

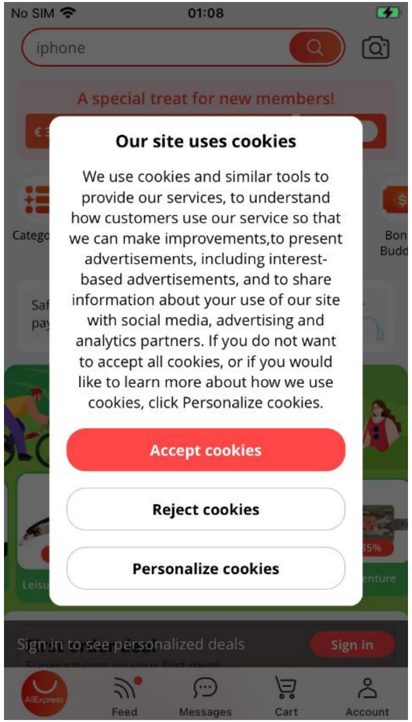
Welcome to Goals!

Let´s bring your fitness to the next level!

I accept terms of use and privacy policy by using the app.

Running Walking Tracker Goals (iOS)

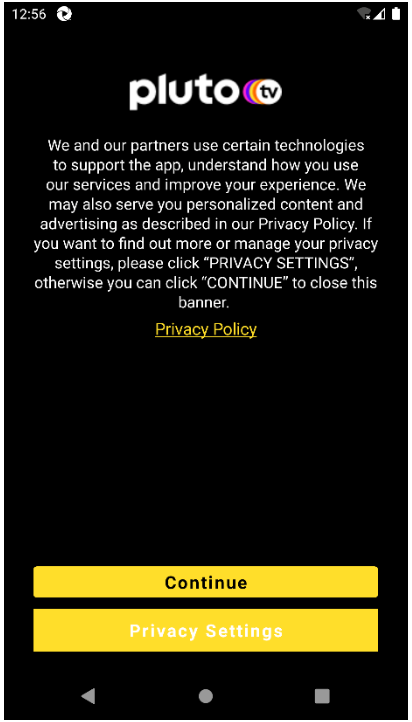
“Accept” button not highlighted by colour



Our site uses cookies

We use cookies and similar tools to provide our services, to understand how customers use our service so that we can make improvements,to present advertisements, including interest-based advertisements, and to share information about your use of our site with social media, advertising and analytics partners. If you do not want to accept all cookies, or if you would like to learn more about how we use cookies, click Personalize cookies.

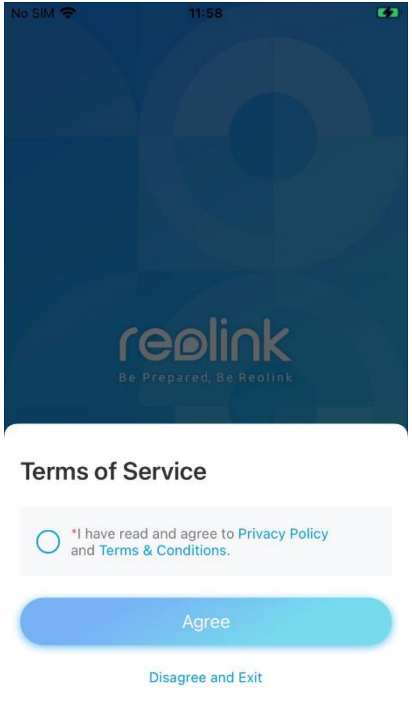
AliExpress Shopping App (iOS)



We and our partners use certain technologies to support the app, understand how you use our services and improve your experience. We may also serve you personalized content and advertising as described in our Privacy Policy. If you want to find out more or manage your privacy settings, please click “PRIVACY SETTINGS”, otherwise you can click “CONTINUE” to close this banner.

Pluto TV - Live TV and Movies (Android)

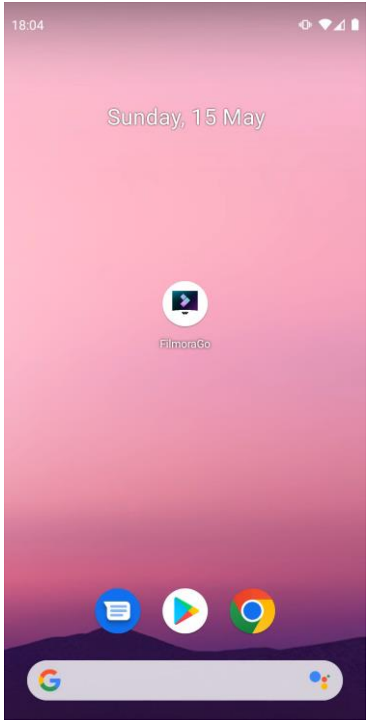
Consent not mandatory



Terms of Service

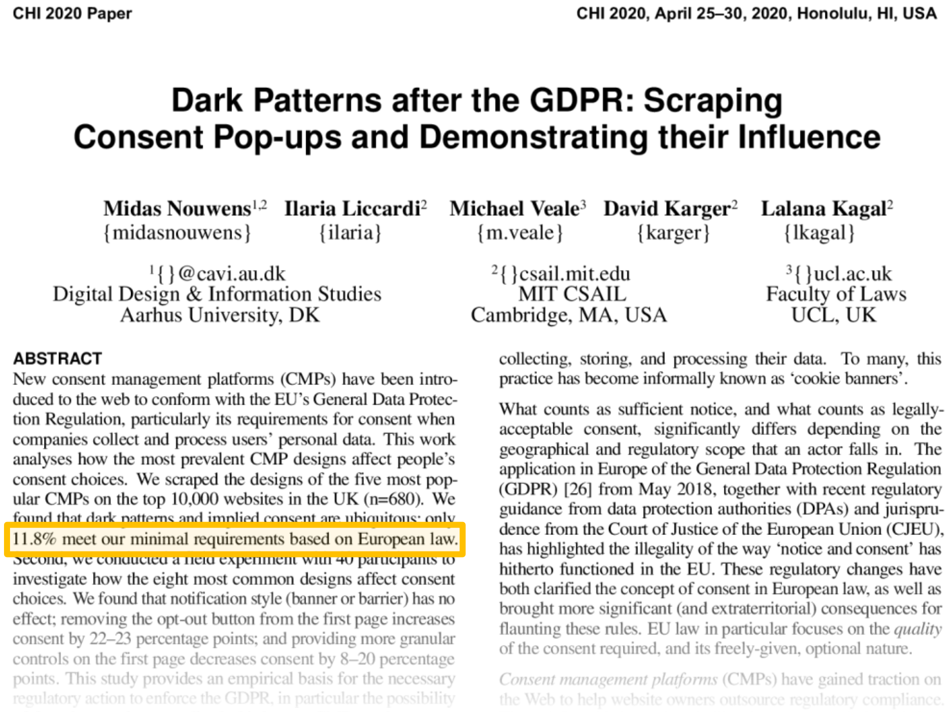
○ *I have read and agree to Privacy Policy and Terms & Conditions.

Reolink (iOS)



FilmoraGo Video Editor & Maker (Android)

Violations are common on the web



CHI 2020 Paper — CHI 2020, April 25–30, 2020, Honolulu, HI, USA

Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence

Midas Nouwens[1,2] {midasnouwens} — Ilaria Liccardi[2] {ilaria} — Michael Veale[3] {m.veale} — David Karger[2] {karger} — Lalana Kagal[2] {lkagal}

[1]{}@cavi.au.dk
Digital Design & Information Studies
Aarhus University, DK

[2]{}csail.mit.edu
MIT CSAIL
Cambridge, MA, USA

[3]{}ucl.ac.uk
Faculty of Laws
UCL, UK

ABSTRACT

New consent management platforms (CMPs) have been introduced to the web to conform with the EU's General Data Protection Regulation, particularly its requirements for consent when companies collect and process users' personal data. This work analyses how the most prevalent CMP designs affect people's consent choices. We scraped the designs of the five most popular CMPs on the top 10,000 websites in the UK (n=680). We found that dark patterns and implied consent are ubiquitous; only 11.8% meet our minimal requirements based on European law. Second, we conducted a field experiment with 40 participants to investigate how the eight most common designs affect consent choices. We found that notification style (banner or barrier) has no effect; removing the opt-out button from the first page increases consent by 22–23 percentage points; and providing more granular controls on the first page decreases consent by 8–20 percentage points. This study provides an empirical basis for the necessary regulatory action to enforce the GDPR, in particular the possibility

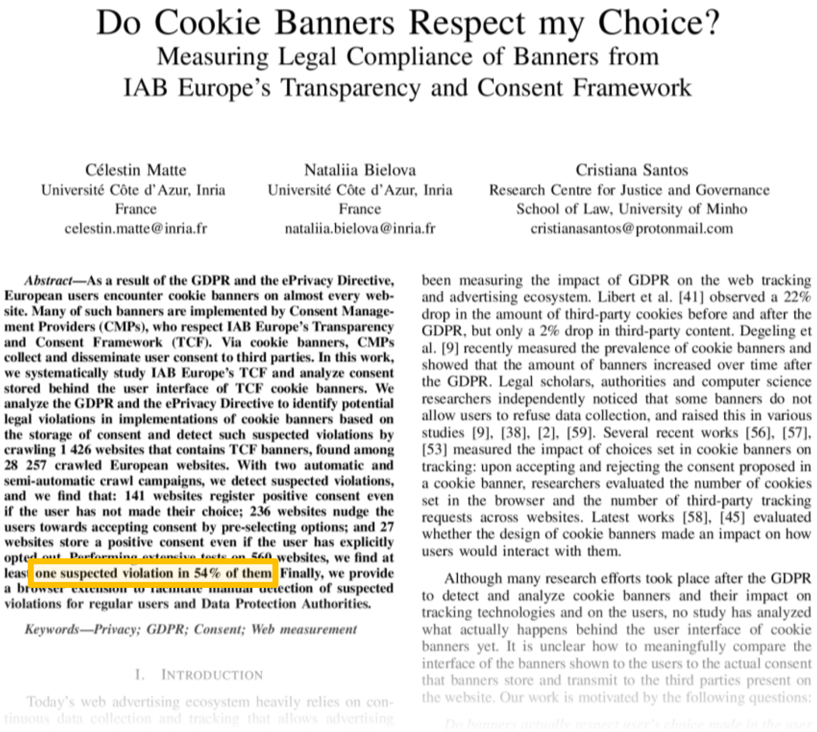
collecting, storing, and processing their data. To many, this practice has become informally known as 'cookie banners'.

What counts as sufficient notice, and what counts as legally-acceptable consent, significantly differs depending on the geographical and regulatory scope that an actor falls in. The application in Europe of the General Data Protection Regulation (GDPR) [26] from May 2018, together with recent regulatory guidance from data protection authorities (DPAs) and jurisprudence from the Court of Justice of the European Union (CJEU), has highlighted the illegality of the way 'notice and consent' has hitherto functioned in the EU. These regulatory changes have both clarified the concept of consent in European law, as well as brought more significant (and extraterritorial) consequences for flaunting these rules. EU law in particular focuses on the *quality* of the consent required, and its freely-given, optional nature.

Consent management platforms (CMPs) have gained traction on the Web to help website owners outsource regulatory compliance.

M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal, "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence," 10.1145/3313831.3376321.

Violations are common on the web



Do Cookie Banners Respect my Choice?

Measuring Legal Compliance of Banners from IAB Europe’s Transparency and Consent Framework

Célestin Matte
Université Côte d’Azur, Inria
France
celestin.matte@inria.fr

Nataliia Bielova
Université Côte d’Azur, Inria
France
nataliia.bielova@inria.fr

Cristiana Santos
Research Centre for Justice and Governance
School of Law, University of Minho
cristianasantos@protonmail.com

***Abstract*—As a result of the GDPR and the ePrivacy Directive, European users encounter cookie banners on almost every website. Many of such banners are implemented by Consent Management Providers (CMPs), who respect IAB Europe’s Transparency and Consent Framework (TCF). Via cookie banners, CMPs collect and disseminate user consent to third parties. In this work, we systematically study IAB Europe’s TCF and analyze consent stored behind the user interface of TCF cookie banners. We analyze the GDPR and the ePrivacy Directive to identify potential legal violations in implementations of cookie banners based on the storage of consent and detect such suspected violations by crawling 1 426 websites that contains TCF banners, found among 28 257 crawled European websites. With two automatic and semi-automatic crawl campaigns, we detect suspected violations, and we find that: 141 websites register positive consent even if the user has not made their choice; 236 websites nudge the users towards accepting consent by pre-selecting options; and 27 websites store a positive consent even if the user has explicitly opted out. Performing extensive tests on 560 websites, we find at least one suspected violation in 54% of them. Finally, we provide a browser extension to facilitate manual detection of suspected violations for regular users and Data Protection Authorities.**

***Keywords*—Privacy; GDPR; Consent; Web measurement**

I. Introduction

Today’s web advertising ecosystem heavily relies on continuous data collection and tracking that allows advertising

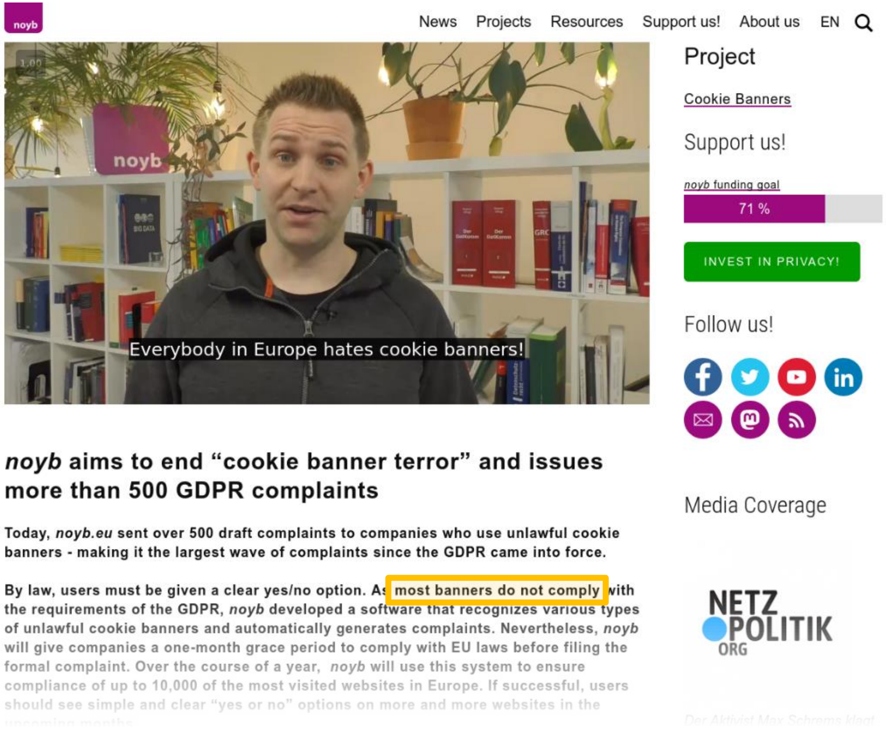
been measuring the impact of GDPR on the web tracking and advertising ecosystem. Libert et al. [41] observed a 22% drop in the amount of third-party cookies before and after the GDPR, but only a 2% drop in third-party content. Degeling et al. [9] recently measured the prevalence of cookie banners and showed that the amount of banners increased over time after the GDPR. Legal scholars, authorities and computer science researchers independently noticed that some banners do not allow users to refuse data collection, and raised this in various studies [9], [38], [2], [59]. Several recent works [56], [57], [53] measured the impact of choices set in cookie banners on tracking: upon accepting and rejecting the consent proposed in a cookie banner, researchers evaluated the number of cookies set in the browser and the number of third-party tracking requests across websites. Latest works [58], [45] evaluated whether the design of cookie banners made an impact on how users would interact with them.

Although many research efforts took place after the GDPR to detect and analyze cookie banners and their impact on tracking technologies and on the users, no study has analyzed what actually happens behind the user interface of cookie banners yet. It is unclear how to meaningfully compare the interface of the banners shown to the users to the actual consent that banners store and transmit to the third parties present on the website. Our work is motivated by the following questions:

Do banners actually respect user’s choice made in the user

C. Matte, N. Bielova, and C. Santos, “Do Cookie Banners Respect my Choice? : Measuring Legal Compliance of Banners from IAB Europe’s Transparency and Consent Framework,” 10.1109/SP40000.2020.00076.

Violations are common on the web



noyb aims to end “cookie banner terror” and issues more than 500 GDPR complaints

Today, *noyb.eu* sent over 500 draft complaints to companies who use unlawful cookie banners - making it the largest wave of complaints since the GDPR came into force.

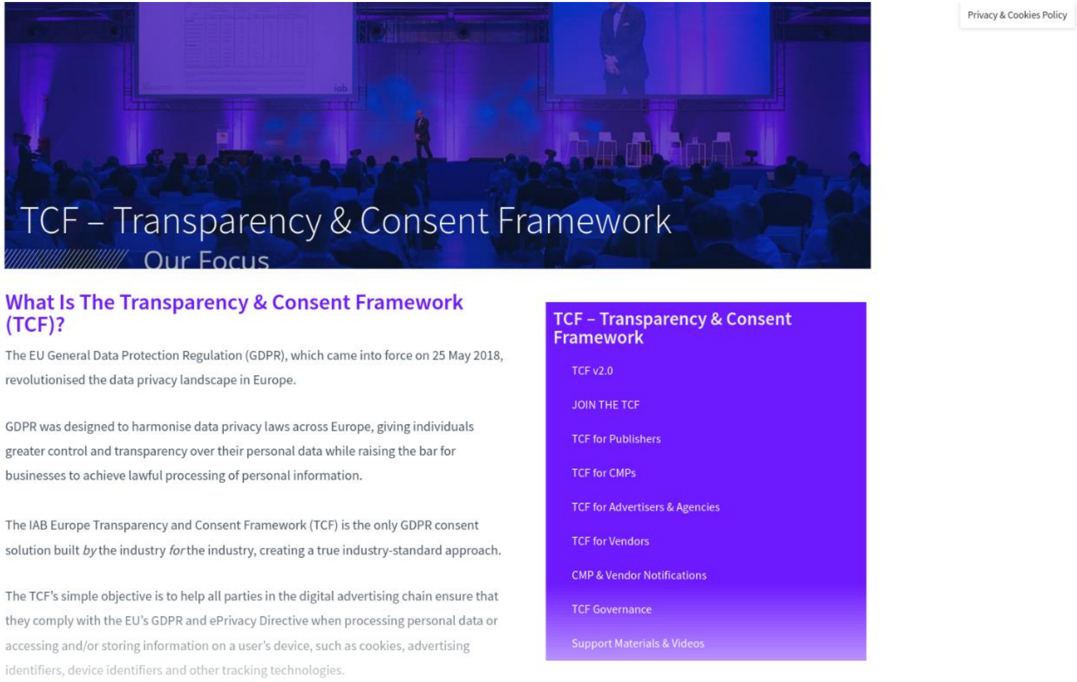
By law, users must be given a clear yes/no option. As most banners do not comply with the requirements of the GDPR, *noyb* developed a software that recognizes various types of unlawful cookie banners and automatically generates complaints. Nevertheless, *noyb* will give companies a one-month grace period to comply with EU laws before filing the formal complaint. Over the course of a year, *noyb* will use this system to ensure compliance of up to 10,000 of the most visited websites in Europe. If successful, users should see simple and clear “yes or no” options on more and more websites in the upcoming months.

https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints

Image: Eirik Solheim (Unsplash license)

Method

So, how can we find dialogs?



Privacy & Cookies Policy

TCF – Transparency & Consent Framework

Our Focus

What Is The Transparency & Consent Framework (TCF)?

The EU General Data Protection Regulation (GDPR), which came into force on 25 May 2018, revolutionised the data privacy landscape in Europe.

GDPR was designed to harmonise data privacy laws across Europe, giving individuals greater control and transparency over their personal data while raising the bar for businesses to achieve lawful processing of personal information.

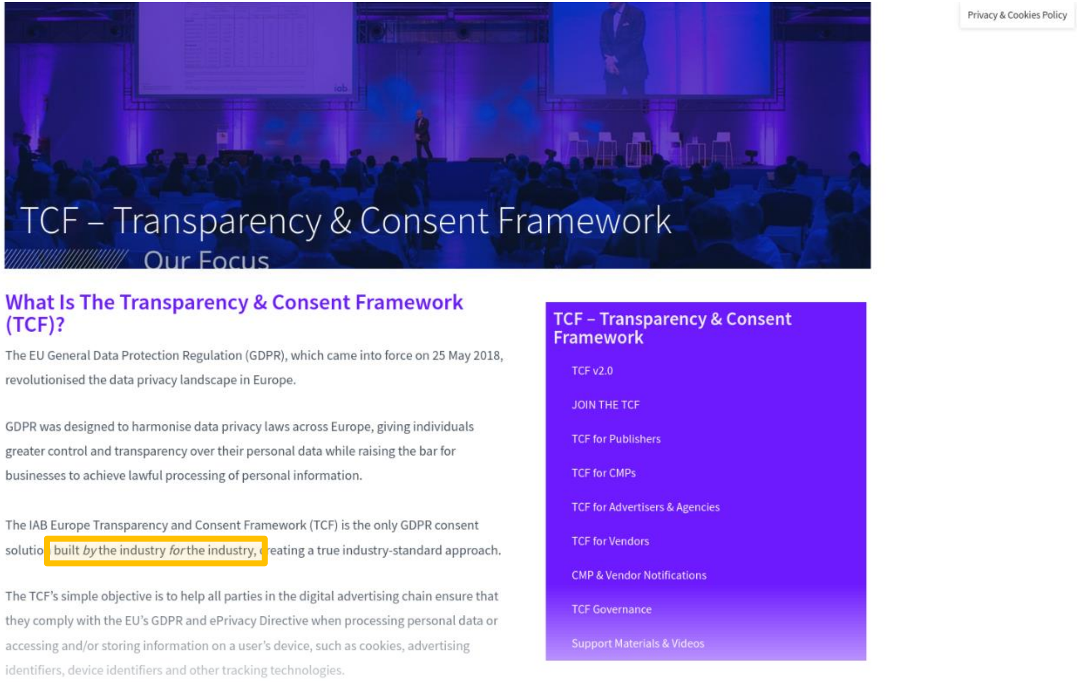
The IAB Europe Transparency and Consent Framework (TCF) is the only GDPR consent solution built *by* the industry *for* the industry, creating a true industry-standard approach.

The TCF's simple objective is to help all parties in the digital advertising chain ensure that they comply with the EU's GDPR and ePrivacy Directive when processing personal data or accessing and/or storing information on a user's device, such as cookies, advertising identifiers, device identifiers and other tracking technologies.

TCF – Transparency & Consent Framework
TCF v2.0
JOIN THE TCF
TCF for Publishers
TCF for CMPs
TCF for Advertisers & Agencies
TCF for Vendors
CMP & Vendor Notifications
TCF Governance
Support Materials & Videos

https://iabeurope.eu/transparency-consent-framework/

So, how can we find dialogs?



Privacy & Cookies Policy

TCF – Transparency & Consent Framework

Our Focus

What Is The Transparency & Consent Framework (TCF)?

The EU General Data Protection Regulation (GDPR), which came into force on 25 May 2018, revolutionised the data privacy landscape in Europe.

GDPR was designed to harmonise data privacy laws across Europe, giving individuals greater control and transparency over their personal data while raising the bar for businesses to achieve lawful processing of personal information.

The IAB Europe Transparency and Consent Framework (TCF) is the only GDPR consent solution built *by* the industry *for* the industry, creating a true industry-standard approach.

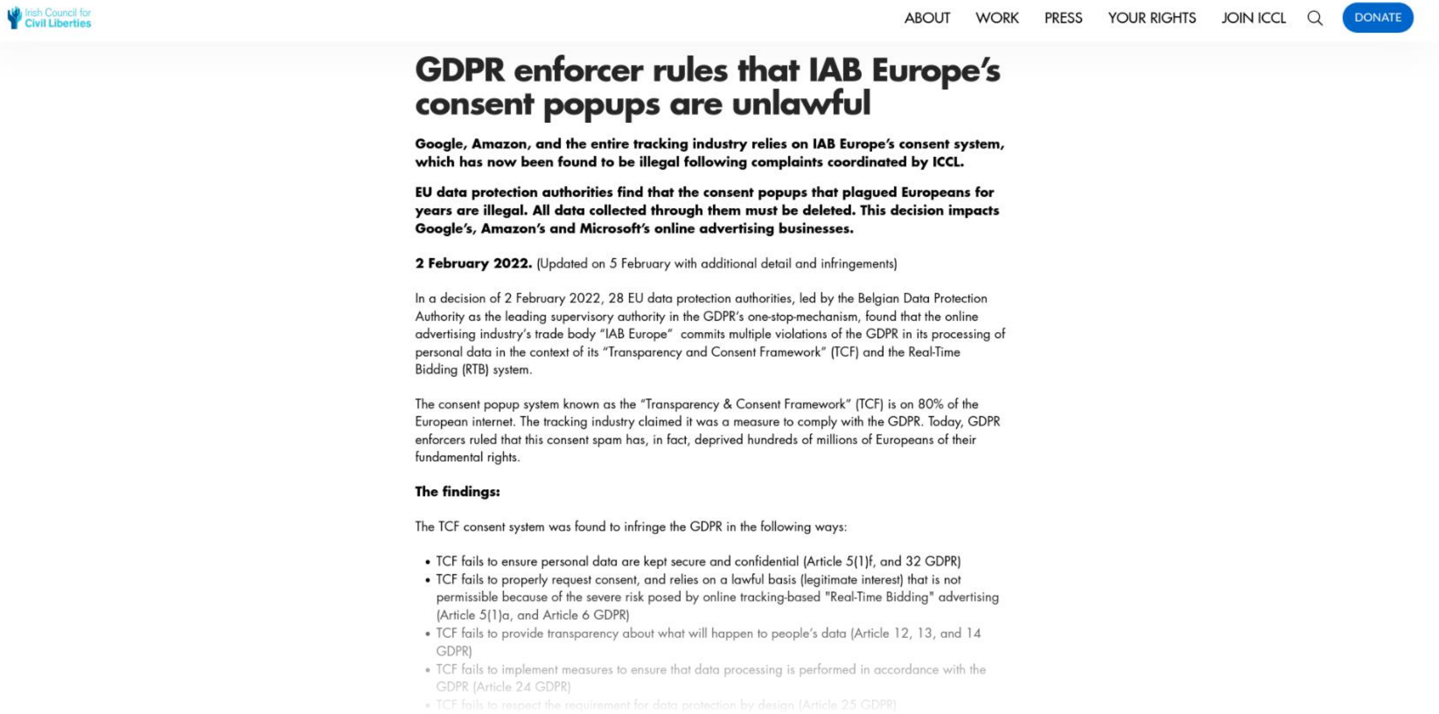
The TCF's simple objective is to help all parties in the digital advertising chain ensure that they comply with the EU's GDPR and ePrivacy Directive when processing personal data or accessing and/or storing information on a user's device, such as cookies, advertising identifiers, device identifiers and other tracking technologies.

TCF – Transparency & Consent Framework

- TCF v2.0
- JOIN THE TCF
- TCF for Publishers
- TCF for CMPs
- TCF for Advertisers & Agencies
- TCF for Vendors
- CMP & Vendor Notifications
- TCF Governance
- Support Materials & Videos

https://iabeurope.eu/transparency-consent-framework/

IAB Transparency & Consent Framework



GDPR enforcer rules that IAB Europe's consent popups are unlawful

Google, Amazon, and the entire tracking industry relies on IAB Europe's consent system, which has now been found to be illegal following complaints coordinated by ICCL.

EU data protection authorities find that the consent popups that plagued Europeans for years are illegal. All data collected through them must be deleted. This decision impacts Google's, Amazon's and Microsoft's online advertising businesses.

2 February 2022. (Updated on 5 February with additional detail and infringements)

In a decision of 2 February 2022, 28 EU data protection authorities, led by the Belgian Data Protection Authority as the leading supervisory authority in the GDPR's one-stop-mechanism, found that the online advertising industry's trade body "IAB Europe" commits multiple violations of the GDPR in its processing of personal data in the context of its "Transparency and Consent Framework" (TCF) and the Real-Time Bidding (RTB) system.

The consent popup system known as the "Transparency & Consent Framework" (TCF) is on 80% of the European internet. The tracking industry claimed it was a measure to comply with the GDPR. Today, GDPR enforcers ruled that this consent spam has, in fact, deprived hundreds of millions of Europeans of their fundamental rights.

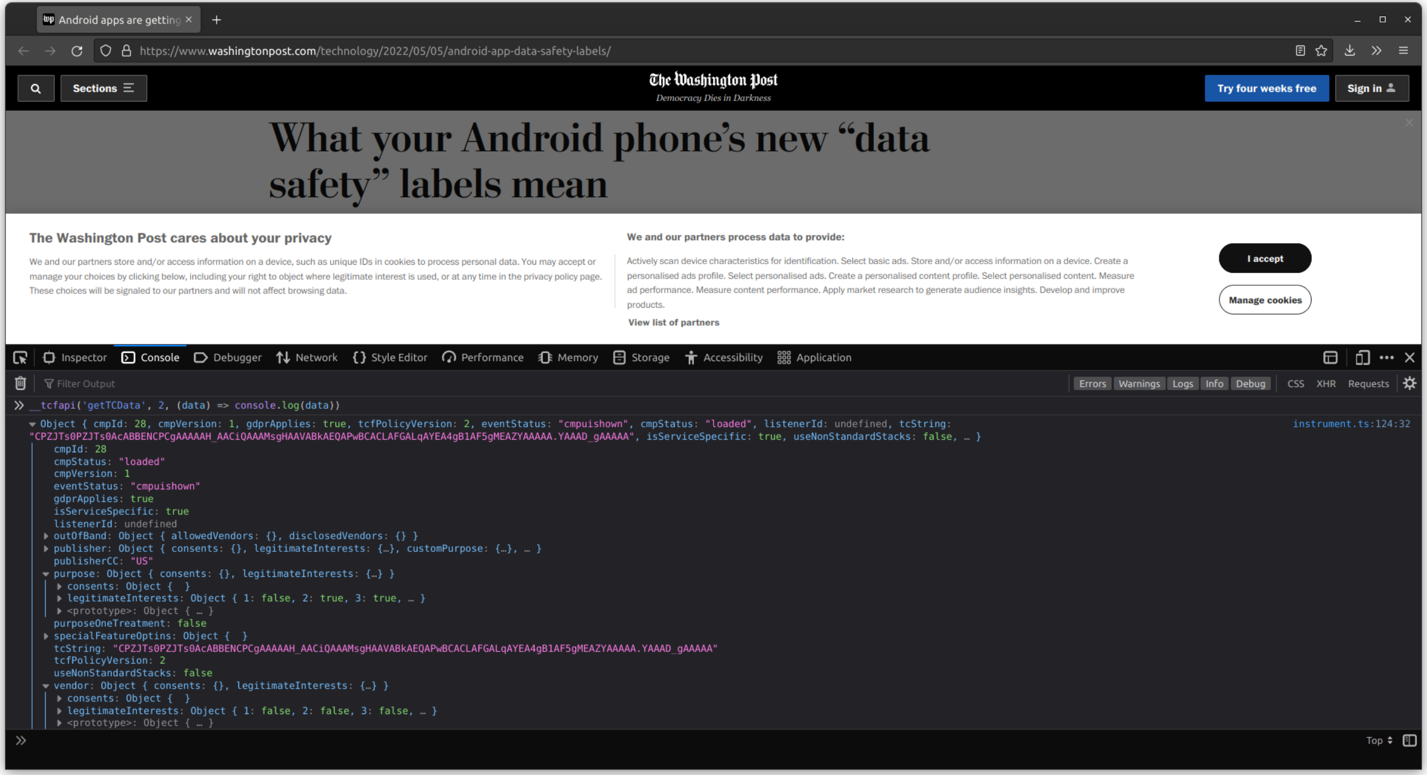
The findings:

The TCF consent system was found to infringe the GDPR in the following ways:

- TCF fails to ensure personal data are kept secure and confidential (Article 5(1)f, and 32 GDPR)
- TCF fails to properly request consent, and relies on a lawful basis (legitimate interest) that is not permissible because of the severe risk posed by online tracking-based "Real-Time Bidding" advertising (Article 5(1)a, and Article 6 GDPR)
- TCF fails to provide transparency about what will happen to people's data (Article 12, 13, and 14 GDPR)
- TCF fails to implement measures to ensure that data processing is performed in accordance with the GDPR (Article 24 GDPR)
- TCF fails to respect the requirement for data protection by design (Article 25 GDPR)

https://www.iccl.ie/news/gdpr-enforcer-rules-that-iab-europes-consent-popups-are-unlawful/

IAB Transparency & Consent Framework



The Washington Post cares about your privacy

We and our partners store and/or access information on a device, such as unique IDs in cookies to process personal data. You may accept or manage your choices by clicking below, including your right to object where legitimate interest is used, or at any time in the privacy policy page. These choices will be signaled to our partners and will not affect browsing data.

We and our partners process data to provide:

Actively scan device characteristics for identification. Select basic ads. Store and/or access information on a device. Create a personalised ads profile. Select personalised ads. Create a personalised content profile. Select personalised content. Measure ad performance. Measure content performance. Apply market research to generate audience insights. Develop and improve products.

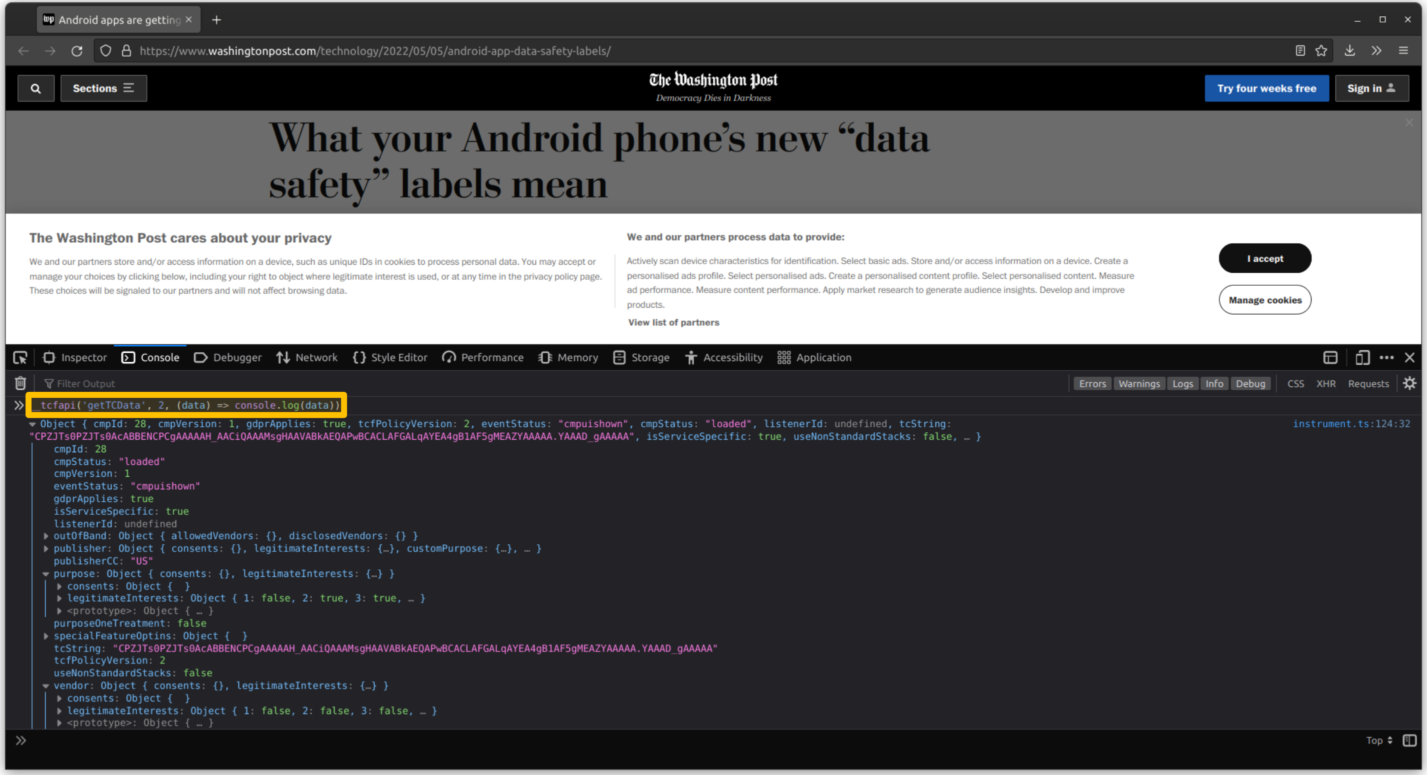
View list of partners

I accept

Manage cookies

```
>> __tcfapi('getTCData', 2, (data) => console.log(data))
  ▼ Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "cmpuishown", cmpStatus: "loaded", listenerId: undefined, tcString:      instrument.ts:124:32
  "CPZJTs0PZJTs0AcABBENCPCgAAAAAH_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: "CPZJTs0PZJTs0AcABBENCPCgAAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAAA.YAAAD_gAAAAA"
      tcfPolicyVersion: 2
      useNonStandardStacks: false
    ▼ vendor: Object { consents: {}, legitimateInterests: {…} }
      ▶ consents: Object {  }
      ▶ legitimateInterests: Object { 1: false, 2: false, 3: false, … }
      ▶ <prototype>: Object { … }
>>
```

IAB Transparency & Consent Framework



The Washington Post cares about your privacy

We and our partners store and/or access information on a device, such as unique IDs in cookies to process personal data. You may accept or manage your choices by clicking below, including your right to object where legitimate interest is used, or at any time in the privacy policy page. These choices will be signaled to our partners and will not affect browsing data.

We and our partners process data to provide:

Actively scan device characteristics for identification. Select basic ads. Store and/or access information on a device. Create a personalised ads profile. Select personalised ads. Create a personalised content profile. Select personalised content. Measure ad performance. Measure content performance. Apply market research to generate audience insights. Develop and improve products.

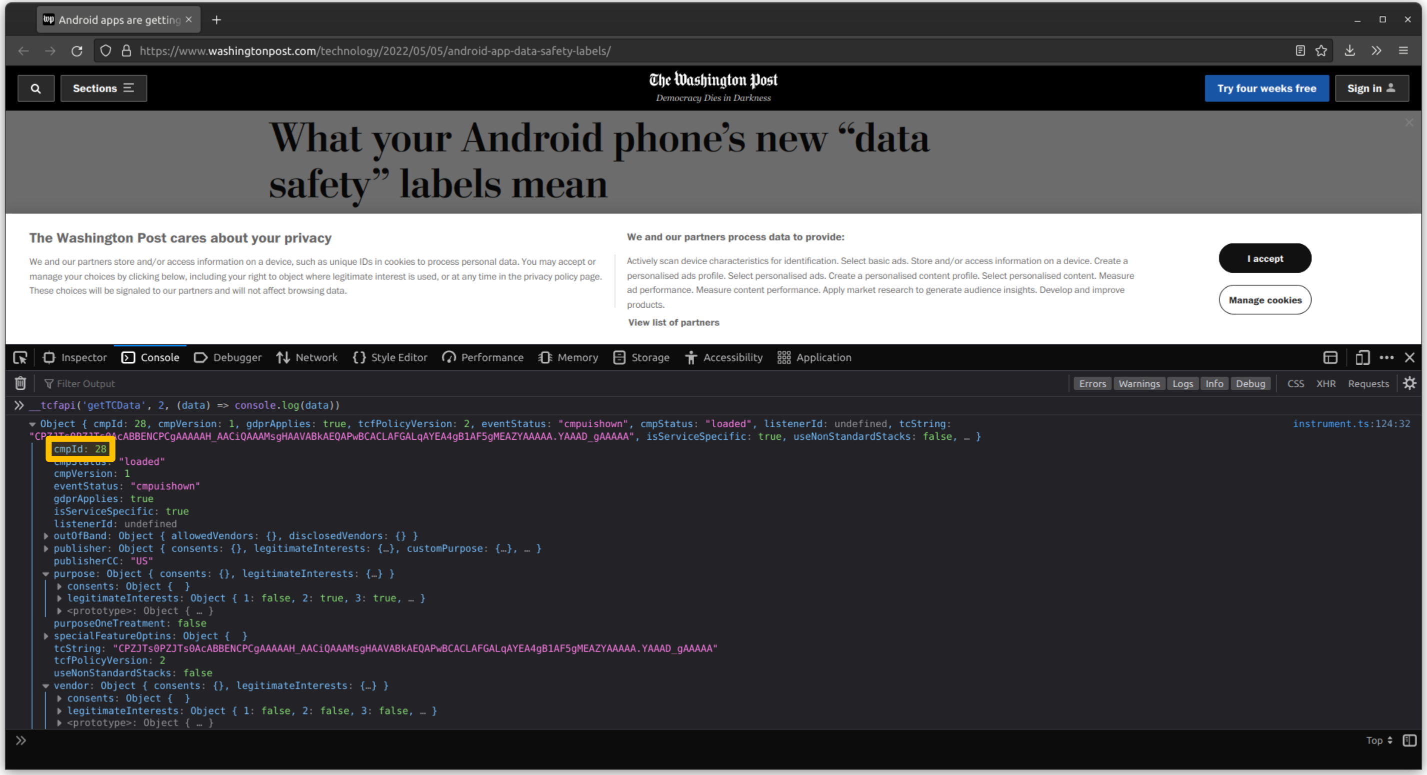
View list of partners

I accept

Manage cookies

```
>> __tcfapi('getTCData', 2, (data) => console.log(data))
  ▾ Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "cmpuishown", cmpStatus: "loaded", listenerId: undefined, tcString:      instrument.ts:124:32
  "CPZJTs0PZJTs0AcABBENCPCgAAAAAH_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: "CPZJTs0PZJTs0AcABBENCPCgAAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAAA.YAAAD_gAAAAA"
      tcfPolicyVersion: 2
      useNonStandardStacks: false
    ▾ vendor: Object { consents: {}, legitimateInterests: {…} }
      ▸ consents: Object {  }
      ▸ legitimateInterests: Object { 1: false, 2: false, 3: false, … }
      ▸ <prototype>: Object { … }
>>
```

IAB Transparency & Consent Framework



Android apps are getting ×
https://www.washingtonpost.com/technology/2022/05/05/android-app-data-safety-labels/
Sections
The Washington Post
Democracy Dies in Darkness
Try four weeks free
Sign in
What your Android phone’s new “data safety” labels mean

The Washington Post cares about your privacy

We and our partners store and/or access information on a device, such as unique IDs in cookies to process personal data. You may accept or manage your choices by clicking below, including your right to object where legitimate interest is used, or at any time in the privacy policy page. These choices will be signaled to our partners and will not affect browsing data.

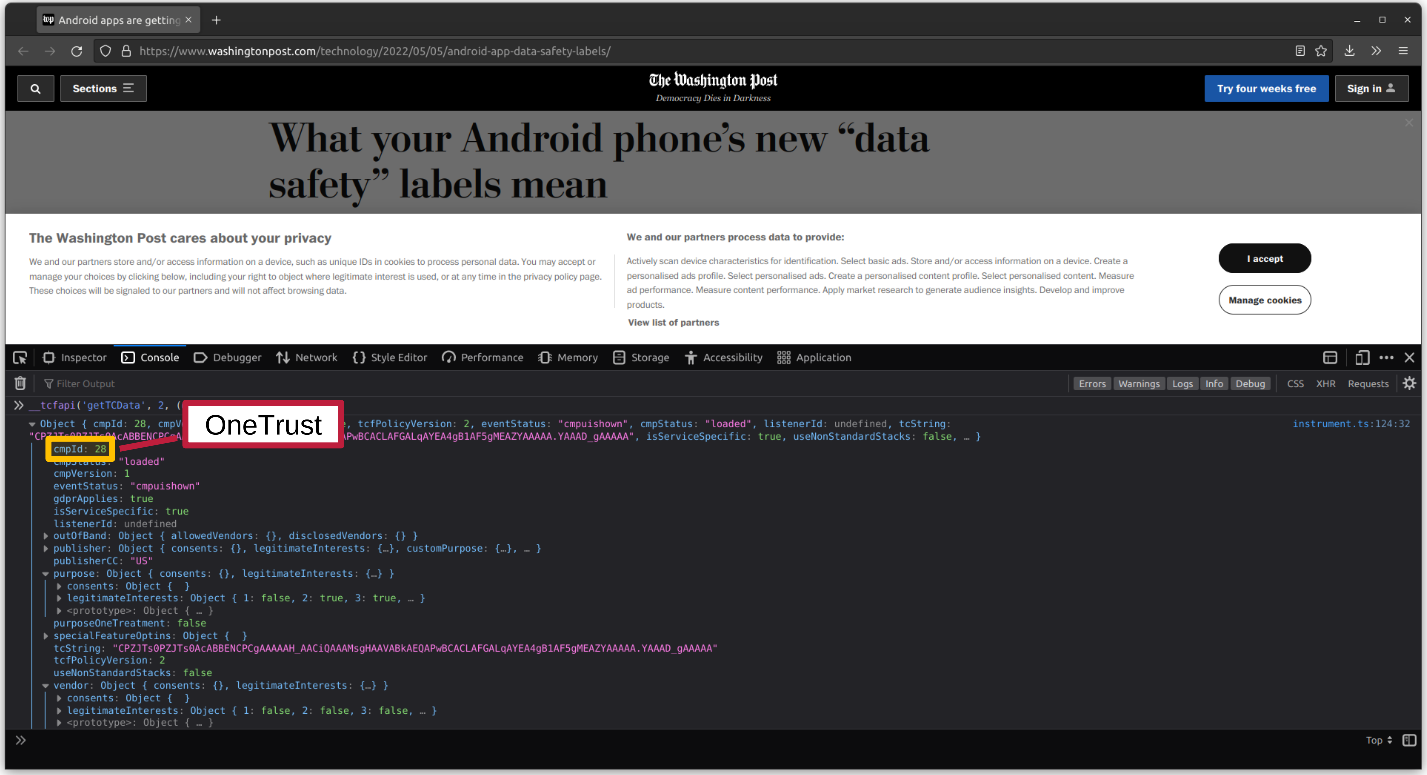
We and our partners process data to provide:

Actively scan device characteristics for identification. Select basic ads. Store and/or access information on a device. Create a personalised ads profile. Select personalised ads. Create a personalised content profile. Select personalised content. Measure ad performance. Measure content performance. Apply market research to generate audience insights. Develop and improve products.

View list of partners

```
>> __tcfapi('getTCData', 2, (data) => console.log(data))
▾ Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "cmpuishown", cmpStatus: "loaded", listenerId: undefined, tcString:
"CPZJTs0PZJTs0AcABBENCPCgAAAAAH_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: "CPZJTs0PZJTs0AcABBENCPCgAAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAAA.YAAAD_gAAAAA"
    tcfPolicyVersion: 2
    useNonStandardStacks: false
  ▾ vendor: Object { consents: {}, legitimateInterests: {…} }
    ▸ consents: Object {  }
    ▸ legitimateInterests: Object { 1: false, 2: false, 3: false, … }
    ▸ <prototype>: Object { … }
>>
```

IAB Transparency & Consent Framework



Android apps are getting ×
https://www.washingtonpost.com/technology/2022/05/05/android-app-data-safety-labels/
Sections
The Washington Post
Democracy Dies in Darkness
Try four weeks free
Sign in
What your Android phone's new “data safety” labels mean

The Washington Post cares about your privacy

We and our partners store and/or access information on a device, such as unique IDs in cookies to process personal data. You may accept or manage your choices by clicking below, including your right to object where legitimate interest is used, or at any time in the privacy policy page. These choices will be signaled to our partners and will not affect browsing data.

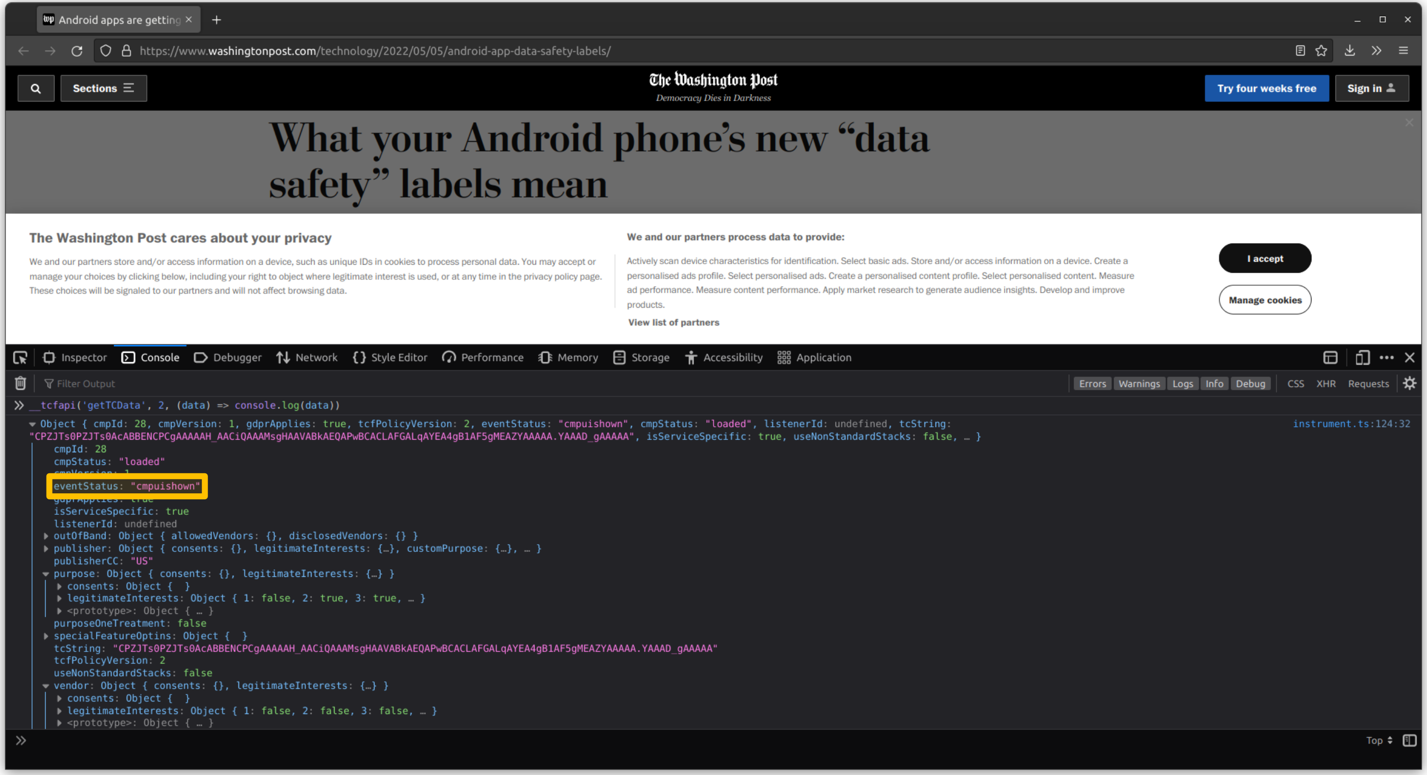
We and our partners process data to provide:

Actively scan device characteristics for identification. Select basic ads. Store and/or access information on a device. Create a personalised ads profile. Select personalised ads. Create a personalised content profile. Select personalised content. Measure ad performance. Measure content performance. Apply market research to generate audience insights. Develop and improve products.

View list of partners

```
» __tcfapi('getTCData', 2, (
  ▾ Object { cmpId: 28, cmpV                    , tcfPolicyVersion: 2, eventStatus: "cmpuishown", cmpStatus: "loaded", listenerId: undefined, tcString:          instrument.ts:124:32
  "CPZJTs0PZJTs0AcABBENCPCgA                    PwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAAA.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: "CPZJTs0PZJTs0AcABBENCPCgAAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAAA.YAAAD_gAAAAA"
      tcfPolicyVersion: 2
      useNonStandardStacks: false
    ▾ vendor: Object { consents: {}, legitimateInterests: {…} }
      ▸ consents: Object {  }
      ▸ legitimateInterests: Object { 1: false, 2: false, 3: false, … }
      ▸ <prototype>: Object { … }
»
```

IAB Transparency & Consent Framework


Android apps are getting
https://www.washingtonpost.com/technology/2022/05/05/android-app-data-safety-labels/
Sections
The Washington Post
Democracy Dies in Darkness
Try four weeks free
Sign in
What your Android phone’s new “data safety” labels mean

The Washington Post cares about your privacy

We and our partners store and/or access information on a device, such as unique IDs in cookies to process personal data. You may accept or manage your choices by clicking below, including your right to object where legitimate interest is used, or at any time in the privacy policy page. These choices will be signaled to our partners and will not affect browsing data.

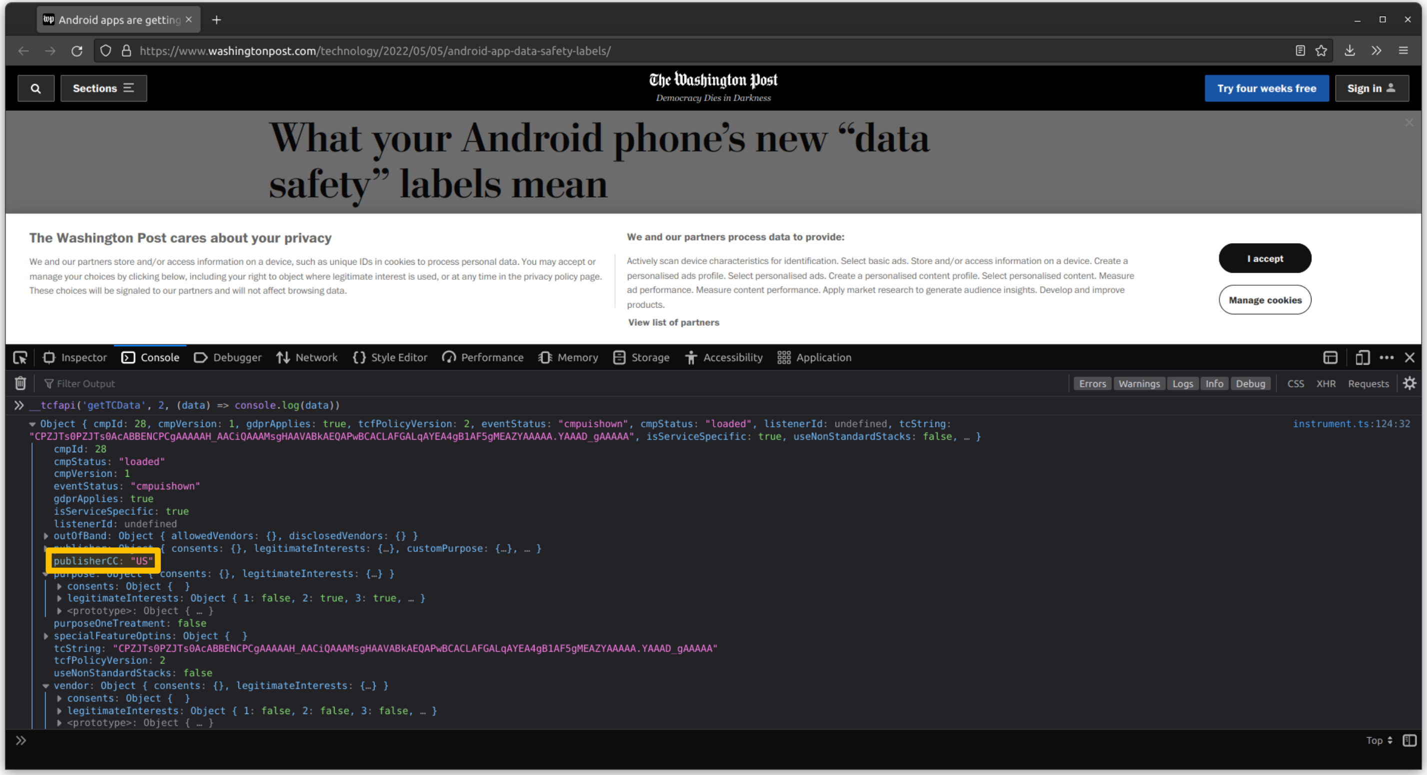
We and our partners process data to provide:

Actively scan device characteristics for identification. Select basic ads. Store and/or access information on a device. Create a personalised ads profile. Select personalised ads. Create a personalised content profile. Select personalised content. Measure ad performance. Measure content performance. Apply market research to generate audience insights. Develop and improve products.

View list of partners

```
» __tcfapi('getTCData', 2, (data) => console.log(data))
▾ Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "cmpuishown", cmpStatus: "loaded", listenerId: undefined, tcString:      instrument.ts:124:32
"CPZJTs0PZJTs0AcABBENCPCgAAAAAH_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: "CPZJTs0PZJTs0AcABBENCPCgAAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAAA.YAAAD_gAAAAA"
    tcfPolicyVersion: 2
    useNonStandardStacks: false
  ▾ vendor: Object { consents: {}, legitimateInterests: {…} }
    ▸ consents: Object {  }
    ▸ legitimateInterests: Object { 1: false, 2: false, 3: false, … }
    ▸ <prototype>: Object { … }
»
```

IAB Transparency & Consent Framework



What your Android phone’s new “data safety” labels mean

The Washington Post cares about your privacy

We and our partners store and/or access information on a device, such as unique IDs in cookies to process personal data. You may accept or manage your choices by clicking below, including your right to object where legitimate interest is used, or at any time in the privacy policy page. These choices will be signaled to our partners and will not affect browsing data.

We and our partners process data to provide:

Actively scan device characteristics for identification. Select basic ads. Store and/or access information on a device. Create a personalised ads profile. Select personalised ads. Create a personalised content profile. Select personalised content. Measure ad performance. Measure content performance. Apply market research to generate audience insights. Develop and improve products.

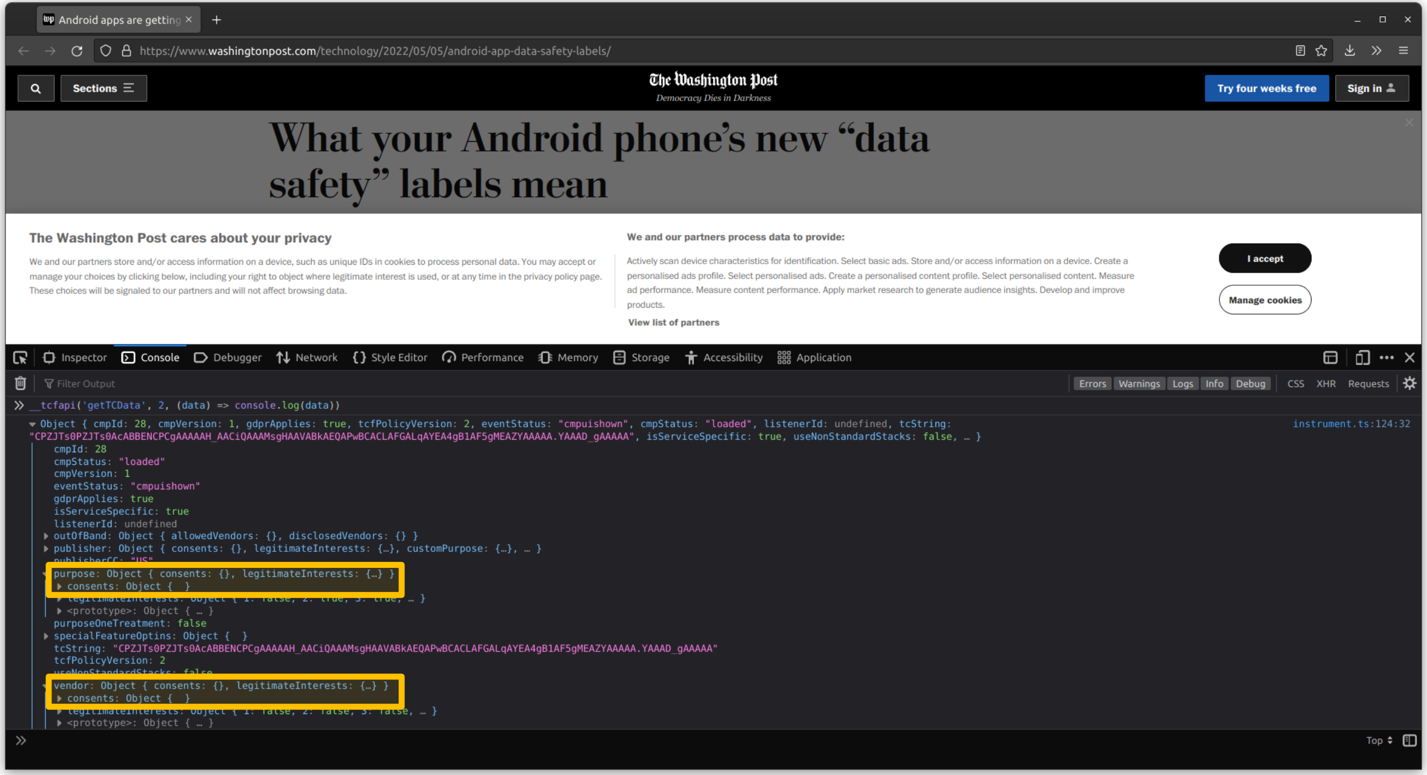
View list of partners

I accept

Manage cookies

```
» __tcfapi('getTCData', 2, (data) => console.log(data))
▾ Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "cmpuishown", cmpStatus: "loaded", listenerId: undefined, tcString:     instrument.ts:124:32
"CPZJTs0PZJTs0AcABBENCPCgAAAAAH_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: "CPZJTs0PZJTs0AcABBENCPCgAAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAAA.YAAAD_gAAAAA"
    tcfPolicyVersion: 2
    useNonStandardStacks: false
  ▾ vendor: Object { consents: {}, legitimateInterests: {…} }
    ▸ consents: Object {  }
    ▸ legitimateInterests: Object { 1: false, 2: false, 3: false, … }
    ▸ <prototype>: Object { … }
»
```

IAB Transparency & Consent Framework



Android apps are getting ×
https://www.washingtonpost.com/technology/2022/05/05/android-app-data-safety-labels/
Sections
The Washington Post
Democracy Dies in Darkness
Try four weeks free
Sign in

What your Android phone’s new “data safety” labels mean

The Washington Post cares about your privacy

We and our partners store and/or access information on a device, such as unique IDs in cookies to process personal data. You may accept or manage your choices by clicking below, including your right to object where legitimate interest is used, or at any time in the privacy policy page. These choices will be signaled to our partners and will not affect browsing data.

We and our partners process data to provide:

Actively scan device characteristics for identification. Select basic ads. Store and/or access information on a device. Create a personalised ads profile. Select personalised ads. Create a personalised content profile. Select personalised content. Measure ad performance. Measure content performance. Apply market research to generate audience insights. Develop and improve products.

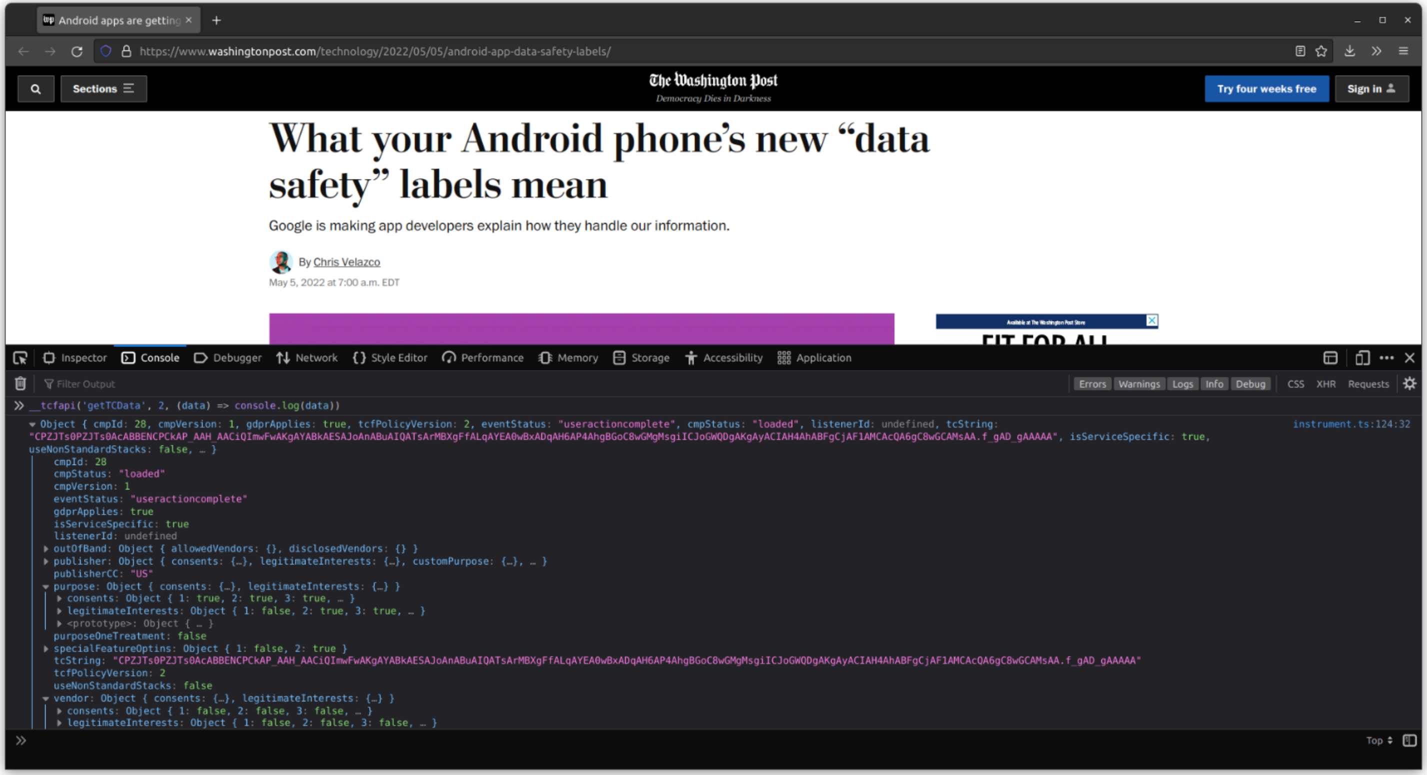
View list of partners

I accept

Manage cookies

```
>> __tcfapi('getTCData', 2, (data) => console.log(data))
▾ Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "cmpuishown", cmpStatus: "loaded", listenerId: undefined, tcString:     instrument.ts:124:32
"CPZJTs0PZJTs0AcABBENCPCgAAAAAH_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: "CPZJTs0PZJTs0AcABBENCPCgAAAAAH_AACiQAAAMsgHAAVABkAEQAPwBCACLAFGALqAYEA4gB1AF5gMEAZYAAAAA.YAAAD_gAAAAA"
    tcfPolicyVersion: 2
    useNonStandardStacks: false
  ▾ vendor: Object { consents: {}, legitimateInterests: {…} }
    ▸ consents: Object {  }
    ▸ legitimateInterests: Object { 1: false, 2: false, 3: false, … }
    ▸ <prototype>: Object { … }
```

IAB Transparency & Consent Framework



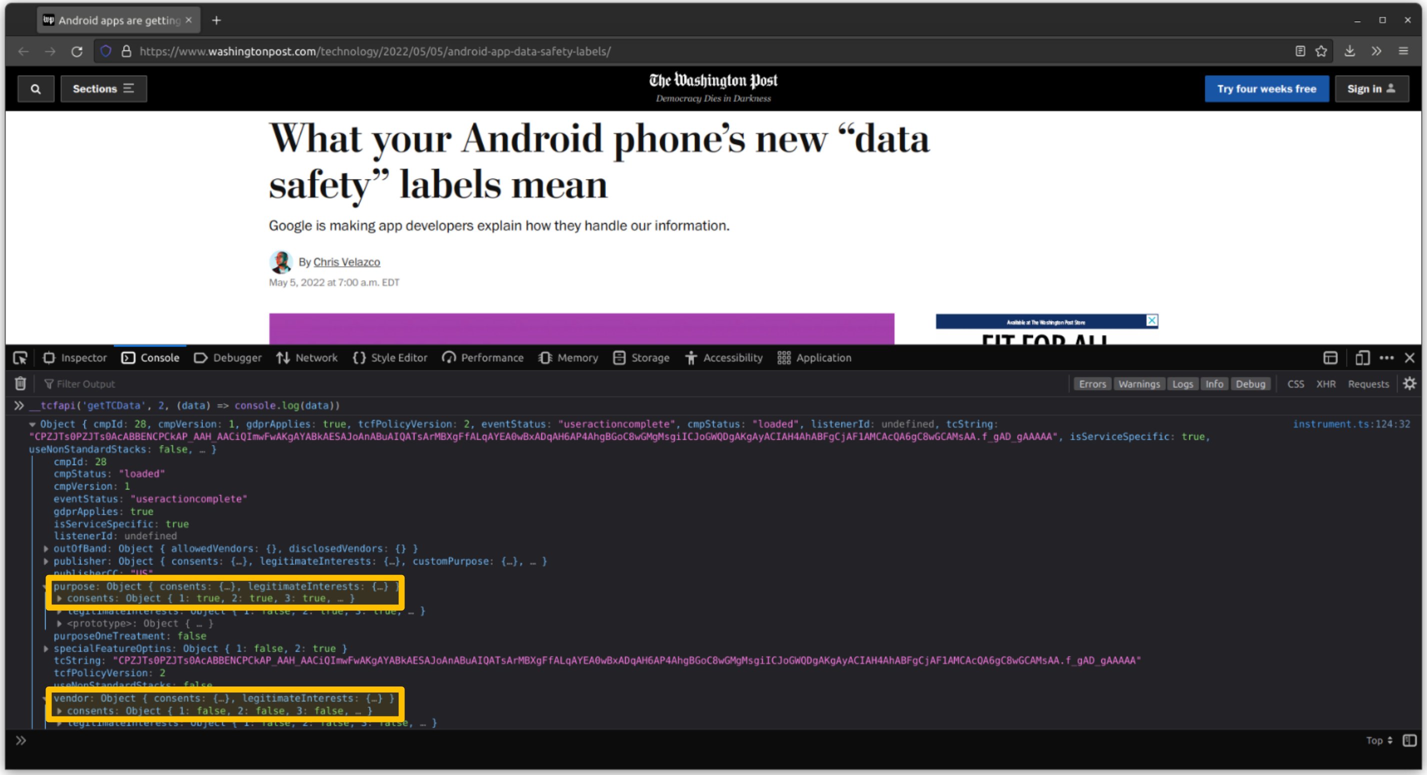
What your Android phone’s new “data safety” labels mean

Google is making app developers explain how they handle our information.

By Chris Velazco
May 5, 2022 at 7:00 a.m. EDT

```
>> __tcfapi('getTCData', 2, (data) => console.log(data))
 ▾ Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "useractioncomplete", cmpStatus: "loaded", listenerId: undefined, tcString:      instrument.ts:124:32
 "CPZJTs0PZJTs0AcABBENCPCkAP_AAH_AACiQImwFwAKgAYABkAESAJoAnABuAIQATsArMBXgFfALqAYEA0wBxADqAH6AP4AhgBGoC8wGMgMsgiICJoGWQDgAKgAyACIAH4AhABFgCjAF1AMCAcQA6gC8wGCAMsAA.f_gAD_gAAAAA", isServiceSpecific: true,
 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_AAH_AACiQImwFwAKgAYABkAESAJoAnABuAIQATsArMBXgFfALqAYEA0wBxADqAH6AP4AhgBGoC8wGMgMsgiICJoGWQDgAKgAyACIAH4AhABFgCjAF1AMCAcQA6gC8wGCAMsAA.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, … }
>>
```

IAB Transparency & Consent Framework



What your Android phone’s new “data safety” labels mean

Google is making app developers explain how they handle our information.

By Chris Velazco

May 5, 2022 at 7:00 a.m. EDT

```
>> __tcfapi('getTCData', 2, (data) => console.log(data))
  ▾ Object { cmpId: 28, cmpVersion: 1, gdprApplies: true, tcfPolicyVersion: 2, eventStatus: "useractioncomplete", cmpStatus: "loaded", listenerId: undefined, tcString:      instrument.ts:124:32
  "CPZJTs0PZJTs0AcABBENCPCkAP_AAH_AACiQImwFwAKgAYABkAESAJoAnABuAIQATsArMBXgFfALqAYEA0wBxADqAH6AP4AhgBGoC8wGMgMsgiICJoGWQDgAKgAyACIAH4AhABFgCjAF1AMCAcQA6gC8wGCAMsAA.f_gAD_gAAAAA", isServiceSpecific: true,
  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_AAH_AACiQImwFwAKgAYABkAESAJoAnABuAIQATsArMBXgFfALqAYEA0wBxADqAH6AP4AhgBGoC8wGMgMsgiICJoGWQDgAKgAyACIAH4AhABFgCjAF1AMCAcQA6gC8wGCAMsAA.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, … }
>>
```

Is that viable?

- Quick experiment on 823 Android apps:
  - 21.99 % showed consent element on screen
  - 2.55 % set TCF preferences

  - => not viable

Is that viable?

- Quick experiment on 823 Android apps:
  - 21.99 % showed consent element on screen
  - 2.55 % set TCF preferences
  - => not viable
- What about CMP-specific adapters?
  - Quick experiment on use of known CMPs: 2.8 % on iOS, 7.15 % on Android (over approximation)
  - => not viable, either

So, what now?

- We have to do text-based matching on common elements in consent dialogs.

So, what now?

- We have to do text-based matching on common elements in consent dialogs.
- For that, we distinguish between:
  - **link**: App only links to privacy policy, e.g. in menu or footer.
  - **notice**: App informs user of processing but gives no choice.
  - **dialog**: App informs user of processing and solicits active consent.

So, what now?

- We have to do text-based matching on common elements in consent dialogs.
- For that, we distinguish between:
  - **link**: App only links to privacy policy, e.g. in menu or footer.
  - **notice**: App informs user of processing but gives no choice.
  - **dialog**: App informs user of processing and solicits active consent.

- We use regexes that match common phrases, e.g.:

```
/have read( and understood)? [^.]{3,35} (privacy|cookie|data
  protection|GDPR) (policy|notice|information|statement)/
```

So, what now?

- We have to do text-based matching on common elements in consent dialogs.
- For that, we distinguish between:
  - **link**: App only links to privacy policy, e.g. in menu or footer.
  - **notice**: App informs user of processing but gives no choice.
  - **dialog**: App informs user of processing and solicits active consent.

- We use regexes that match common phrases, e.g.:

```
/have read( and understood)? [^.]{3,35} (privacy|cookie|data
  protection|GDPR) (policy|notice|information|statement)/
```

- In addition: keyword score to weed out terms of services notices.

Device instrumentation framework

- Basic instrumentation tooling from prior work extended for this thesis.

Device instrumentation framework

- Basic instrumentation tooling from prior work extended for this thesis.
- Uses emulator for Android, physical iPhone for iOS.

Device instrumentation framework

- Basic instrumentation tooling from prior work extended for this thesis.

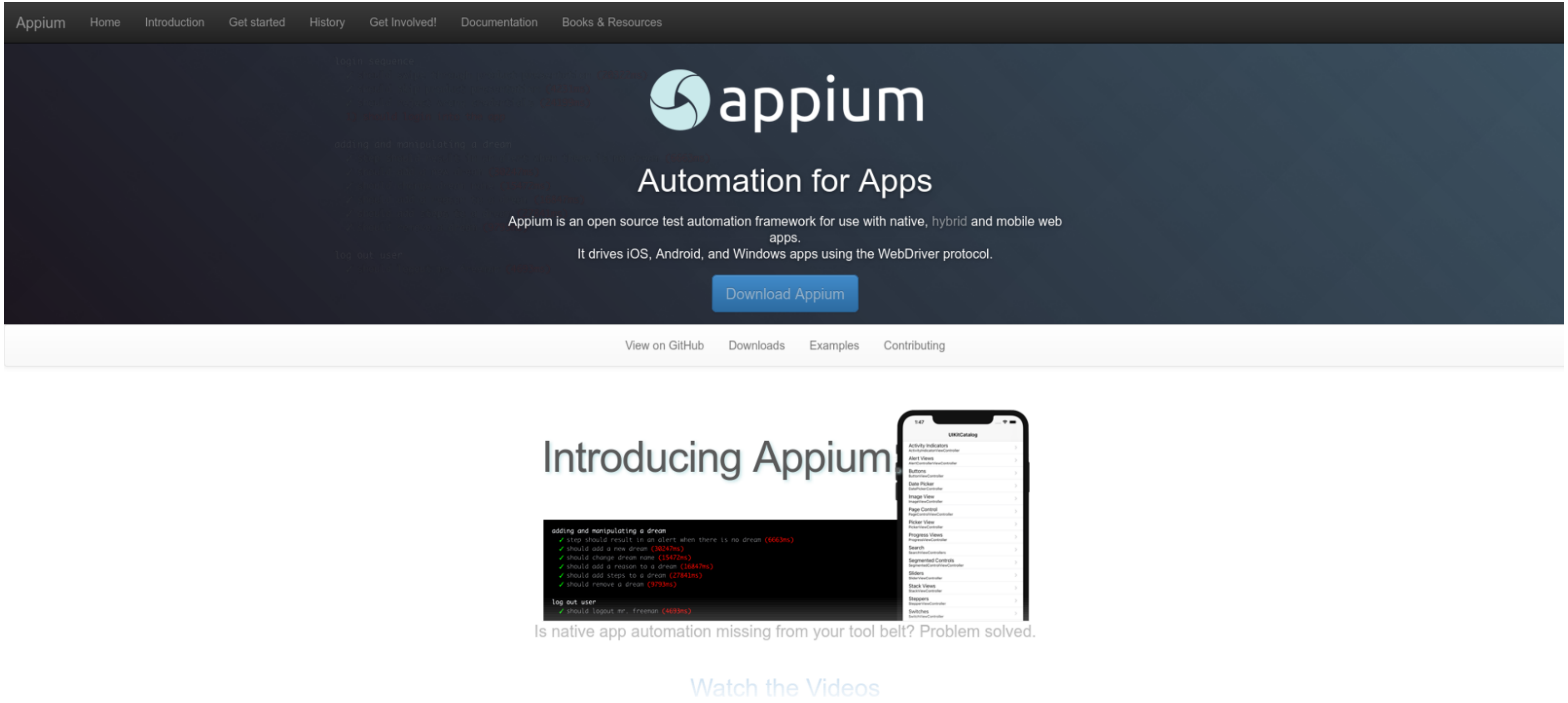
- Uses emulator for Android, physical iPhone for iOS.
- Manages apps, sets permissions, resets device, and starts apps.

Device instrumentation framework

- Basic instrumentation tooling from prior work extended for this thesis.

- Uses emulator for Android, physical iPhone for iOS.
- Manages apps, sets permissions, resets device, and starts apps.
- Traffic collected using mitmproxy and objection/SSL Kill Switch 2.

Elements on screen



Automation for Apps

Appium is an open source test automation framework for use with native, hybrid and mobile web apps.
It drives iOS, Android, and Windows apps using the WebDriver protocol.

Introducing Appium

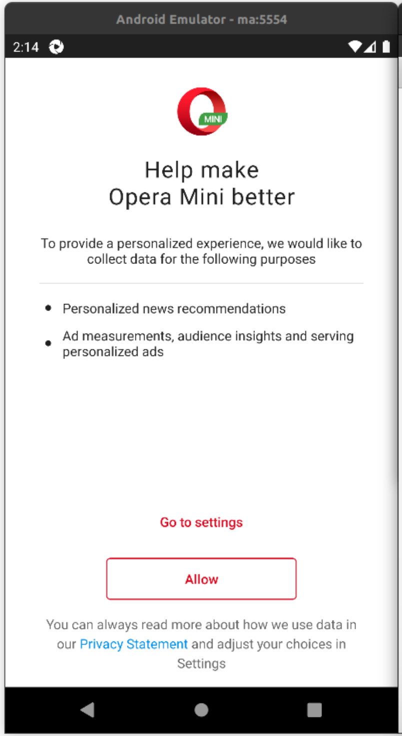
```
adding and manipulating a dream
  ✓ step should result in an alert when there is no dream (6663ms)
  ✓ should add a new dream (30247ms)
  ✓ should change dream name (15472ms)
  ✓ should add a reason to a dream (16847ms)
  ✓ should add steps to a dream (27841ms)
  ✓ should remove a dream (9793ms)

log out user
  ✓ should logout mr. freeman (4693ms)
```

Is native app automation missing from your tool belt? Problem solved.

https://appium.io/

Elements on screen



Android Emulator - ma:5554

2:14

Help make
Opera Mini better

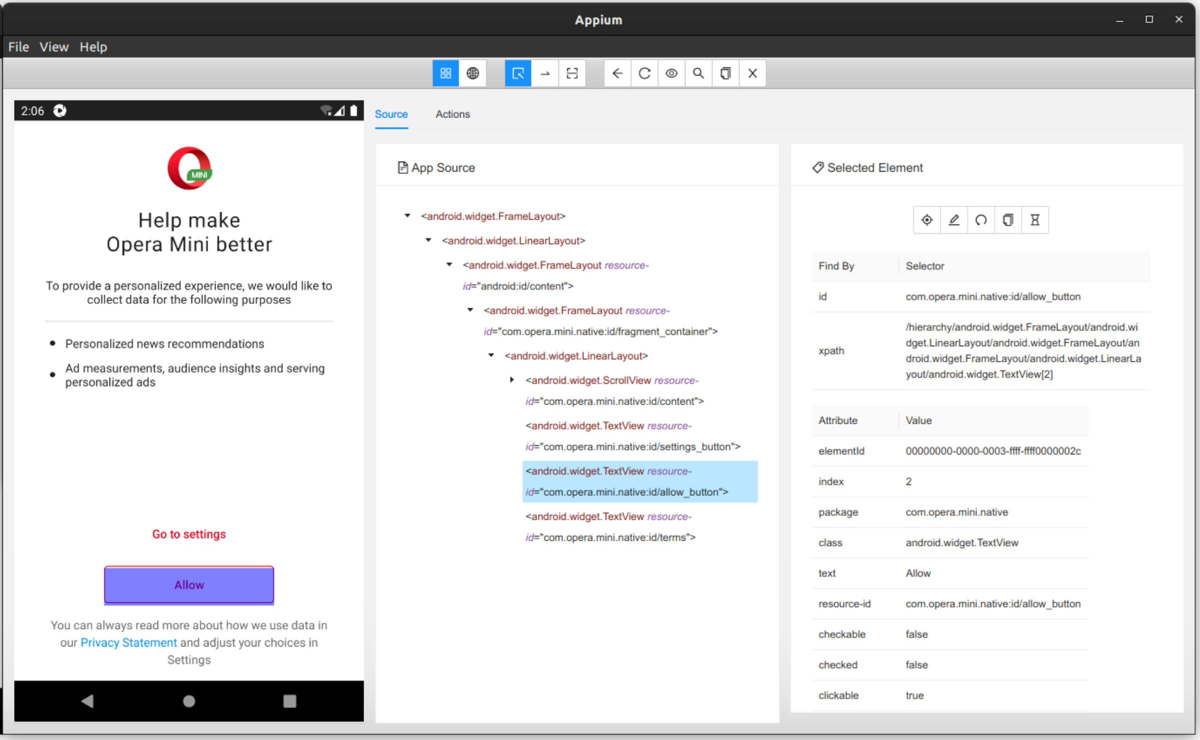
To provide a personalized experience, we would like to collect data for the following purposes

- Personalized news recommendations
- Ad measurements, audience insights and serving personalized ads

Go to settings

Allow

You can always read more about how we use data in our Privacy Statement and adjust your choices in Settings



2:06

Help make
Opera Mini better

To provide a personalized experience, we would like to collect data for the following purposes

- Personalized news recommendations
- Ad measurements, audience insights and serving personalized ads

Go to settings

Allow

You can always read more about how we use data in our Privacy Statement and adjust your choices in Settings

App Source

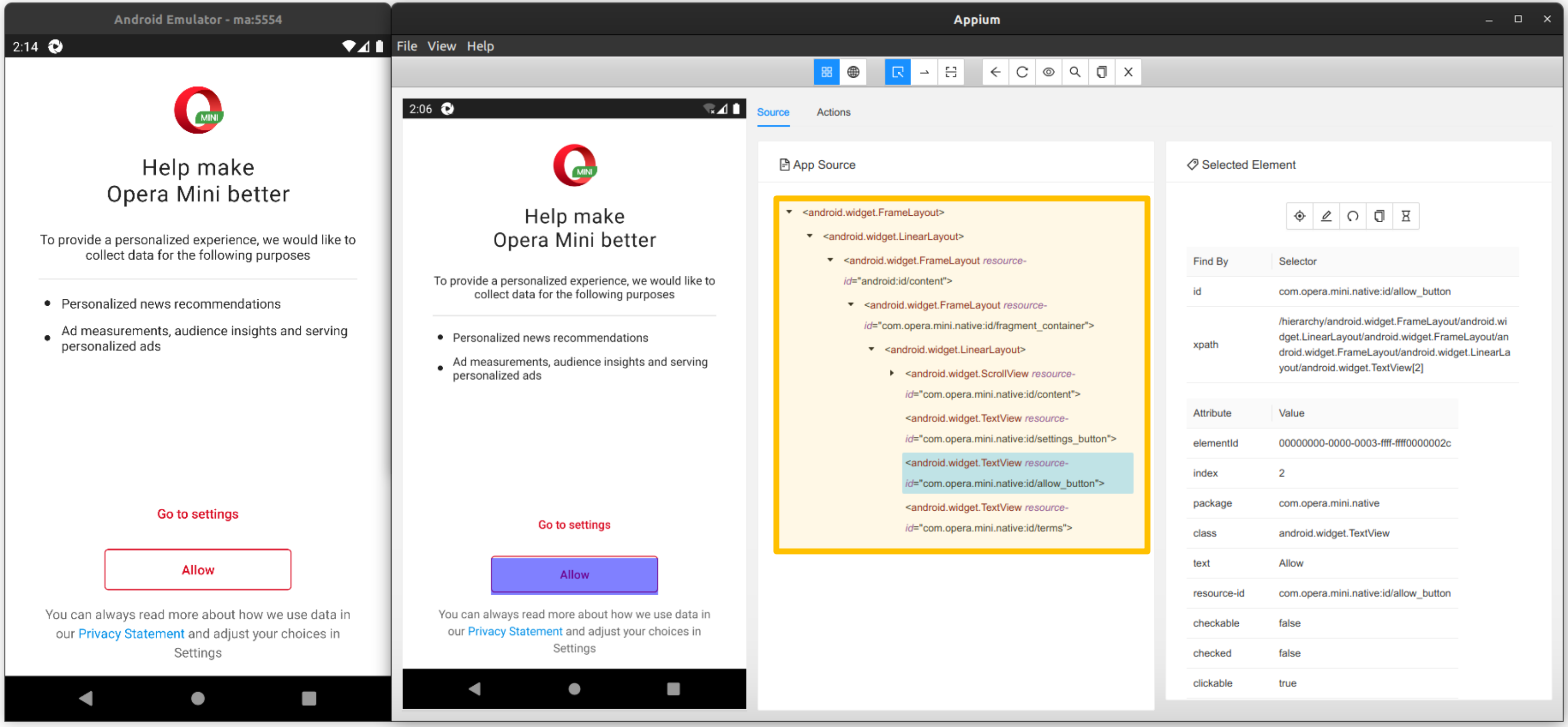
```
<android.widget.FrameLayout>
  <android.widget.LinearLayout>
    <android.widget.FrameLayout resource-id="android:id/content">
      <android.widget.FrameLayout resource-id="com.opera.mini.native:id/fragment_container">
        <android.widget.LinearLayout>
          <android.widget.ScrollView resource-id="com.opera.mini.native:id/content">
          <android.widget.TextView resource-id="com.opera.mini.native:id/settings_button">
          <android.widget.TextView resource-id="com.opera.mini.native:id/allow_button">
          <android.widget.TextView resource-id="com.opera.mini.native:id/terms">
```

Selected Element

Find By	Selector
id	com.opera.mini.native:id/allow_button
xpath	/hierarchy/android.widget.FrameLayout/android.widget.LinearLayout/android.widget.FrameLayout/android.widget.FrameLayout/android.widget.LinearLayout/android.widget.TextView[2]

Attribute	Value
elementId	00000000-0000-0003-ffff-ffff0000002c
index	2
package	com.opera.mini.native
class	android.widget.TextView
text	Allow
resource-id	com.opera.mini.native:id/allow_button
checkable	false
checked	false
clickable	true

Elements on screen



Help make
Opera Mini better

To provide a personalized experience, we would like to collect data for the following purposes

- Personalized news recommendations
- Ad measurements, audience insights and serving personalized ads

Go to settings

Allow

You can always read more about how we use data in our Privacy Statement and adjust your choices in Settings

Help make
Opera Mini better

To provide a personalized experience, we would like to collect data for the following purposes

- Personalized news recommendations
- Ad measurements, audience insights and serving personalized ads

Go to settings

Allow

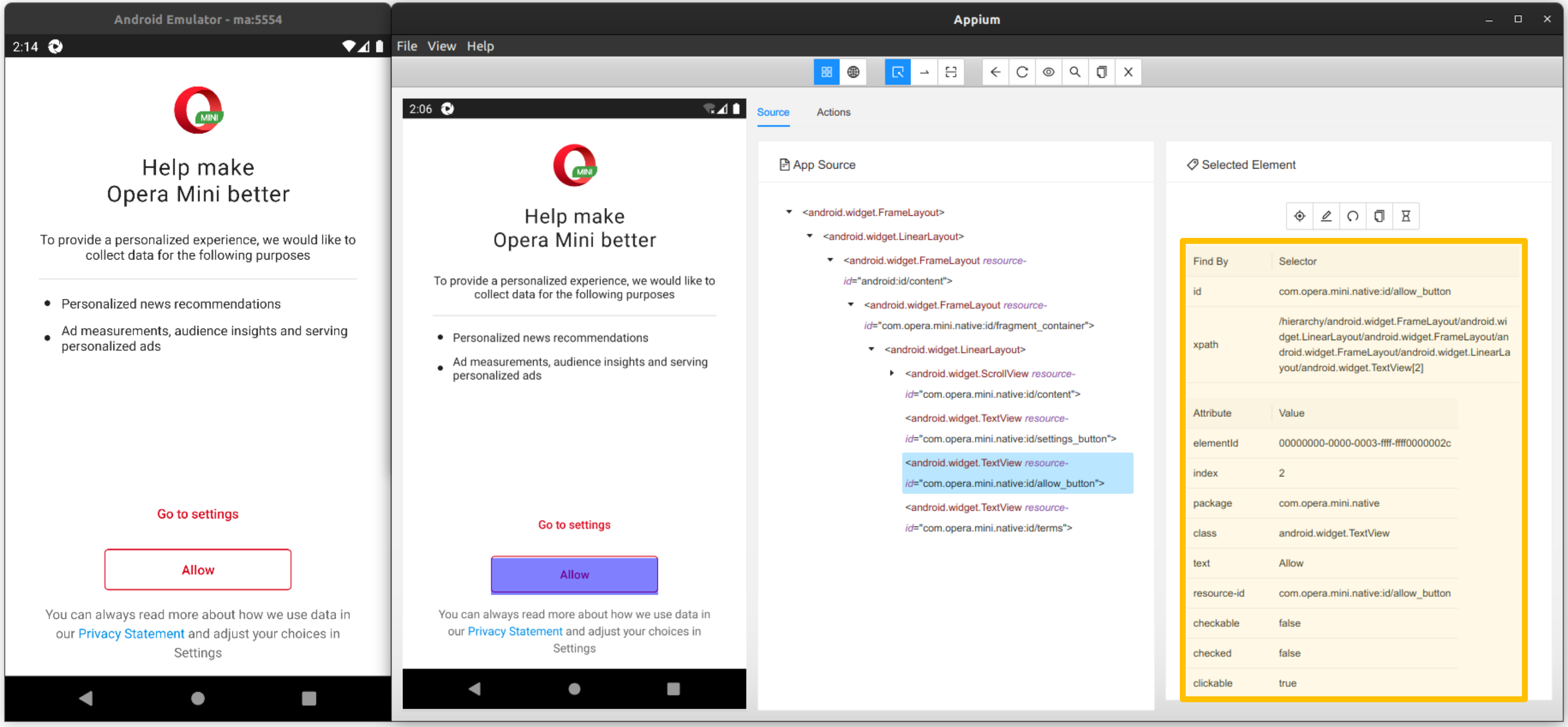
You can always read more about how we use data in our Privacy Statement and adjust your choices in Settings

```
▾ <android.widget.FrameLayout>
  ▾ <android.widget.LinearLayout>
    ▾ <android.widget.FrameLayout resource-id="android:id/content">
      ▾ <android.widget.FrameLayout resource-id="com.opera.mini.native:id/fragment_container">
        ▾ <android.widget.LinearLayout>
          ▸ <android.widget.ScrollView resource-id="com.opera.mini.native:id/content">
            <android.widget.TextView resource-id="com.opera.mini.native:id/settings_button">
            <android.widget.TextView resource-id="com.opera.mini.native:id/allow_button">
            <android.widget.TextView resource-id="com.opera.mini.native:id/terms">
```

Find By	Selector
id	com.opera.mini.native:id/allow_button
xpath	/hierarchy/android.widget.FrameLayout/android.widget.LinearLayout/android.widget.FrameLayout/android.widget.FrameLayout/android.widget.LinearLayout/android.widget.TextView[2]

Attribute	Value
elementId	00000000-0000-0003-ffff-ffff0000002c
index	2
package	com.opera.mini.native
class	android.widget.TextView
text	Allow
resource-id	com.opera.mini.native:id/allow_button
checkable	false
checked	false
clickable	true

Elements on screen



Android Emulator - ma:5554

2:14

Help make
Opera Mini better

To provide a personalized experience, we would like to collect data for the following purposes

- Personalized news recommendations
- Ad measurements, audience insights and serving personalized ads

Go to settings

Allow

You can always read more about how we use data in our Privacy Statement and adjust your choices in Settings

Appium

File View Help

2:06

Help make
Opera Mini better

To provide a personalized experience, we would like to collect data for the following purposes

- Personalized news recommendations
- Ad measurements, audience insights and serving personalized ads

Go to settings

Allow

You can always read more about how we use data in our Privacy Statement and adjust your choices in Settings

Source Actions

App Source

```
▾ <android.widget.FrameLayout>
  ▾ <android.widget.LinearLayout>
    ▾ <android.widget.FrameLayout resource-id="android:id/content">
      ▾ <android.widget.FrameLayout resource-id="com.opera.mini.native:id/fragment_container">
        ▾ <android.widget.LinearLayout>
          ▸ <android.widget.ScrollView resource-id="com.opera.mini.native:id/content">
            <android.widget.TextView resource-id="com.opera.mini.native:id/settings_button">
            <android.widget.TextView resource-id="com.opera.mini.native:id/allow_button">
            <android.widget.TextView resource-id="com.opera.mini.native:id/terms">
```

Selected Element

Find By	Selector
id	com.opera.mini.native:id/allow_button
xpath	/hierarchy/android.widget.FrameLayout/android.widget.LinearLayout/android.widget.FrameLayout/android.widget.FrameLayout/android.widget.LinearLayout/android.widget.TextView[2]

Attribute	Value
elementId	00000000-0000-0003-ffff-ffff0000002c
index	2
package	com.opera.mini.native
class	android.widget.TextView
text	Allow
resource-id	com.opera.mini.native:id/allow_button
checkable	false
checked	false
clickable	true

Device instrumentation framework

- Basic instrumentation tooling from prior work extended for this thesis.

- Uses emulator for Android, physical iPhone for iOS.
- Manages apps, sets permissions, resets device, and starts apps.
- Traffic collection using mitmproxy and objection/SSL Kill Switch 2.
- Analysis of and interaction with elements on screen using Appium.

Device instrumentation framework

- Basic instrumentation tooling from prior work extended for this thesis.

- Uses emulator for Android, physical iPhone for iOS.
- Manages apps, sets permissions, resets device, and starts apps.
- Traffic collection using mitmproxy and objection/SSL Kill Switch 2.
- Analysis of and interaction with elements on screen using Appium.
- Extraction of app preferences using Frida.

Now, we only need apps

- Pretty easy on Android:
    - We scrape the top charts from the Play Store website.
    - We use PlaystoreDownloader to download them.

Now, we only need apps

- Pretty easy on Android:
  - We scrape the top charts from the Play Store website.
  - We use PlaystoreDownloader to download them.
  - From the top 100 apps per category, we successfully downloaded 3,313 apps.

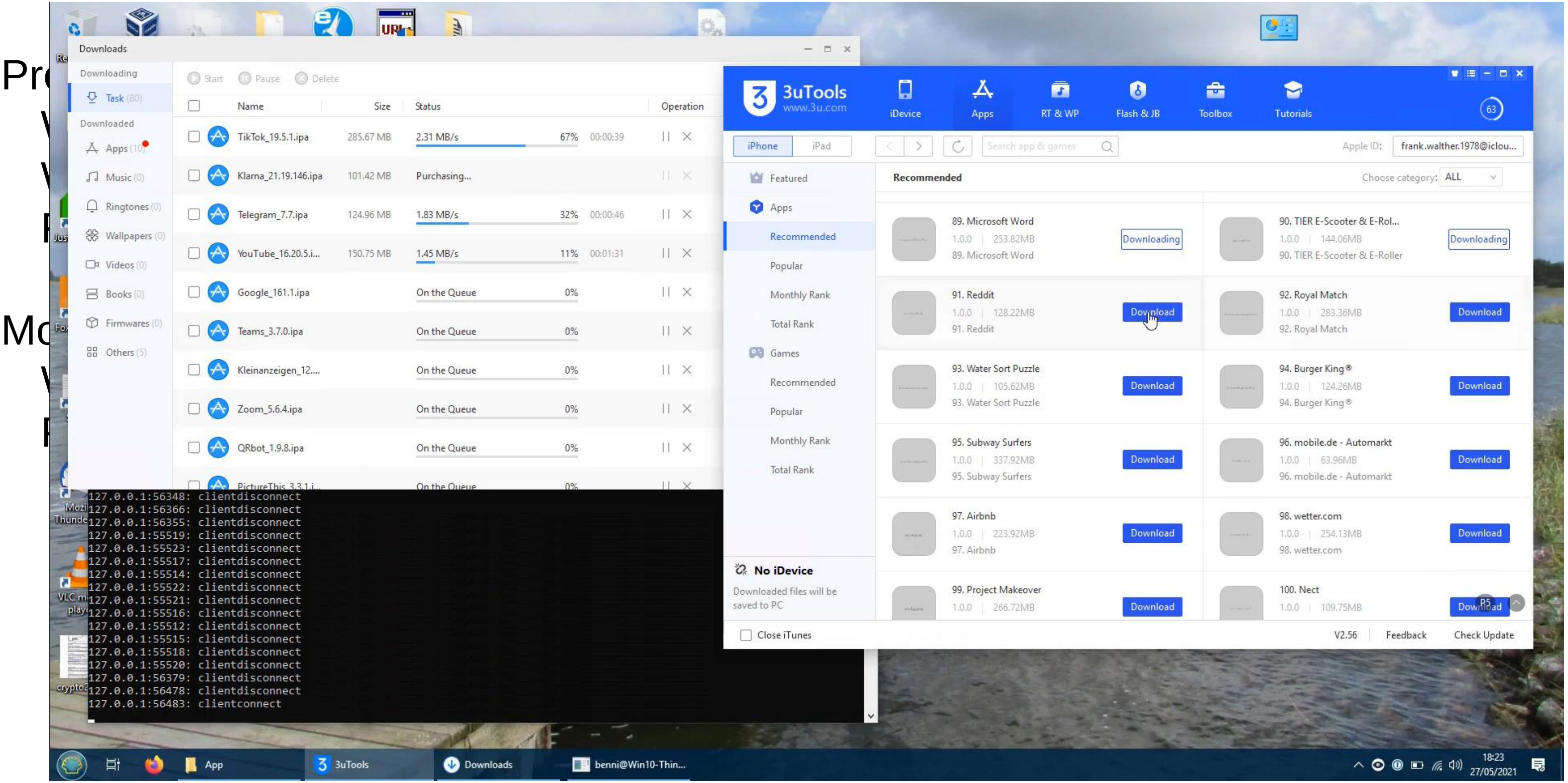
Now, we only need apps

- Pretty easy on Android:
  - We scrape the top charts from the Play Store website.
  - We use PlaystoreDownloader to download them.
  - From the top 100 apps per category, we successfully downloaded 3,313 apps.

- More involved on iOS:
  - We discovered an old internal iTunes API for the top charts.
  - Previous download approaches were manual and unreliable.

Now, we only need apps

- Pr
  - V
  - V
  - F
- Mc
  - V
  - F



☐	Name	Size	Status			Operation
☐	TikTok_19.5.1.ipa	285.67 MB	2.31 MB/s	67%	00:00:39	‖ ✕
☐	Klarna_21.19.146.ipa	101.42 MB	Purchasing...			‖ ✕
☐	Telegram_7.7.ipa	124.96 MB	1.83 MB/s	32%	00:00:46	‖ ✕
☐	YouTube_16.20.5.i...	150.75 MB	1.45 MB/s	11%	00:01:31	‖ ✕
☐	Google_161.1.ipa		On the Queue	0%		‖ ✕
☐	Teams_3.7.0.ipa		On the Queue	0%		‖ ✕
☐	Kleinanzeigen_12....		On the Queue	0%		‖ ✕
☐	Zoom_5.6.4.ipa		On the Queue	0%		‖ ✕
☐	QRbot_1.9.8.ipa		On the Queue	0%		‖ ✕
☐	PictureThis_3.3.1.i...		On the Queue	0%		‖ ✕

```
127.0.0.1:56348: clientdisconnect
127.0.0.1:56366: clientdisconnect
127.0.0.1:56355: clientdisconnect
127.0.0.1:55519: clientdisconnect
127.0.0.1:55523: clientdisconnect
127.0.0.1:55517: clientdisconnect
127.0.0.1:55514: clientdisconnect
127.0.0.1:55522: clientdisconnect
127.0.0.1:55521: clientdisconnect
127.0.0.1:55516: clientdisconnect
127.0.0.1:55512: clientdisconnect
127.0.0.1:55515: clientdisconnect
127.0.0.1:55518: clientdisconnect
127.0.0.1:55520: clientdisconnect
127.0.0.1:56379: clientdisconnect
127.0.0.1:56478: clientdisconnect
127.0.0.1:56483: clientconnect
```

Apple ID: frank.walther.1978@iclou...

Recommended

Choose category: ALL

App	Version	Size	Subtitle	
89. Microsoft Word	1.0.0	253.82MB	89. Microsoft Word	Downloading
90. TIER E-Scooter & E-Rol...	1.0.0	144.06MB	90. TIER E-Scooter & E-Roller	Downloading
91. Reddit	1.0.0	128.22MB	91. Reddit	Download
92. Royal Match	1.0.0	283.36MB	92. Royal Match	Download
93. Water Sort Puzzle	1.0.0	105.62MB	93. Water Sort Puzzle	Download
94. Burger King®	1.0.0	124.26MB	94. Burger King®	Download
95. Subway Surfers	1.0.0	337.92MB	95. Subway Surfers	Download
96. mobile.de - Automarkt	1.0.0	63.96MB	96. mobile.de - Automarkt	Download
97. Airbnb	1.0.0	223.92MB	97. Airbnb	Download
98. wetter.com	1.0.0	254.13MB	98. wetter.com	Download
99. Project Makeover	1.0.0	266.72MB		Download
100. Nect	1.0.0	109.75MB		Download

No iDevice

Downloaded files will be saved to PC

☐ Close iTunes

V2.56 Feedback Check Update

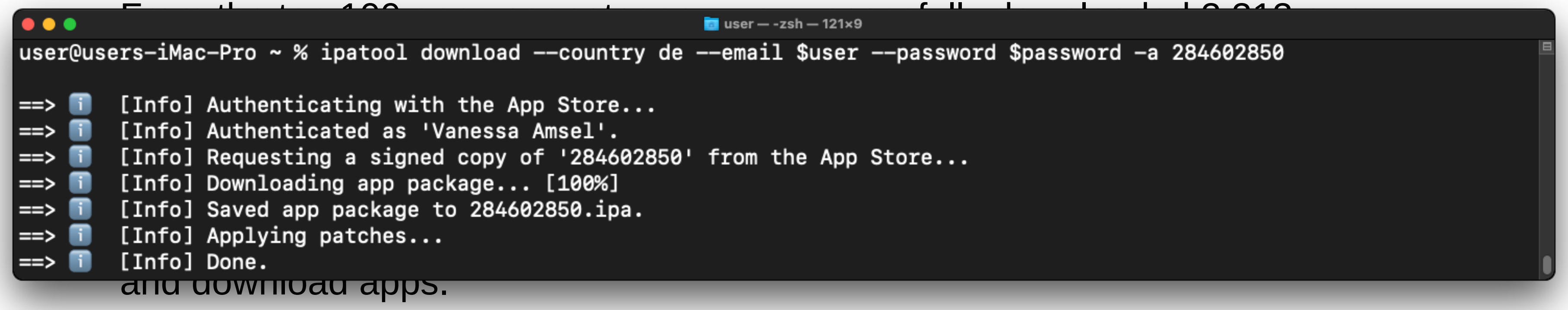
Now, we only need apps

- Pretty easy on Android:
  - We scrape the top charts from the Play Store website.
  - We use PlaystoreDownloader to download them.
  - From the top 100 apps per category, we successfully downloaded 3,313 apps.

- More involved on iOS:
  - We discovered an old internal iTunes API for the top charts.
  - Previous download approaches were manual and unreliable.
  - After a lot of arguing with Apple's servers, we found a way to programmatically "buy" and download apps.
    - Extended IPATool with support for that.

Now, we only need apps

- Pretty easy on Android:
  - We scrape the top charts from the Play Store website.
  - We use PlaystoreDownloader to download them.



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

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

and download apps.

- Extended IPATool with support for that.

Now, we only need apps

- Pretty easy on Android:
  - We scrape the top charts from the Play Store website.
  - We use PlaystoreDownloader to download them.
  - From the top 100 apps per category, we successfully downloaded 3,313 apps.

- More involved on iOS:
  - We discovered an old internal iTunes API for the top charts.
  - Previous download approaches were manual and unreliable.
  - After a lot of arguing with Apple’s servers, we found a way to programmatically “buy” and download apps.
    - Extended IPATool with support for that.
  - From the top 100 apps per category, we successfully downloaded 2,481 apps.

Image: Adeolu Eletu (Unsplash license)

Results

Prevalence of consent elements

- We successfully analysed 4,388 apps: 2,068 (62.42 %) on Android, 2,320 (93.51 %) on iOS.

Prevalence of consent elements

- We successfully analysed 4,388 apps: 2,068 (62.42 %) on Android, 2,320 (93.51 %) on iOS.
- High number of failures on Android mainly due to certificate pinning bypass.

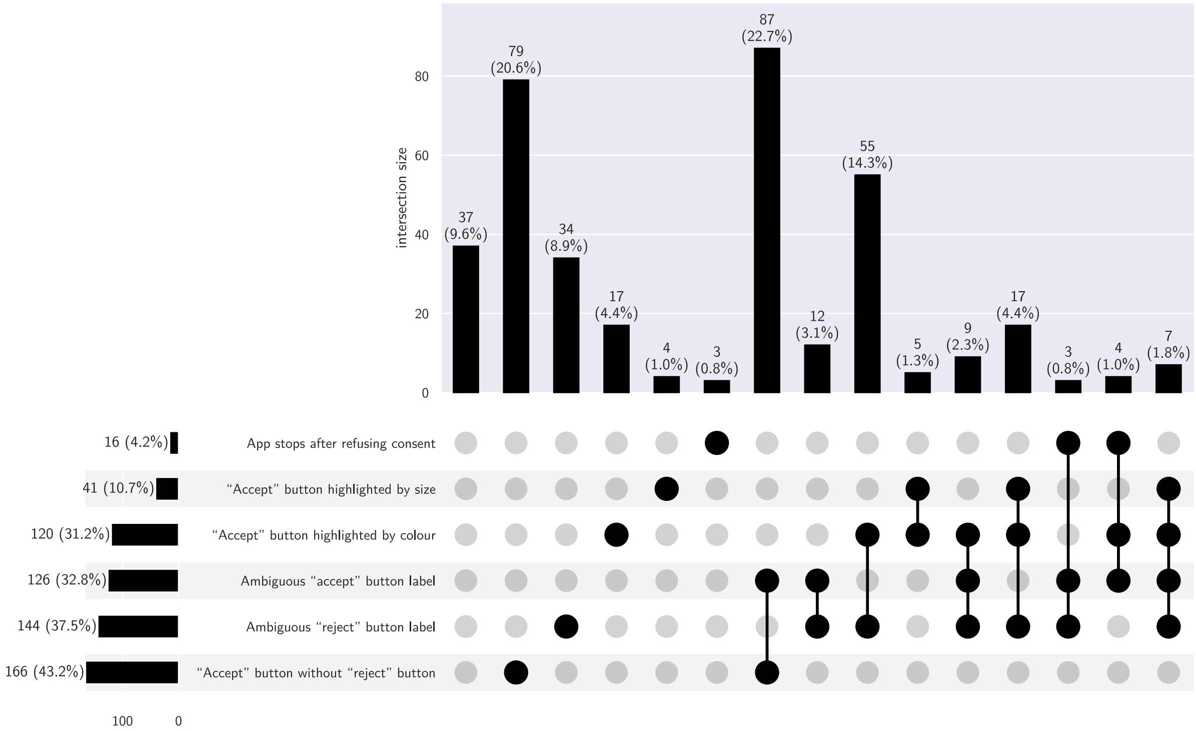
Prevalence of consent elements

- We successfully analysed 4,388 apps: 2,068 (62.42 %) on Android, 2,320 (93.51 %) on iOS.
- High number of failures on Android mainly due to certificate pinning bypass.

Classification	Detections on Android	Detections on iOS	Detections in total
dialog	149 (7.21 %)	235 (10.13 %)	384 (8.75 %)
notice	108 (5.22 %)	87 (3.75 %)	195 (4.44 %)
link	103 (4.98 %)	103 (4.44 %)	206 (4.69 %)
neither	1,708 (82.59 %)	1,895 (81.68 %)	3,603 (82.11 %)

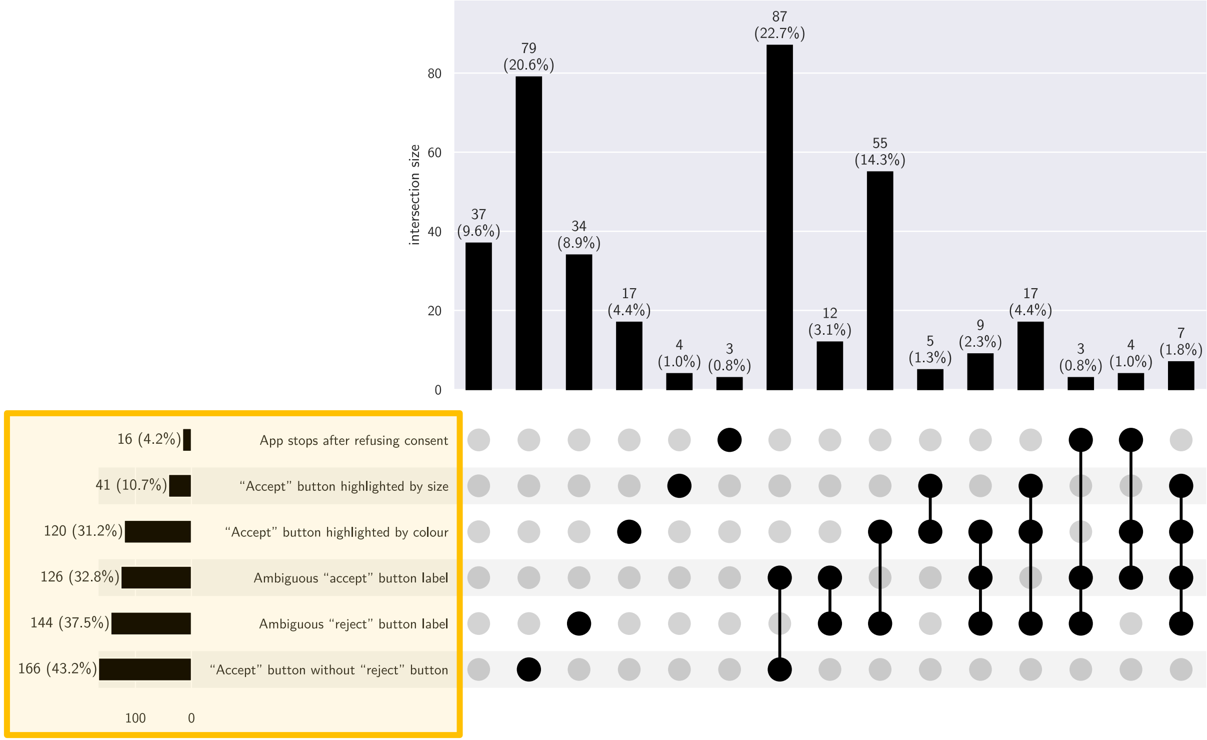
- In total: 785 apps (17.89 %) had one of the consent elements we detect.

Dark patterns in consent dialogs



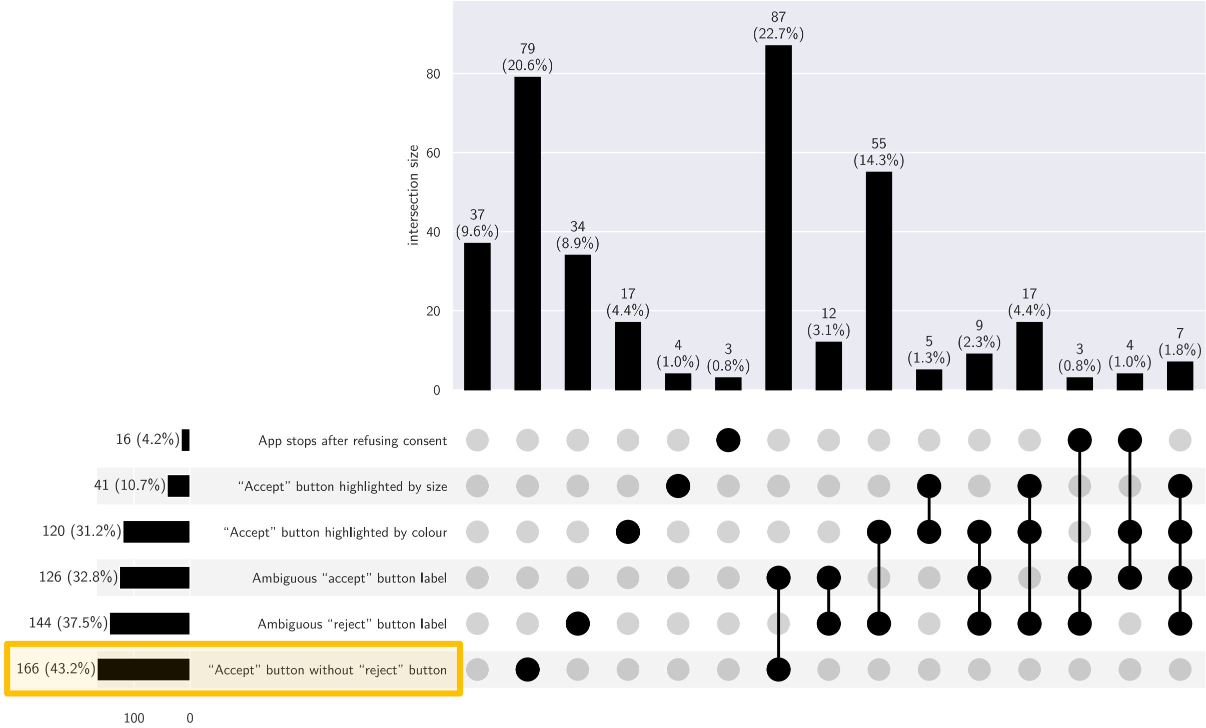
UpSet plot of the different combinations of dark patterns we have detected in consent dialogs. **Subsets with less than three elements are omitted.** Also note that not all combinations are possible.

Dark patterns in consent dialogs



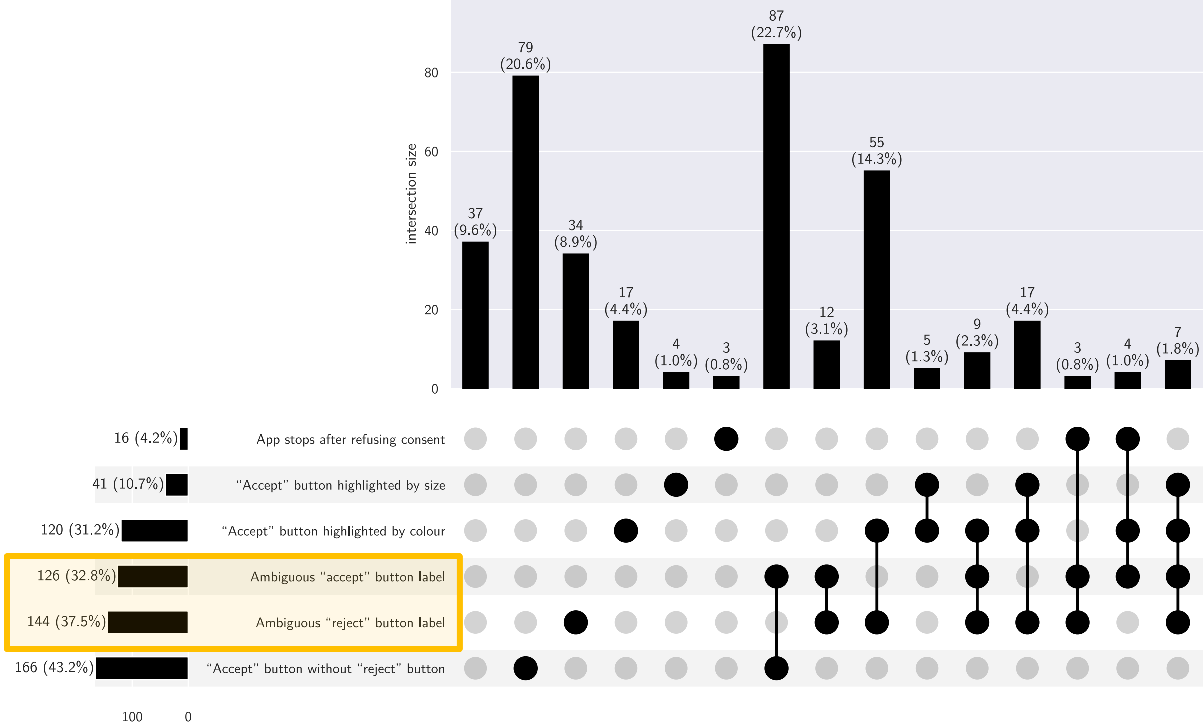
UpSet plot of the different combinations of dark patterns we have detected in consent dialogs. **Subsets with less than three elements are omitted.** Also note that not all combinations are possible.

Dark patterns in consent dialogs



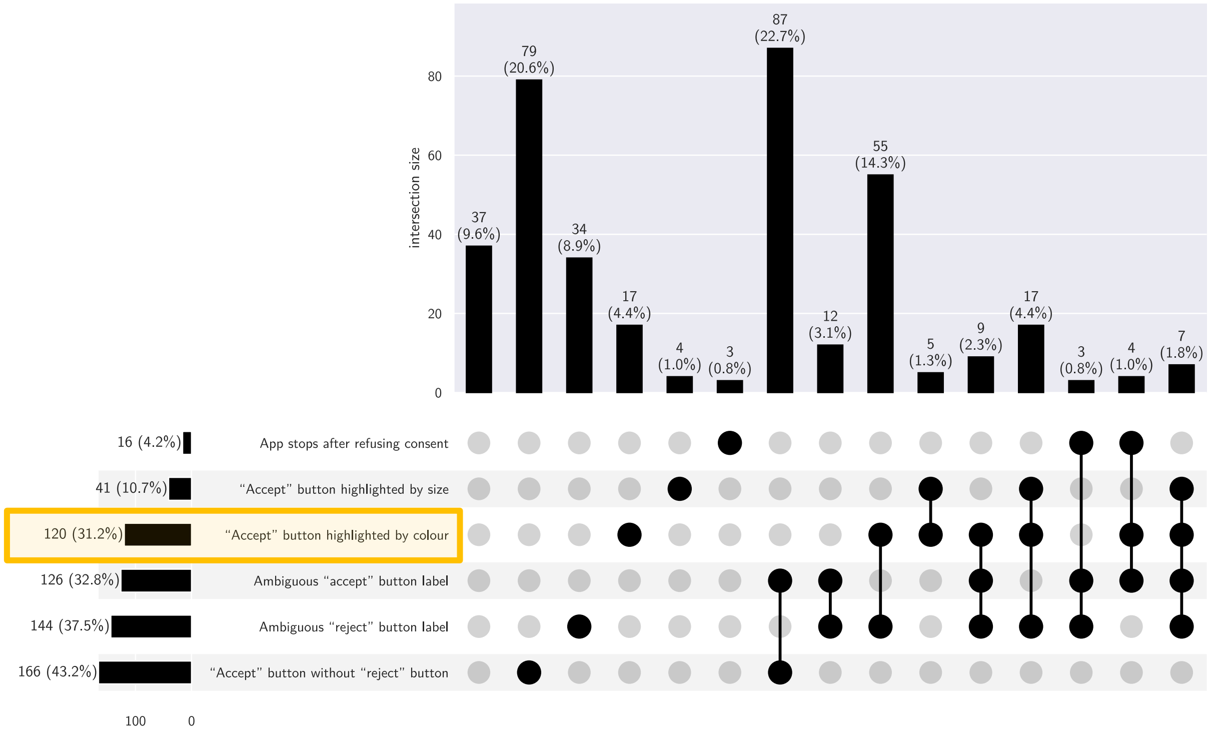
UpSet plot of the different combinations of dark patterns we have detected in consent dialogs. **Subsets with less than three elements are omitted.** Also note that not all combinations are possible.

Dark patterns in consent dialogs



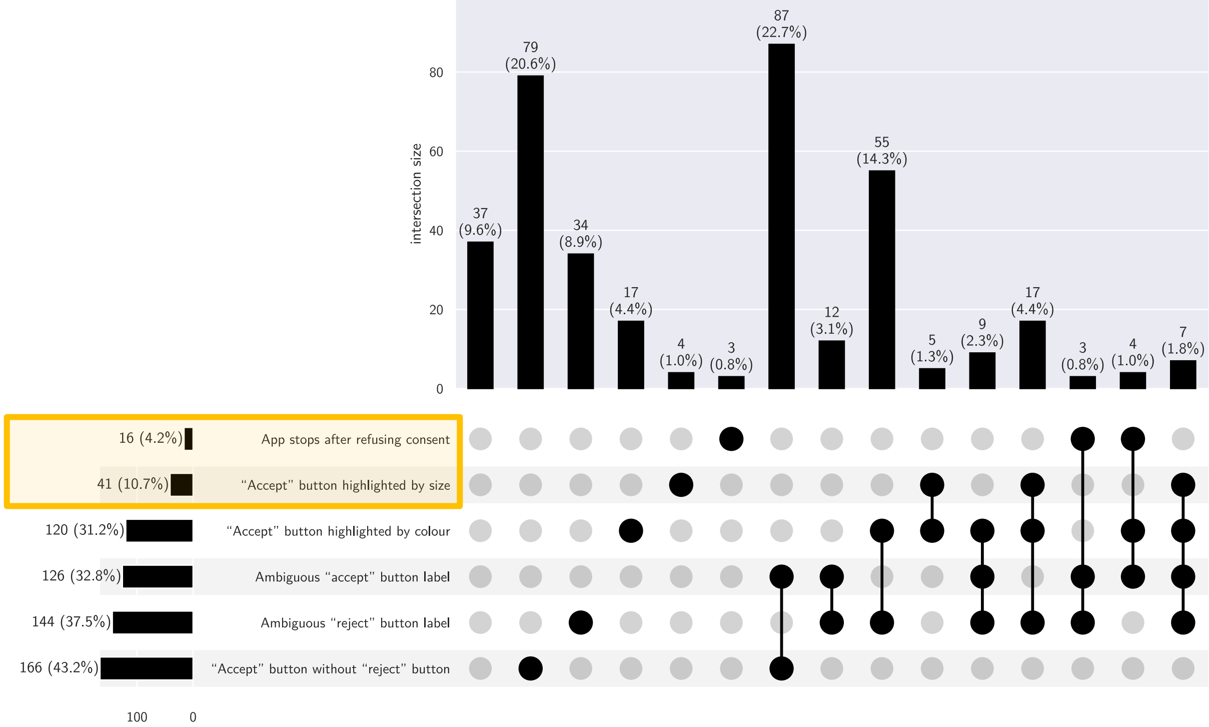
UpSet plot of the different combinations of dark patterns we have detected in consent dialogs. **Subsets with less than three elements are omitted.** Also note that not all combinations are possible.

Dark patterns in consent dialogs



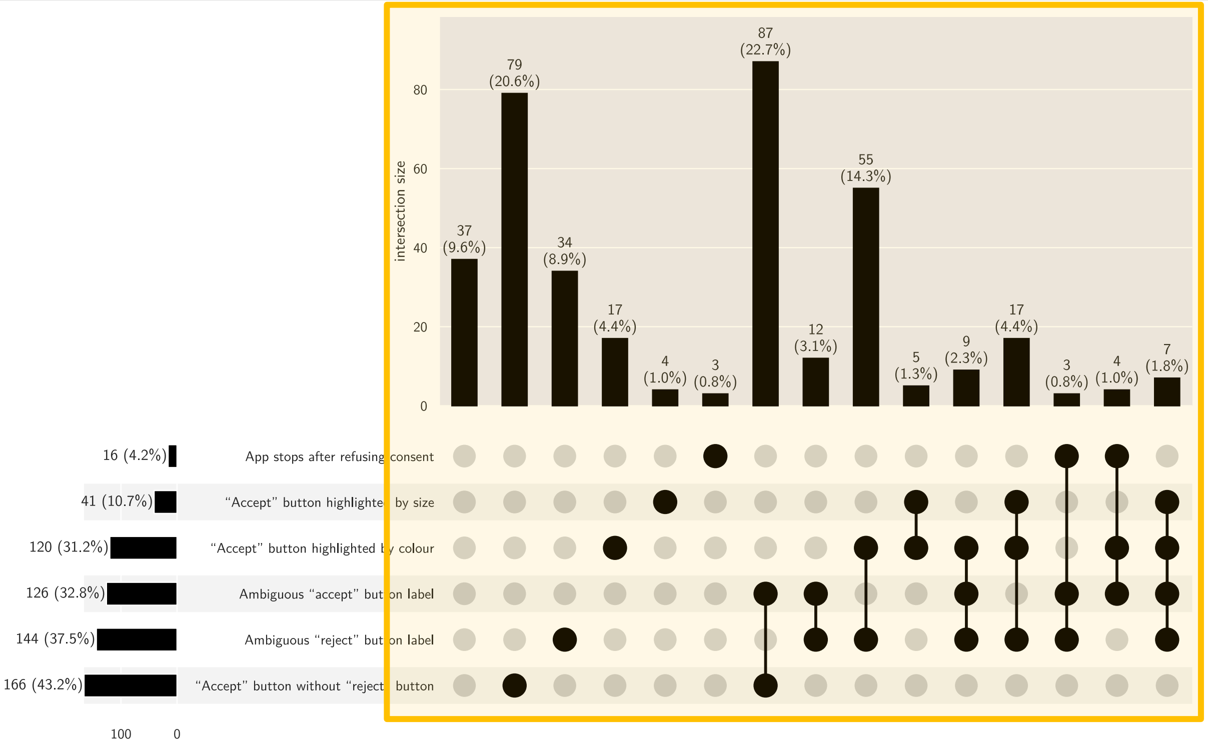
UpSet plot of the different combinations of dark patterns we have detected in consent dialogs. **Subsets with less than three elements are omitted.** Also note that not all combinations are possible.

Dark patterns in consent dialogs



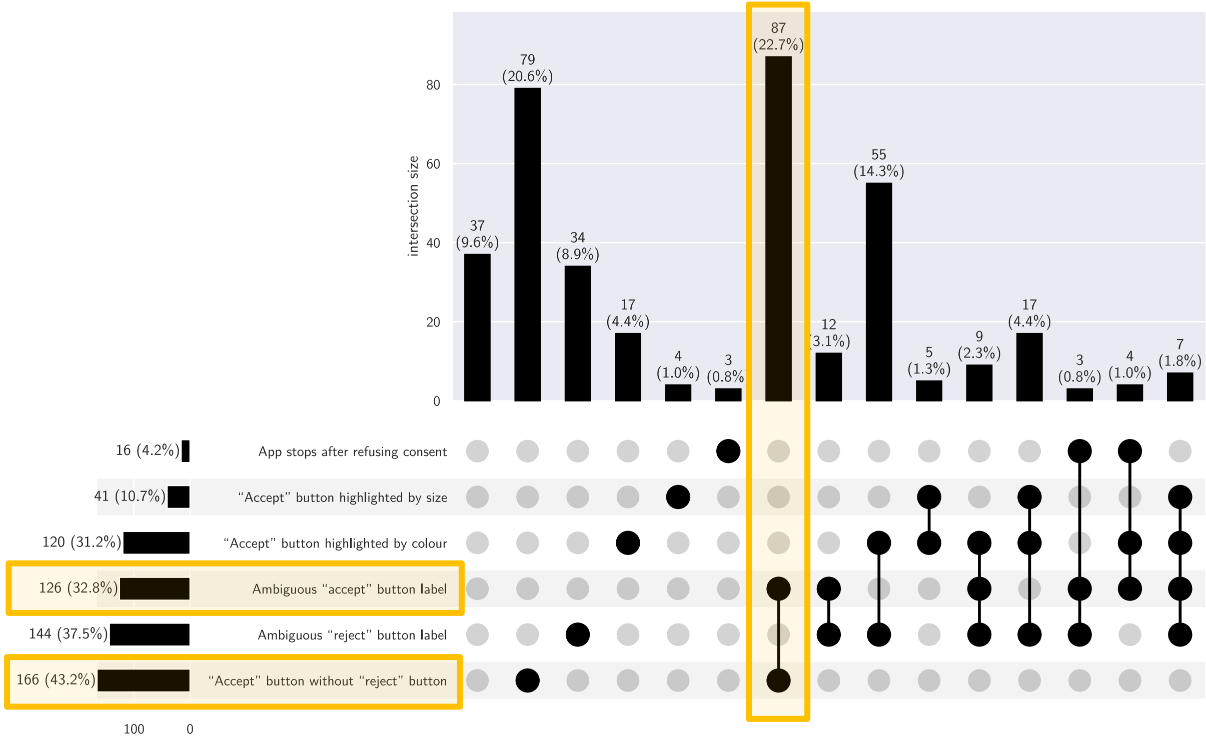
UpSet plot of the different combinations of dark patterns we have detected in consent dialogs. **Subsets with less than three elements are omitted.** Also note that not all combinations are possible.

Dark patterns in consent dialogs



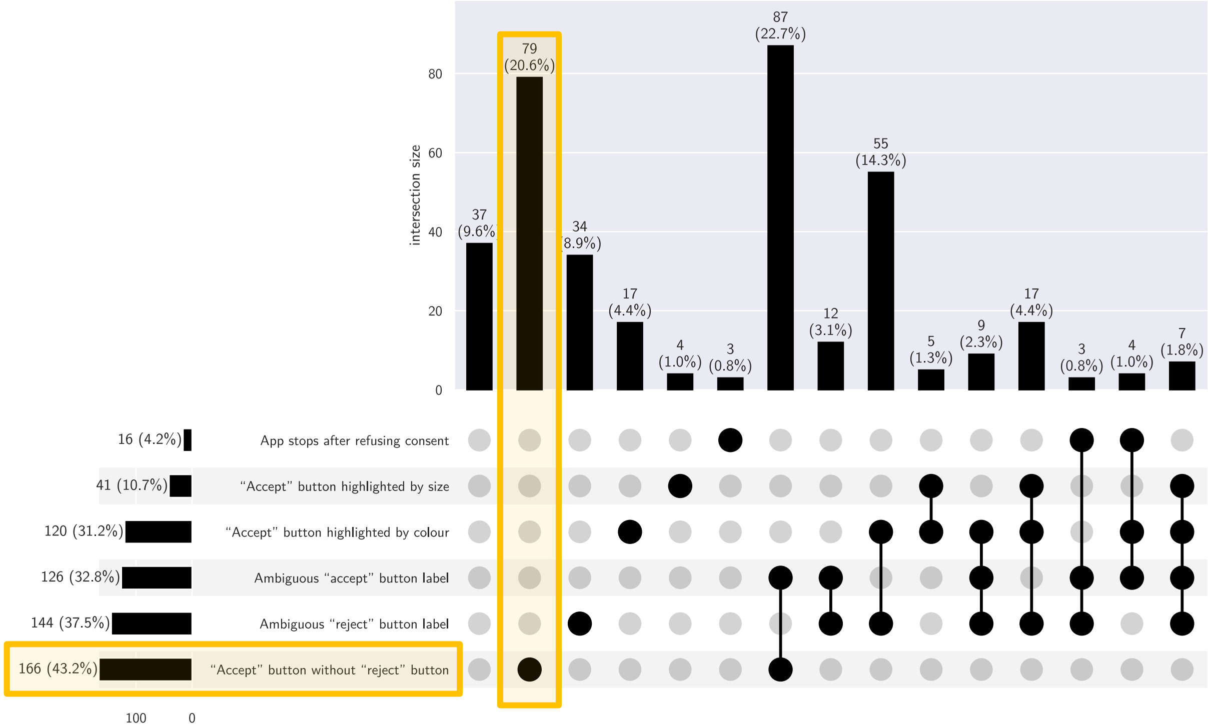
UpSet plot of the different combinations of dark patterns we have detected in consent dialogs. **Subsets with less than three elements are omitted.** Also note that not all combinations are possible.

Dark patterns in consent dialogs



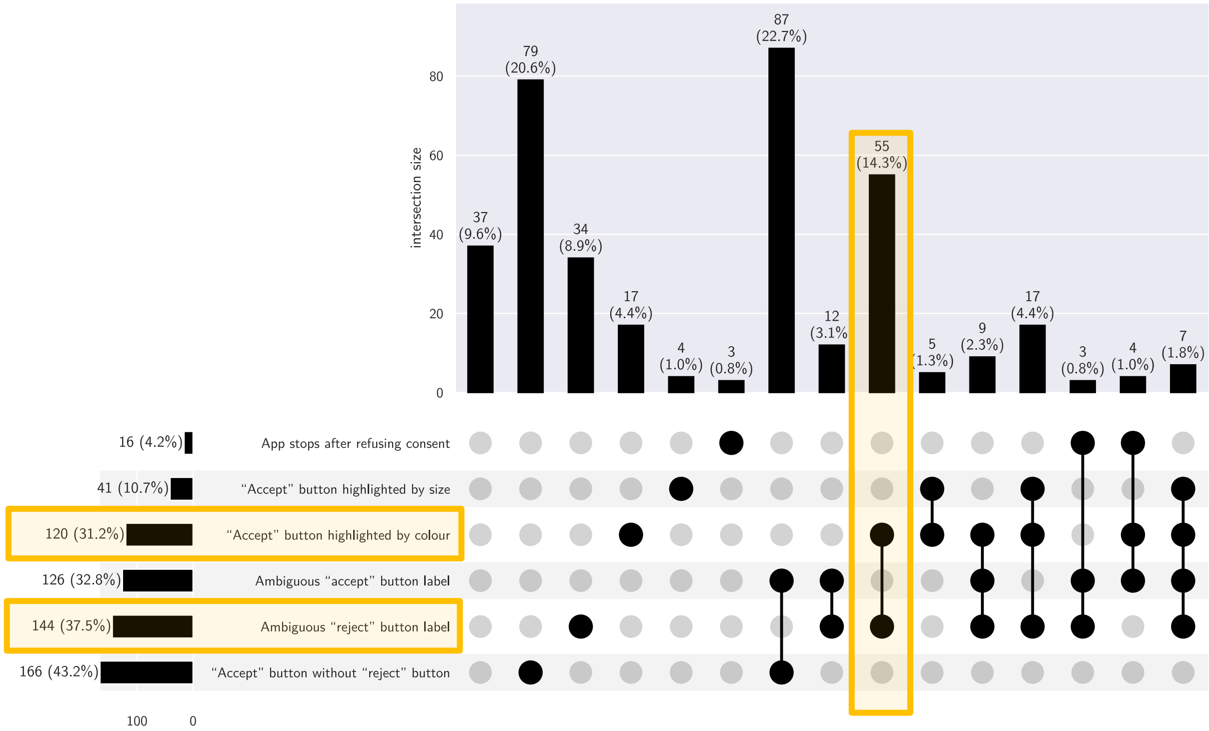
UpSet plot of the different combinations of dark patterns we have detected in consent dialogs. **Subsets with less than three elements are omitted.** Also note that not all combinations are possible.

Dark patterns in consent dialogs



UpSet plot of the different combinations of dark patterns we have detected in consent dialogs. **Subsets with less than three elements are omitted.** Also note that not all combinations are possible.

Dark patterns in consent dialogs



UpSet plot of the different combinations of dark patterns we have detected in consent dialogs. **Subsets with less than three elements are omitted.** Also note that not all combinations are possible.

Violations in consent dialogs

- In total: at least one dark pattern in 347 of the 384 apps with a dialog (90.36 %).

  The share of dark patterns in dialogs is slightly higher on Android (91.28 %) compared to iOS (89.79 %).

Violations in consent dialogs

- In total: at least one dark pattern in 347 of the 384 apps with a dialog (90.36 %).

  The share of dark patterns in dialogs is slightly higher on Android (91.28 %) compared to iOS (89.79 %).

- **These are not violations on their own!** Dark patterns only result in the obtained consent being invalid. The actual violation is tracking based on that supposed consent.

Violations in consent dialogs

- In total: at least one dark pattern in 347 of the 384 apps with a dialog (90.36 %).

  The share of dark patterns in dialogs is slightly higher on Android (91.28 %) compared to iOS (89.79 %).

- **These are not violations on their own!** Dark patterns only result in the obtained consent being invalid. The actual violation is tracking based on that supposed consent.
- 297 of the 347 apps with a detected dark pattern in their dialog (85.59 %) transmitted pseudonymous data in any of our runs.

  => 77.34 % of the detected dialogs failed to acquire valid consent for the tracking they perform.

Validation of consent dialog results

- Manual validation of consent element detection using screenshots for 250 apps:

Detected	Actual	Count
neither	link	1
neither	notice	2
neither	dialog	15
link	notice	2
link	dialog	5

- Notably: not a single false positive. False negatives expected due to approach and don’t impact validity of detected violations (as these are only for dialogs).

Validation of consent dialog results

- Manual validation of consent element detection using screenshots for 250 apps:

Detected	Actual	Count
neither	link	1
neither	notice	2
neither	dialog	15
link	notice	2
link	dialog	5

- Notably: not a single false positive. False negatives expected due to approach and don’t impact validity of detected violations (as these are only for dialogs).

- Manual validation of detected dark patterns for 25 apps: no false positives either, one “accept” button larger than the “reject” button was not detected.

Data sent to trackers

- To analyse transmitted data: as request data is often obfuscated and ridiculously nested, we wrote 26 adapters for common tracking endpoints.

Data sent to trackers

- To analyse transmitted data: as request data is often obfuscated and ridiculously nested, we wrote 26 adapters for common tracking endpoints.
  - These already cover more than 10% of all traffic!

Data sent to trackers

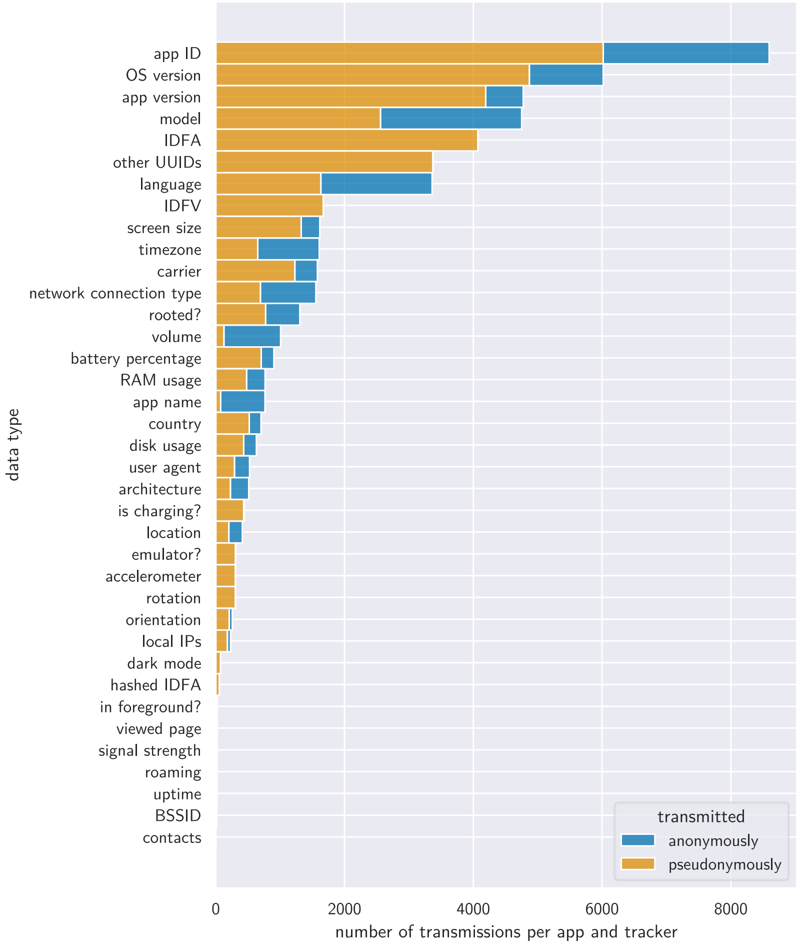
- To analyse transmitted data: as request data is often obfuscated and ridiculously nested, we wrote 26 adapters for common tracking endpoints.
  - These already cover more than 10% of all traffic!
  - For everything else: indicator matching of honey data.

Data sent to trackers

- To analyse transmitted data: as request data is often obfuscated and ridiculously nested, we wrote 26 adapters for common tracking endpoints.
  - These already cover more than 10% of all traffic!
  - For everything else: indicator matching of honey data.

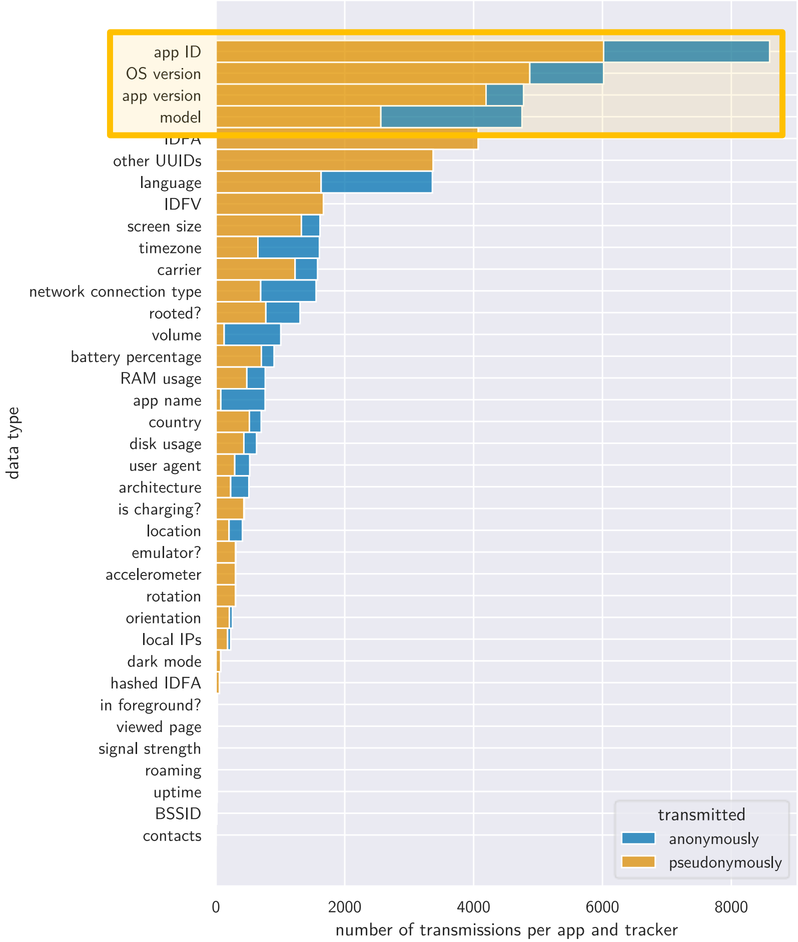
- 72.95 % of apps transmitted unique device ID without interaction.
- Also, 33.32 % of requests before interaction were identified as going to trackers according to Exodus, with 78.08 % of apps making at least one request to a tracker.

Data types



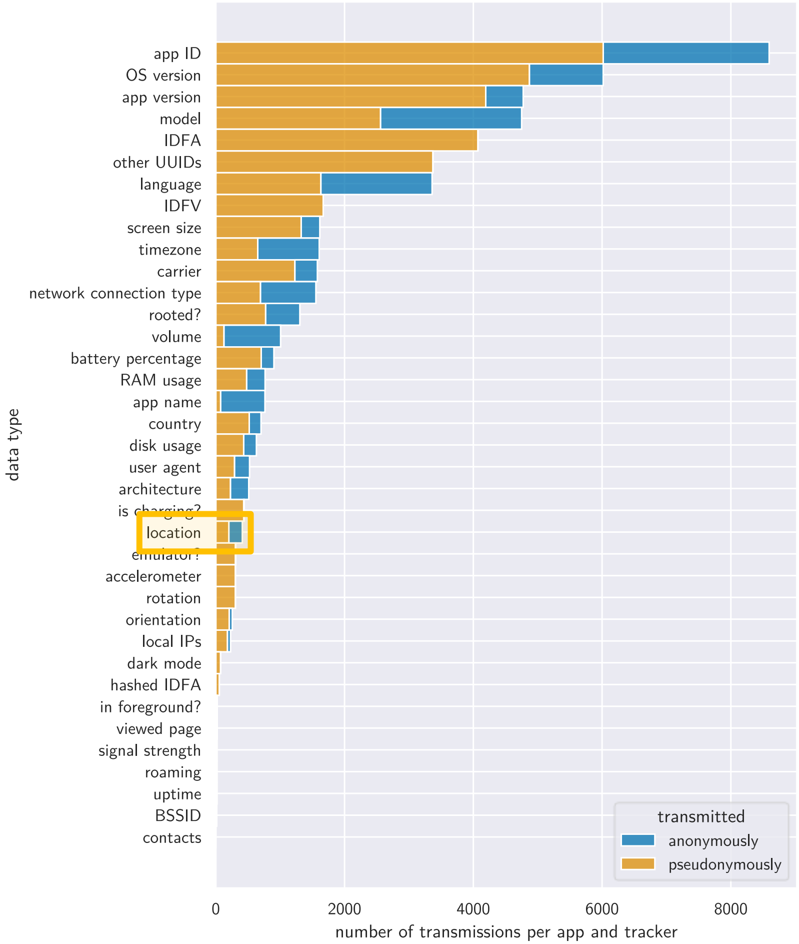
Number of times the observed data types were transmitted per app and tracker **before interaction**. Note that we are also using the term “IDFA” for the Android advertising ID here.

Data types



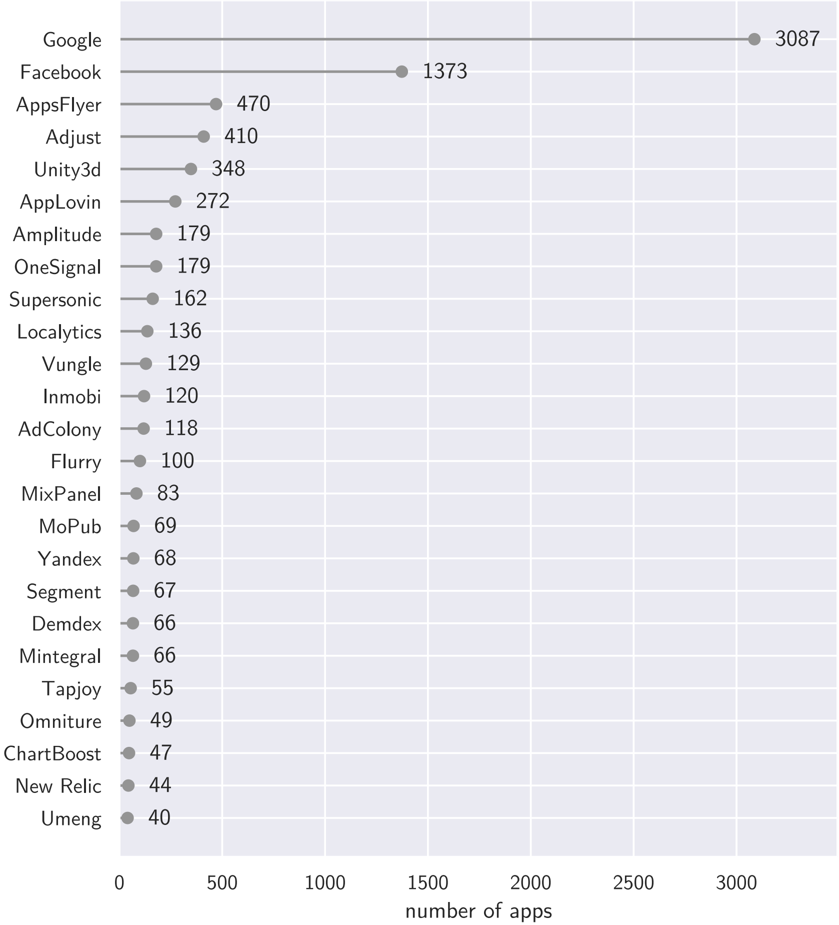
Number of times the observed data types were transmitted per app and tracker **before interaction**. Note that we are also using the term “IDFA” for the Android advertising ID here.

Data types



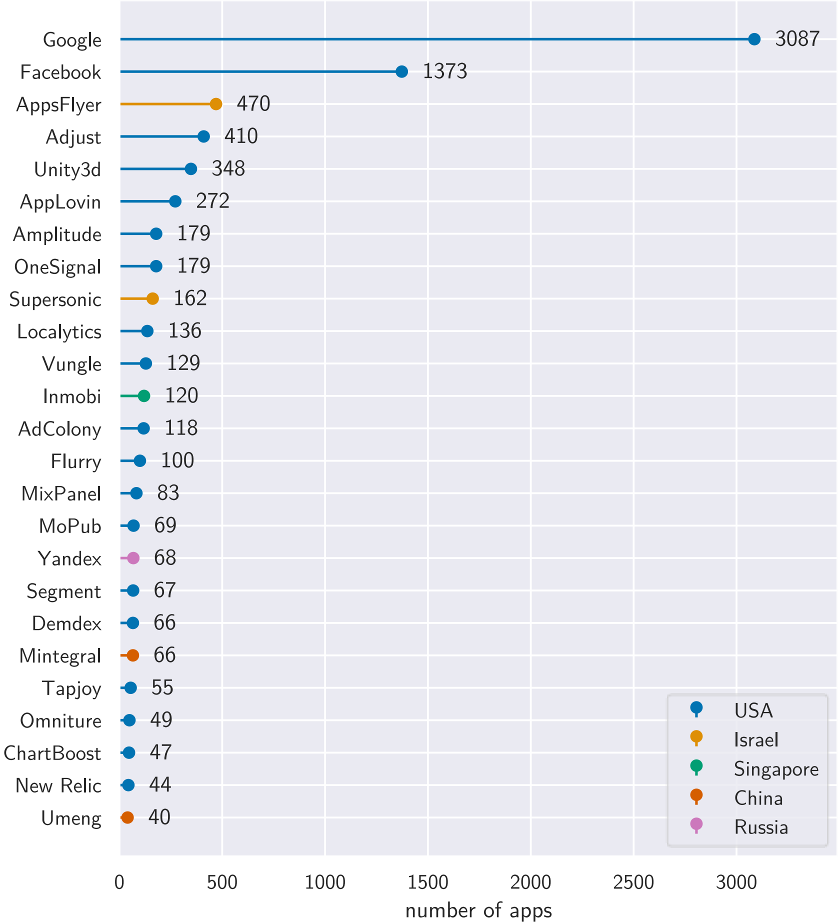
Number of times the observed data types were transmitted per app and tracker **before interaction**. Note that we are also using the term “IDFA” for the Android advertising ID here.

Trackers

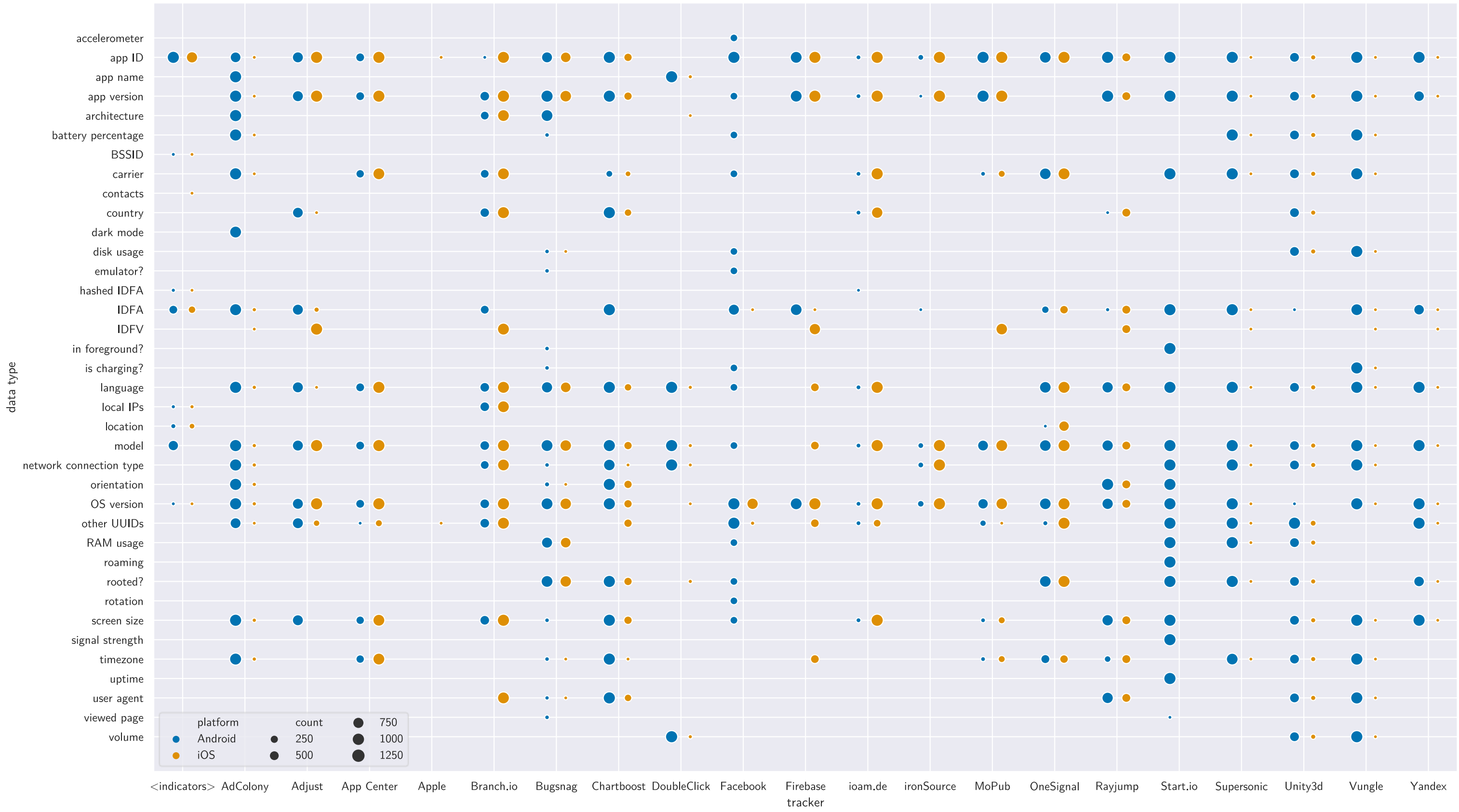


Number of apps that sent requests to the 25 most common trackers in our dataset according to Exodus **without user interaction**.

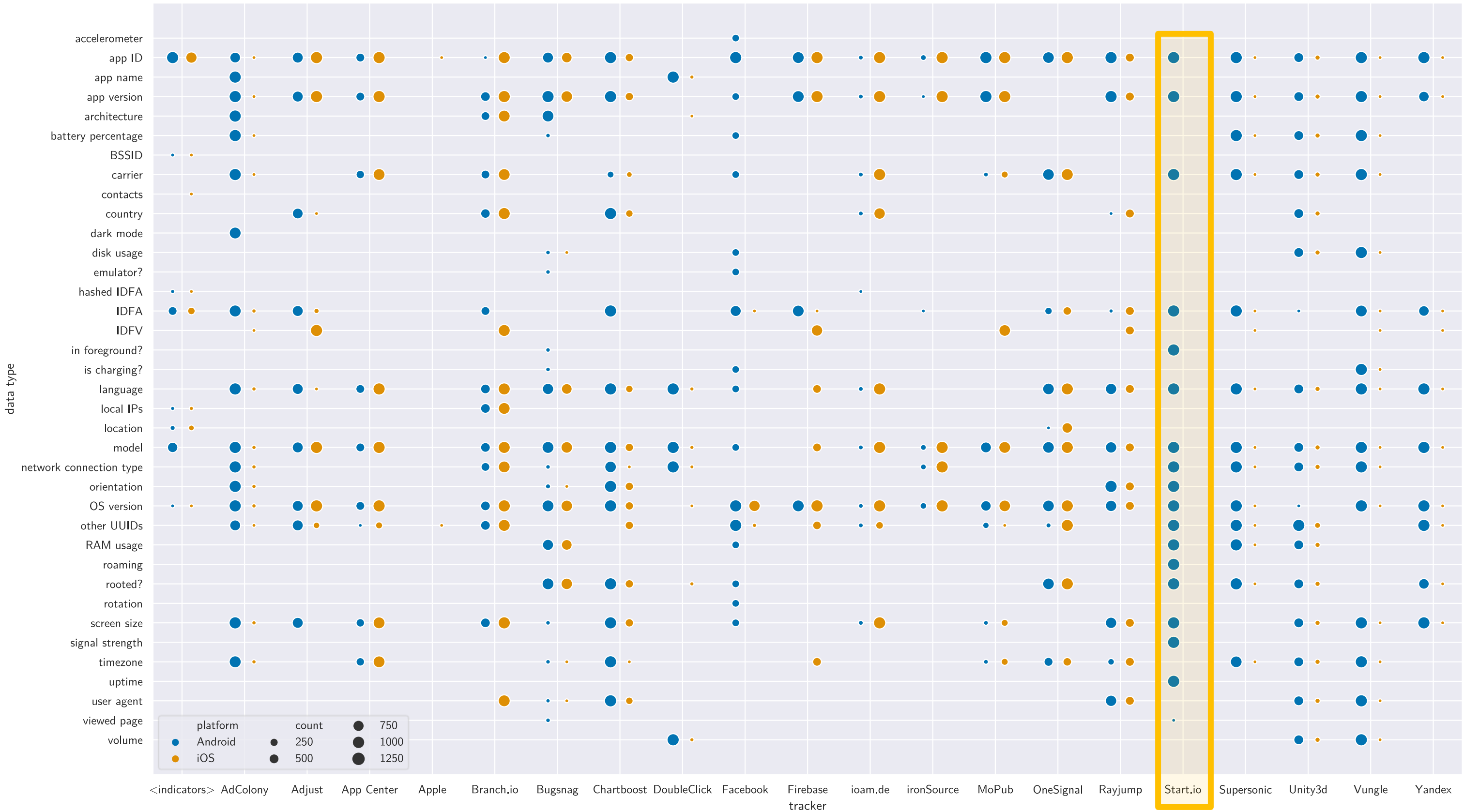
Trackers



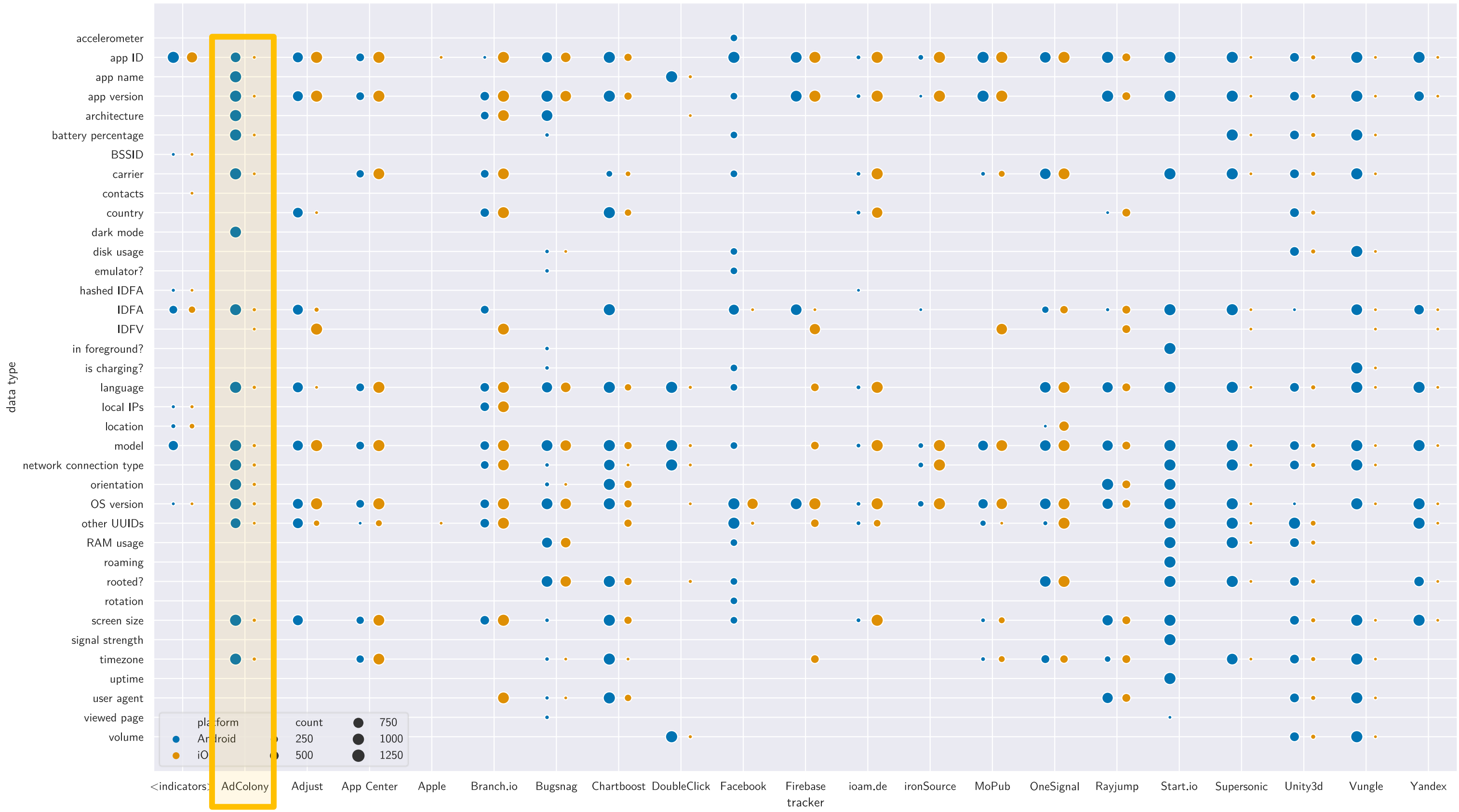
Number of apps that sent requests to the 25 most common trackers in our dataset according to Exodus **without user interaction**.



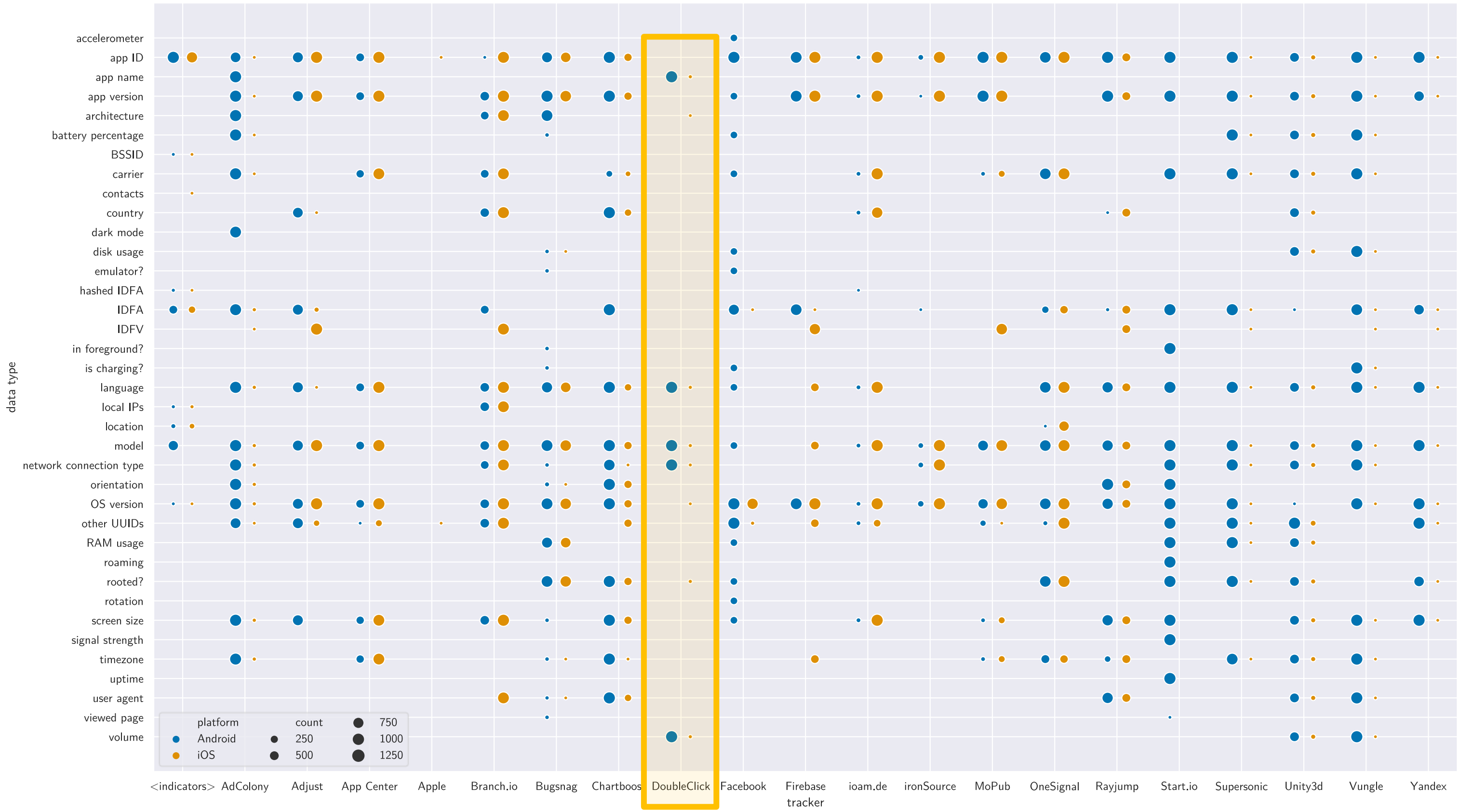
Observed transmissions of data types to trackers **without interaction**. We are also using “IDFA” for the Android ad ID here. Each point represents a number of apps transmitting the row’s data type to the column’s tracker, with the size indicating how many apps transmitted at least once. The “<indicators>” observations came from indicator matching in the requests not covered by an endpoint-specific tracking request adapter.



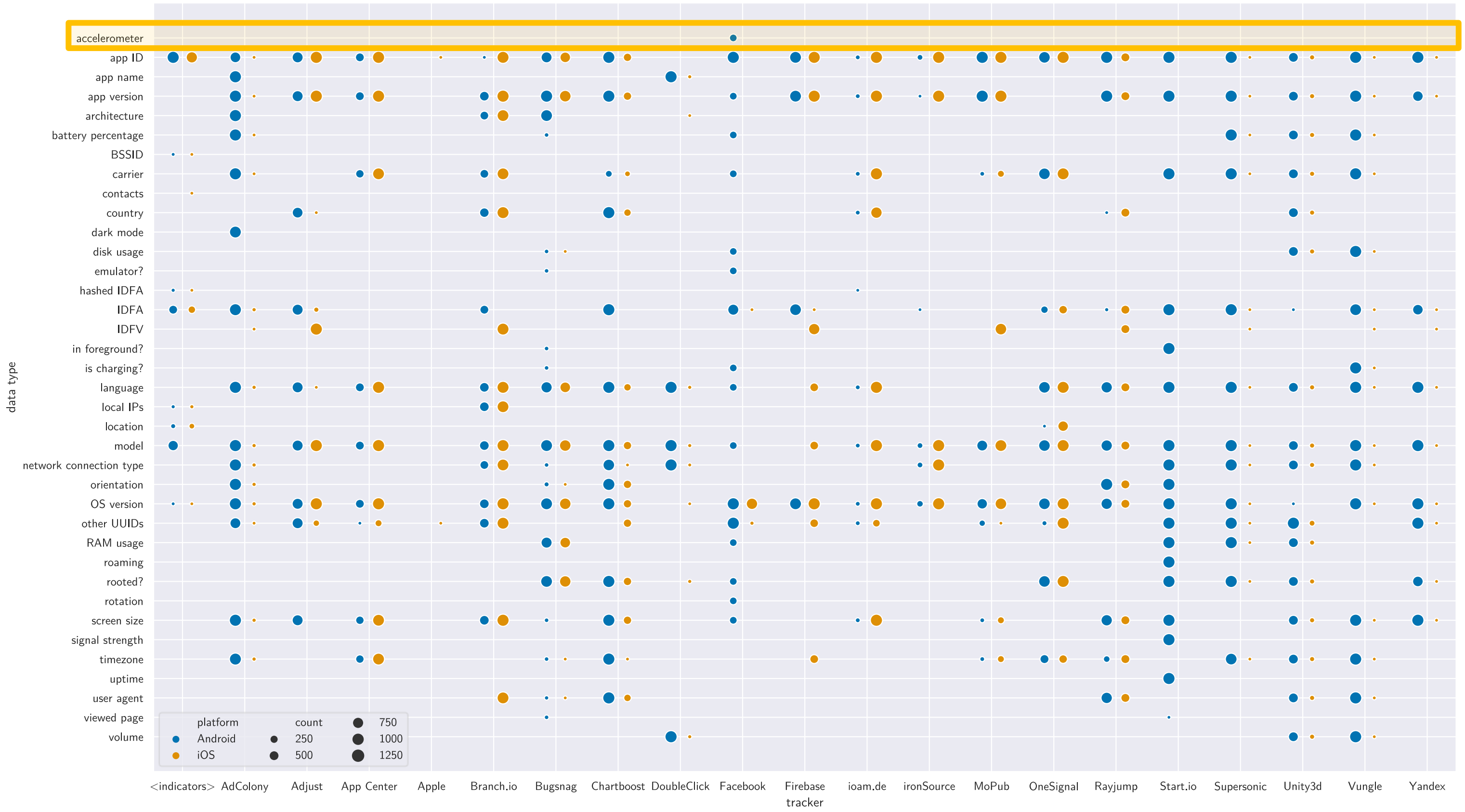
Observed transmissions of data types to trackers **without interaction**. We are also using “IDFA” for the Android ad ID here. Each point represents a number of apps transmitting the row’s data type to the column’s tracker, with the size indicating how many apps transmitted at least once. The “<indicators>” observations came from indicator matching in the requests not covered by an endpoint-specific tracking request adapter.



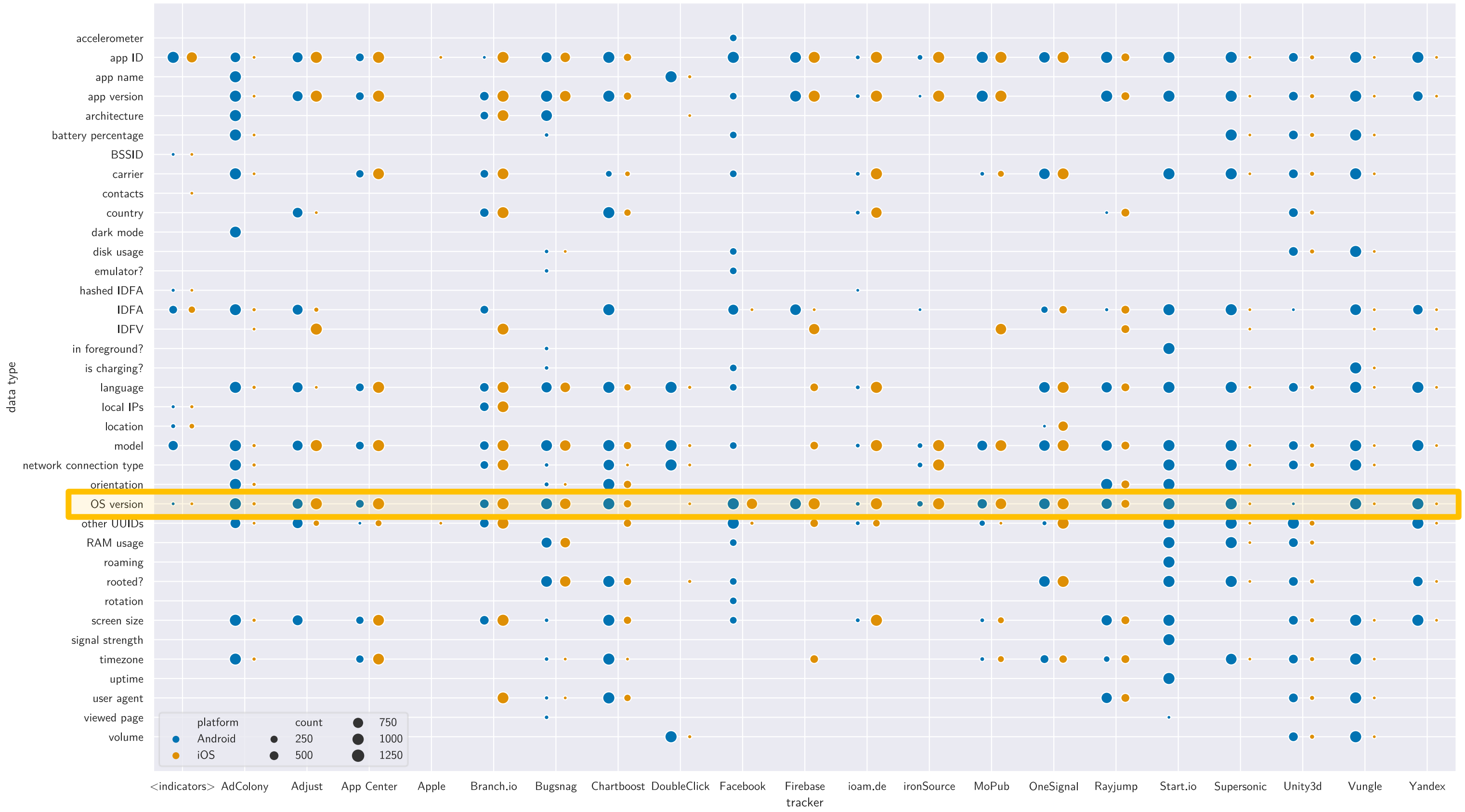
Observed transmissions of data types to trackers **without interaction**. We are also using “IDFA” for the Android ad ID here. Each point represents a number of apps transmitting the row’s data type to the column’s tracker, with the size indicating how many apps transmitted at least once. The “<indicators>” observations came from indicator matching in the requests not covered by an endpoint-specific tracking request adapter.



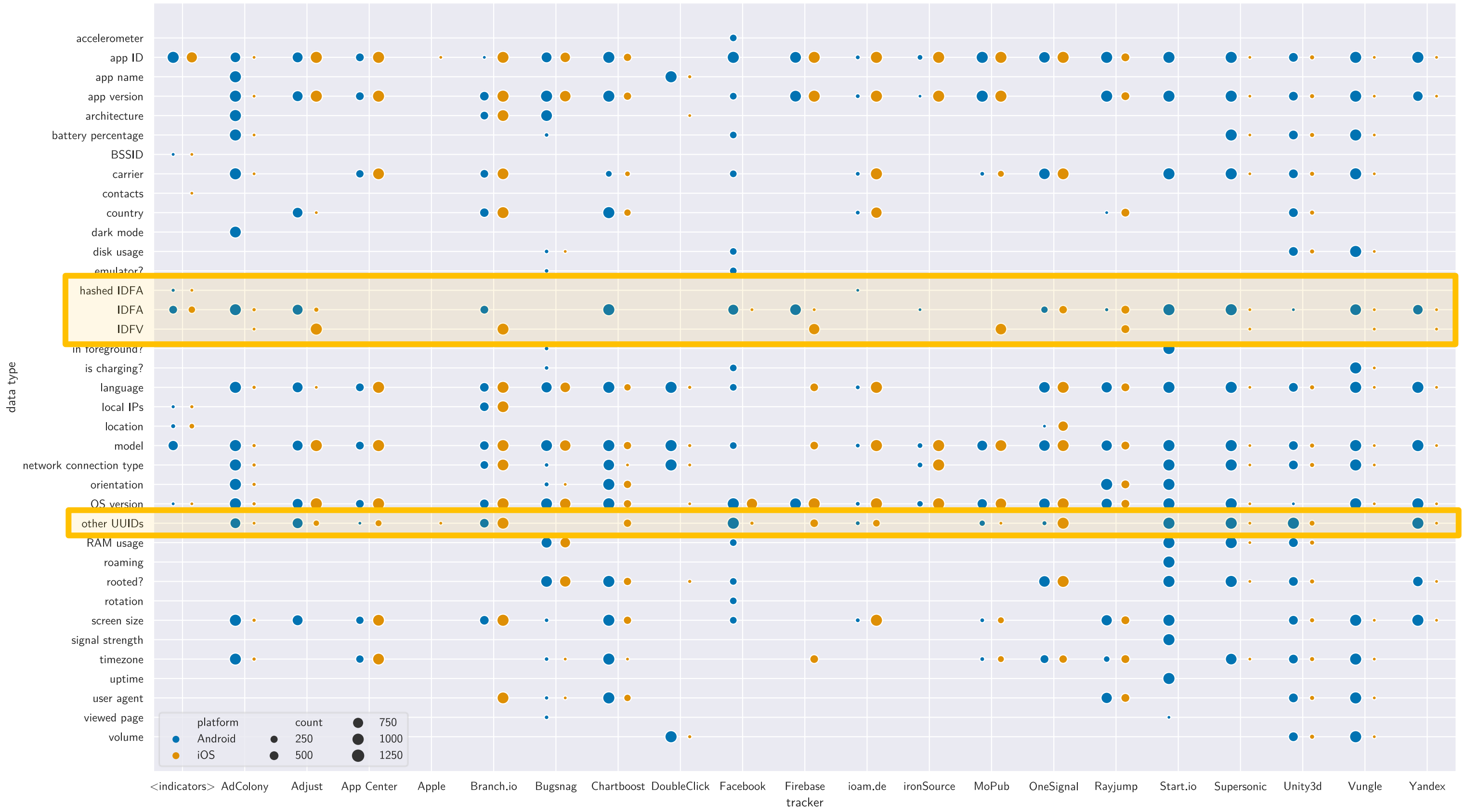
Observed transmissions of data types to trackers **without interaction**. We are also using “IDFA” for the Android ad ID here. Each point represents a number of apps transmitting the row’s data type to the column’s tracker, with the size indicating how many apps transmitted at least once. The “<indicators>” observations came from indicator matching in the requests not covered by an endpoint-specific tracking request adapter.



Observed transmissions of data types to trackers **without interaction**. We are also using “IDFA” for the Android ad ID here. Each point represents a number of apps transmitting the row’s data type to the column’s tracker, with the size indicating how many apps transmitted at least once. The “<indicators>” observations came from indicator matching in the requests not covered by an endpoint-specific tracking request adapter.



Observed transmissions of data types to trackers **without interaction**. We are also using “IDFA” for the Android ad ID here. Each point represents a number of apps transmitting the row’s data type to the column’s tracker, with the size indicating how many apps transmitted at least once. The “<indicators>” observations came from indicator matching in the requests not covered by an endpoint-specific tracking request adapter.



Observed transmissions of data types to trackers **without interaction**. We are also using “IDFA” for the Android ad ID here. Each point represents a number of apps transmitting the row’s data type to the column’s tracker, with the size indicating how many apps transmitted at least once. The “<indicators>” observations came from indicator matching in the requests not covered by an endpoint-specific tracking request adapter.

Effect of user choices

- Analysis interacted with discovered “accept” and “reject” buttons.

Effect of user choices

- Analysis interacted with discovered “accept” and “reject” buttons.
- Collected traffic for 330 apps (9,342 requests) after accepting, 28 apps (323 requests) after rejecting.

Effect of user choices

- Analysis interacted with discovered “accept” and “reject” buttons.
- Collected traffic for 330 apps (9,342 requests) after accepting, 28 apps (323 requests) after rejecting.
  - Remember the low number of dialogs which even *have* a “reject” button we could click.
  - => Results for rejected runs not representative.

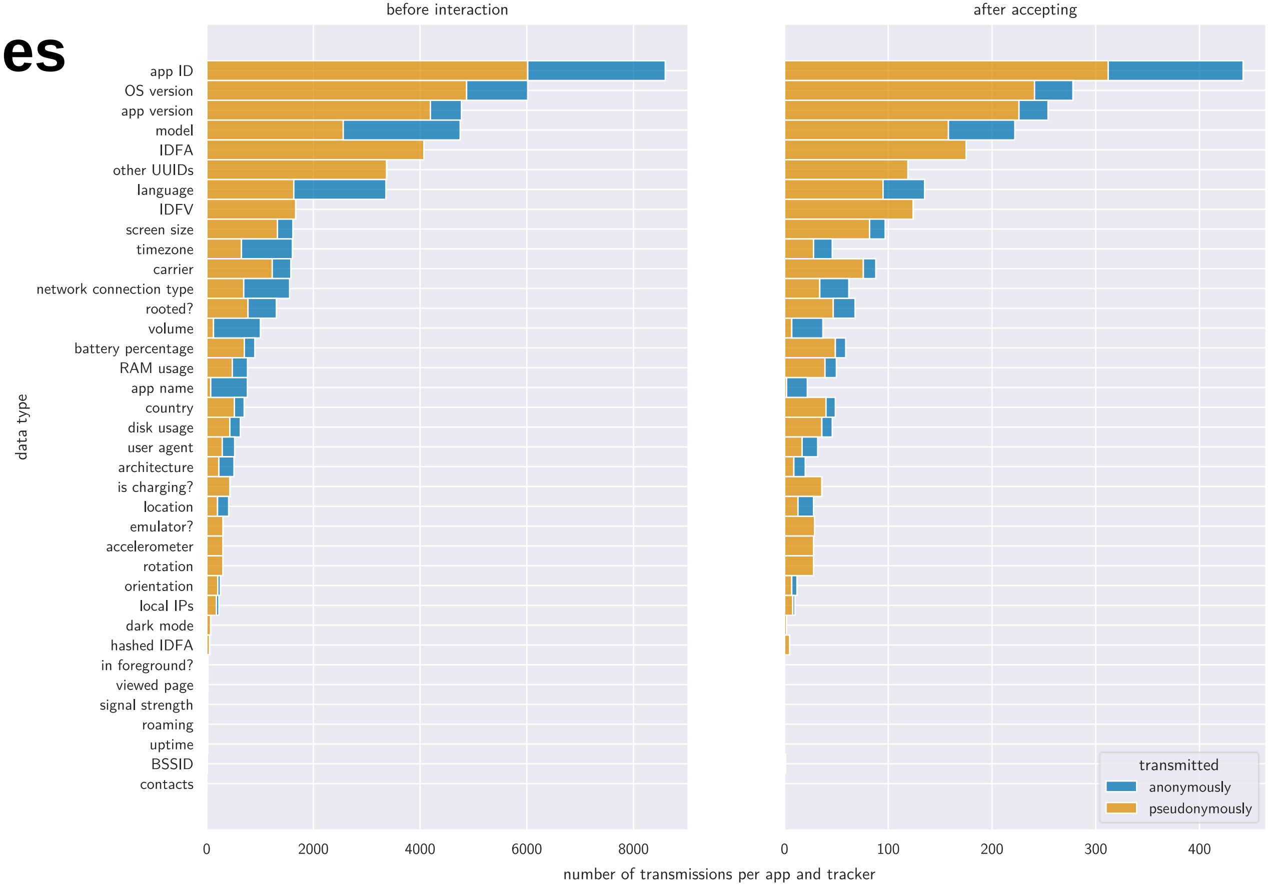
Effect of user choices

- Analysis interacted with discovered “accept” and “reject” buttons.
- Collected traffic for 330 apps (9,342 requests) after accepting, 28 apps (323 requests) after rejecting.
    - Remember the low number of dialogs which even *have* a “reject” button we could click.
    - => Results for rejected runs not representative.

- Of the 384 apps with a detected dialog, 282 (73.44 %) already transmitted pseudonymous data before receiving a consent choice.

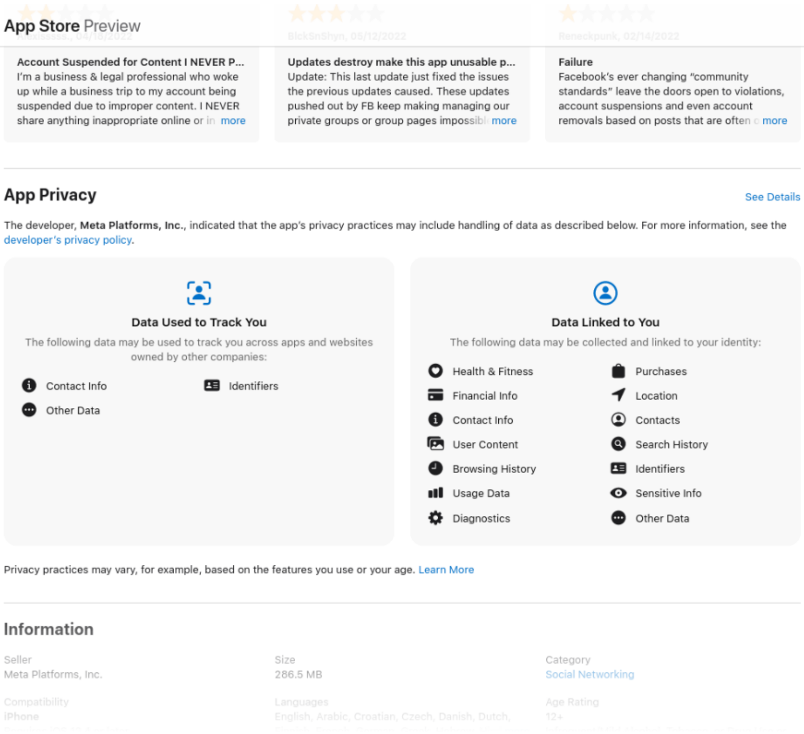
	requests identified as trackers	apps contacting at least one tracker	apps transmitting pseudonymous data
initial runs	33.32 %	78.08 %	72.95 %
accepted runs	31.90 %	+ 25 apps	+ 46 apps
rejected runs	47.06 %	+ 1 apps	+ 1 apps

Data types



Number of times the observed data types were transmitted per app and tracker. Note that we are also using the term “IDFA” for the Android advertising ID here.

Apple privacy labels



App Store Preview

Alexisssss., 04/18/2022

Account Suspended for Content I NEVER P...
I'm a business & legal professional who woke up while a business trip to my account being suspended due to improper content. I NEVER share anything inappropriate online or in more

BlckSnShyn, 05/12/2022

Updates destroy make this app unusable p...
Update: This last update just fixed the issues the previous updates caused. These updates pushed out by FB keep making managing our private groups or group pages impossibl more

Reneckpunk, 02/14/2022

Failure
Facebook's ever changing "community standards" leave the doors open to violations, account suspensions and even account removals based on posts that are often c more

App Privacy

See Details

The developer, **Meta Platforms, Inc.**, indicated that the app's privacy practices may include handling of data as described below. For more information, see the developer's privacy policy.

Data Used to Track You

The following data may be used to track you across apps and websites owned by other companies:

- Contact Info
- Other Data
- Identifiers

Data Linked to You

The following data may be collected and linked to your identity:

- Health & Fitness
- Financial Info
- Contact Info
- User Content
- Browsing History
- Usage Data
- Diagnostics
- Purchases
- Location
- Contacts
- Search History
- Identifiers
- Sensitive Info
- Other Data

Privacy practices may vary, for example, based on the features you use or your age. Learn More

Information

Seller
Meta Platforms, Inc.

Size
286.5 MB

Category
Social Networking

Compatibility
iPhone

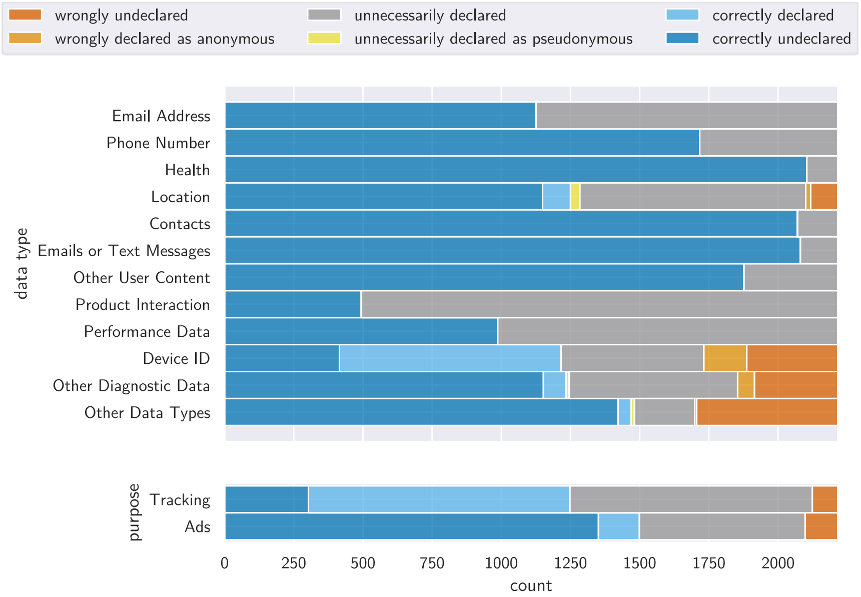
Languages
English, Arabic, Croatian, Czech, Danish, Dutch,

Age Rating
12+

https://apps.apple.com/us/app/facebook/id284882215

Apple privacy labels

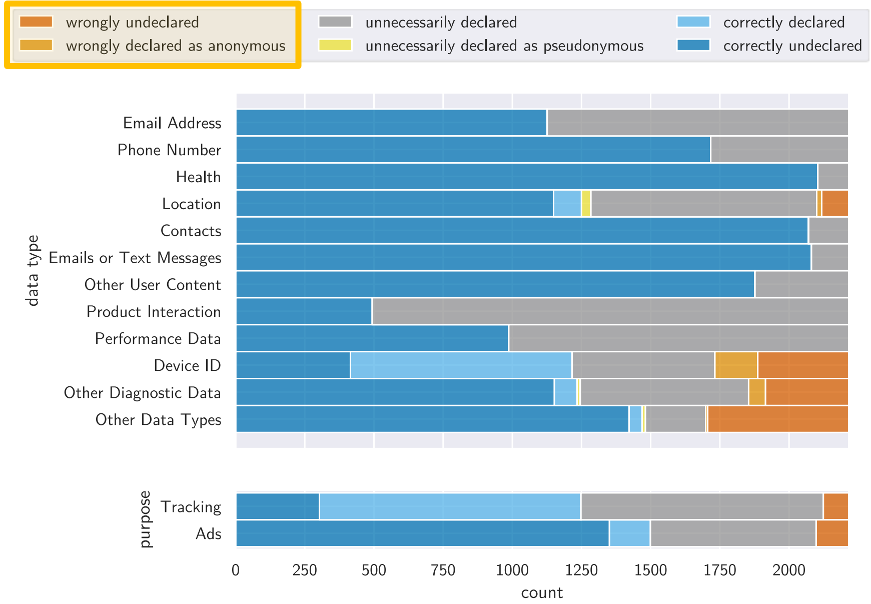
- 112 of the 2,481 apps on iOS (4.51 %) had an empty privacy label. 182 of them (7.68 %) claimed not to collect any data.



Correctness of data types and purposes in privacy labels on iOS. We can only definitively say when data is collected but if we don't observe data being transmitted, it does not necessarily mean that it is never collected.

Apple privacy labels

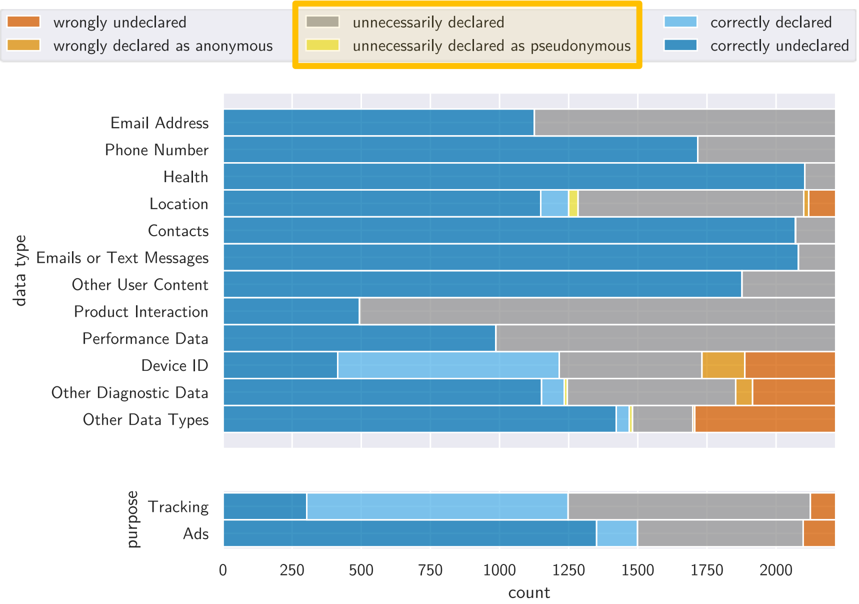
- 112 of the 2,481 apps on iOS (4.51 %) had an empty privacy label. 182 of them (7.68 %) claimed not to collect any data.



Correctness of data types and purposes in privacy labels on iOS. We can only definitively say when data is collected but if we don’t observe data being transmitted, it does not necessarily mean that it is never collected.

Apple privacy labels

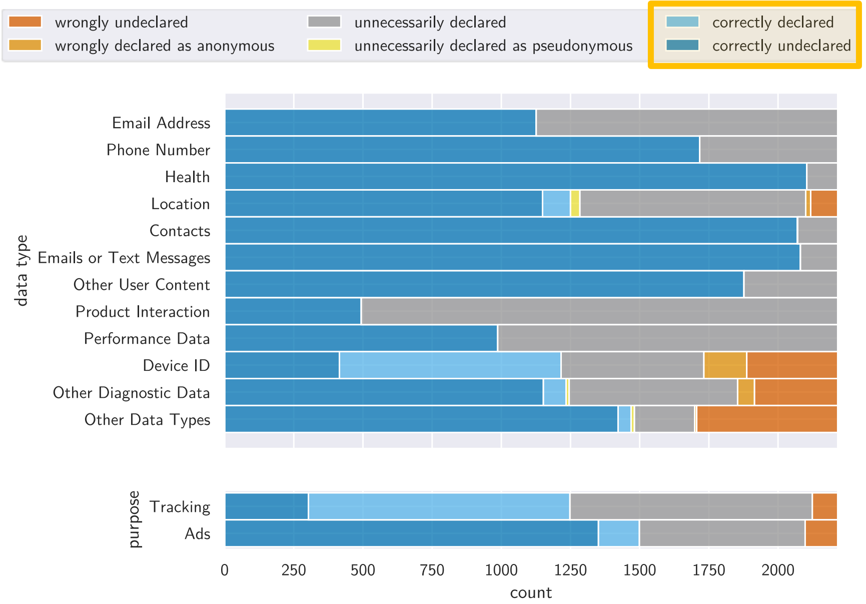
- 112 of the 2,481 apps on iOS (4.51 %) had an empty privacy label. 182 of them (7.68 %) claimed not to collect any data.



Correctness of data types and purposes in privacy labels on iOS. We can only definitively say when data is collected but if we don’t observe data being transmitted, it does not necessarily mean that it is never collected.

Apple privacy labels

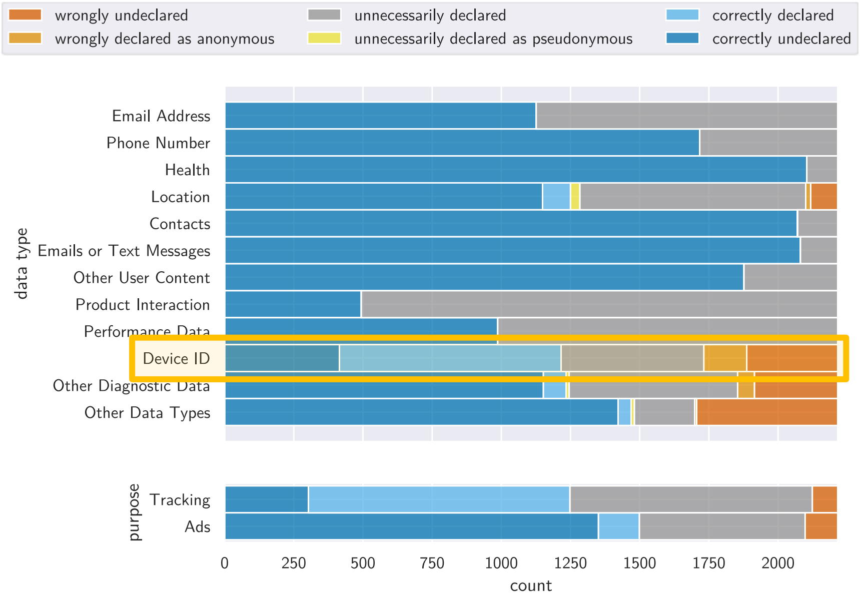
- 112 of the 2,481 apps on iOS (4.51 %) had an empty privacy label. 182 of them (7.68 %) claimed not to collect any data.



Correctness of data types and purposes in privacy labels on iOS. We can only definitively say when data is collected but if we don’t observe data being transmitted, it does not necessarily mean that it is never collected.

Apple privacy labels

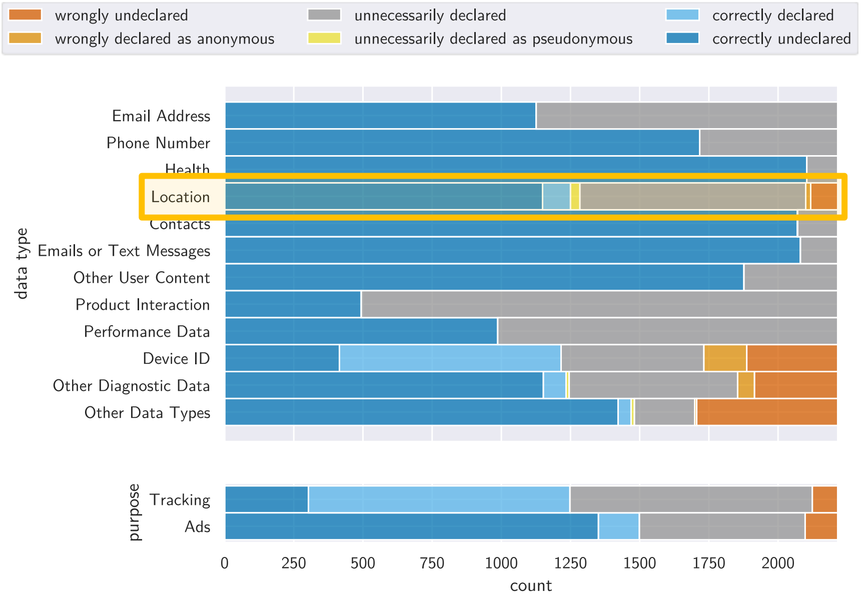
- 112 of the 2,481 apps on iOS (4.51 %) had an empty privacy label. 182 of them (7.68 %) claimed not to collect any data.



Correctness of data types and purposes in privacy labels on iOS. We can only definitively say when data is collected but if we don’t observe data being transmitted, it does not necessarily mean that it is never collected.

Apple privacy labels

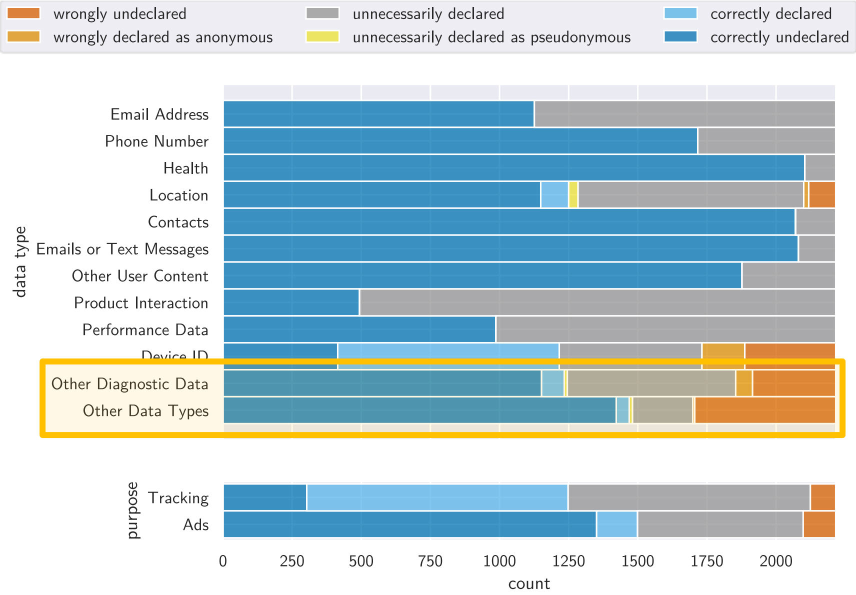
- 112 of the 2,481 apps on iOS (4.51 %) had an empty privacy label. 182 of them (7.68 %) claimed not to collect any data.



Correctness of data types and purposes in privacy labels on iOS. We can only definitively say when data is collected but if we don't observe data being transmitted, it does not necessarily mean that it is never collected.

Apple privacy labels

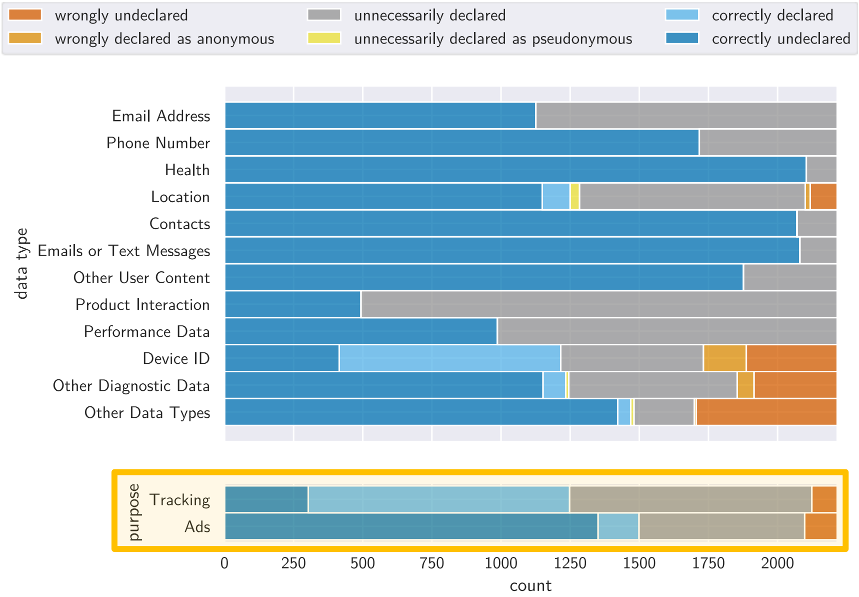
- 112 of the 2,481 apps on iOS (4.51 %) had an empty privacy label. 182 of them (7.68 %) claimed not to collect any data.



Correctness of data types and purposes in privacy labels on iOS. We can only definitively say when data is collected but if we don’t observe data being transmitted, it does not necessarily mean that it is never collected.

Apple privacy labels

- 112 of the 2,481 apps on iOS (4.51 %) had an empty privacy label. 182 of them (7.68 %) claimed not to collect any data.



Correctness of data types and purposes in privacy labels on iOS. We can only definitively say when data is collected but if we don't observe data being transmitted, it does not necessarily mean that it is never collected.

Conclusion

- We detected consent elements in around 18 % of apps, with 9 % dialogs, 4 % notices, and 5 % privacy policy links.

Conclusion

- We detected consent elements in around 18 % of apps, with 9 % dialogs, 4 % notices, and 5 % privacy policy links.

- There are strict criteria for legally compliant consent dialogs.
- More than 90 % of analysed apps violate at least one of these criteria, especially the requirement of a first-layer “reject” button.

Conclusion

- We detected consent elements in around 18 % of apps, with 9 % dialogs, 4 % notices, and 5 % privacy policy links.

- There are strict criteria for legally compliant consent dialogs.
- More than 90 % of analysed apps violate at least one of these criteria, especially the requirement of a first-layer “reject” button.

- One third of all network traffic was tracking. Google and Facebook are the most common trackers by far.
- 73 % of apps sent pseudonymous data before any interaction. This also applies to the ones with a dialog.

Conclusion

- We detected consent elements in around 18 % of apps, with 9 % dialogs, 4 % notices, and 5 % privacy policy links.

- There are strict criteria for legally compliant consent dialogs.
- More than 90 % of analysed apps violate at least one of these criteria, especially the requirement of a first-layer “reject” button.

- One third of all network traffic was tracking. Google and Facebook are the most common trackers by far.
- 73 % of apps sent pseudonymous data before any interaction. This also applies to the ones with a dialog.

- What companies fail to mention when they blame the GDPR for the flood of consent dialogs: Most of them blatantly violate the GDPR!

Future work

- Fix problems with certificate pinning bypass on Android.

Future work

- Fix problems with certificate pinning bypass on Android.
- Interact with apps beyond consent dialog (being careful not to accidentally give consent).

Future work

- Fix problems with certificate pinning bypass on Android.
- Interact with apps beyond consent dialog (being careful not to accidentally give consent).
- Monitor changes over time.

Future work

- Fix problems with certificate pinning bypass on Android.
- Interact with apps beyond consent dialog (being careful not to accidentally give consent).
- Monitor changes over time.

- Research defenses against tracking and metadata extraction.

More reading and watching material

- B. Altpeter and M. Wessels, “Do they track? Automated analysis of Android apps for privacy violations,” https://benjamin-altpeter.de/doc/presentation-android-privacy.pdf.

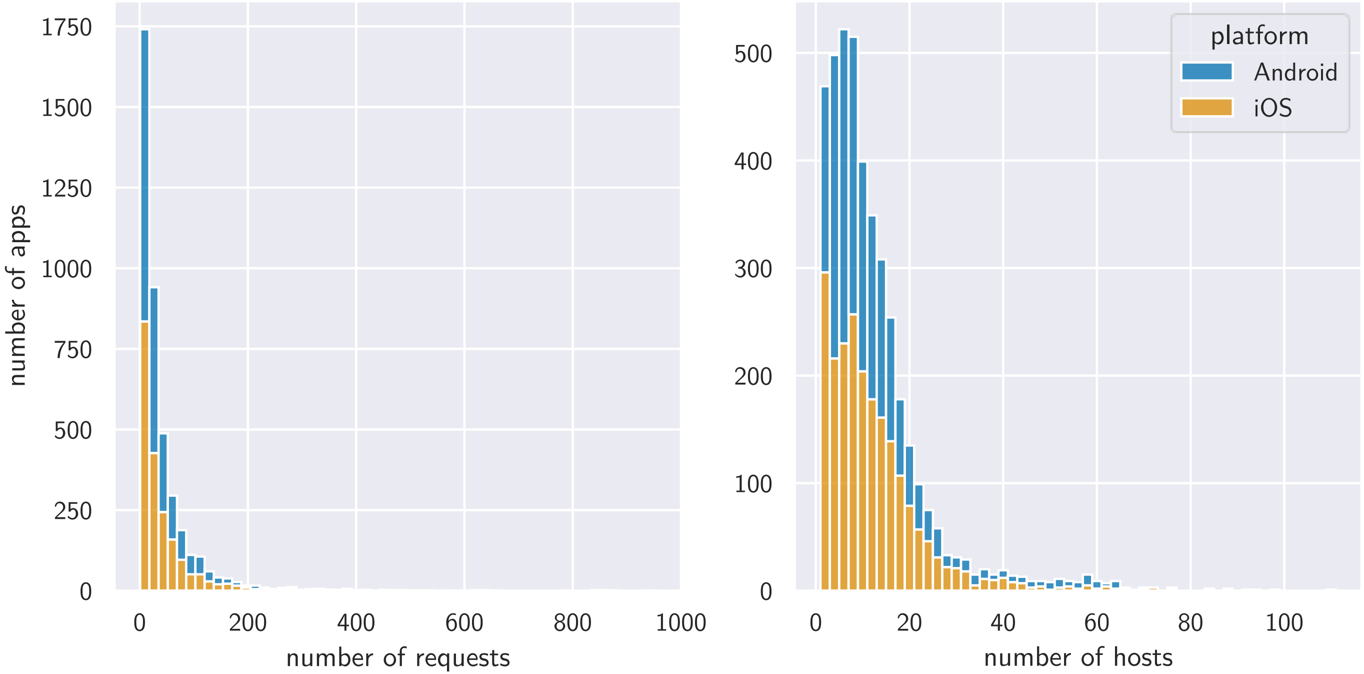
- B. Altpeter, “iOS watching you: Automated analysis of ‘zero-touch’ privacy violations under iOS,” https://benjamin-altpeter.de/doc/presentation-ios-privacy.pdf.

- M. Schrems, “Datenschutz skalieren,” https://www.bfdi.bund.de/SharedDocs/Videos/DE/Veranstaltungen/20220322_Datenschutz-skalieren.html.

- Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, “Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021,” https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf.

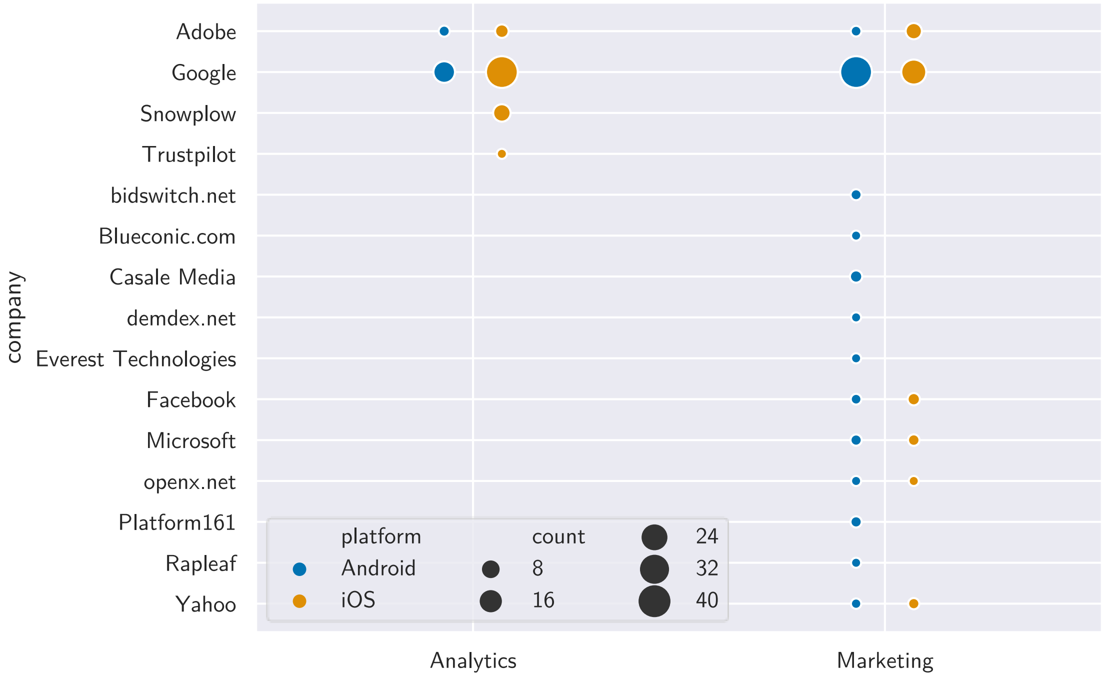
This slide intentionally left blank.

Requests and hosts



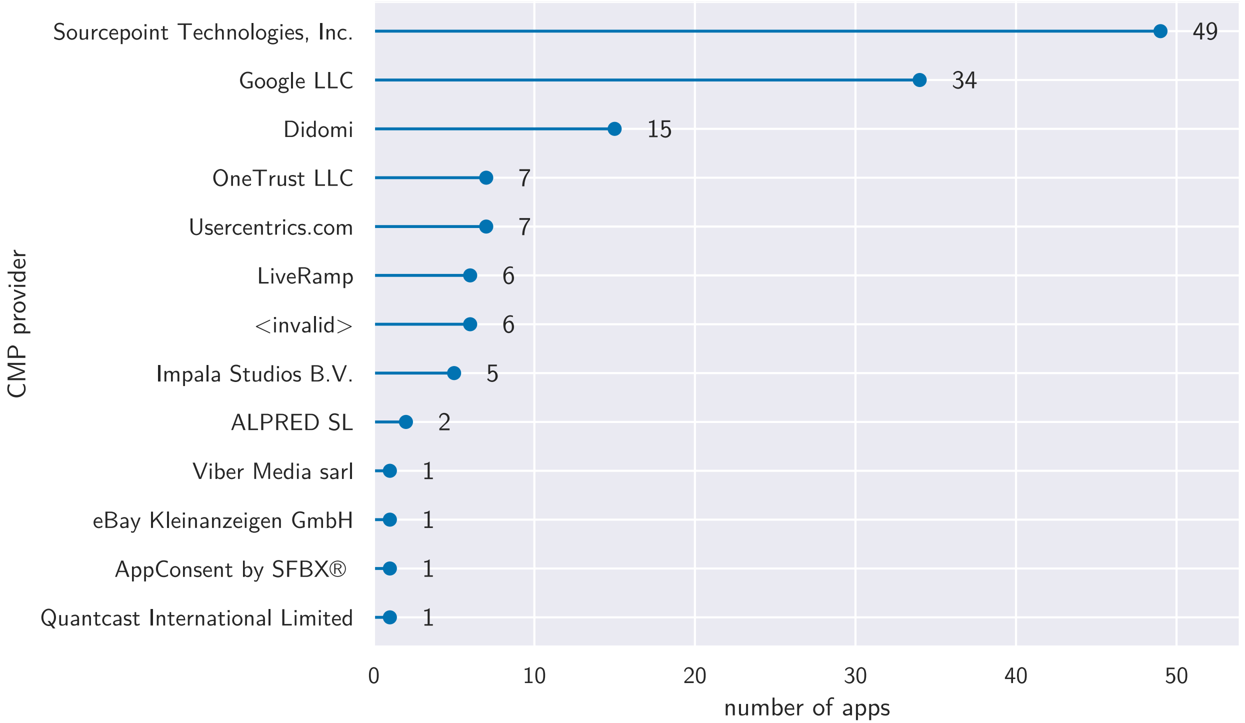
Number of requests and unique hosts contacted per app without any user interaction. Three apps with more than 1,000 requests are omitted in this graph: `com.prequel.app` on Android with 2,500 requests, and `com.audiomack.iphone` and `com.storycover` on iOS with 2,383 and 1,019 requests, respectively.

Cookies



Prevalence of cookies by various companies and their categories (**across all runs**). Each point represents the number of times a cookie by the company in the respective row and belonging to the category in the respective column was set by an app to a different value, with the size of the point indicating how often the cookie was set.

IAB TCF data



Prevalence of CMP providers according to IAB TCF data.

IAB TCF data

- 163 of the analysed apps have saved IABTCF preferences (64 on Android, and 99 on iOS).
- Of those, 61 were not detected as having a consent dialog by our approach. Manually analysing those showed that 17 do in fact show a dialog that we did not detect but the remaining 44 do not.
  Conversely, 282 apps were detected as showing a dialog but have not saved IABTCF preferences.

- The apps most often set the IABTCF_gdprApplies property, with 125 apps setting the property initially, another 27 only setting it after accepting the dialog, and one app setting it only after rejecting. In total, 145 apps determine the GDPR to be applicable, 6 apps (incorrectly) determine it not to be, and 2 apps set non-spec-compliant values . None of the apps changed their determination after accepting or rejecting the dialog.

IAB TCF data

- IABTCF_PublisherCC specifies the app publisher's country. 62 apps are from Germany according to this, for 22 the CMP didn't know the country, seven are from the US, five from the Netherlands, and three from Spain. The following countries are each represented once: France, Hong Kong, Luxembourg, Japan, United Kingdom, and Australia.

- Most apps store consent for all ten purposes, with an average of 9.10 and a median of 10.
- The average for the amount of stored vendor consents is 361.75, the median is 158 (maximum possible: 860). All possible vendors were requested by at least seven apps.

- Of the 68 apps that initially store a TC string, 63 showed an English consent dialog (our devices were set to English), and five showed a dialog in German.

Failed apps

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.

Limitations

- We only provide lower bound on consent element prevalence and dark patterns.
  - Appium doesn’t expose the text in all games, sometimes missing (esp. games).
  - Appium only allows limited access to element attributes, e.g. no link targets or styling.
- String matching approach limits the details we can extract.
- We only detect English and German consent elements.

- Apps could try to re-identify our device using fingerprinting despite us resetting it.
- Apps could interpret lack of IDFA permission on iOS as refusal of consent.

- 32 % of apps on Android quit immediately due to objection.
- Root/jailbreak and emulator could affect app behaviour.
- HTTPS proxy and certificate pinning bypass could affect app behaviour.