

# GDPR and ePrivacy Compliance with Consent



**Cristiana Santos**  
**Assist. Prof. School of Law**  
**Utrecht University**



Summer School on real-world crypto and privacy 2024



## Joint work with...



Nataliia Bielova  
Inria



Imane Fouad  
Inria



Michael Toth  
Inria



Colin M. Gray  
Indiana Univ. Bloomington



Gilles Mertens  
Inria



Midas Nouwens  
Aarhus University



Victor Morel  
Chalmers University

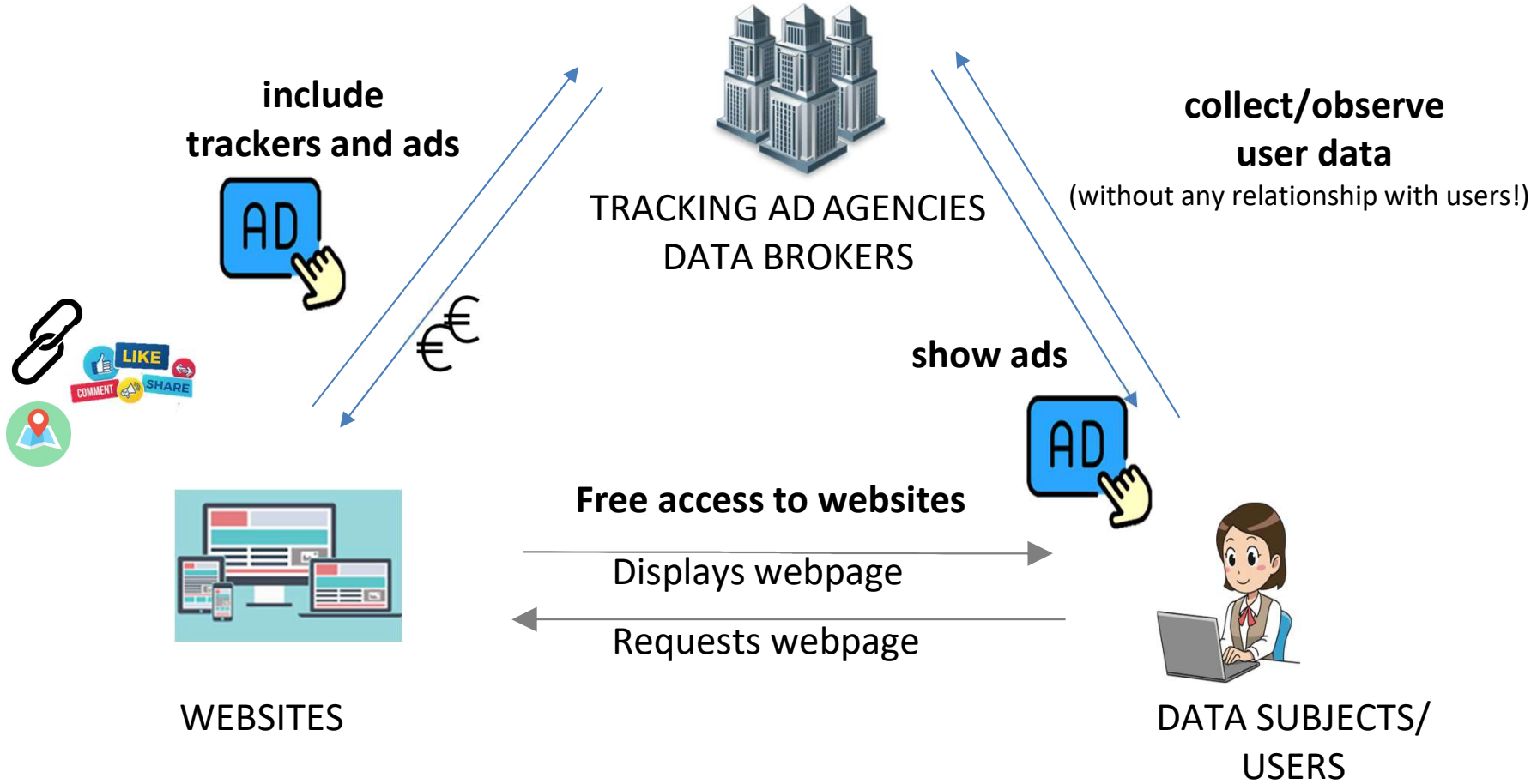


Celestin Matte  
Inria



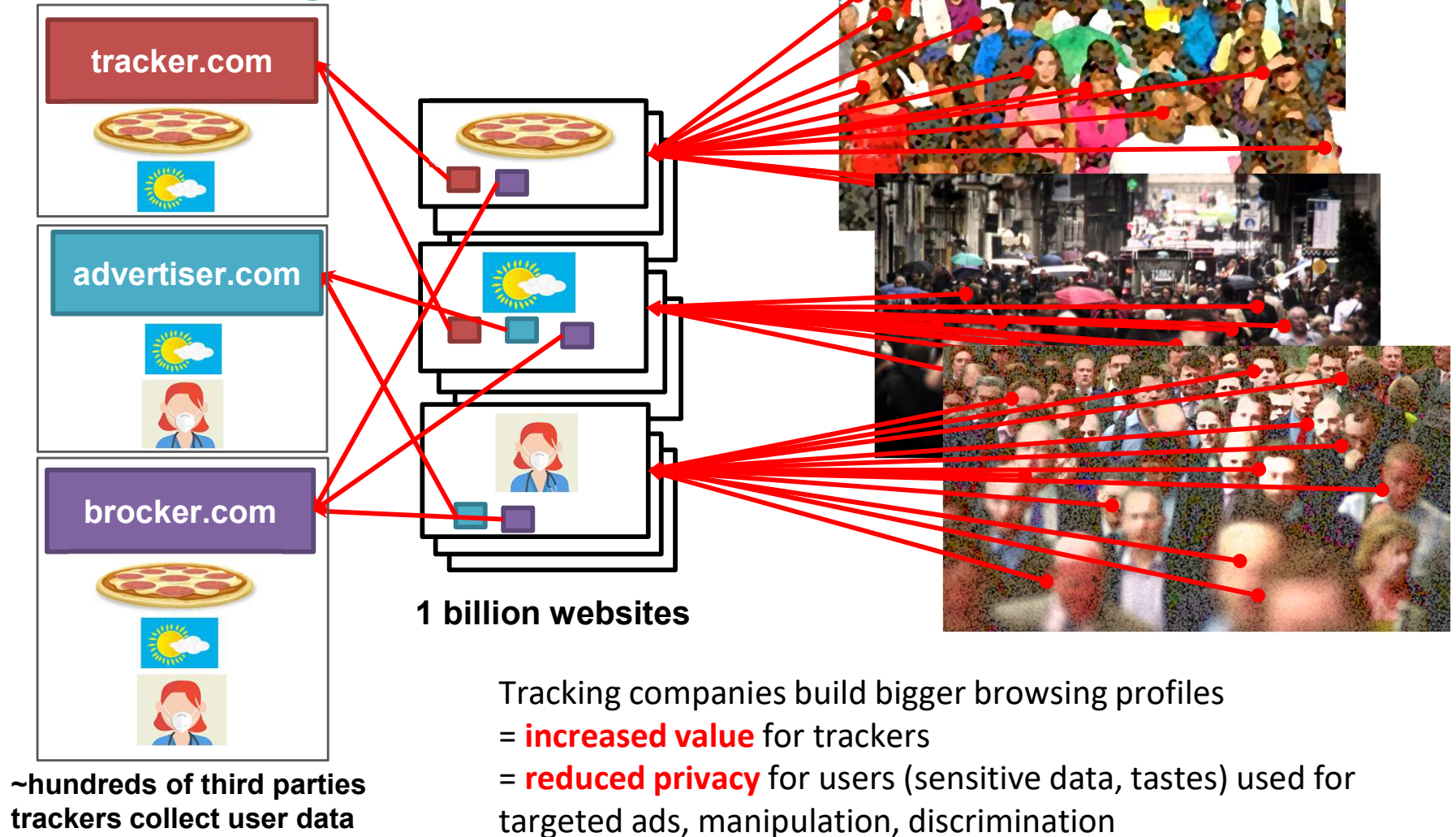
Vincent Roca  
Inria

# Context: the business model of Web tracking



Slide courtesy Michael Toth

# Web Tracking at scale



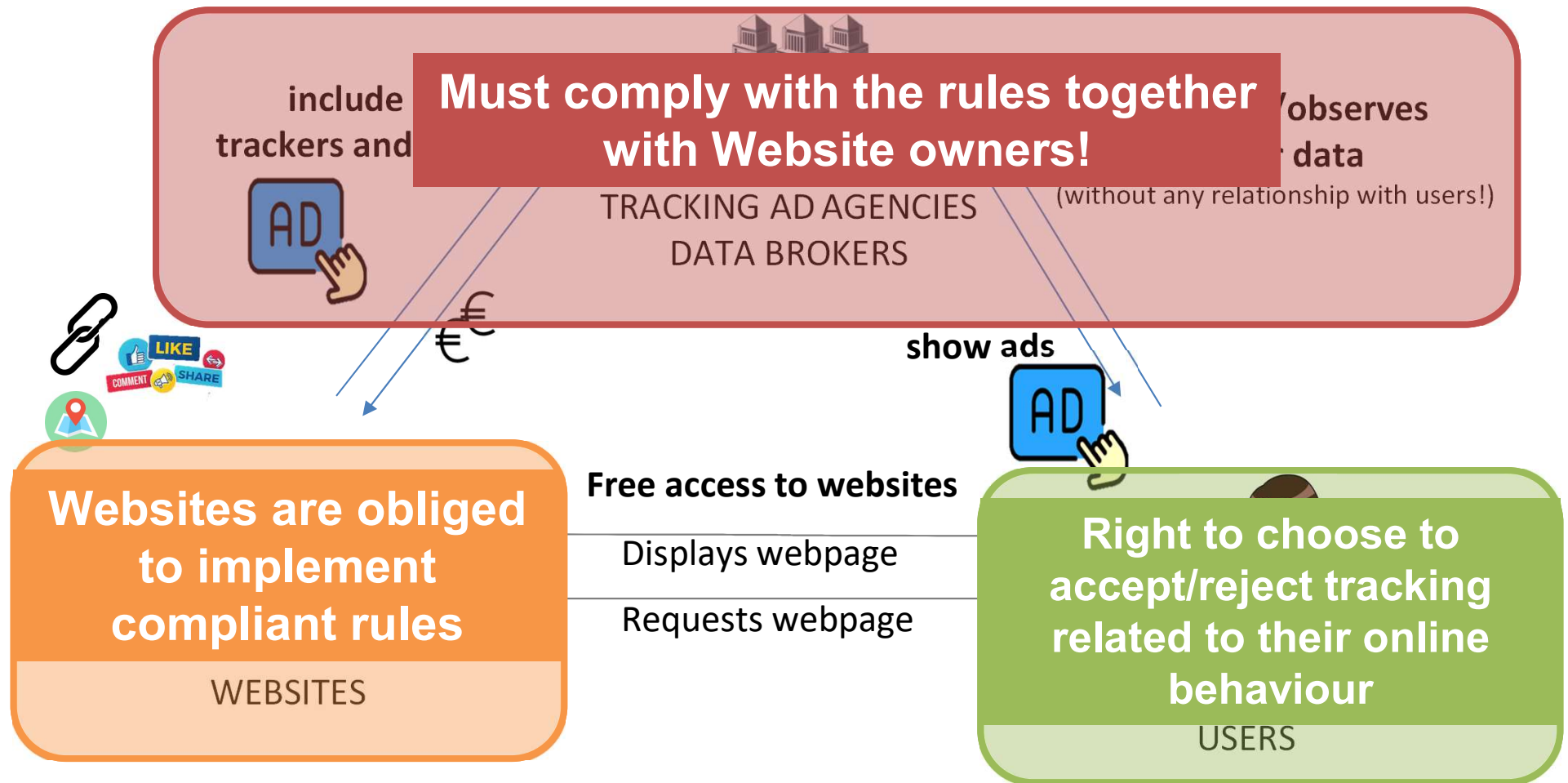
# A lot of what you do on the Web is tracked! How are you tracked on the Web?

- Ability to store/create user identity in the browser
  - HTTP/web cookies
  - HTTP headers
  - Browser storages (html5)
  - Pixels
  - Cross device tracking
  - Device fingerprinting:
    - browser properties
    - OS properties
    - IP address...
- Ability to communicate user identity back to tracker
  - HTTP requests by the browser
  - JavaScript



Every click leaves a trail that hundreds of adtech companies are happy to pick up.

# Context: do these actors have obligations/rights?





**The dream... mawebbsite users would like to...**



## Website users would like to....



1. say no to tracking that is not necessary for the website to function properly
2. avoid being manipulated
3. avoid paying to have access to a website or platform



# The reality ...



1. our personal data is collected even before we give our consent because consent banners do not prevent unwanted tracking
2. many consent banners include **dark patterns** to coerce the user towards accepting consent
3. we might need to **pay** to access websites!



**DARK  
PATTERNS**

# Reality of non-compliance practices of ...

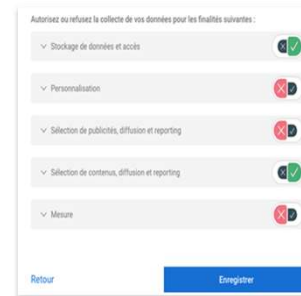


## Providers of intermediate services

Analytics, Google Tag Managers, WordPress, Shopify



## Third-party Web Tracking companies



## Consent Management Platforms



## Website Publishers

# Companies need a legal basis to process personal data

- **Consent**
- **Contract**, eg. If someone orders a pizza, the pizzeria can give the customer's address to the delivery person, because the address is "necessary" to deliver the pizza, and to perform the contract
- **Legal Obligation**, eg. an employer sends the data of payments too employees to the IRS
- **Public Interest**, eg. a state statistical authority uses data to create reports
- Protecting **Vital Interests** of the data subject, eg. a person is unconscious after a car accident and the hospital needs to know from his family's doctor whether he uses certain medication
- **Legitimate Interest** of the data controller, eg. Website publishers store IP addresses of website visitors for a brief period if that is necessary for security or for fraud prevention

# GDPR & ePrivacy compliance

Art. 4, 7 define **conditions for consent** to be legally valid

Art. 5(3): **consent** asked before processing data

## GDPR

(applies to personal data)

## ePrivacy Directive

(information stored on/retrieved from devices)

**Web tracking technologies require consent unless** used for:

- **Communication:** used for the sole purpose of enabling the communication on the web
- **Strict necessity** to enable the service requested by the user.



# Cookies that are necessary for a website to provide a service ... without it, no service!

**If not consent, what else?**



keeping track of items I placed in my **shopping cart**



**authentication**: verify Id in transactions, keeping you logged in, so users don't have to remember login password, eg. email services, eBanking service



**user interface (UI) preferences** (customization): language, display format (nr of results), personalized services, also called as functional purposes



**web audience measuring** of a website, eg. nr visits p/ page, average duration of visit, parts/pages browsed, kwords, navigation, clicks pp (analytic/statistic)



**user-security cookies**: protect login system from abuses



**multimedia session cookies**: render image, audio/video content



> Necessary	Always Enabled
> Non-necessary	Disabled



**But what is personal data?**





### **ANY INFORMATION**

Objective (earns 10k per year); Subjective (opinion); and, Sensitive data (gay woman).



### **RELATING TO**

An individual, about a particular person, impacts a specific person.



### **IDENTIFIED OR IDENTIFIABLE**

Direct or indirectly e.g. You know me by name, direct, you know me as "a Lawyer doing these graphics", indirect.



### **NATURAL PERSON**

applies ONLY to a living human being. National Law may give rules for deceased persons.



### **ONLINE IDENTIFIER & LOCATION DATA**

Include data provided by the electronic devices we use: mobiles, cookies identifiers, IP address, others.



### **TO ONE OR MORE FACTORS**

Include data that when combined with unique identifiers and other info create a profile and identify a person.

# Any information

**Any information** can be personal data, **regardless** of its **nature, content, or format:**

## Nature

- true/inaccurate **FAKE**
- objective/subjective (opinions, assessments)




## Content

- eg. private/family life
- person's professional life, other capacities



## Format

- alphabetical, numerical, graphical, **photographical** or **acoustic**
- kept on paper, stored in a computer memory as a binary code
- structured or unstructured
- video, voice recording   
eg. child's drawing can contain PD of both child/parents





### **ANY INFORMATION**

Objective (earns 10k per year); Subjective (opinion); and, Sensitive data (gay woman).



### **RELATING TO**

An individual, about a particular person, impacts a specific person.



### **IDENTIFIED OR IDENTIFIABLE**

Direct or indirectly e.g. You know me by name, direct, you know me as "a Lawyer doing these graphics", indirect.



### **NATURAL PERSON**

applies ONLY to a living human being. National Law may give rules for deceased persons.



### **ONLINE IDENTIFIER & LOCATION DATA**

Include data provided by the electronic devices we use: mobiles, cookies identifiers, IP address, others.



### **TO ONE OR MORE FACTORS**

Include data that when combined with unique identifiers and other info create a profile and identify a person.

# Identified or Identifiable art. 4(1), rec 26



**Identification:** description of a person in such a way that she is distinguishable from all other persons and recognisable as an individual

👁️ **Identified:** person who is known, or distinguished from all others in a group

👁️ **Identifiable:** person who is not identified yet, but identification is possible

**Directly:** directly from the information in question e.g. name (unique)

**Indirectly:** using combinations of identifiers that allow a person to be singled out from others, eg. age+ job+ hobbies+ work schedule+ photo

Direct Identifiers	Online Identifiers	Indirect Identifiers
Name Address Postal code @ ID number Phone nr	IP address Cookies RFID Tags MAC addresses Advertising IDs Pixel tags Account usernames Device fingerprints	Physical Physiological Genetic Mental Economic Cultural Social Identity

# How can a person be identifiable? § Recital 26



“reasonably  
likelihood”  
of  
identification

- **all means “reasonably likely”** to be used to identify a person, directly or indirectly
  - eg. public registry, reverse directory
- **by the data controller or any person**
  - anyone possessing the means to identify a user will render such a user identifiable
  - eg. ordinary person, investigative journalist, ex-partner, stalker, industrial spie

## Objective factors:

- Cost/time needed for identification, security developments, or changes to the public availability of certain records
  - Purposes
  - Available tools for identification
  - Risk of organizational dysfunctions, eg. breaches of confidentiality duties, technical failures
  - State of the art of technology at the time of processing, and technological developments
- The reasonable likelihood of someone linking any piece of information to another person renders more plausible because combining databases becomes daily practice, permits to distinguish and allows for the identification of a person (intelligence agencies, ‘smart city’ municipalities, ML algorithms, etc)

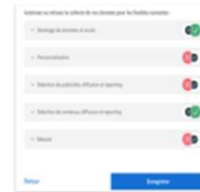
# How can we understand when consent is compliant?



**Providers of intermediate services**



**Third-party Web Tracking companies**



**Consent Management Platforms**



**Website Publishers**

**Easy and simple... just read the GDPR**



# You need to be an expert!

<https://techreg.org/index.php/techreg/article/view/43>



Consent must be:

1. Prior to any data collection
2. Freely given
3. Specific
4. Informed
5. Unambiguous
6. Readable and accessible
7. Revocable



consent, cookie banners, GDPR, ePrivacy Directive, web tracking technologies

c.teixeirasantos@uu.nl  
natalia.bielova@inria.fr  
celestin.matte@cmate.me

In this paper, we describe how cookie banners, as a consent mechanism in web applications, should be designed and implemented to be compliant with the ePrivacy Directive and the GDPR, defining 22 legal requirements. While some are provided by legal sources, others result from the domain expertise of computer scientists. We perform a technical assessment of whether technical (with computer science tools), manual (with a human operator) or user studies verification is needed. We show that it is not possible to assess legal compliance for the majority of requirements because of the current architecture of the web. With this approach, we aim to support policy makers assessing compliance in cookie banners, especially under the current revision of the EU ePrivacy framework.

## 1. Introduction

The ePrivacy Directive<sup>1</sup> 2002/58/EC, as amended by Directive 2009/136/EC, stipulates the need for consent for the storage of or access to cookies (and any tracking technology, e.g. device fingerprinting) on the user's terminal equipment, as the lawfulness ground, pursuant to Article 5(3) thereof. The rationale behind this obligation aims to give users control of their data. Hence, website publishers processing personal data are duty-bound to collect consent. Consequently, an increasing number of websites now display (cookie) consent banners.<sup>2</sup>

However, there is no established canonical form for the consent request. It is clear from Recital 17 of the ePrivacy Directive (hereinafter ePD) that a user's consent may be given by any appropriate method. Website operators are free to use or develop consent flows that suit their organization, as long as this consent can be deemed

valid under EU legislation.<sup>3,4</sup> As such, excessive focus is being placed on the manufacturing of consent, taken up by consent management platforms and tools. The most well-known way to collect consent is through "cookie banners", also often referred to as *prompts*, *overlays*, *cookie bars*, or *cookie pop-up boxes* that pop up or slide atop websites prominently.<sup>5</sup> Their design and functionality differ – the simplest banners merely state that the website uses cookies without any option, whereas the most complex ones allow users to individually (de)select each third-party service used by the website.

Amid information overload and the development of manipulative dark patterns<sup>6, 7</sup> that lead to nudging users to consent, data subjects are

<sup>1</sup> In this paper we will only refer to the recent amended version of the ePrivacy Directive, the Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance) OJ L 337, 11–36 (hereinafter named "ePD").

<sup>2</sup> Jannick Sørensen, Sokol Kostja (2019), "Before and After GDPR: The Changes in Third Party Presence at Public and Private European Websites", *Proceedings of the World Wide Web Conference*, ACM, NY, USA, 1590–1600.

<sup>3</sup> In this paper, we provide many excerpts of the opinions and guidelines of the Article 29 Working Party. For readability and presentation purposes, we convey in the text of the article the abbreviation "29WP", followed by the reference number of each opinion. Even if the European Data Protection Board has endorsed the endorsed the GDPR related WP29 Guidelines, for simplicity purposes, we only mention Article 29 Working Party.

<sup>4</sup> Article 29 Working Party, "Guidelines on consent under Regulation 2016/679" (WP29 rev.0), 10 April 2018.

<sup>5</sup> For example, the French DPA (henceforth named CNIL) decided to remove its cookie banner and to leave no tracer until the user has consented by going actively to the cookie management menu or directly through the content pages. This choice not to use a banner is neither an obligation nor a recommendation for other websites that are free to adopt solutions tailored to their situation, in compliance with Regulations, CNIL (2019), "The legal framework relating to consent has evolved, and so does the website of the CNIL" [www.cnil.fr/en/legal-framework-relating-consent-has-evolved-and-so-does-website-cnil](http://www.cnil.fr/en/legal-framework-relating-consent-has-evolved-and-so-does-website-cnil) accessed 7 May 2020.

<sup>6</sup> Harry Brignall, "What are Dark Patterns?" (2018) <https://darkpatterns.org> accessed 7 May 2020.

<sup>7</sup> Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L.

Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. Cristiana Santos, Nataliia Bielova and Célestin Matte. *International Journal on Technology and Regulation*, 2020.

# How to verify compliance of consent?

## 22 requirements



consent, cookie banners, GDPR, ePrivacy Directive, web tracking technologies

c.teixeirasantos@uu.nl  
natalia.bielova@inria.fr  
celestin.matte@cmat.te

In this paper, we describe how cookie banners, as a consent mechanism in web applications, should be designed and implemented to be compliant with the ePrivacy Directive and the GDPR, defining 22 legal requirements. While some are provided by legal sources, others result from the domain expertise of computer scientists. We perform a technical assessment of whether technical (with computer science tools), manual (with a human operator) or user studies verification is needed. We show that it is not possible to assess legal compliance for the majority of requirements because of the current architecture of the web. With this approach, we aim to support policy makers assessing compliance in cookie banners.

Requirements		Sources at low-level requirement				the paper (e)
High-Level Requirements	Low-Level Requirements	Binding	Non-binding	Interpretation: Legal (L) or Computer Science (CS)		
Prior	R1 Prior to storing an identifier	M (partially)	M (fully)	M (fully)	M (fully)	111
	R2 Prior to sending an identifier					
Free	R3 No merging into a contract	M (fully)	M (fully)	M (fully)	M (fully)	112
	R4 No tracking walls					
Specific	R5 Separate consent per purpose	M (fully)	M (fully)	M (fully)	M (fully)	113
Informed	R6 Accessibility of information page	M (fully) or T (partially) with U	M (fully)	M (fully)	M (fully)	114
	R7 Necessary information on BTT	M (fully) or T (partially)	✓	✓	-	111
	R8 Information on consent banner configuration	M (fully) or T (partially)	-	✓	-	113
	R9 Information on the data controller	M (fully) or T (partially)	✓	✓	-	113
	R10 Information on rights	M (fully) or T (partially)	✓	✓	-	113
	R11 Affirmative action design	Combination of M and T (partially)	✓	✓	-	114
Unambiguous	R12 Configurable banner	M or T (partially)	-	✓	L	115
	R13 Balanced choice	M (fully)	-	✓	L	117
	R14 Post-consent registration	T (partially)	-	✓	CS	118
	R15 Correct consent registration	Combination of M and T (partially)	-	✓	CS	119
	Readable and accessible	R16 Distinguishable	M (fully) or T (partially)	✓	✓	-
R17 Intelligible		U	✓	✓	-	121
R18 Accessible		U	✓	✓	-	121
R19 Clear and plain language		U	✓	✓	-	121
R20 No consent wall		M (fully) or T (partially)	-	✓	L	122
Revocable	R21 Possible to change in the future	M (fully)	✓	✓	-	124
	R22 Delete "consent cookie" and communicate to third parties	Not possible	-	-	CS	125

### Sources at low-level requirement

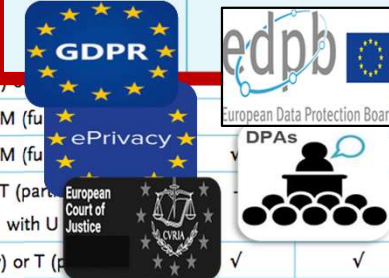
Binding

Non-binding

Interpretation:

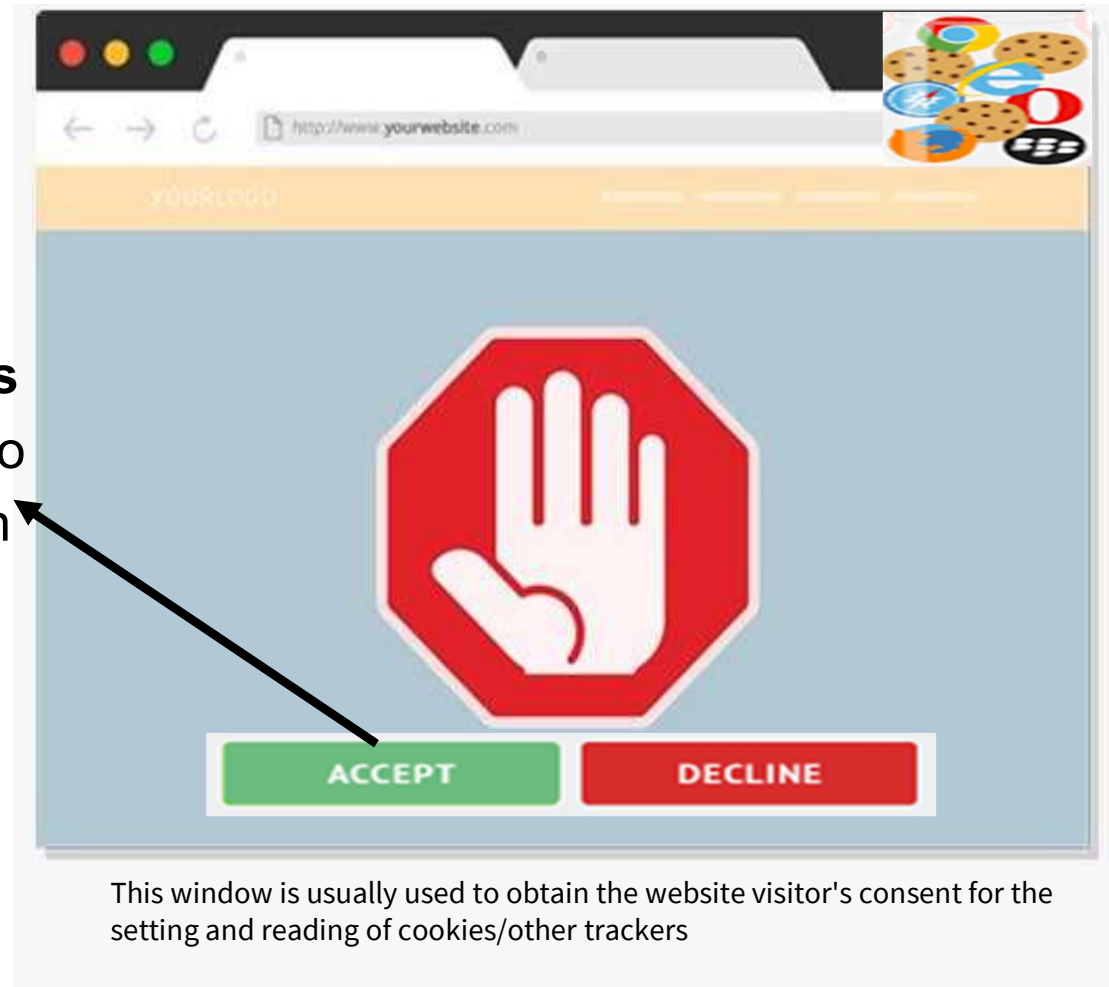
Legal (L) or

Computer Science (CS)



# Consent given through consent banners

**consent banners**  
common method to  
collect consent on  
websites





# Consent must be given prior to storing and sending an identifier



Art. 6: data subject “has given” consent



Consent should be requested to users before cookies/other trackers are set/stored in the **user’s terminal equipment** (those requiring consent)



- PC or laptop
- mobile phone
- IoT internet-connected device on which information may be stored
- toy or a voice-activated assistant

Do not set  
**Cookies**  
before you get  
**Consent**





# Consent must be freely given



Arts. 4(11), 7(4): consent freely given  
Rec. 42: **reject/revoke without detriment**



Rec. 25: access to functionalities cannot be made dependent on consent when not necessary to provide service requested by user



**No pressure, deception, manipulation coercion, significant negative consequences** (extra costs)



Freedom to **reject** non-necessary trackers without detriment







# Consent must be given through an affirmative action

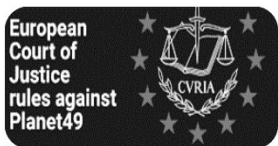


Art. 4(11) "unambiguous indication of wishes by a statement, or by **a clear affirmative action**, expressing agreement to the processing"

Consent must be registered only after an affirmative action of a user, like **clicking on a button, or checking a box**



- No pre-ticked boxes which the user must deselect to refuse consent
- No assumed consent, no silence



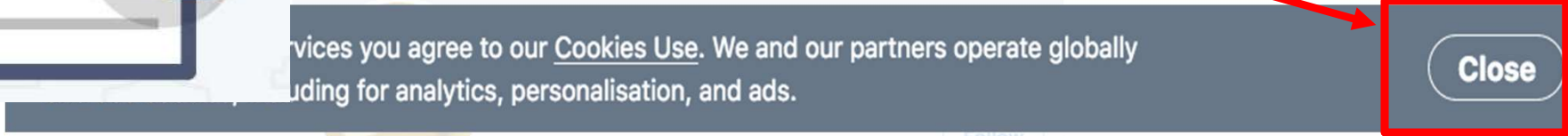




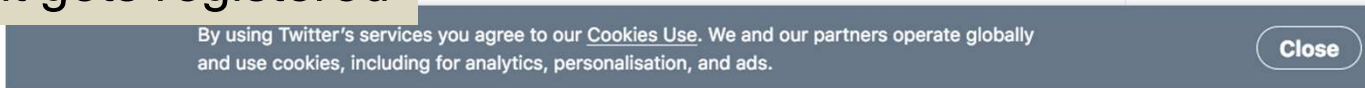
# Violation of Affirmative Action



The only option to close the banner and forcing to consent, does not allow any affirmative action from the user!



Banner disappears and positive consent gets registered



# Reality of non-compliance practices of ...

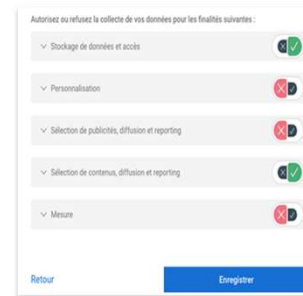


## Providers of intermediate services

Analytics, Google Tag Managers, WordPress, Shopify (eg code, plugins, software)



## Third-party Web Tracking companies



## Consent Management Platforms



## Website Publishers

### Providers of intermediate services



Include

### Third-party Web Tracking

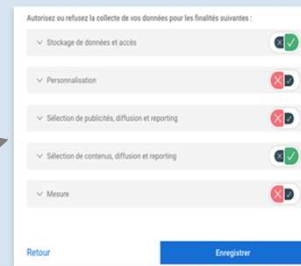


### Compliance solutions

#### CMP Scanners



#### CMPs



Collect user's choice and store in the browser



End User

Visit the website

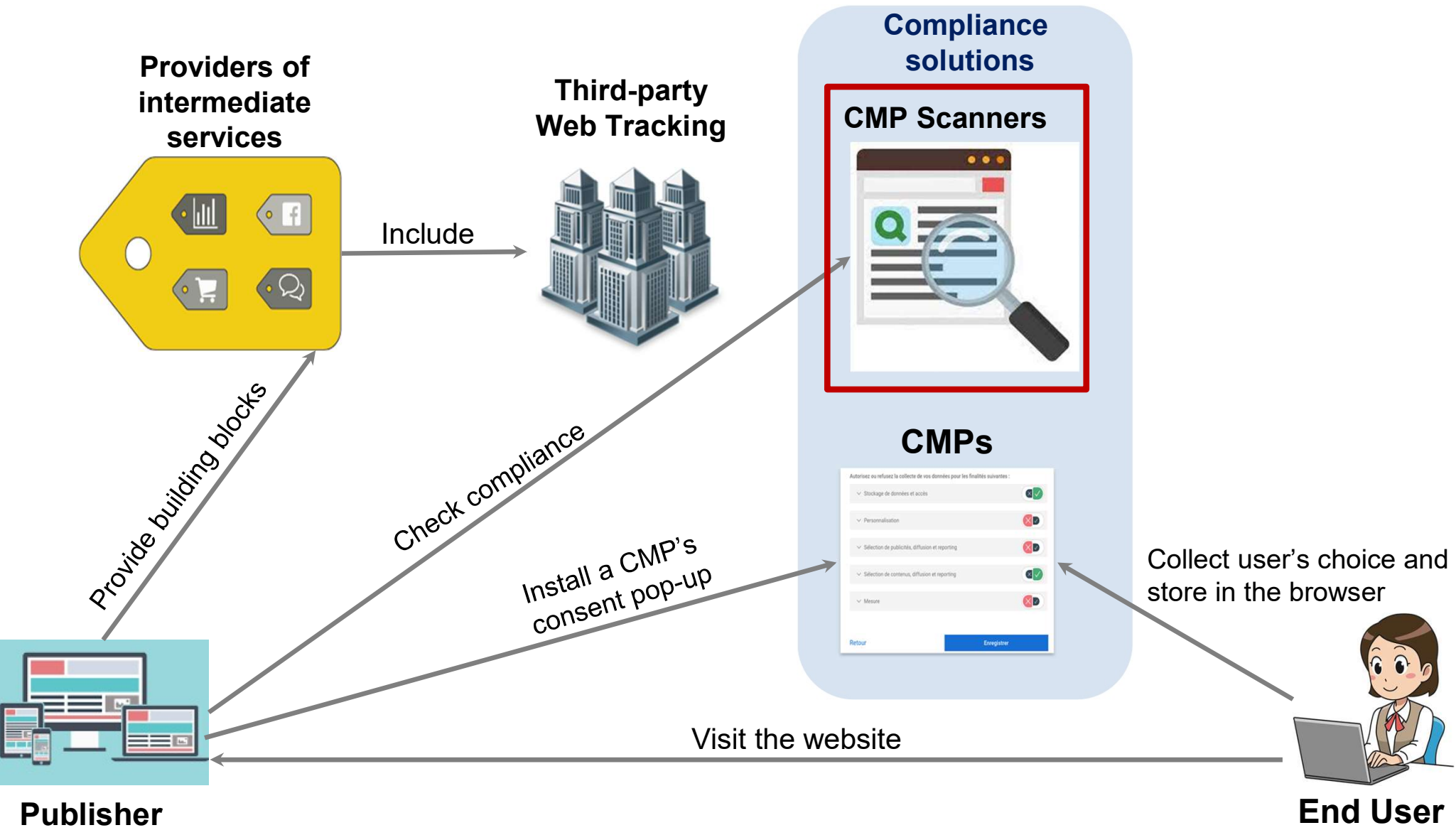
Check compliance

Install a CMP's consent pop-up

Provide building blocks

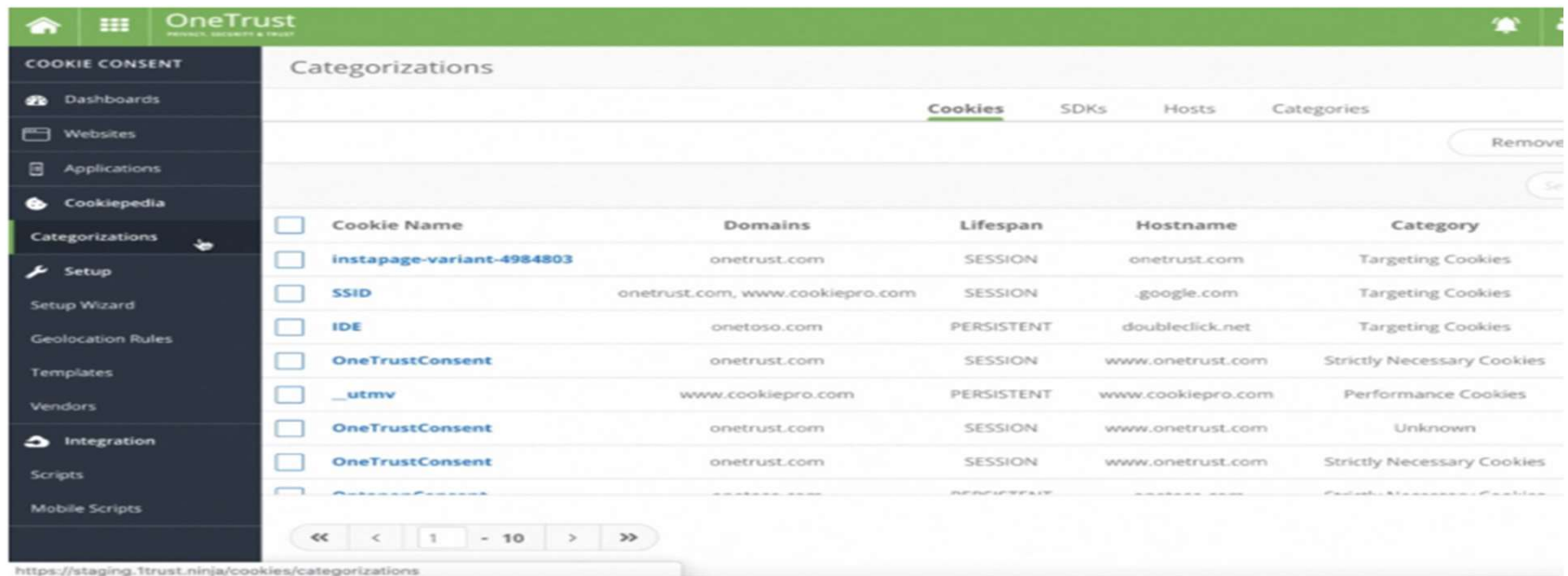


Publisher



# CMP Website scanners

- **False negatives:** only scan cookies, but miss other Web tracking technologies, such as browser fingerprinting - **data processed without legal basis!** [APF'21]



The screenshot shows the OneTrust website scanner interface. The left sidebar contains navigation options: COOKIE CONSENT, Dashboards, Websites, Applications, Cookiepedia, Categorizations (selected), Setup, Setup Wizard, Geolocation Rules, Templates, Vendors, Integration, Scripts, and Mobile Scripts. The main content area is titled 'Categorizations' and has tabs for Cookies, SDKs, Hosts, and Categories. Below the tabs is a table with columns: Cookie Name, Domains, Lifespan, Hostname, and Category. The table lists several cookies, including 'instapage-variant-4984803', 'SSID', 'IDE', 'OneTrustConsent', and '\_utmv'. A pagination control at the bottom shows '1 - 10'.

<input type="checkbox"/>	Cookie Name	Domains	Lifespan	Hostname	Category
<input type="checkbox"/>	instapage-variant-4984803	onetrust.com	SESSION	onetrust.com	Targeting Cookies
<input type="checkbox"/>	SSID	onetrust.com, www.cookiepro.com	SESSION	.google.com	Targeting Cookies
<input type="checkbox"/>	IDE	onetoso.com	PERSISTENT	doubleclick.net	Targeting Cookies
<input type="checkbox"/>	OneTrustConsent	onetrust.com	SESSION	www.onetrust.com	Strictly Necessary Cookies
<input type="checkbox"/>	_utmv	www.cookiepro.com	PERSISTENT	www.cookiepro.com	Performance Cookies
<input type="checkbox"/>	OneTrustConsent	onetrust.com	SESSION	www.onetrust.com	Unknown
<input type="checkbox"/>	OneTrustConsent	onetrust.com	SESSION	www.onetrust.com	Strictly Necessary Cookies
<input type="checkbox"/>	...	...	...	...	...

[APF 2021] Consent Management Platforms under the GDPR: processors and/or controllers? Cristiana Santos, Midas Nouwens, Michael Toth, Nataliia Bielova, Vincent Roca. *Annual Privacy Forum, 2021.*

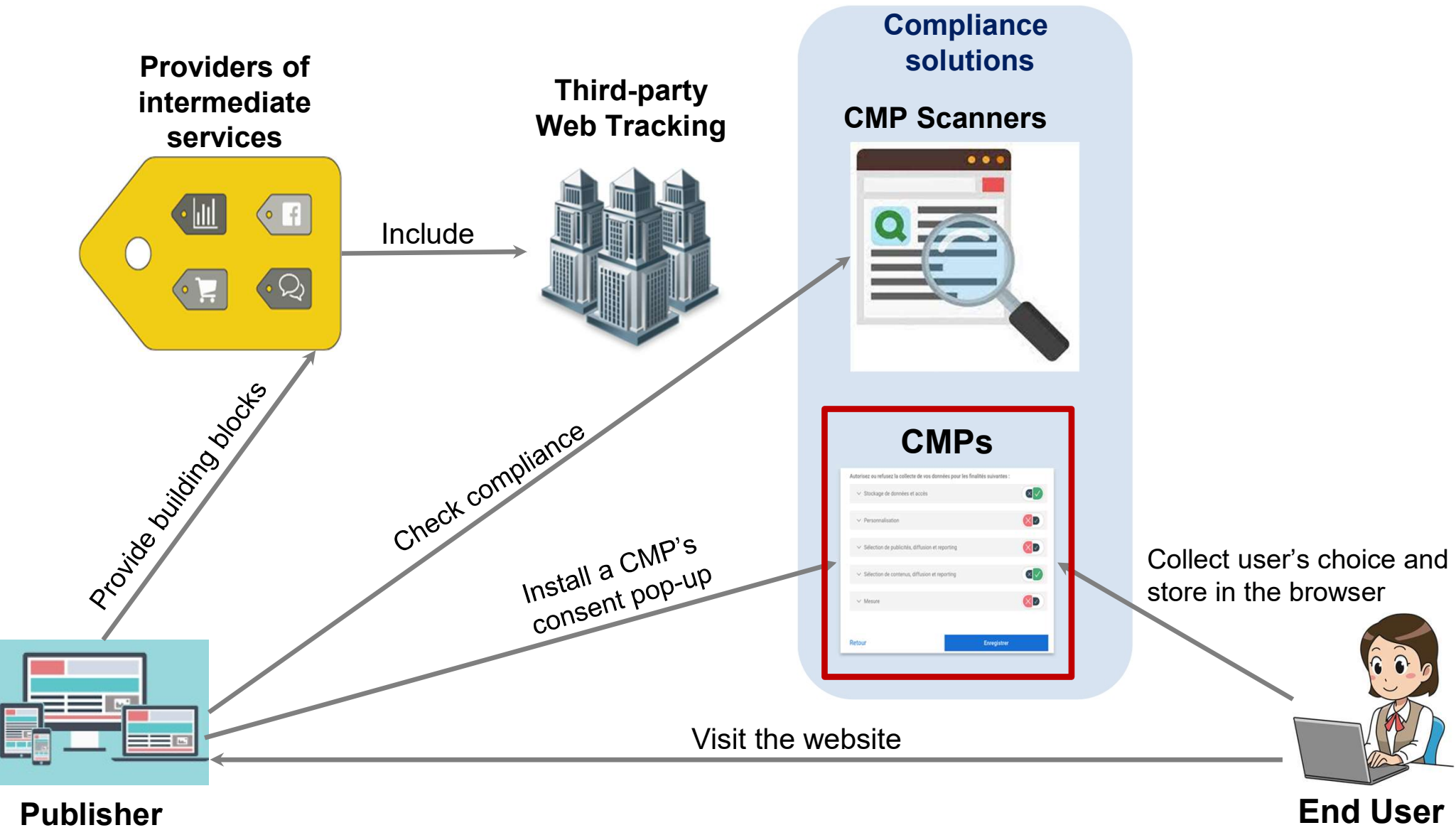
# CMP Website Scanners

- **False positives:** deceive Website Publishers stating in the report page that a consent banner is needed on an empty website without trackers!  
[PoPETS'22]




**“Add cookie compliance!”**





# CMPs/Publishers don't respect users' choice

[IEEE S&P'20]			[ACM CHI'21]	
Number of websites with violation	Suspected violation 	Description	Number of websites analysed	<b>DARK PATTERNS</b>
27 (5.3%)	<b>Non-respect of choice</b>	The pop-up stores a positive consent even when the user <b>refused</b> consent.	508	Sneaking
141 (9.9%)	<b>Consent stored before choice</b>	A positive consent stored <b>before</b> the user made their choice. When advertisers (up to 600 of them!) request for consent, the consent pop-up responds with “user accepts”.	1,426	Sneaking
38 (6.8%)	<b>No way to opt out</b>	The pop-up does not offer a way to refuse consent.	560	Obstruction
236 (46.5%)	<b>Pre-selected choices</b>	Some of the purposes or advertisers are pre-selected: pre-ticked boxes or sliders set to “accept”.	508	Pre-selection

[IEEE S&P'20] Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. Célestin Matte, Nataliia Bielova, Cristiana Santos. *IEEE Symposium on Security and Privacy, 2020.*

[ACM CHI'21] Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. Colin M. Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, Damian Clifford. ACM CHI Conference on Human Factors in Computing Systems, 2021.

# CMPs track website users by themselves!

## Quantcast

We value your privacy


Our site is supported by advertising and we and our partners use technology such as cookies on our site to personalize content and ads, provide social media features, and analyze our traffic. Click "I Accept" below to consent to the use of this technology across the web. You can change your mind and change your consent choices at any time by returning to this site and clicking the Privacy Choices link.

By choosing I Accept below you are also helping to support our site and improve your browsing experience.

I DO NOT ACCEPT

I ACCEPT

[More Options](#) | [See Vendors](#)

Powered by  Quantcast

The QuantCast CMP on <https://sourceforge.net> as of September 2019.

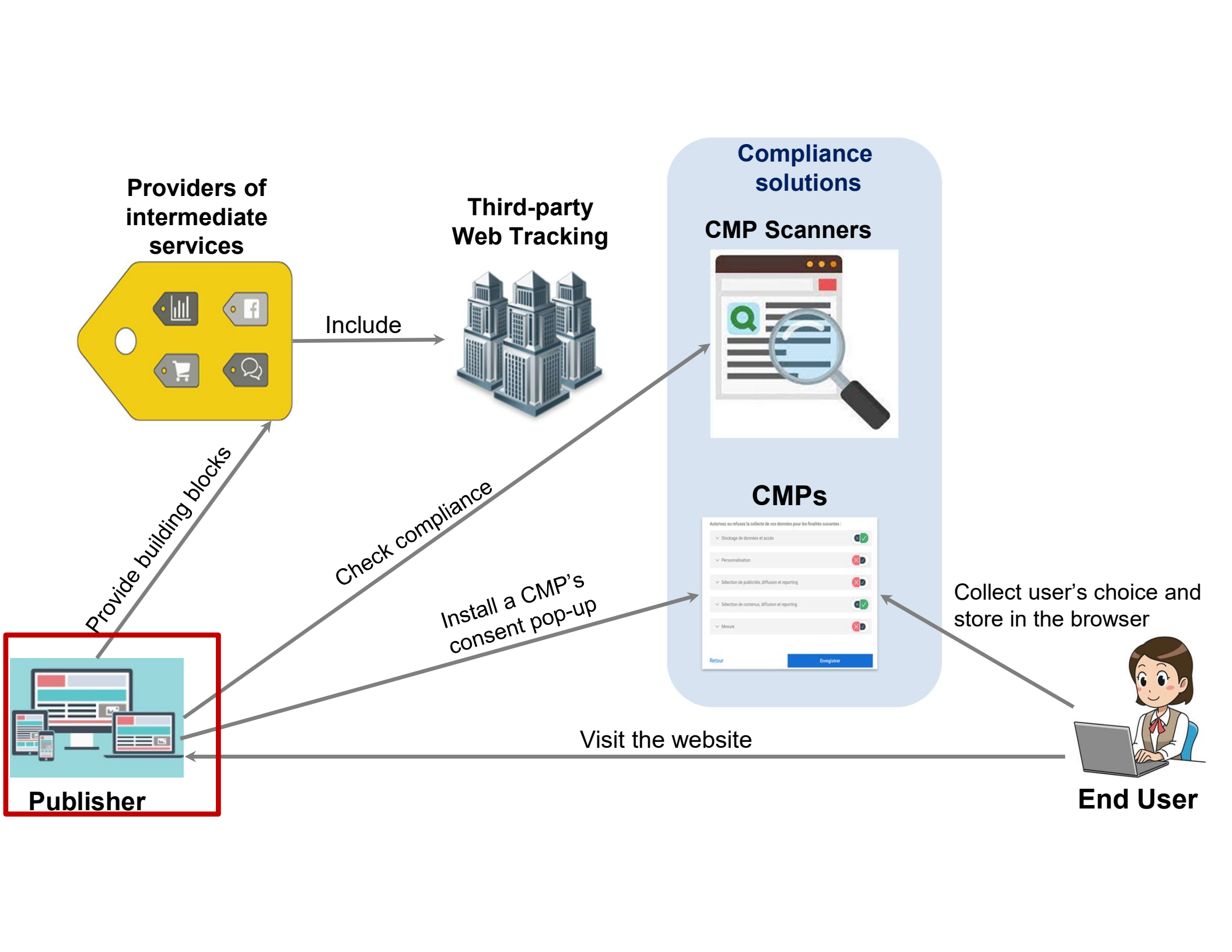
```

```



**QuantCast script installs a consent banner + sets and sends QuantCast cookie to its server without a legal basis**

[APF 2021] [Consent Management Platforms under the GDPR: processors and/or controllers?](#) Cristiana Santos, Midas Nouwens, Michael Toth, Natalia Bielova, Vincent Roca. *Annual Privacy Forum, 2021.*



Do you remember the dream of not paying to have access to a website or platform?





# Der Standard

<https://www.derstandard.at/consent/tcf>

## Willkommen bei DERSTANDARD

### Mit Werbung weiterlesen

Nutzen Sie derStandard.at mit Ihrer Zustimmung zur Verwendung von Cookies für Webanalyse und personalisierte Werbemaßnahmen.

Details finden Sie in der Datenschutzerklärung.

EINVERSTANDEN

Continue reading with ads. Use derStandard.at with your consent to the use of cookies for web analytics and personalized advertising. Details can be found in the privacy policy. **I agree**

### derStandard.at PUR

Das Abo für derStandard.at ganz ohne Werbung und Daten-Tracking auf allen Endgeräten. Jederzeit monatlich kündbar.

JETZT ABONNIEREN

"Subscribe to derStandard.at without any advertising or data tracking on all devices. It can be cancelled monthly at any time. **Subscribe now.**"

To access DS you either

- give **consent** to tracking, or
- **pay** to access that website

Now the first month for EUR 1.00, then EUR 8.00 per month

Continue



## Cookie Paywalls: consent should be freely given, but there is room for interpretation...



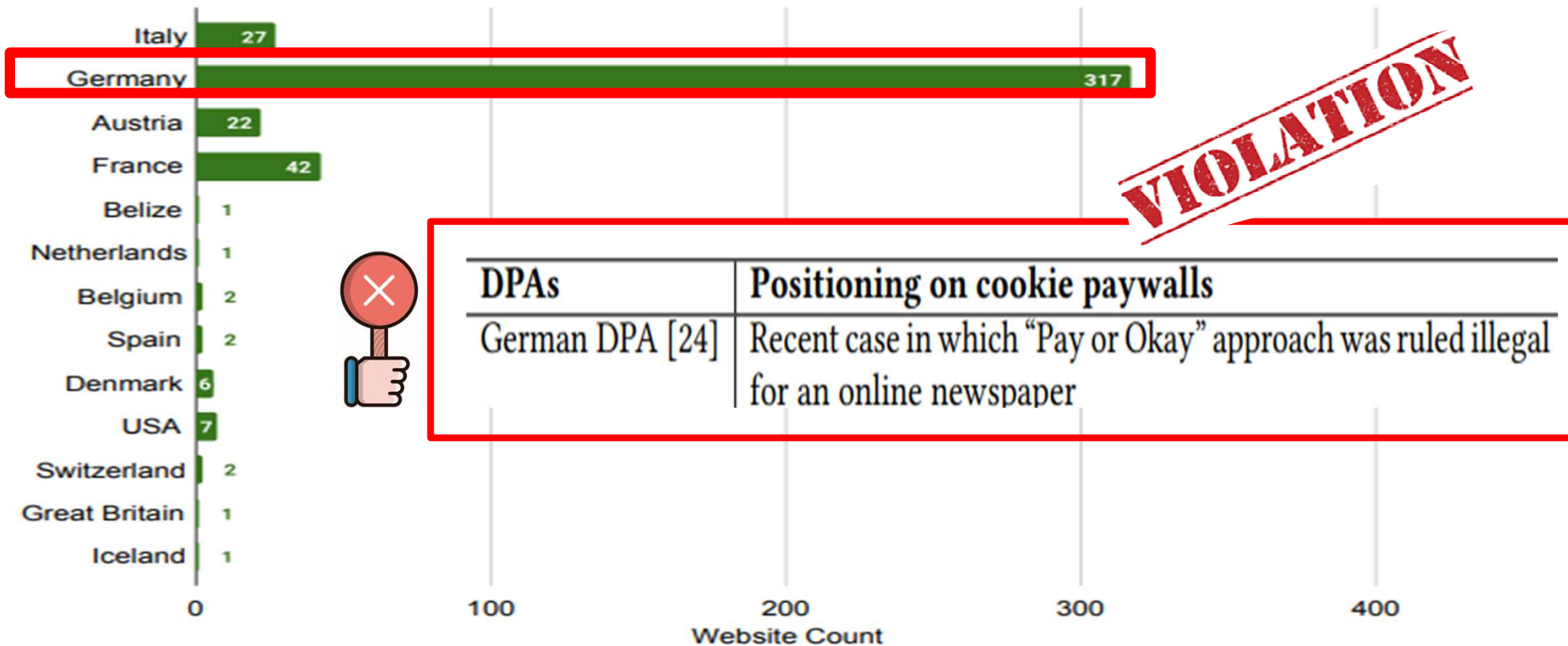
DPAs	Positioning on cookie paywalls
German DPA [24]	Recent case in which “Pay or Okay” approach was ruled illegal for an online newspaper
Spanish DPA [1]	Guidelines state that access cannot be conditioned to consent to cookies, but exceptions can be made if alternatives are offered (not necessarily free ones) and users informed
French DPA [6]	Case by case assessment. Websites need to show there is a real and fair alternative way to access other websites without tracking; reasonable price; fair remuneration
Austrian DPA [12]	Dual position: Recent decision: paywalls are generally permissible, but users must have the possibility to say “yes” or “no” to any specific data processing.

**[WPES'23]** Victor Morel, Cristiana Santos, Viktor Fredholm, Adam Thunberg, Legitimate Interest is the New Consent--Large-Scale Measurement and Legal Compliance of IAB TCF Paywalls



# Paywalls prevalent in Germany and France

Distribution of geographical website basis



**VIOLATION**



[WPES'23] Legitimate Interest is the New Consent – Large-Scale Measurement and Legal Compliance of IAB Europe TCF Paywalls. Victor Morel, Cristiana Santos, Viktor Fredholm, and Adam Thunberg. 2023

# Personalized pricing of paywalls?




## Websites present different versions when visited:

- on different **browsers**
- or via a different **OS**
- or with different **IPs**



<https://dennikn.sk/>  
= OS and IP

**Chceme vám zobrazovať Denník N a reklamy v rovnakej podobe ako doteraz, podľa zákona preto potrebujeme váš súhlas na:**

-  Personalizované reklamy a obsah, meranie reklamy a obsahu, štatistiky cieľových skupín a vývoj produktov
-  Uchovávanie a/alebo prístup k informáciám na zariadení
-  Ďalšie informácie

Vaše osobné údaje budú spracované a informácie z vášho zariadenia (súbory cookie, jedinečné identifikátory a ďalšie údaje zariadenia) môžu byť uchovávané, používané a zdieľané s **odávateľmi tretích strán**, prípadne používané konkrétne týmto webom alebo aplikáciou.

Niektorí odávatelia môžu spracúvať vaše osobné údaje na základe oprávneného záujmu, proti ktorému môžete vzniesť námietku pomocou možnosti nižšie. Súhlas môžete zrušiť prejením na odkaz v dolnej časti tejto stránky alebo v našich pravidlách ochrany súkromia.

**Súhlas**

[Spravovať možnosti](#)

**Chrome**

„Prišiel akýsi chlapík a vedel všetko, o niekoľko tried prevyšoval ostatných uchádzačov o toto miesto," hovoril o Mečiarovi vtedajší podpredseda vlády Vladimír Ondruš. Čo všetko Mečiar vedel? Podľa spomienok vtedajších aktérov ovládal aj štruktúru ministerstva, ani samotní ľudia z VPN ju tak nepoznali.

Jeden z lídrov VPN, Fedor Gál, si na prvý dojem z Mečiara spomína podobne: „Mal som dojem razantného, rozhodného a rýchleho chlapa. Bol mi sympatický."

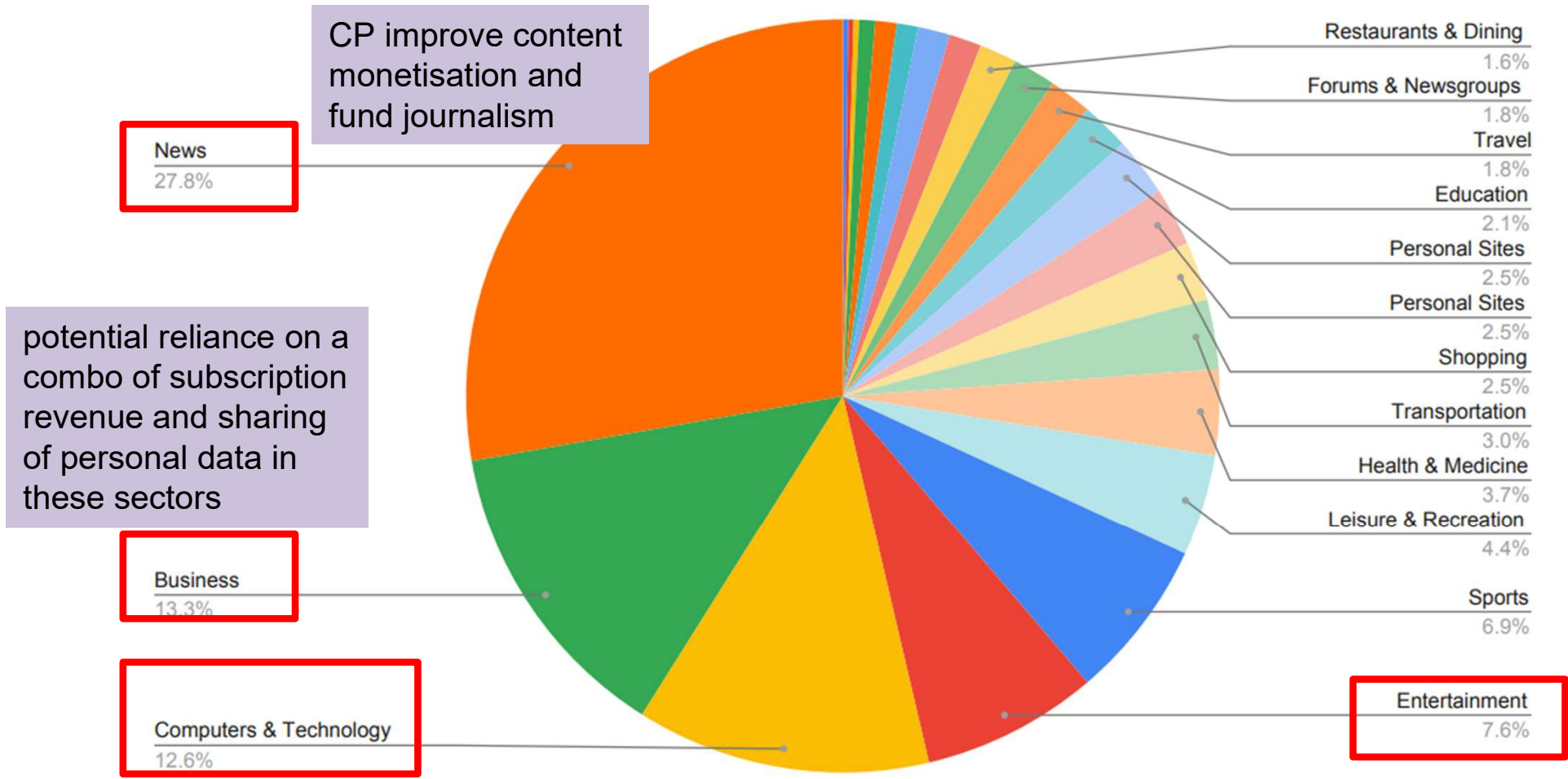
**Tento článok je exkluzívnym obsahom pre predplatiteľov Denníka N.**

Ste predplatiteľom?

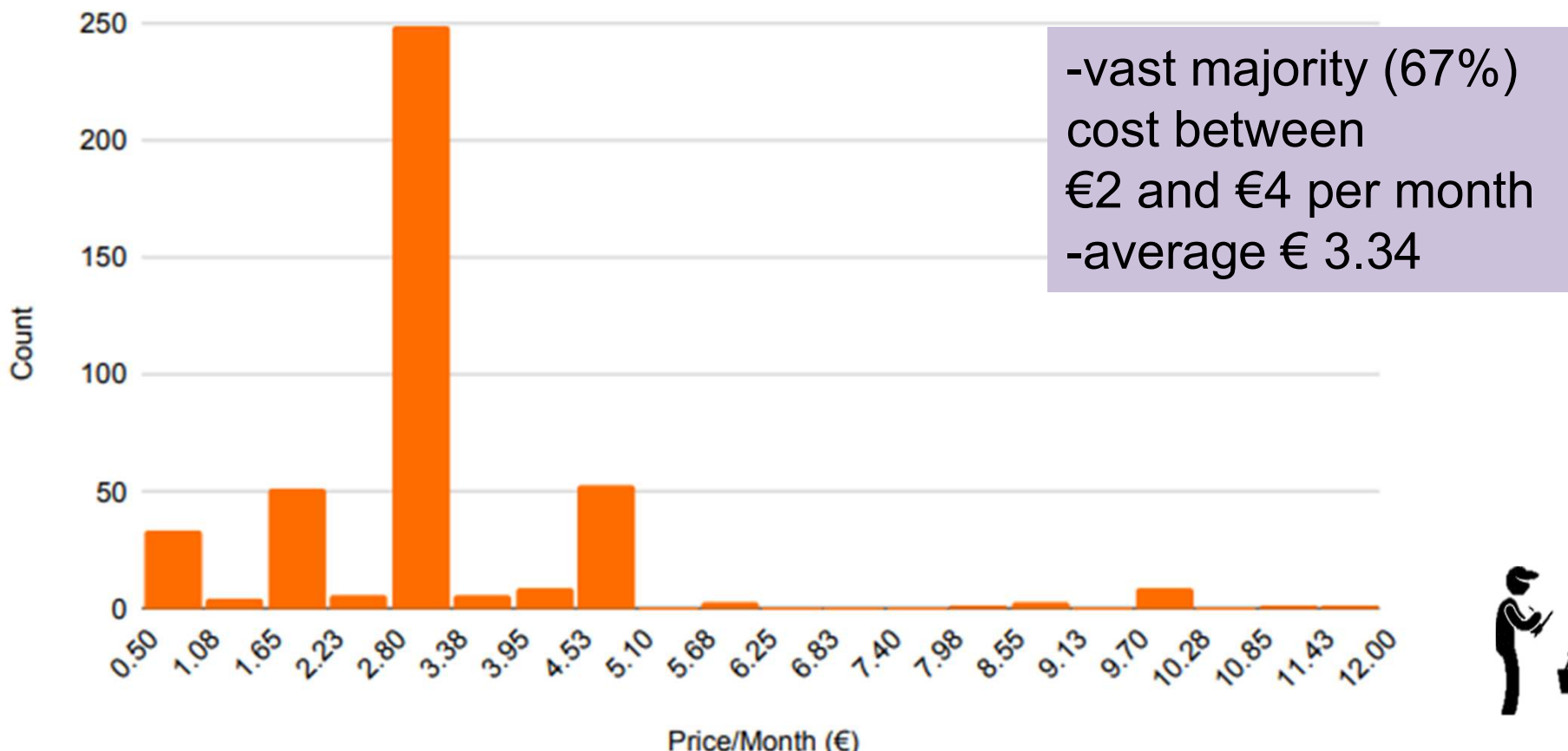
[PRIDAĽTE SA K PREDPLATITEĽOM](#) [PRIHLÁSTE SA](#)

**Firefox**

# Paywall website categories: spread into business, tech, entertainment websites



# Prices: €3.34 on average per website per month

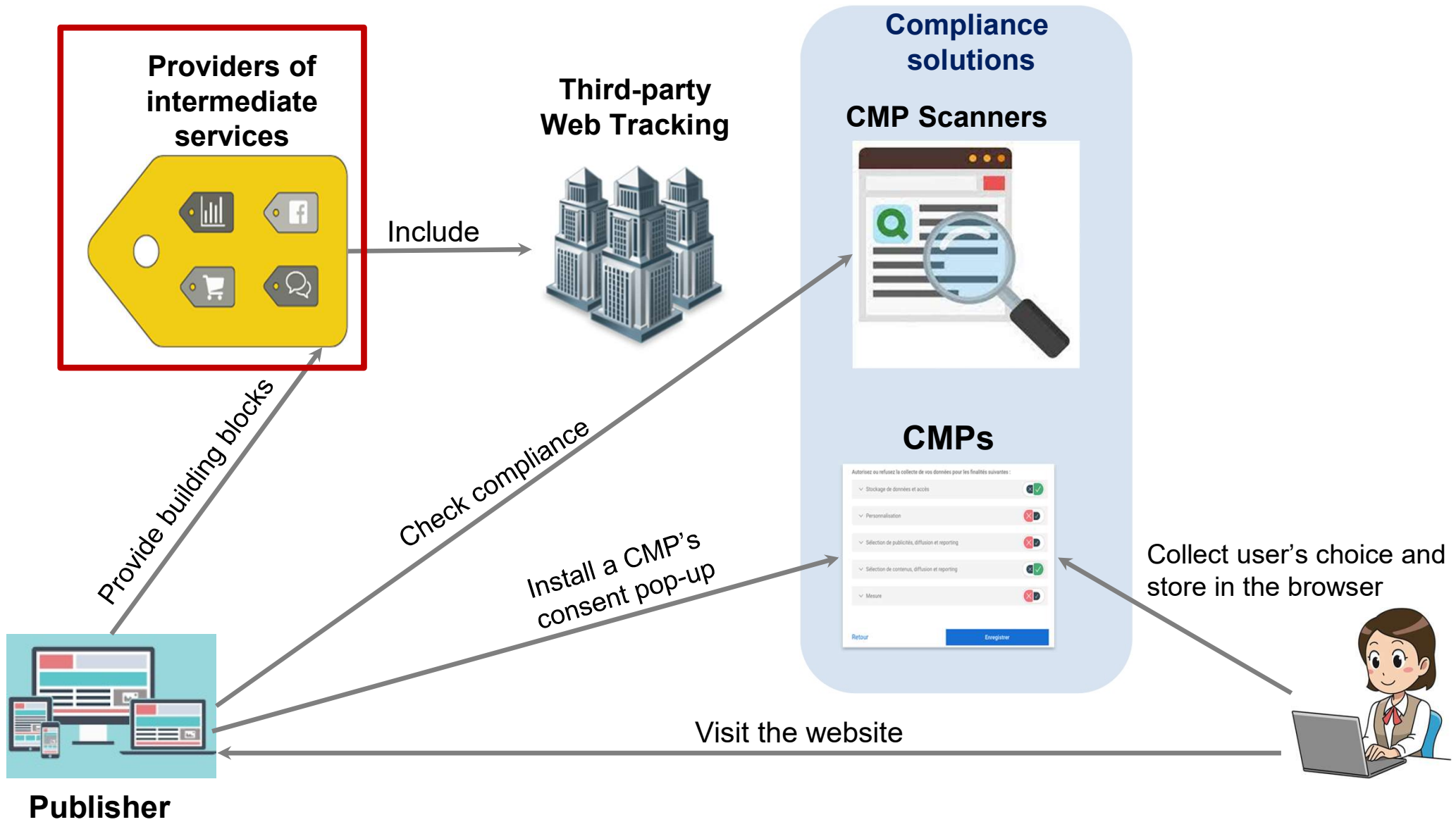


[WPES'22] Victor Morel, Cristiana Santos, Yvonne Lintao, and Soheil Human. 2022. Your Consent Is Worth 75 Euros A Year – Measurement and Lawfulness of Cookie Paywalls.



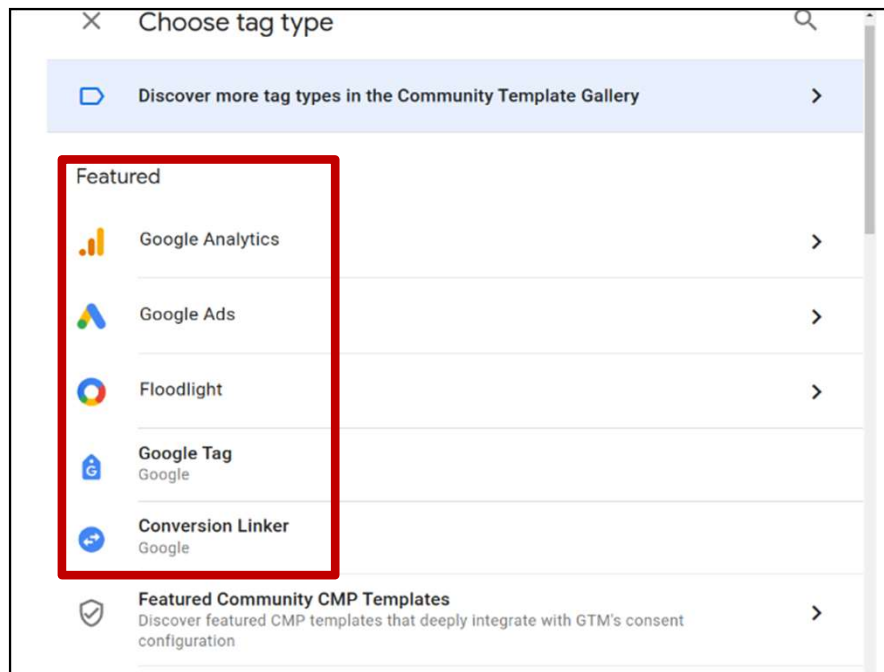
## Violations: you're tracked even when you pay!

- **Data is collected under LI** (14 websites)
  - “Develop and improve products”
- **Purposes under LI are vague and generic** (3 websites)
- **Data collected for advertising purposes under LI** (3 websites)
  - “Select basic ads”, “Measure ad performance”, “Measure content performance”, “Apply market research to generate audience insights”, and “Develop and improve products”

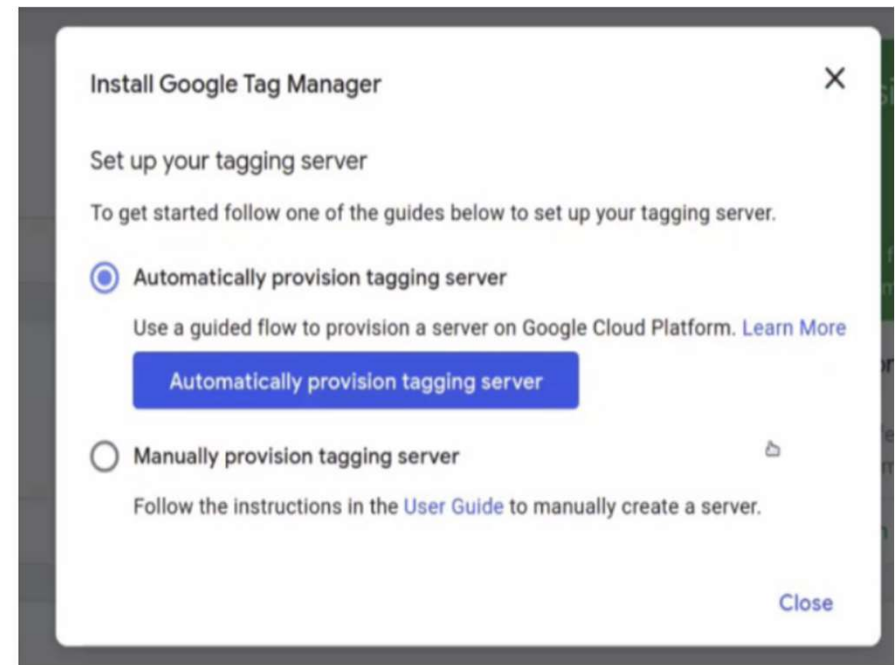


# GTM hides non-Google Tags

- GTM facilitates inclusion of third-party JScripTs for Publishers
- currently present on 28 million websites



interface for tag installation (GTM prioritizes its own natively supported tags vs other tags in template community gallery)

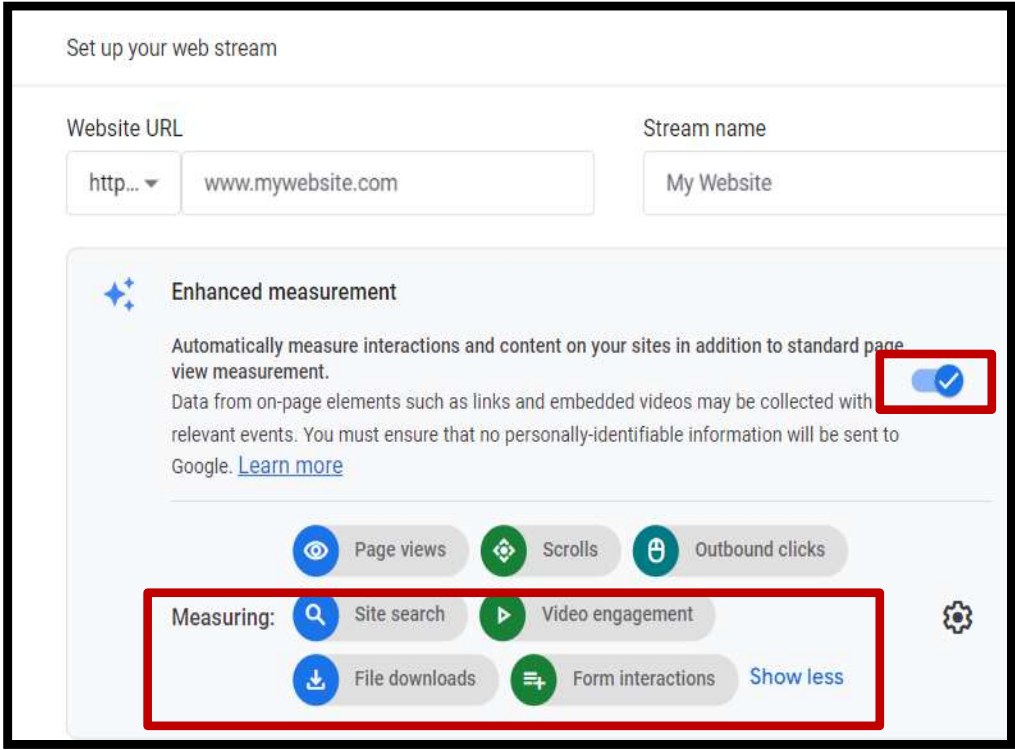
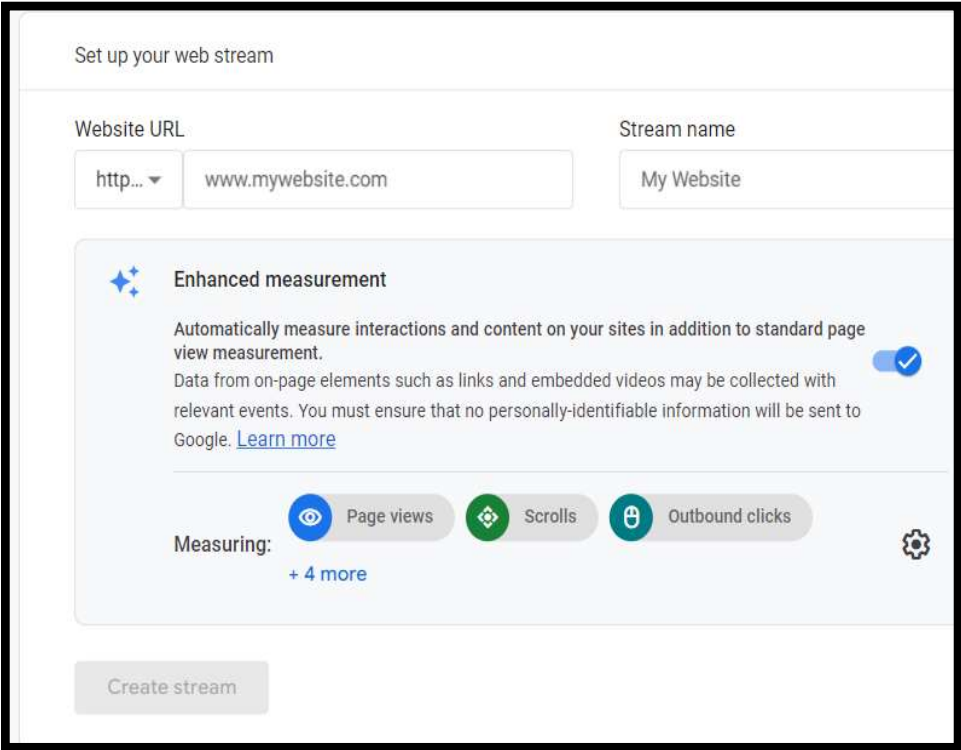


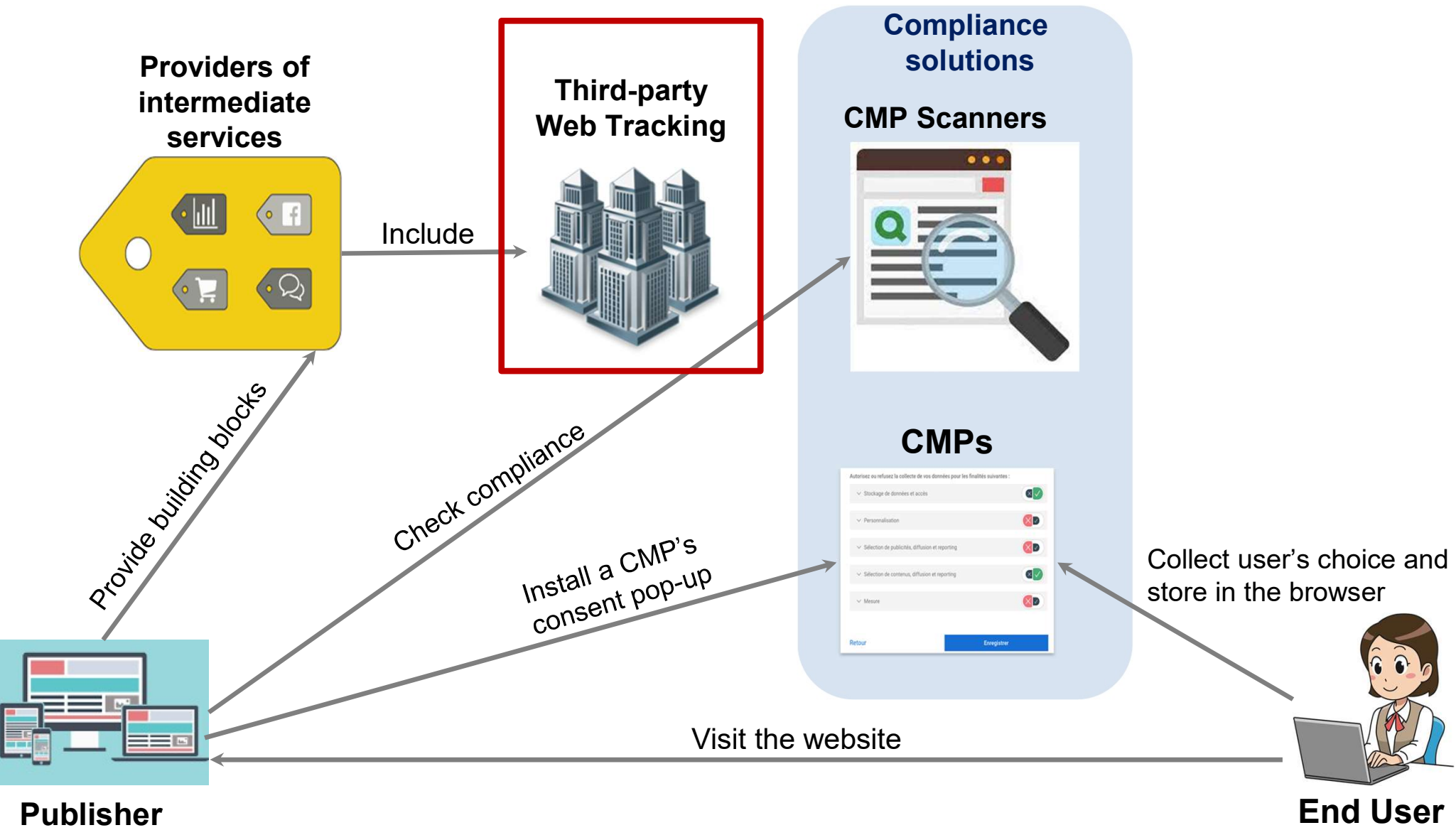
installation step of Google Tag Manager: requires more steps to install tags in the community template gallery!



# Google Analytics

- 3-party JS code monitoring users (mouse moves, clicks) and send statistics to websites. Used by 69% of top 9K websites, has 96% share





# Respawned trackers appeared after being deleted!

- Ability to **store/create user identity** in the browser

- HTTP cookies
- HTTP headers
- browser storages



**Stateful tracking**

- (+) Stable over time
- (-) Storage can be cleaned

- browser fingerprinting:
  - ✓ browser properties
  - ✓ OS properties
  - ✓ IP address...



**Stateless tracking**

- (+) Does not require any storage
- (-) Not stable over time

**1,425 respawned cookies appeared**  
**on 1,105 visited websites**  
**out of 30,000 websites**

Trackers benefit from both  
stateful and stateless tracking!

# Compliance results



- **There is no legal interpretation of cookie deletion!**
- **1,425 respawned cookies violate the fairness principle**
  - Users do not expect that cookies deleted from their browser are respawned
- **130 (out of 336 respawned cookies requiring consent) violate the lawfulness principle**
  - If a cookie is recreated and needs consent, the data collected is illegal due to lack of legal basis
- **Owners of the top 10 popular respawned cookies violate the transparency principle**
  - None of their policies refer to cookie respawning; 5 policies mention browser features without referring its consequences

**Thank you!**  
**Questions?**  
**Suggestions?**



[c.teixeirasantos@uu.nl](mailto:c.teixeirasantos@uu.nl)



[@cristianapt](https://twitter.com/cristianapt)

# Impact of our research

- **Feedback to regulators**

- ✓ **French DPA:** “Cookies and other trackers”
- ✓ **European Data Protection Board (EDPB):** “Concepts of controller and processor in the GDPR”; Data subject requests
- ✓ **Italian DPA (Garante Privacy):** “On the use of cookies and other tracking tools”

- **Our [ACM CHI'2021] paper cited in dark patterns reports**

- **OECD report** on Dark commercial patterns in 2022
- **European Commission** study on unfair commercial practices in the digital environment in 2022
- **UK Competition & Markets Authority** report on Online Choice Architecture in 2022
- **Norwegian Consumer Council** report in 2021



**Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective.** Colin M. Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, Damian Clifford. ACM CHI Conference on Human Factors in Computing Systems (**ACM CHI 2021**).

# References

[APF'2021] Consent Management Platforms under the GDPR: processors and/or controllers?

Cristiana Santos, Midas Nouwens, Michael Toth, Nataliia Bielova, Vincent Roca. Annual Privacy Forum (APF 2021).

[IEEE S&P'20] Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. Célestin Matte, Nataliia Bielova, Cristiana Santos. IEEE Symposium on Security and Privacy (IEEE S&P 2020).

[ASIACCS'19] Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control. Iskander Sanchez-Rola, Matteo Dell'Amico, Platon Kotzias, Davide Balzarotti, Leyla Bilge, Pierre-Antoine Vervier, and Igor Santos. In Proceedings of the 14th ACM Asia Conference on Computer and Communications Security (ACM ASIACCS 2019).

[PoPETS'22] On dark patterns and manipulation of website publishers by CMPs. Michael Toth, Nataliia Bielova, Vincent Roca. Privacy Enhancing Technologies Symposium, (PETs).

[ACM CHI'2021] Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective Colin M. Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, Damian Clifford. ACM CHI Conference on Human Factors in Computing Systems (ACM CHI 2021)