The TCF doesn't really A(A)ID – Automatic Privacy Analysis and Compliance of TCF-based Android Applications

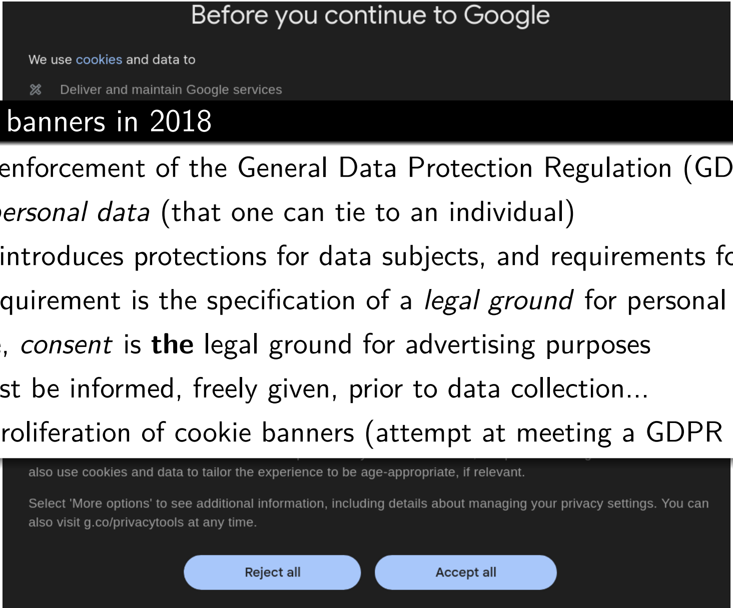
On the articulation between law and technology in privacy issues

Victor Morel – https://victor-morel.net/

Chalmers University of Technology – *morelv@chalmers.se*

12^{th} December 2025

Cookie banners



Before you continue to Google

We use cookies and data to

- Deliver and maintain Google services

also use cookies and data to tailor the experience to be age-appropriate, if relevant.

Select 'More options' to see additional information, including details about managing your privacy settings. You can also visit g.co/privacytools at any time.

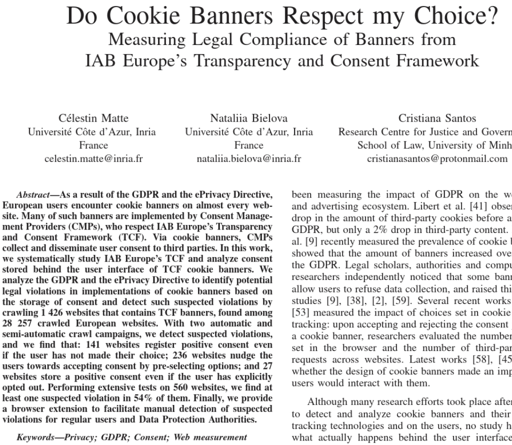
Surge in cookie banners in 2018

- Year of the enforcement of the General Data Protection Regulation (GDPR)
- Applies to *personal data* (that one can tie to an individual)
- The GDPR introduces protections for data subjects, and requirements for data controllers
- One such requirement is the specification of a *legal ground* for personal data processing
- For instance, *consent* is **the** legal ground for advertising purposes
- Consent must be informed, freely given, prior to data collection...
- Hence the proliferation of cookie banners (attempt at meeting a GDPR requirement)

The Transparency and Consent Framework (TCF)

The *de-facto* standard behind cookie banners

- Created in 2018 by the Interactive Advertising Bureau (IAB) Europe (an advertising business organization) to *facilitate* compliance ✅
- Many websites using the TCF were still violating data protection law ⚖️
- The Belgian Data Protection Authority (DPA) ruled in 2022 that it was non-compliant with the GDPR 🛑 since it allowed websites to *avoid* consent for advertising



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 Govern
School of Law, University of Minh
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

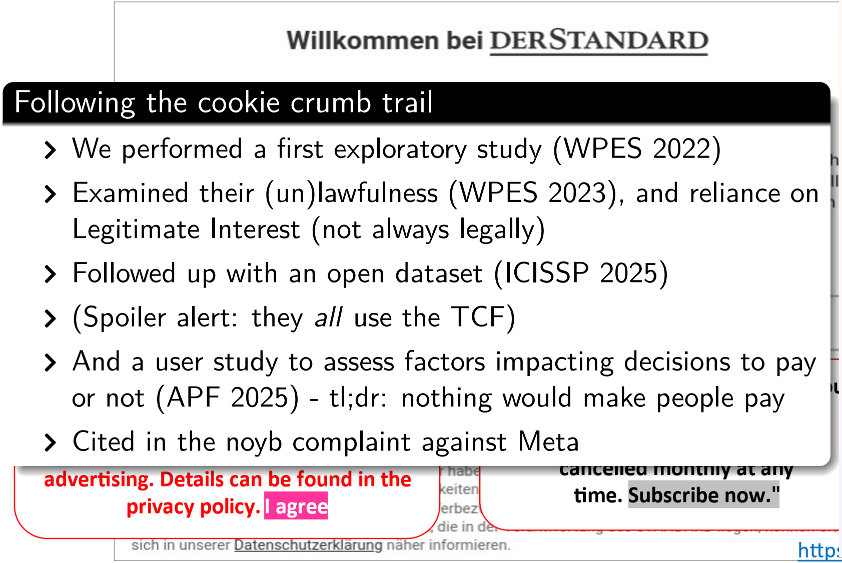
been measuring the impact of GDPR on the w
and advertising ecosystem. Libert et al. [41] obse
drop in the amount of third-party cookies before a
GDPR, but only a 2% drop in third-party content.
al. [9] recently measured the prevalence of cookie
showed that the amount of banners increased ove
the GDPR. Legal scholars, authorities and compu
researchers independently noticed that some bann
allow users to refuse data collection, and raised thi
studies [9], [38], [2], [59]. Several recent works
[53] measured the impact of choices set in cookie
tracking: upon accepting and rejecting the consent
a cookie banner, researchers evaluated the number
set in the browser and the number of third-par
requests across websites. Latest works [58], [45
whether the design of cookie banners made an imp
users would interact with them.

Although many research efforts took place afte
to detect and analyze cookie banners and their
tracking technologies and on the users, no study h
what actually happens behind the user interface

Cookie paywalls

Following the cookie crumb trail

- We performed a first exploratory study (WPES 2022)
- Examined their (un)lawfulness (WPES 2023), and reliance on Legitimate Interest (not always legally)
- Followed up with an open dataset (ICISSP 2025)
- (Spoiler alert: they *all* use the TCF)
- And a user study to assess factors impacting decisions to pay or not (APF 2025) - tl;dr: nothing would make people pay
- Cited in the noyb complaint against Meta

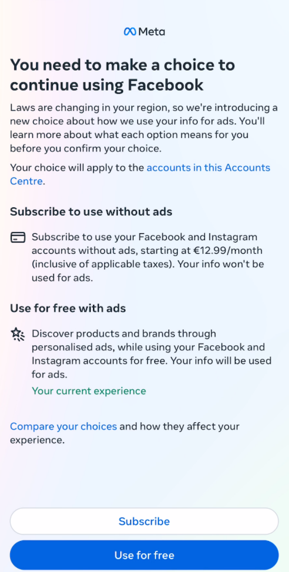


Willkommen bei DERSTANDARD

advertising. Details can be found in the privacy policy. I agree

cancelled monthly at any time. Subscribe now."

sich in unserer Datenschutzerklärung näher informieren.



Meta

You need to make a choice to continue using Facebook

Laws are changing in your region, so we're introducing a new choice about how we use your info for ads. You'll learn more about what each option means for you before you confirm your choice.

Your choice will apply to the accounts in this Accounts Centre.

Subscribe to use without ads

Subscribe to use your Facebook and Instagram accounts without ads, starting at €12.99/month (inclusive of applicable taxes). Your info won't be used for ads.

Use for free with ads

Discover products and brands through personalised ads, while using your Facebook and Instagram accounts for free. Your info will be used for ads.

Your current experience

Compare your choices and how they affect your experience.

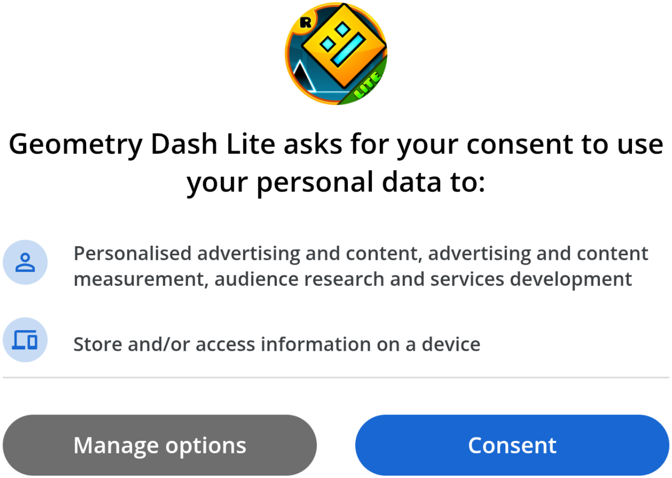
https:// … nt/tcf

27

Can we find cookie banners elsewhere, in other contexts?

Rhetorical question - yes

- Android applications start having cookie banners too
- Take a guess, which standard (previously convicted on multiple occasions to violate EU data protection law) is behind many mobile cookie banners?
- 🥁
- The TCF ✨



Geometry Dash Lite asks for your consent to use your personal data to:

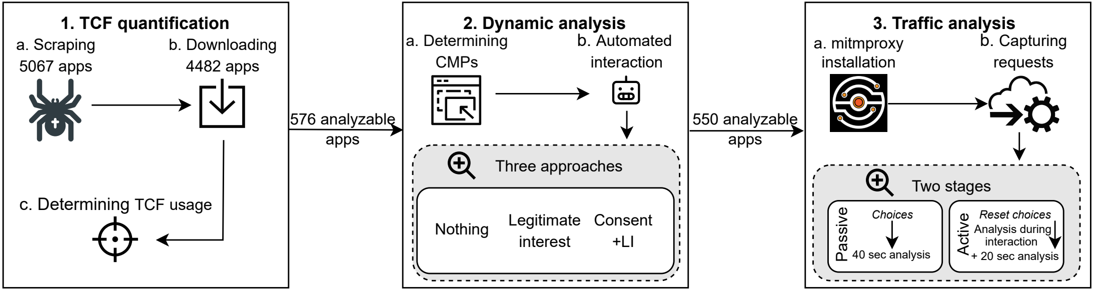
Personalised advertising and content, advertising and content measurement, audience research and services development

Store and/or access information on a device

Master thesis project

One semester project - two students: Joel and Pontus

- Very prospective, only a handful of papers on the topic, no expectation
- But there must be something to find, somewhere...



1. TCF quantification

a. Scraping 5067 apps

b. Downloading 4482 apps

c. Determining TCF usage

576 analyzable apps

2. Dynamic analysis

a. Determining CMPs

b. Automated interaction

Three approaches

Nothing

Legitimate interest

Consent +LI

550 analyzable apps

3. Traffic analysis

a. mitmproxy installation

b. Capturing requests

Two stages

Passive

Choices

40 sec analysis

Active

Reset choices

Analysis during interaction

+ 20 sec analysis

Quantifying the TCF

First contribution

- No one quantified the TCF with these details before
- TCF-based apps are widely spread across categories
- Most apps were developed outside the EU/EEA
- Google is *by far* (82.54%) the main Consent Management Provider
- 18.8% of apps in our dataset use the TCF (vs. 6.6% in 2023)

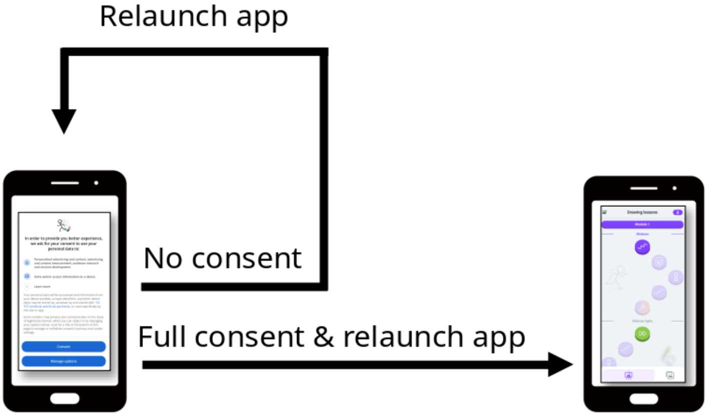
Table: Top 10 TCF-based app categories

App Category	**TCF usage**
PERSONALIZATION	61/101 (60.4%)
MUSIC_AND_AUDIO	35/85 (41.2%)
LIBRARIES_AND_DEMO	31/76 (40.8%)
ART_AND_DESIGN	32/79 (40.5%)
PRODUCTIVITY	25/67 (37.3%)
WEATHER	24/65 (36.9%)
VIDEO_PLAYERS	23/67 (34.3%)
TOOLS	30/90 (33.3%)
MAPS_AND_NAVIGATION	28/86 (32.6%)
PHOTOGRAPHY	24/77 (31.2%)

Dynamic analysis

Do apps store our choices correctly?

- Mostly yes
- Although 15 of them only stored our banner choices if provided with consent to all data processing



Relaunch app

No consent

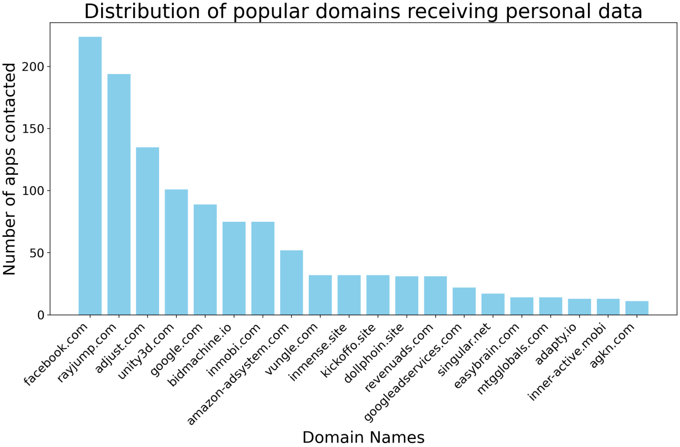
Full consent & relaunch app

In order to provide you better experience, we ask for your consent to use your personal data to:
Personalised advertising and content, advertising and content measurement, audience research and services development
Store and/or access information on a device
Learn more
Consent
Manage options
Drawing lessons
Module 1

Traffic analysis

Here comes trouble

- 66.2% of apps share personal data without consent
- 55.3% of them *before* interaction with the cookie banner!
- Specifically, they transmit the Google Advertising ID (AAID), the *de-facto* identifier on Android for targeted advertising (which requires consent)
- Games apps are the top violators



What does it tell us about the TCF?

Several things

- That its prevalence is growing (x 2.8 in two years)
- That it is structurally flawed - since TCF-based apps share AAID without consent at scale
- (We previously warned that it is too flexible technically (cf. cookie paywalls))
- And that it fails at facilitating compliance
- The upcoming update (February 2026) won't fix any of that

What does it tell us about Google/Alphabet?

Google is in a position of domination

- It owns Android
- It owns the Play Store
- It is the most prevalent CMP in our dataset (82.54%)
- Amongst the top data brokers (number 5)
  → The entire ecosystem is structured around Google's interests

We need effective regulatory oversight that consider the responsibilities of dominant platform providers, and not limit accountability to app-level practices.

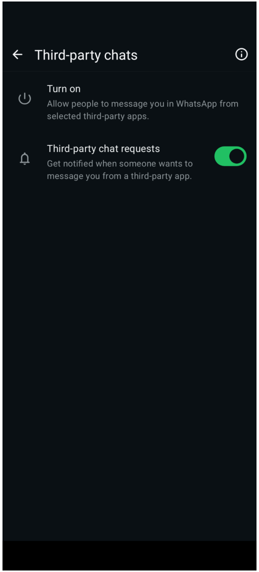
The role of technologists in techno-legal privacy issues

General lessons

- Many privacy issues are not purely technical
- However, technologists can bring a much needed knowledge
- We can provide measurements, technical explanations, and better designs
- It is important to find the right folks to talk to
- And to learn how to talk with them (not just with technical jargon)
- Also, we need to address the right issues (not to fall into a techno-solutionism mindset)

Take: commercial surveillance makes mass surveillance easier.

Upcoming interdisciplinary work - more directly related to crypto



← Third-party chats

Turn on

Allow people to message you in WhatsApp from selected third-party apps.

Third-party chat requests ●

Get notified when someone wants to message you from a third-party app.

Interoperability in messaging apps

- The Digital Market Act (DMA) requires that *gatekeepers* (large players) interoperate their *number-independent interpersonal communication services* (NIICS, e.g., WhatsApp) with third parties upon request and free of charge. They must preserve “the level of security, including the end-to-end encryption”.
- Basically solved for P2P communications
- But what about contact discovery?
- Also, can we do better than the current state of affairs?
- Privacy-friendly mutual contact discovery in interopable messaging apps!
- An example of a (potential) better design