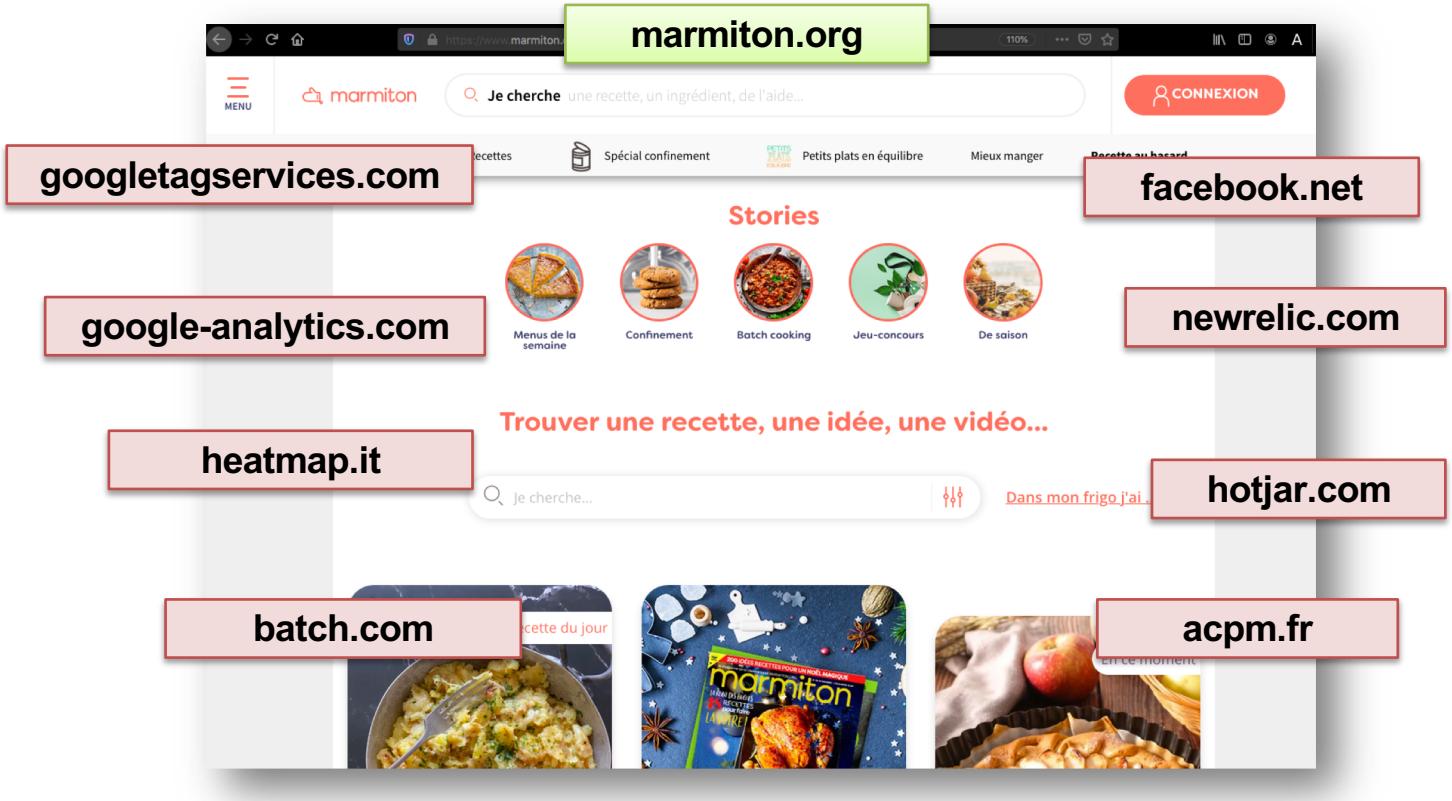
Detecting online tracking and GDPR violations in Web applications

Nataliia Bielova
Researcher in Online Privacy
PRIVATICS team Inria

joint work with Arnaud Legout, Celestin Matte, Cristiana Santos, Imane Fouad

Online tracking



*Website visited on 10 November, 2020

It all started with a seminal work in 2012*…

2012 IEEE Symposium on Security and Privacy

Third-Party Web Tracking: Policy and Technology

Jonathan R. Mayer and John C. Mitchell
Stanford University Stanford, CA
{*jmayer,mitchell*}*@cs.stanford.edu*

***Abstract*—In the early days of the web, content was designed and hosted by a single person, group, or organization. No longer. Webpages are increasingly composed of content from myriad unrelated "third-party" websites in the business of advertising, analytics, social networking, and more. Third-party services have tremendous value: they support free content and facilitate web innovation. But third-party services come at a privacy cost: researchers, civil society organizations, and policymakers have increasingly called attention to how third parties can track a user's browsing activities across websites.**

This paper surveys the current policy debate surrounding third-party web tracking and explains the relevant technology. It also presents the *FourthParty* web measurement platform and studies we have conducted with it. Our aim is to inform researchers with essential background and tools for contributing to public understanding and policy debates about web tracking.

unrelated first-party websites ("third-party web tracking" or "tracking" for short).[3]

This paper is intended to comprehensively familiarize computer security and privacy researchers with current policy and technology research on third-party web tracking. Much of the discussion is based on recent results from a new dynamic web measurement platform, FourthParty. We begin by presenting by FourthParty. The remainder of the paper is organized into two parts on third-party web tracking: one on policy, and one on technology.

The policy part opens by reviewing why third-party web tracking gives rise to privacy concerns and ways in which policy might be structured to address those concerns. It then provides an overview of regulation and self-regulation in

Third-Party Web Tracking: Policy and Technology. Jonathan R. Mayer and John C. Mitchell. IEEE Symposium on Security and Privacy (IEEE S&P), 2012.

*at least for me ☺

Detecting trackers by analyzing behavior of third-party cookies

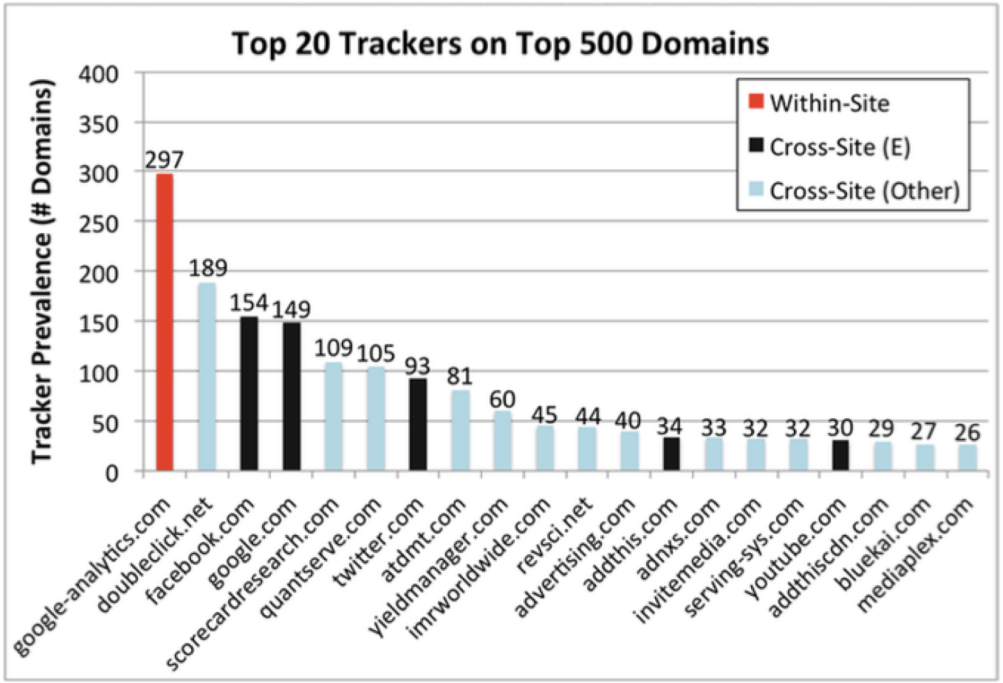
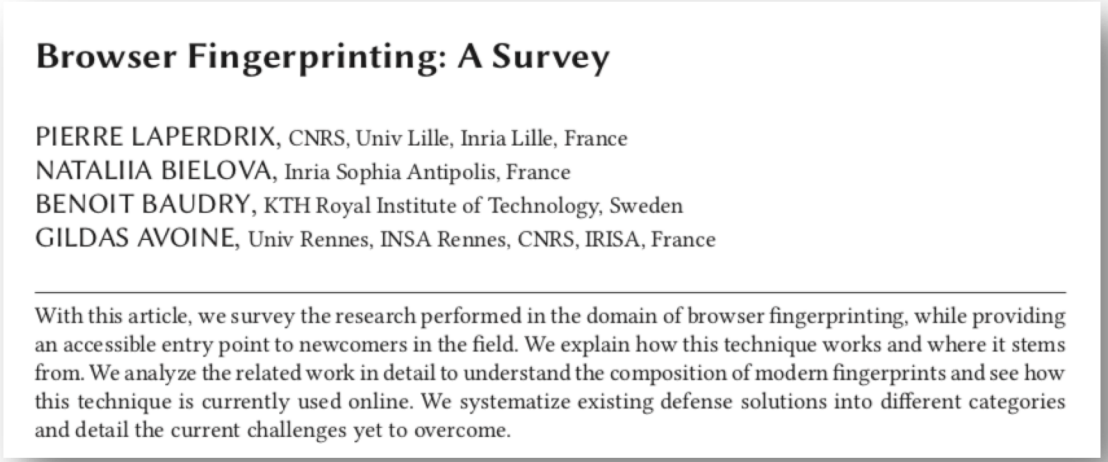


Figure 6: *Prevalence of Trackers on Top 500 Domains.*

Detecting and Defending Against Third-Party Tracking on the Web. Franziska Roesner, Tadayoshi Kohno, and David Wetherall. 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2012.

Research field on Web tracking exploded…

- Researchers were detecting and measuring prevalence of
  - **third party cookies** and unique identifiers stored in them
  - **cookie respawning** with HTML5 localStorage and browser cache (ETag)
  - **cookie synchronization**
  - **browser fingerprinting**
    - ✓ survey at ACM TWEB



Browser Fingerprinting: A Survey

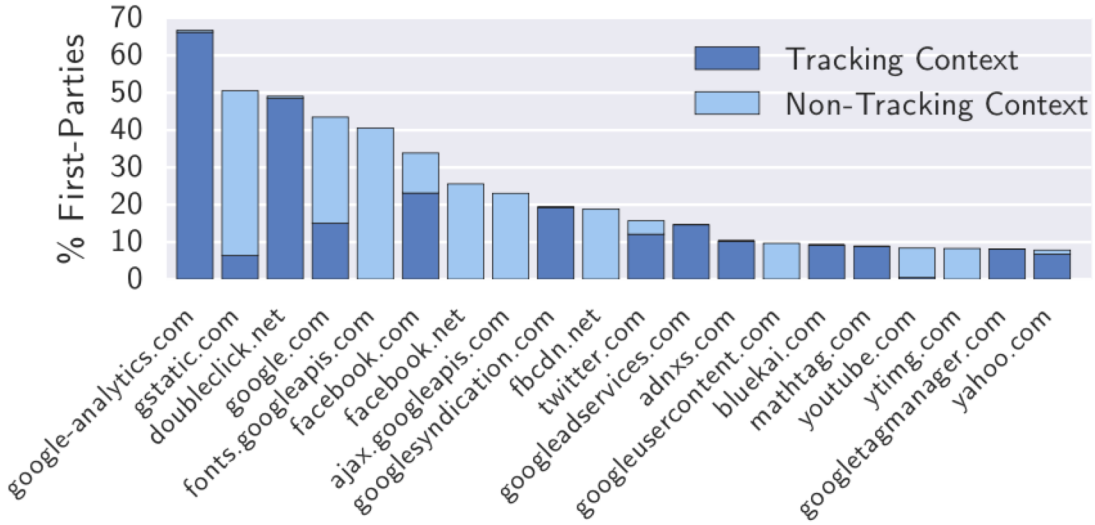
PIERRE LAPERDRIX, CNRS, Univ Lille, Inria Lille, France
NATALIIA BIELOVA, Inria Sophia Antipolis, France
BENOIT BAUDRY, KTH Royal Institute of Technology, Sweden
GILDAS AVOINE, Univ Rennes, INSA Rennes, CNRS, IRISA, France

With this article, we survey the research performed in the domain of browser fingerprinting, while providing an accessible entry point to newcomers in the field. We explain how this technique works and where it stems from. We analyze the related work in detail to understand the composition of modern fingerprints and see how this technique is currently used online. We systematize existing defense solutions into different categories and detail the current challenges yet to overcome.

Browser Fingerprinting: A survey. Pierre Laperdrix, Nataliia Bielova, Benoit Baudry and Gildas Avoine. *ACM Transactions on the Web (ACM TWEB), 2020.*

But most of works detect trackers with filter lists

- 1-million site measurement relied on EasyList & EasyPrivacy lists
- Third party request is a tracker if it matches the rule in the list



Online tracking: A 1-million-site measurement and analysis. S. Englehardt and A. Narayanan. ACM CCS 2016.

EasyList & EasyPrivacy lists

- Only until 2018, most measurement studies detected trackers with EasyList & EasyPrivacy

Paper	Venue	EasyList	EasyPrivacy	Detection	Dependency
Englehardt and Narayanan [24]	ACM CCS 2016	✓	✓	Req.	Rely
Bashir et al. [11]	USENIX Security 2016	✓		Custom.	Rely
Lauinger et al. [30]	NDSS 2017	✓	✓	Req.+Follow	Rely
Razaghpanah et al. [42]	NDSS 2018	✓		Custom.	Rely
Ikram et al. [28]	PETs 2017	✓		Req.+Follow	Verif.
Englehardt et al.[23]	PETs 2018	✓	✓	Req.+Follow	Verif.
Bashir and Wilson [12]	PETs 2018	✓	✓	Custom.	Rely+Verif.
Bashir et al.[10]	IMC 2018	✓	✓	Custom.	Rely
Iordanou et al.[29]	IMC 2018	✓	✓	Req.+Follow	Rely

Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels. Imane Fouad, Nataliia Bielova, Arnaud Legout, Natasa Sarafijanovic-Djukic.To appear in Privacy Enhancing Technologies Symposium (PETS 2020).

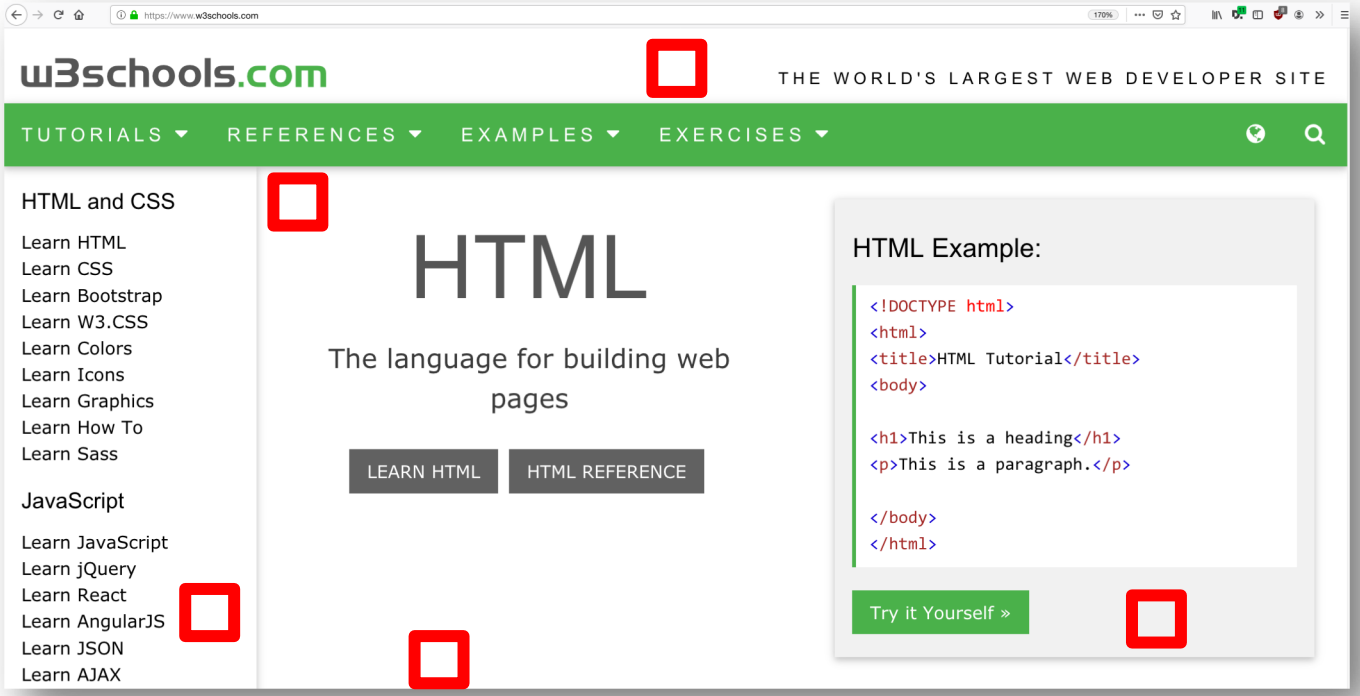
Filter lists are also used in tracking protection

But how many trackers are filter lists detecting?

Do browser extensions miss trackers?

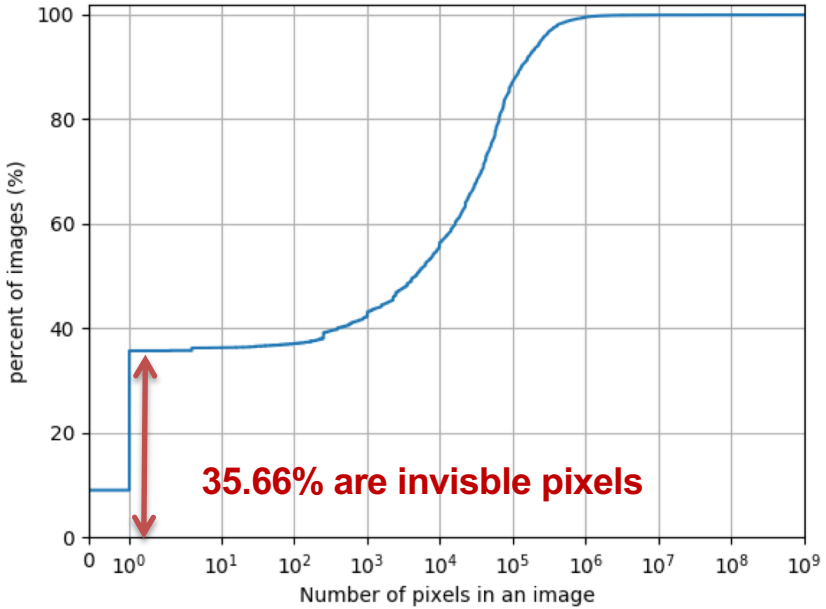
(but what is the ground truth?)

Invisible pixels



Data collection with OpenWPM

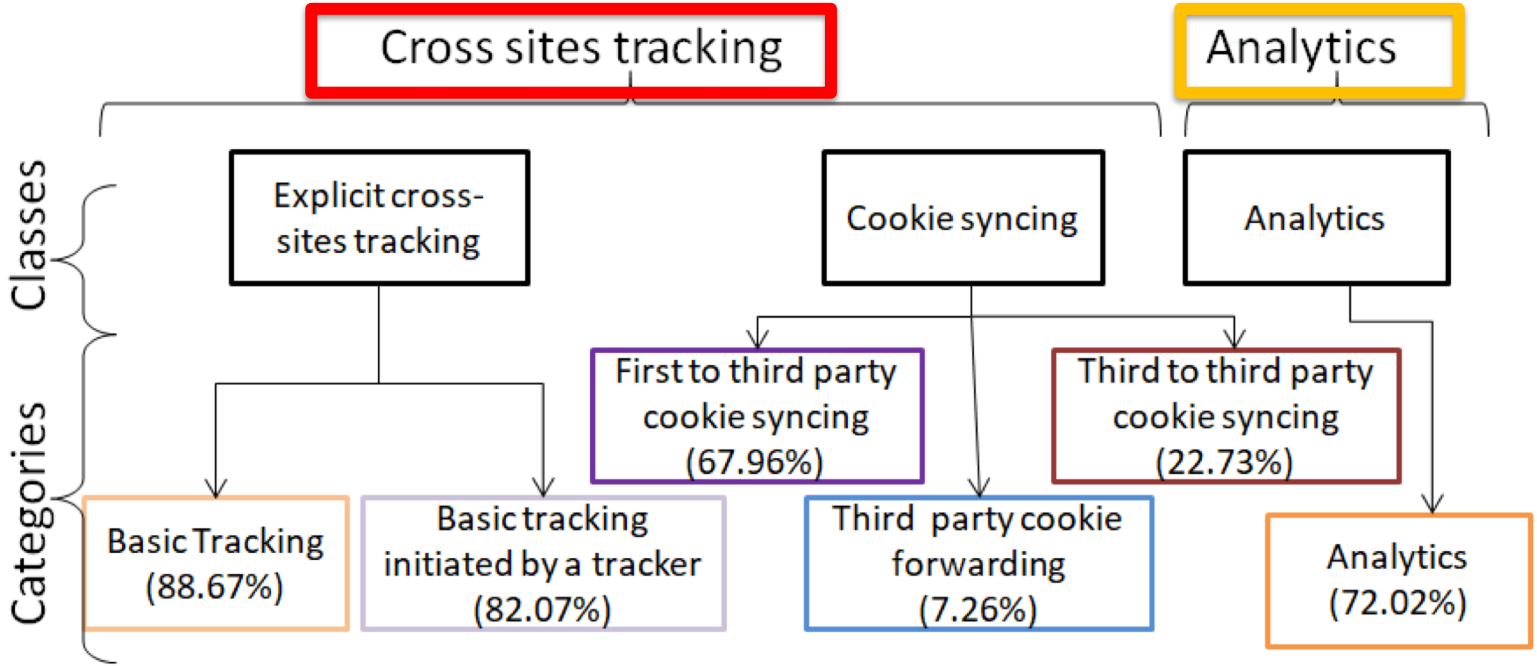
- Crawl Top 10,000 Alexa domains in February 2019
- For each domain we visit
  - Homepage + 10 first links
- Successfully crawled:
  - 8,744 domains, 84,658 pages
- Results:
  - 2,297,716 images <100KB collected
  - **35.66% images are invisible**
  - **95% domains** contain at least one invisible image



Invisible pixels are perfect suspect for tracking and widely present on the Web

Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels. Imane Fouad, Nataliia Bielova, Arnaud Legout, Natasa Sarafijanovic-Djukic.To appear in Privacy Enhancing Technologies Symposium (PETS 2020).

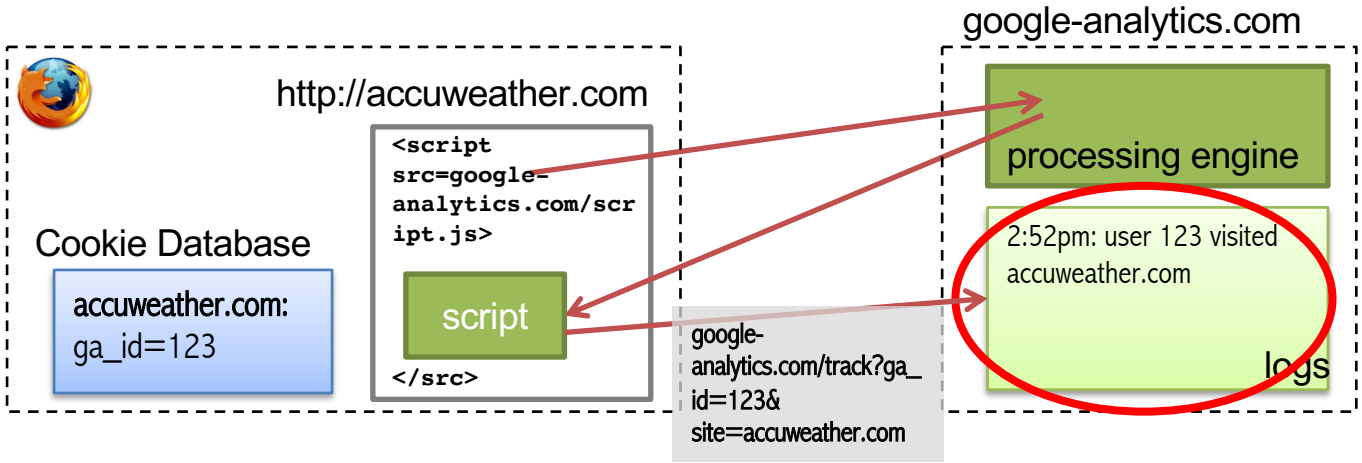
Classification: six cookie-based tracking behaviors



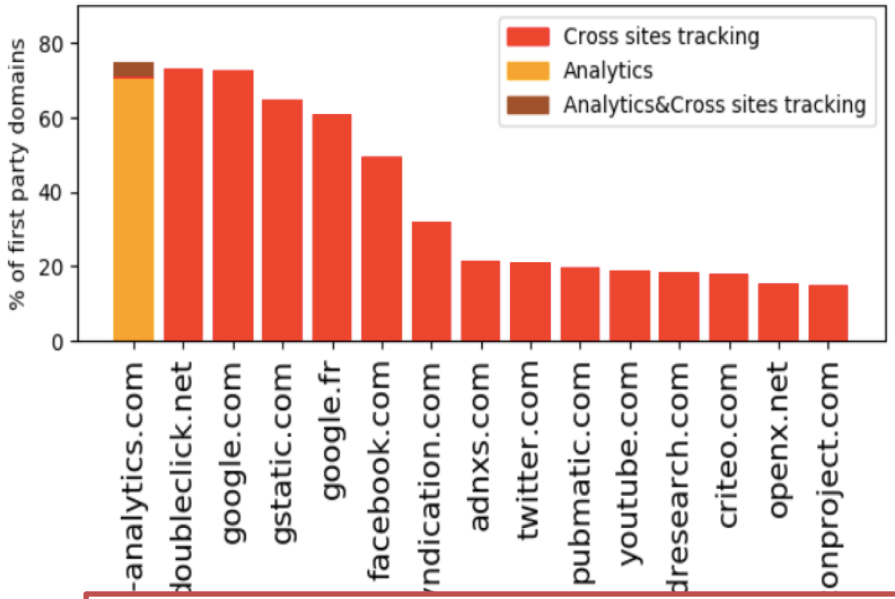
At least one type of tracking found on 92% of domains!

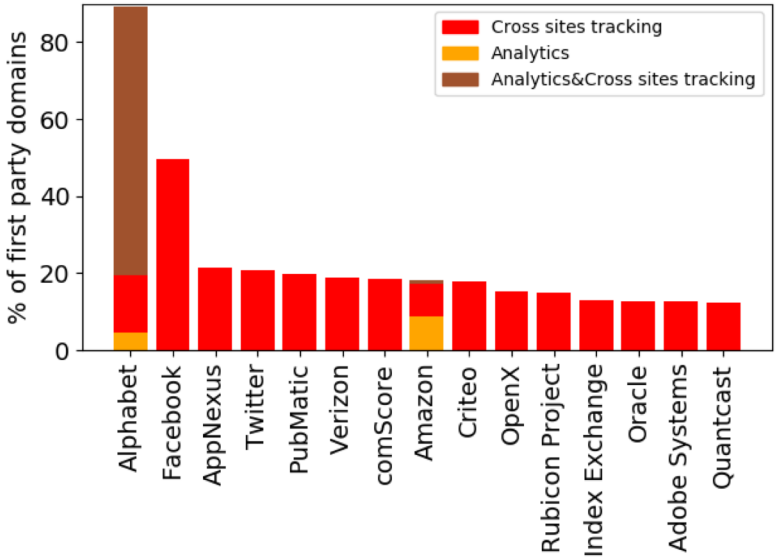
Analytics (within-site tracking only)

- Uses **first-party cookies** to track repeat visits to a site.
- **Is not able** to collect user's browsing history across sites.



Third-party tracking domains and companies





Some third parties combine privacy-invasive tracking and analytics behaviors on the same website!

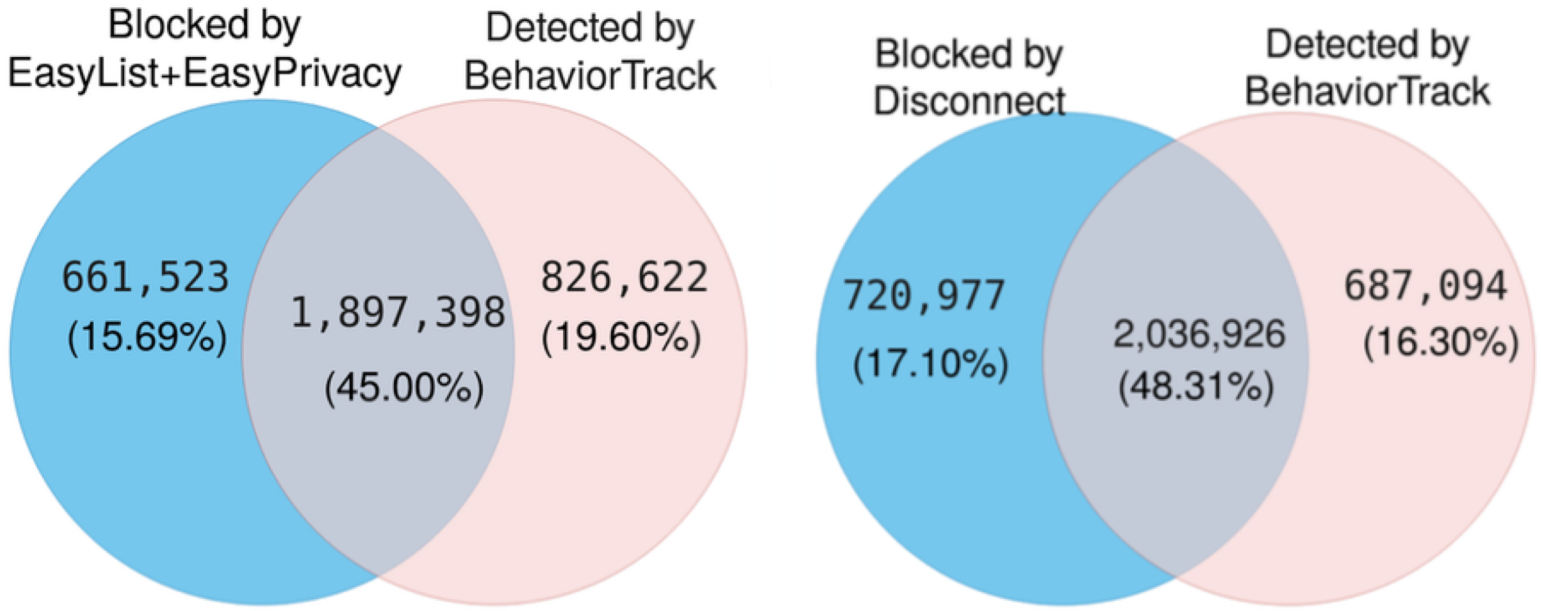
What content is tracking users?

- 4,216,454 third-party requests
- **2,724,020 (64.6%)** third-party requests are tracking

Content type	% requests
Script	34.36%
Invisible images	23.34 %
Text/html	20.01%
Big images	8.54 %
Application/json	4.32%

Top 5 types of content used in the 2,724,020 third-party tracking requests.

Filter lists miss tracking requests



(a) EasyList and EasyPrivacy (b) Disconnect

Effectiveness of filter lists at detecting trackers on 4,216,454 third party requests from 84,658 pages.

How much tracking is missed?

- EasyList&EasyPrivacy and Disconnect together miss third-party trackers on **68.7%** of domains

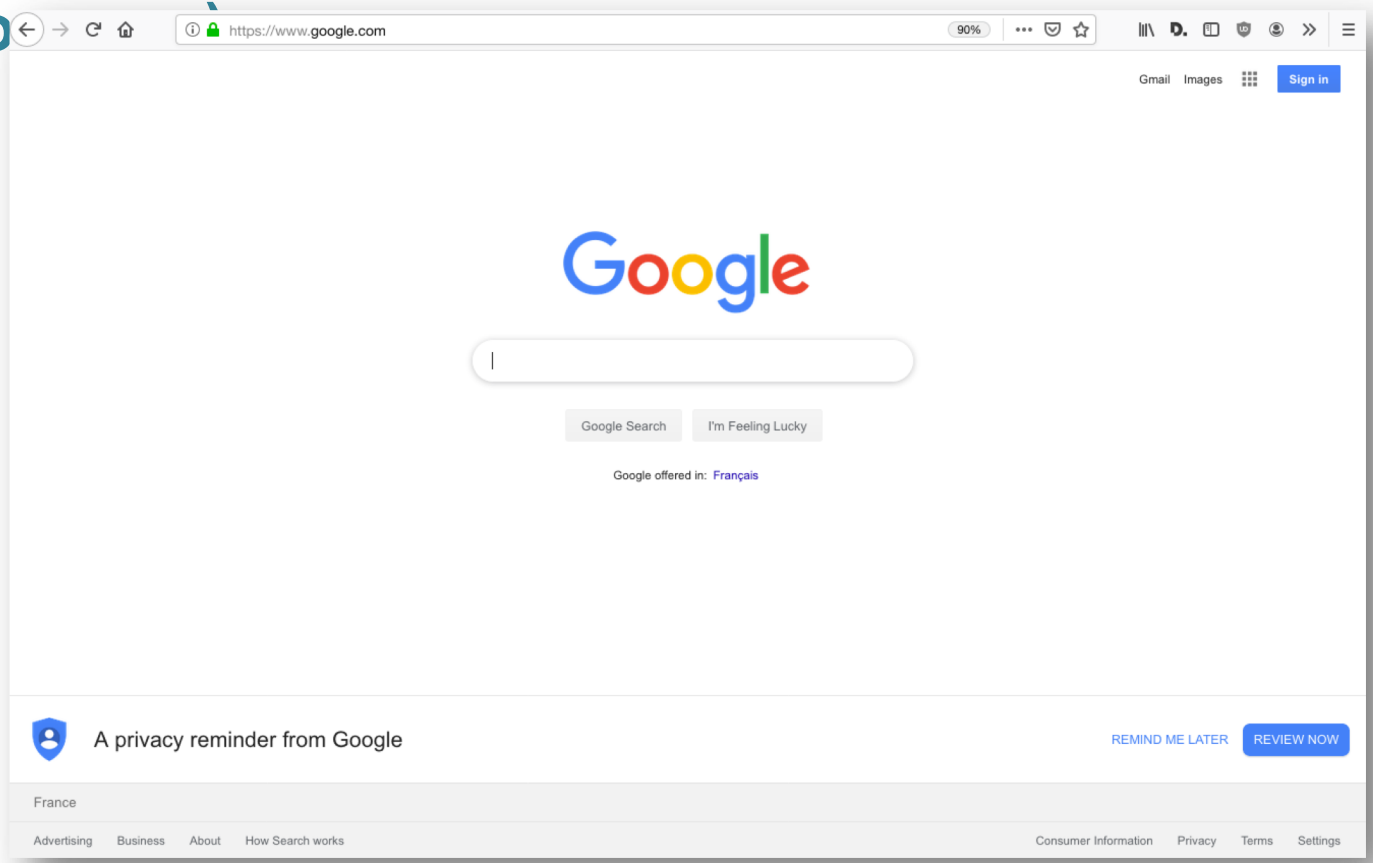
Full domain	Prevalence of tracking in first-parties	Cookie name	Cookie expiration	Category	Company	Country
code.jquery.com	756 (8.65 %)	__cfduid	1 years	Technology/Internet	jQuery Foundation	US
s3.amazonaws.com	412 (4.71 %)	s_fid	5 years	Content Servers	Amazon	US
ampcid.google.com	282 (3.23 %)	NID	6 months	Search Engines	Google LLC	US
cse.google.com	307 (3.51 %)	NID	1 year	Search Engines	Google LLC	US
use.fontawesome.com	221 (2.53 %)	__stripe_mid	1 years	Technology/Internet	WhoisGuard Protected	_
siteintercept.qualtrics.com	99 (1.13 %)	t_uid	100 years	Business/Economy	Qualtrics, LLC	US
push.zhanzhang.baidu.com	98 (1.12 %)	BAIDUID	68 years	Search Engines	Beijing Baidu Netcom Science Technology Co., Ltd.	CN

Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels. Imane Fouad, Nataliia Bielova, Arnaud Legout, Natasa Sarafijanovic-Djukic.To appear in Privacy Enhancing Technologies Symposium (PETS 2020).

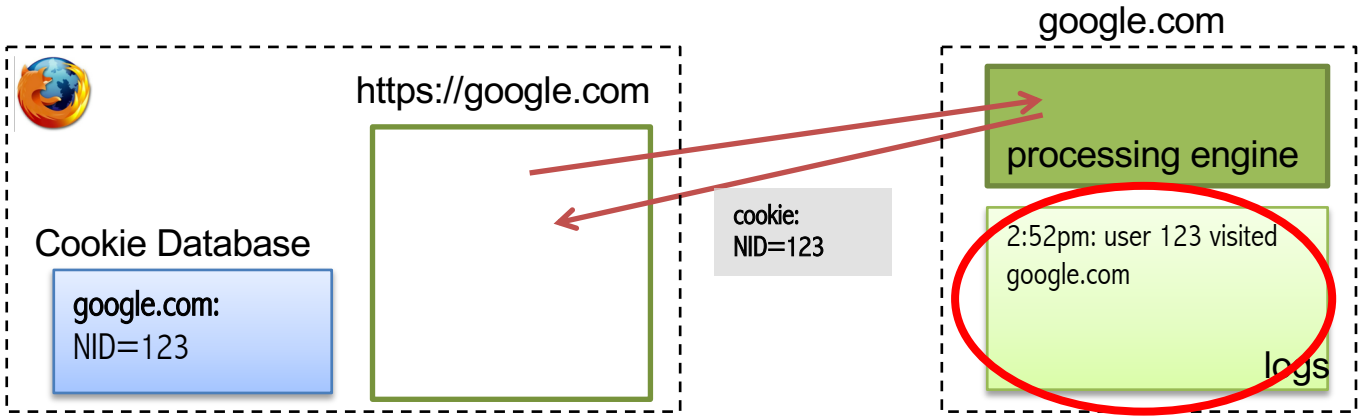
Why filter lists miss trackers?

Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels. Imane Fouad, Nataliia Bielova, Arnaud Legout, Natasa Sarafijanovic-Djukic.To appear in Privacy Enhancing Technologies Symposium (PETS 2020).

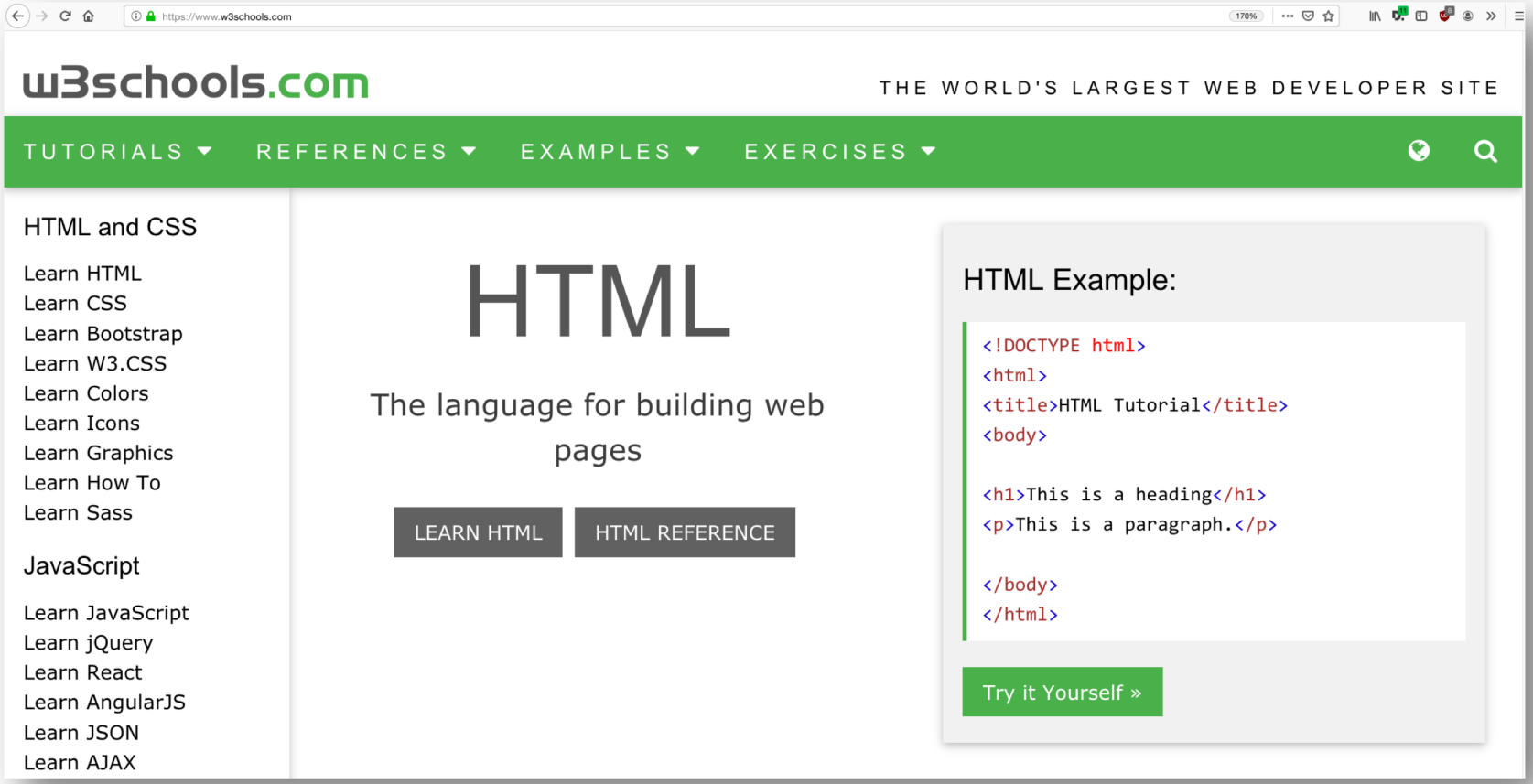
User visits google.com (homepage in many bro



User visits google.com (homepage in many browsers)

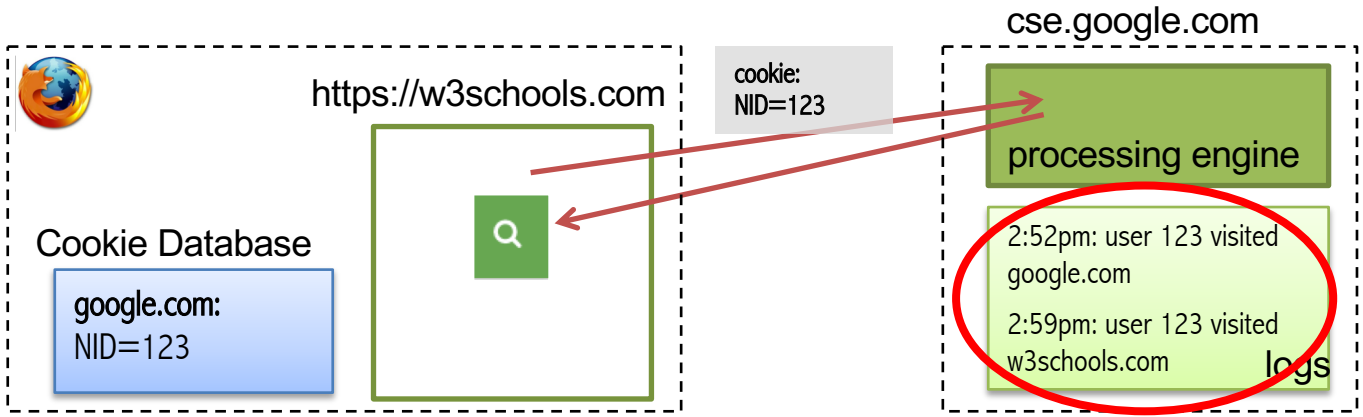


User visits w3schools.com



User visits w3schools.com

- **Third-party cookies are passively sent** to cse.google.com, not blocked by Disconnect because of its functionality



❶ Because first-party cookies become third-party

- EasyList & EasyPrivacy: in 32% of missed requests
- Disconnect: in 45% of missed requests

Initially first-party tracking cookies are sent with requests to fetch (functional) third-party content

❷ Because of the large scope of cookies

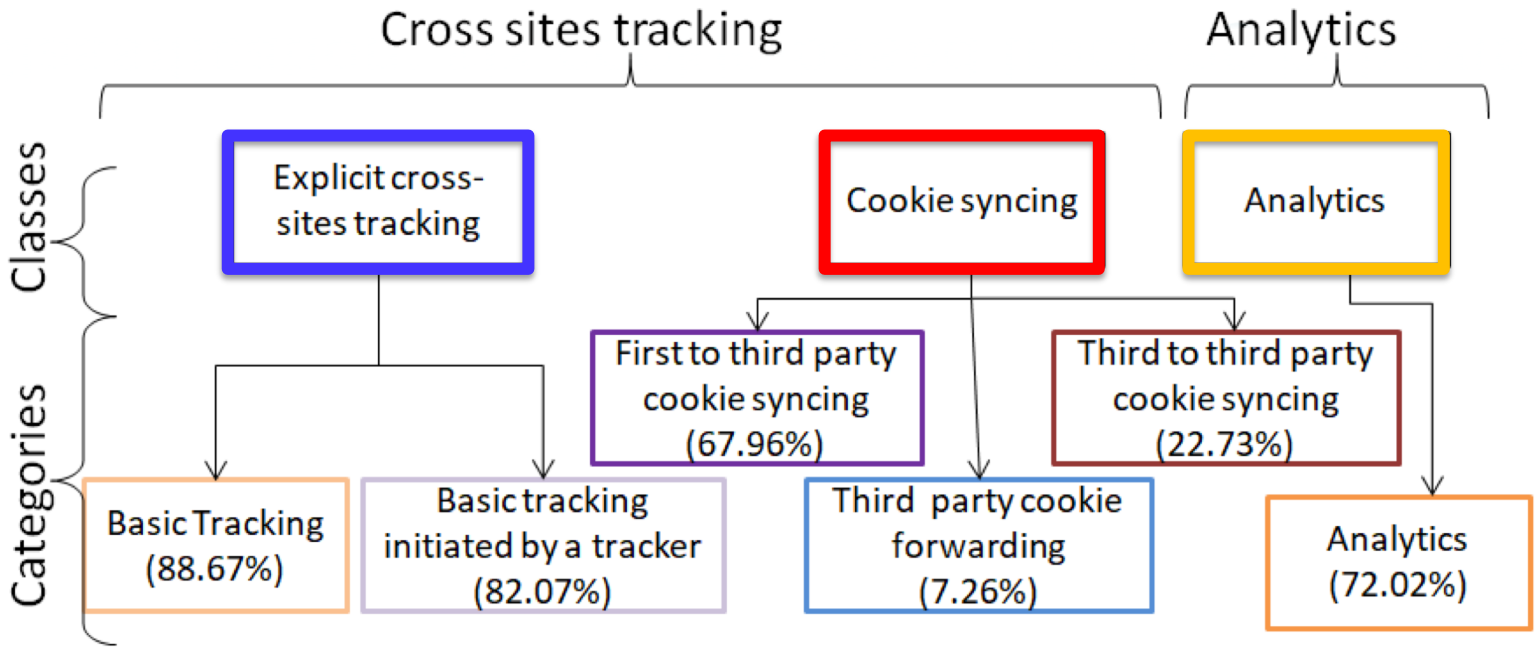
- EasyList & EasyPrivacy: 77% third-party cookies are 2nd level TLD
- Disconnect: 75% third-party cookies are 2nd level TLD

The scope of cookies should be limited to the subdomain that sets it (e.g., cse.google.com instead of google.com)

Do browser extensions block all trackers?

Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels. Imane Fouad, Nataliia Bielova, Arnaud Legout, Natasa Sarafijanovic-Djukic.To appear in Privacy Enhancing Technologies Symposium (PETS 2020).

Classification: six cookie-based tracking behaviors



Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels. Imane Fouad, Nataliia Bielova, Arnaud Legout, Natasa Sarafijanovic-Djukic.To appear in Privacy Enhancing Technologies Symposium (PETS 2020).

Do browser extensions block all trackers?

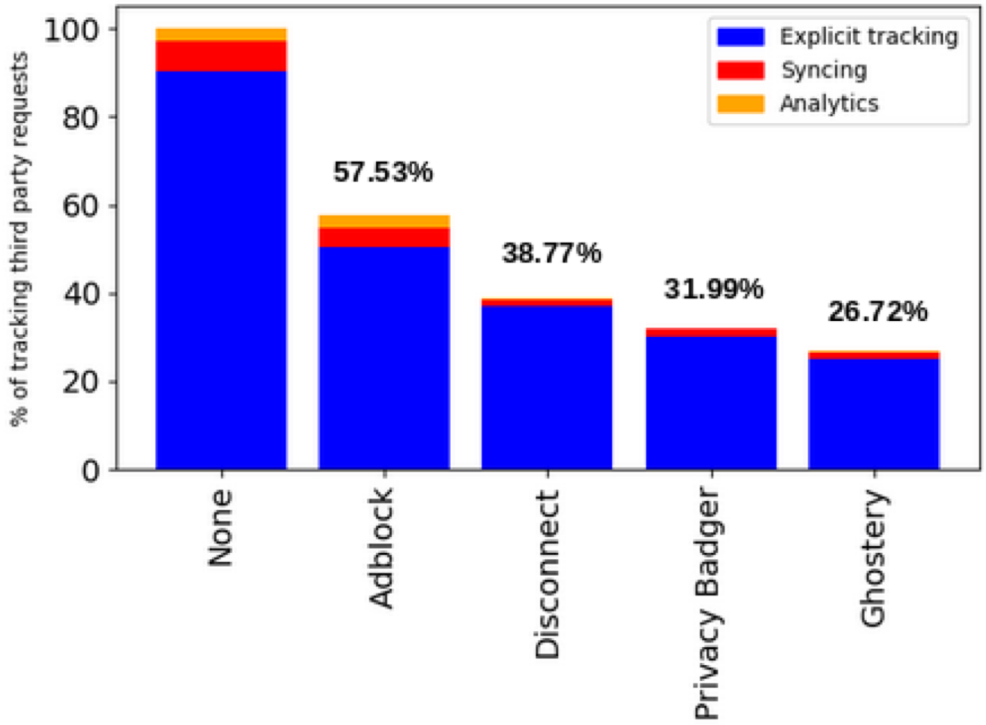
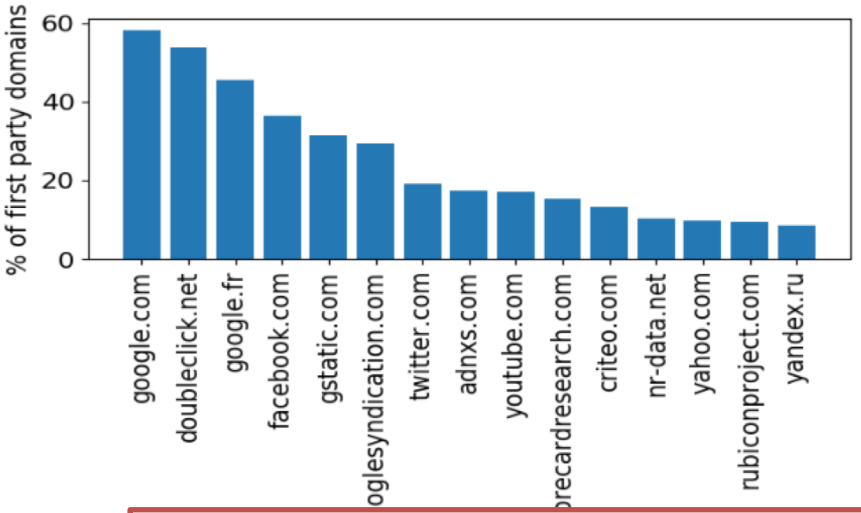


Fig. 12. Third party requests allowed by privacy protecting browser extensions out of 4,519,975 tracking requests.

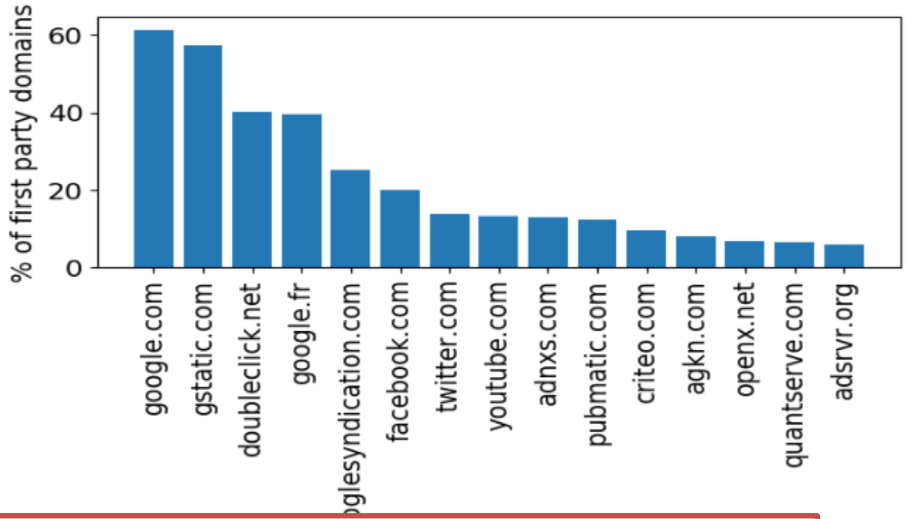
More insights into detected Web tracking…

Trackers often get included in websites indirectly

Basic tracking included directly is present on **88.7%** domains

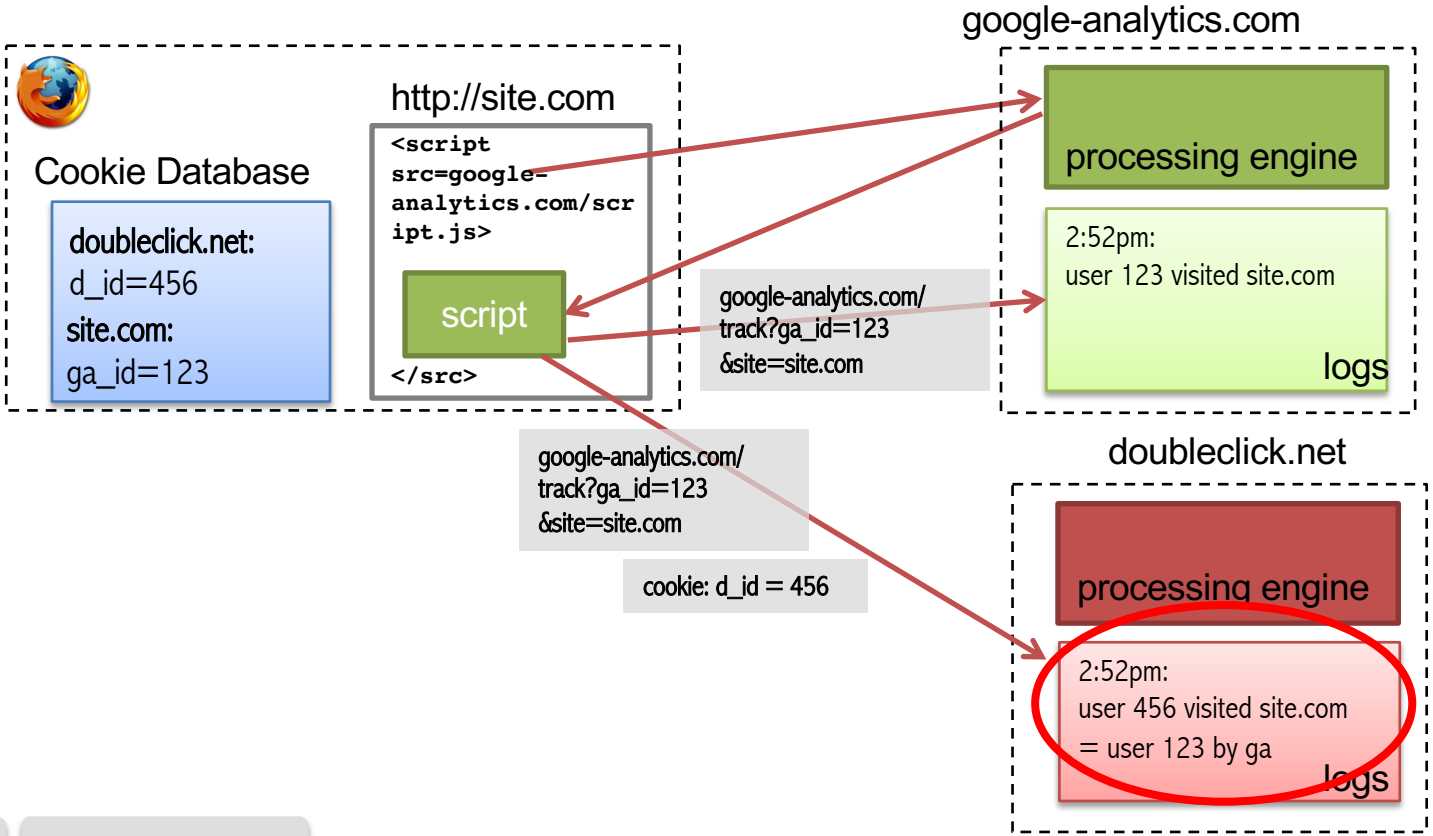


Basic tracking initiated by a tracker (via redirection or inclusion) is present on **82%** domains



It's hard for website developers to control all tracking!

First party analytics cookies synchronized with third party cookies



First party analytics cookies synchronized with third party cookies

- First to third party cookie syncing detected on **67.96% of domains**
- We found **17,415 different partners involved** in synching

Partners	# requests
First party cookie synced through an intermediate service	
google-analytics.com → doubleclick.net	8,297
Direct First to third party cookie syncing	
hibapress.com → criteo.com	460
alleng.org → yandex.ru	332
arstechnica.com → condenastdigital.com	243
thewindowsclub.com → doubleclick.net	228
digit.in → doubleclick.net	224
misionesonline.net → doubleclick.net	221
wired.com → condenastdigital.com	219
newyorker.com → condenastdigital.com	218
uol.com.br → tailtarget.com	198

Table 4. First to third party cookie syncing: Top 10 partners.

Configure Analytics to display Demographics and Interests data

Before you can see or work with Demographics and Interests data in Analytics, you need to:

1. Enable Advertising Reporting Features for your property
2. Enable the Demographics and Interests reports for the property

Where Analytics gets the data

Once you update Analytics to support Advertising Reporting Features, Analytics collects Demographics and Interests data from the following sources:

Source	Applies to	Condition	Result
Third-party DoubleClick cookie	Web-browser activity only	Cookie is present	Analytics collects any demographic and interests information available in the cookie
Android Advertising ID	App activity only	You update the Analytics tracking code in an Android app to collect the Advertising ID	Analytics generates an identifier based on the ID that includes demographic and interests information associated with users' app activity
iOS Identifier for Advertisers (IDFA)	App activity only	You update the Analytics tracking code in an iOS app to collect the IDFA	Analytics generates an identifier based on the IDFA that includes demographic and interests information associated with users' app activity

Demographics and interests data may only be available for a subset of your users, and may not represent the overall composition of your traffic: Analytics cannot collect the demographics and interests information if the DoubleClick cookie or the Device Advertising ID is not present, or if no activity profile is included.

The graphs and the first row of the Sessions column in the Overview report display the percentage of your overall data that is represented (for example, Age - 41.39% of total sessions).

Neither analytics.js nor AMP tracking collects demographics and interests data.

Demographics and Interests

About Demographics and Interests

Enable Demographics and Interests reports

Analyze Demographics and Interests data

CNIL sanction against CARREFOUR FRANCE (18 November 2020)

175. La formation restreinte relève qu'en l'espèce, le dépôt de trente-neuf cookies était automatique dès l'arrivée sur la page d'accueil du site, et avant tout action de l'utilisateur. Parmi ces trente-neuf cookies, trois appartenaient à la solution Google Analytics (cookies _gid , _ga et _gat_gtag_UA_3928615_46).

176. S'agissant de ces trois cookies, dits *Google analytics,* la formation restreinte souligne qu'il ne fait pas débat que les données collectées par ces cookies peuvent être recoupées avec des données issues d'autres traitements pour poursuivre des finalités différentes que celles limitativement prévues par l'article 82 de la loi informatique et libertés , notamment pour mener à bien de la publicité personnalisée. En effet, il ressort du guide pratique Association des comptes Analytics et Google Ads , mis en ligne sur un des sites de la société Google, que *l'intégration de Google Analytics dans Google Ads (…) permet [aux annonceurs] de savoir précisément dans quelle mesure [leurs] annonces se traduisent par des conversions, puis d'ajuster rapidement les* *conséquence. [Les annonceurs peuvent] également combiner les produits afin d'identifier [leurs] seg* *susciter l'intérêt de ces utilisateurs à l'aide de messages personnalisés .*

177. Dès lors, ces cookies n'ont pas pour finalité exclusive de permettre ou de faciliter la communic sont pas strictement nécessaires à la fourniture du service. Leur dépôt aurait donc dû obliger la société à recueillir préalablement le consentement des utilisateurs.

First party Google Analytics cookies detected

Synchronisation of Google Analytics and Google Ads (doubleclick.net) allows advertisers to collect more data

Consent is needed for such cookies (while not necessary for pure analytics!)

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042563756
accessed on Dec 17th, 2020

EU Data Protection Regulations

Applies to all people physically located in the EU

GDPR
(applies to personal data)

ePrivacy Directive
(information stored on/retrieved from devices)

Applies to any information, not only personal data

Regulation = applies directly to all member states

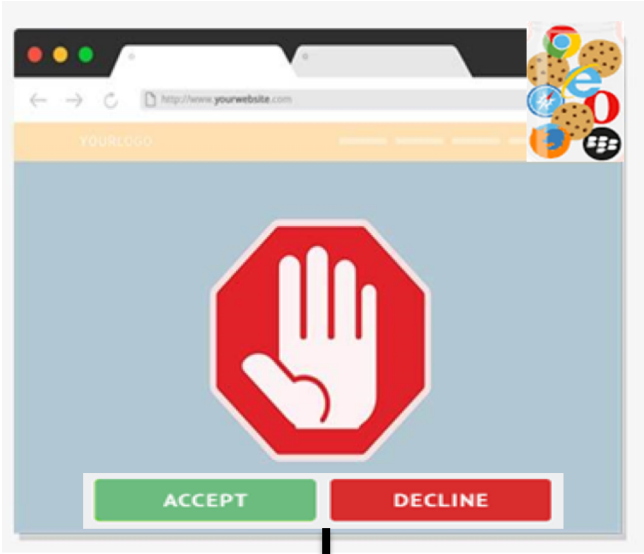
Cookies and other trackers require **consent** unless they are used for

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

Consent given through cookie banner options

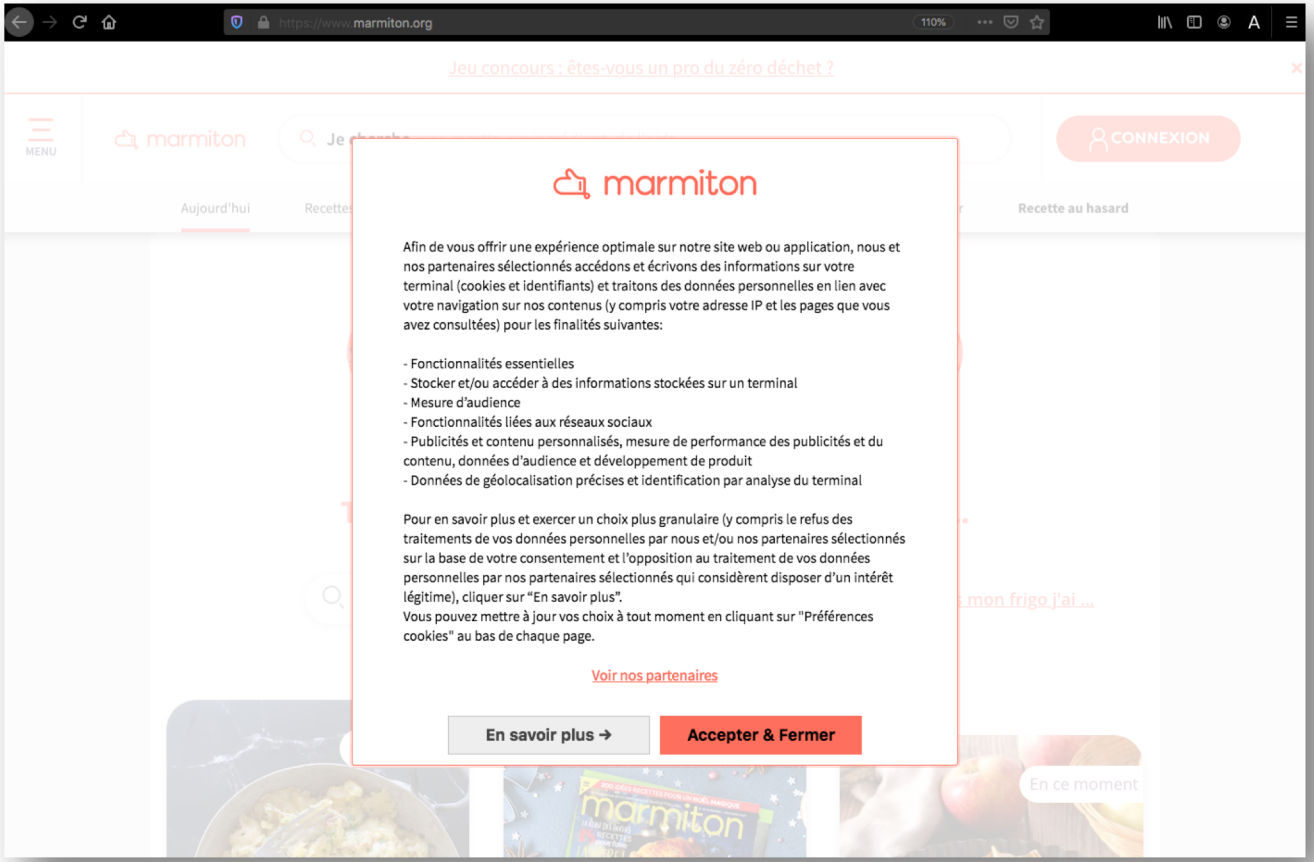
Protects user's privacy in online communications

- Applies to any form of web tracking, such as cookies and similar technologies, that collect/store data of any website user
- Art. 5(3): **consent** before processing data through cookies



cookie banners
common method
to collect consent

Cookie banner



How can we understand when a banner is compliant?

It is easy, 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

- Expertise in Web tracking technologies
- Compliance verification: manual, computer science tools, user studies

Technology and Regulation

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***

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

c.teixeirasantos@uu.nl
nataliia.bielova@inria.fr
celestin.matte@cmatte.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[1] 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.[2]

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.[3,4] 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.[5] 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[6,7,8] that lead to nudging users to consent, data subjects are

[1] In this paper we will only regard 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").

[2] Jannick Sørensen, Sokol Kosta (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.

[3] 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.

[4] Article 29 Working Party, "Guidelines on consent under Regulation 2016/679" (WP259 rev.01, 10 April 2018).

[5] 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 accessed 7 May 2020.

[6] Harry Brignull, "What are Dark Patterns?" (2018) https://darkpatterns.org accessed 7 May 2020.

[7] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L.

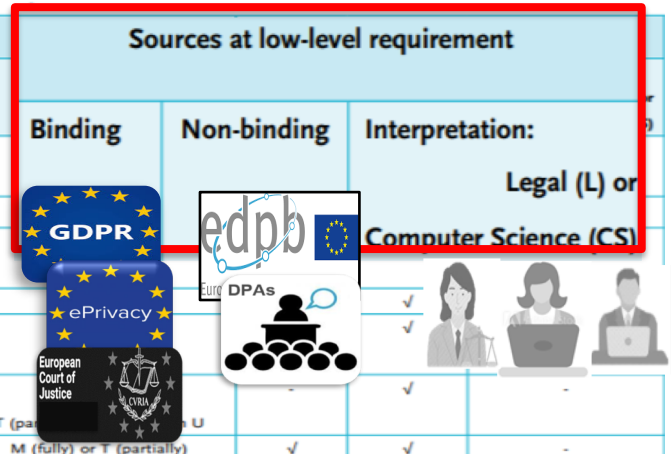
Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. Cristiana Santos, Nataliia Bielova and Célestin Matte. *International Journal on Technology and Regulation, 2020.*

22 requirements for cookie banners compliance!

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

22 requirements for cookie banners compliance!

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



Scope: cookies and tracking tech that require consent

Filling online forms
Shopping cart

Purposes exempted of consent	Purposes needing consent
Local analytics (anonymized and aggregated)	**Non-local analytics** (statistics, measurement)
Session user input (functionality)	**Advertising (targeting)**
Social media plugin – functionality requested by user	**Social media plugin** – functionality not requested by user
Customization – short termed (preferences/personalization)	**Customization** – long termed

22 requirements for cookie banners compliance!

Requirements		Assessment		at low-level requirement	
High-Level Requirements	Low-Level Requirements	Manual (M), Technical (T) or User study (U)	-binding		Interpretation: Legal (L) or Computer Science (CS)
Prior	R1 Prior to storing an identifier			√	-
	R2 Prior to sending an identifier			-	CS
Free	R3 No merging into a contract			√	-
	R4 No tracking walls	M (fully)	-	√	-
Specific	R5 Separate consent per purpose	M (fully)	√	√	-
Informed	R6 Accessibility of information page	M (fully) or T (partially) together with U	-	√	-
	R7 Necessary information on BTT	M (fully) or T (partially)	√	√	-
	R8 Information on consent banner configuration	M (fully) or T (partially)	-	√	-
	R9 Information on the data controller	M (fully) or T (partially)	√	√	-
	[illegible]	[illegible]	[illegible]	[illegible]	-
Unambiguous	R11 Affirmative action design	Combination of M and T (partially)			-
	[illegible]	[illegible]	[illegible]	[illegible]	L
	R13 Balanced choice	M (fully)	-	√	L
	R14 Post-consent registration	T (partially)	-	√	CS
	R15 Correct consent registration	Combination of M and T (partially)	-	√	CS
Readable and accessible	R16 Distinguishable	M (fully) or T (partially)	√	√	-
	R17 Intelligible	U	√	√	-
	R18 Accessible	U	√	√	
	R19 Clear and plain language	U	√	√	-
	R20 No consent wall	M (fully) or T (partially)	-	√	L
Revocable	R21 Possible to change in the future	M (fully)	√	√	-
	R22 Delete "consent cookie" and communicate to third parties	Not possible	-	-	CS

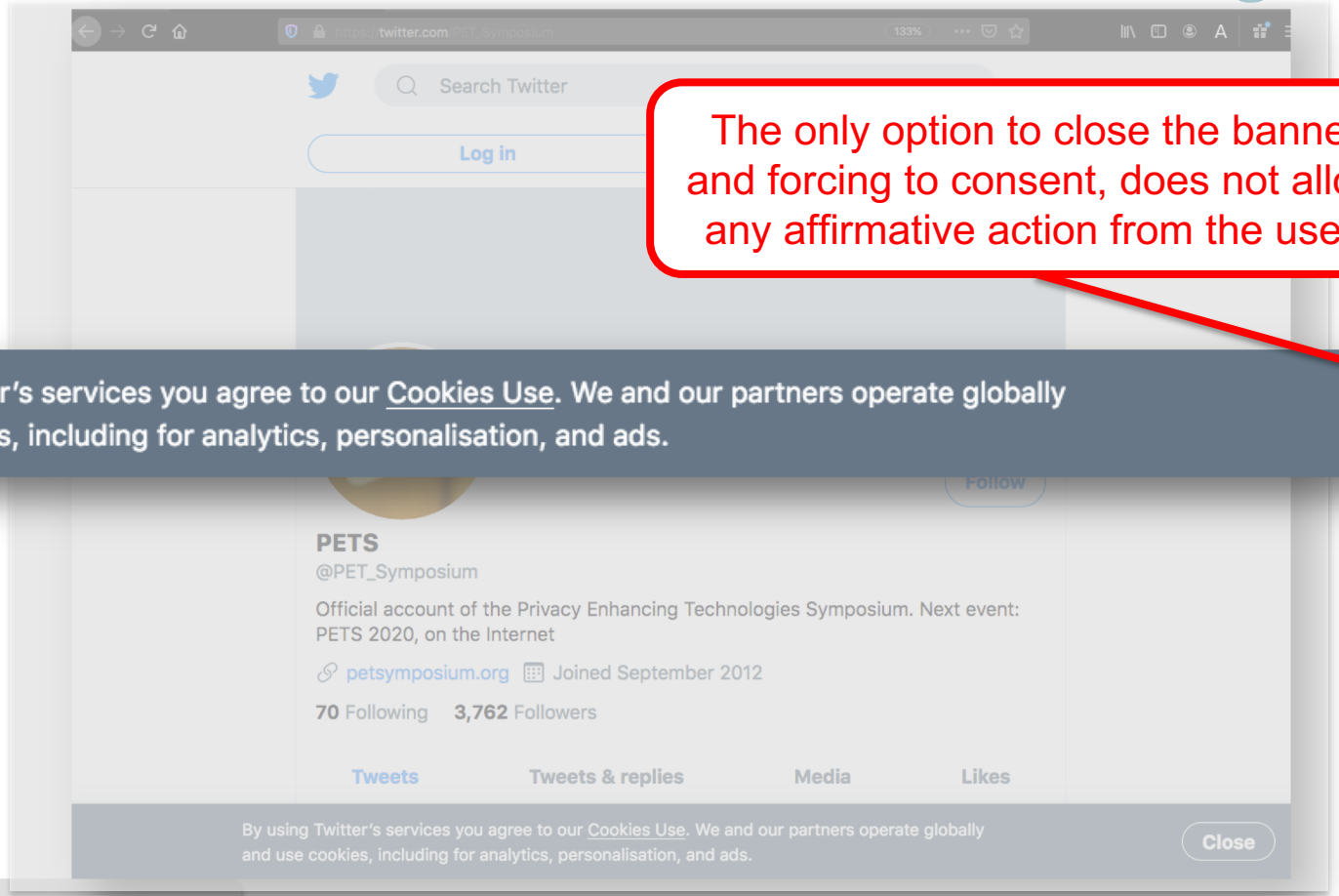
R11 Affirmative Action Design

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

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

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

Violation of R11: Affirmative Action Design



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

By using Twitter's services you agree to our Cookies Use. We and our partners operate globally and use cookies, including for analytics, personalisation, and ads.

Close

22 requirements for cookie banners compliance!

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

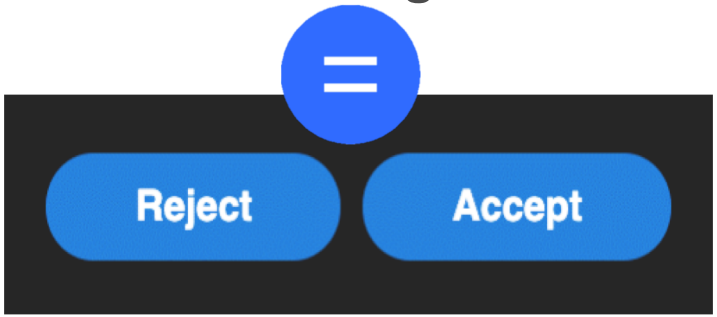
R13 Balanced choice

Art. 7(3)“it shall be **as easy to** withdraw as to give consent”

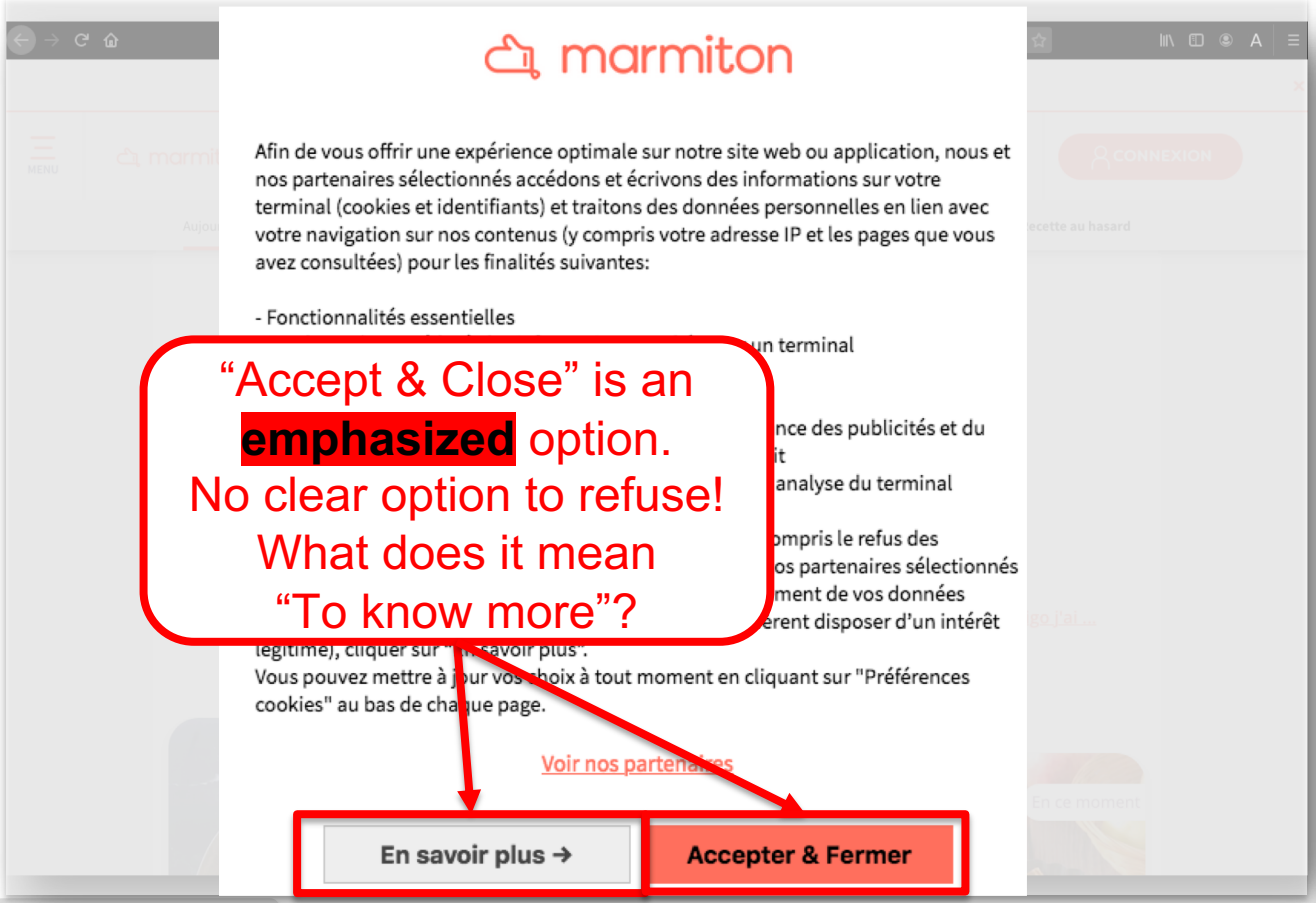
actions presented on an equal footing

- “**same level**”= format, size, color
- bring the same ease of reading to the attention of the user
- design big impact in the user choice

A banner must present a fair or **balanced design choice**



Violation of R13: Balanced choice



"Accept & Close" is an **emphasized** option.
No clear option to refuse!
What does it mean "To know more"?

https://www.marmiton.org

Jeu concours : êtes-vous un pro du zéro déchet ?

MENU marmiton Je cherche CONNEXION

Aujourd'hui Recettes

marmiton

Afin de vous offrir une expérience optimale sur notre site web ou application, nous et nos partenaires sélectionnés accédons et écrivons des informations sur votre terminal (cookies et identifiants) et traitons des données personnelles en lien avec votre navigation sur nos contenus (y compris votre adresse IP et les pages que vous avez consultées) pour les finalités suivantes:

- Fonctionnalités essentielles
- Stocker et/ou accéder à des informations stockées sur un terminal
- Mesure d'audience
- Fonctionnalités liées aux réseaux sociaux
- Publicités et contenu personnalisés, mesure de performance des publicités et du contenu, données d'audience et développement de produit
- Données de géolocalisation précises et identification par analyse du terminal

Pour en savoir plus et exercer un choix plus granulaire (y compris le refus des traitements de vos données personnelles par nous et/ou nos partenaires sélectionnés sur la base de votre consentement et l'opposition au traitement de vos données personnelles par nos partenaires sélectionnés qui considèrent disposer d'un intérêt légitime), cliquer sur "En savoir plus".
Vous pouvez mettre à jour vos choix à tout moment en cliquant sur "Préférences cookies" au bas de chaque page.

Voir nos partenaires

En savoir plus → Accepter & Fermer

Recette du jour

En ce moment

DARK PATTERNS

- **False-hierarchy**
- **Hidden information**
- **Obstruction**

Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. Colin Gray, Cristiana Santos, Nataliia Bielova, Michael Toth and Damian Clifford. Accepted for publication at ACM CHI. *ArXiv* abs/2009.10194 (2020)

22 requirements for cookie banners compliance!

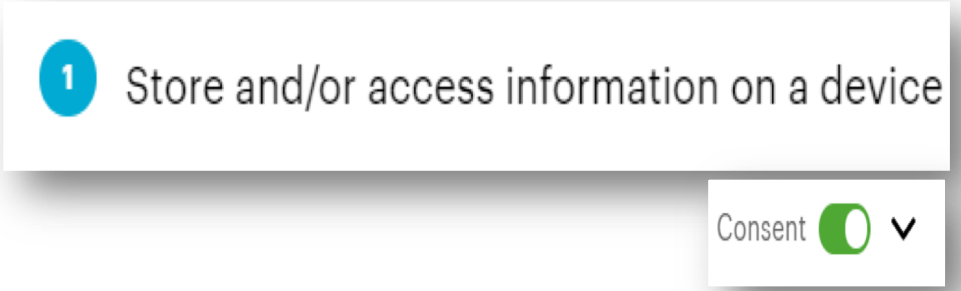
Requirements		Assessment	Sources at low-level requirement		
High-Level Requirements	Low-Level Requirements	Manual (M), Technical (T) or User study (U)	Binding	Non-binding	Interpretation: Legal (L) or Computer Science (CS)
Prior	R1 Prior to storing an identifier	M (partially) or T (partially)	√	√	-
	R2 Prior to sending an identifier	T (partially)	-	-	CS
Free	R3 No merging into a contract	M (fully) or T (partially)	√	√	-
				√	-
Specific	R5 Separate consent per purpose	M (fully)		√	-
Informed		T (partially) together with U		√	-
	R7 Necessary information on BTT	M (fully) or T (partially)	√	√	-
	R8 Information on consent banner configuration	M (fully) or T (partially)	-	√	-
	R9 Information on the data controller	M (fully) or T (partially)	√	√	-
	R10 Information on rights	M (fully) or T (partially)	√	√	-
Unambiguous	R11 Affirmative action design	Combination of M and T (partially)	√	√	-
	R12 Configurable banner	M or T (partially)	-	√	L
	R13 Balanced choice	M (fully)	-	√	L
	R14 Post-consent registration	T (partially)	-	√	CS
	R15 Correct consent registration	Combination of M and T (partially)	-	√	CS
Readable and accessible	R16 Distinguishable	M (fully) or T (partially)	√	√	-
	R17 Intelligible	U	√	√	-
	R18 Accessible	U	√	√	
	R19 Clear and plain language	U	√	√	-
	R20 No consent wall	M (fully) or T (partially)	-	√	L
Revocable	R21 Possible to change in the future	M (fully)	√	√	-
	R22 Delete "consent cookie" and communicate to third parties	Not possible	-	-	CS

R5 Separate consent per purpose

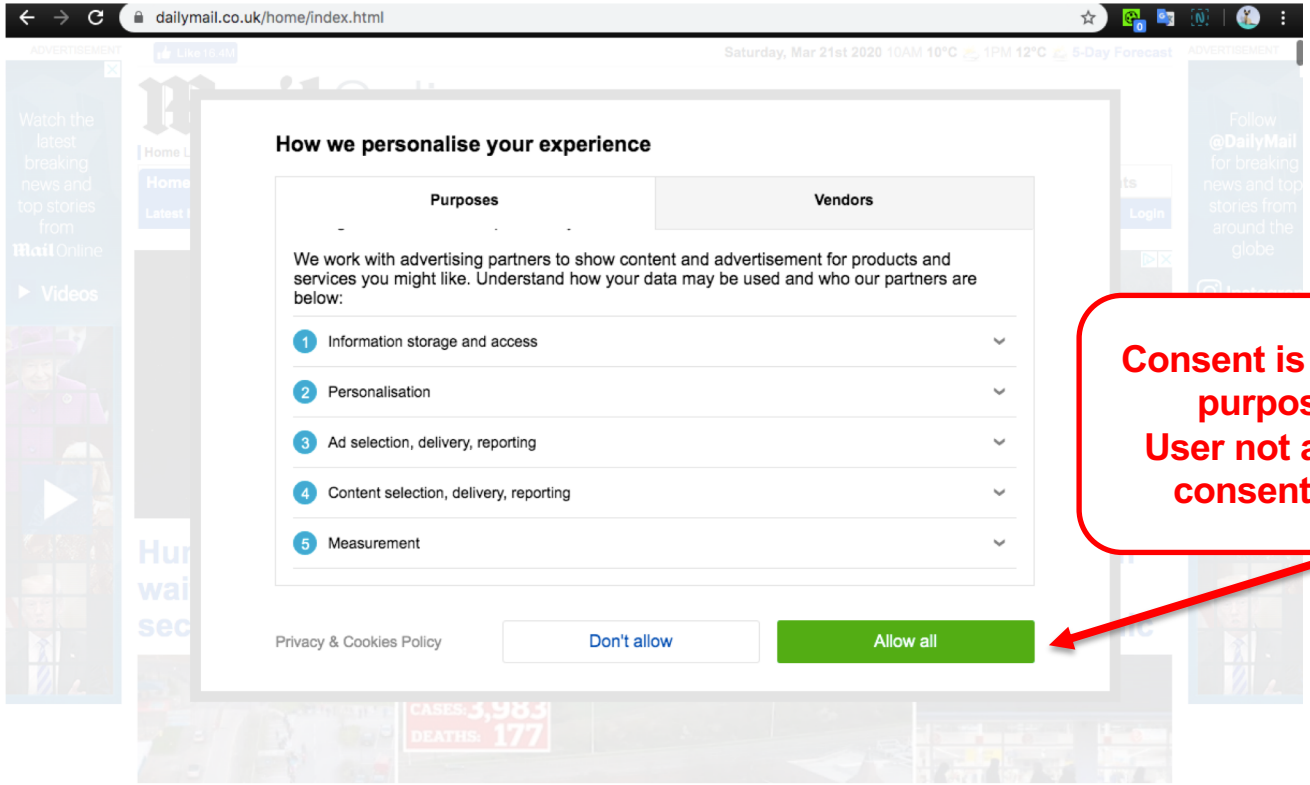
- Recital 32: consent given per purpose(s)
- Recital 43: separate consent per operation(s)

granular request: user able to accept/reject each specific purpose separately

- consent specific: related to processing at stake
- cannot be inferred from other purposes



Violation of R5: Separate consent per purpose



Consent is given for all the purposes at once.
User not allowed to give consent per purpose

https://www.dailymail.co.uk/home/index.html
accessed on 17 May 2019

22 requirements for cookie banners compliance!

Requirements		Assessment	Sources at low-level requirement		
High-Level Requirements	Low-Level Requirements	Manual (M), Technical (T) or User study (U)	Binding	Non-binding	Interpretation: Legal (L) or Computer Science (CS)
Prior	R1 Prior to storing an identifier	M (partially) or T (partially)	√	√	-
	R2 Prior to sending an identifier	T (partially)	-	-	CS
Free	R3 No merging into a contract	M (fully) or	√	√	-
					-
Specific					-
Informed		T (partially) together with U			-
	R7 Necessary information on BTT	M (fully) or T (partially)	√	√	-
	R8 Information on consent banner configuration	M (fully) or T (partially)	-	√	-
	R9 Information on the data controller	M (fully) or T (partially)	√	√	-
	R10 Information on rights	M (fully) or T (partially)	√	√	-
Unambiguous	R11 Affirmative action design	Combination of M and T (partially)	√	√	-
	R12 Configurable banner	M or T (partially)	-	√	L
	R13 Balanced choice	M (fully)	-	√	L
	R14 Post-consent registration	T (partially)	-	√	CS
	R15 Correct consent registration	Combination of M and T (partially)	-	√	CS
Readable and accessible	R16 Distinguishable	M (fully) or T (partially)	√	√	-
	R17 Intelligible	U	√	√	-
	R18 Accessible	U	√	√	
	R19 Clear and plain language	U	√	√	-
	R20 No consent wall	M (fully) or T (partially)	-	√	L
Revocable	R21 Possible to change in the future	M (fully)	√	√	-
	R22 Delete "consent cookie" and communicate to third parties	Not possible	-	-	CS

R4 No tracking walls — M (fully)

R4 No tracking walls

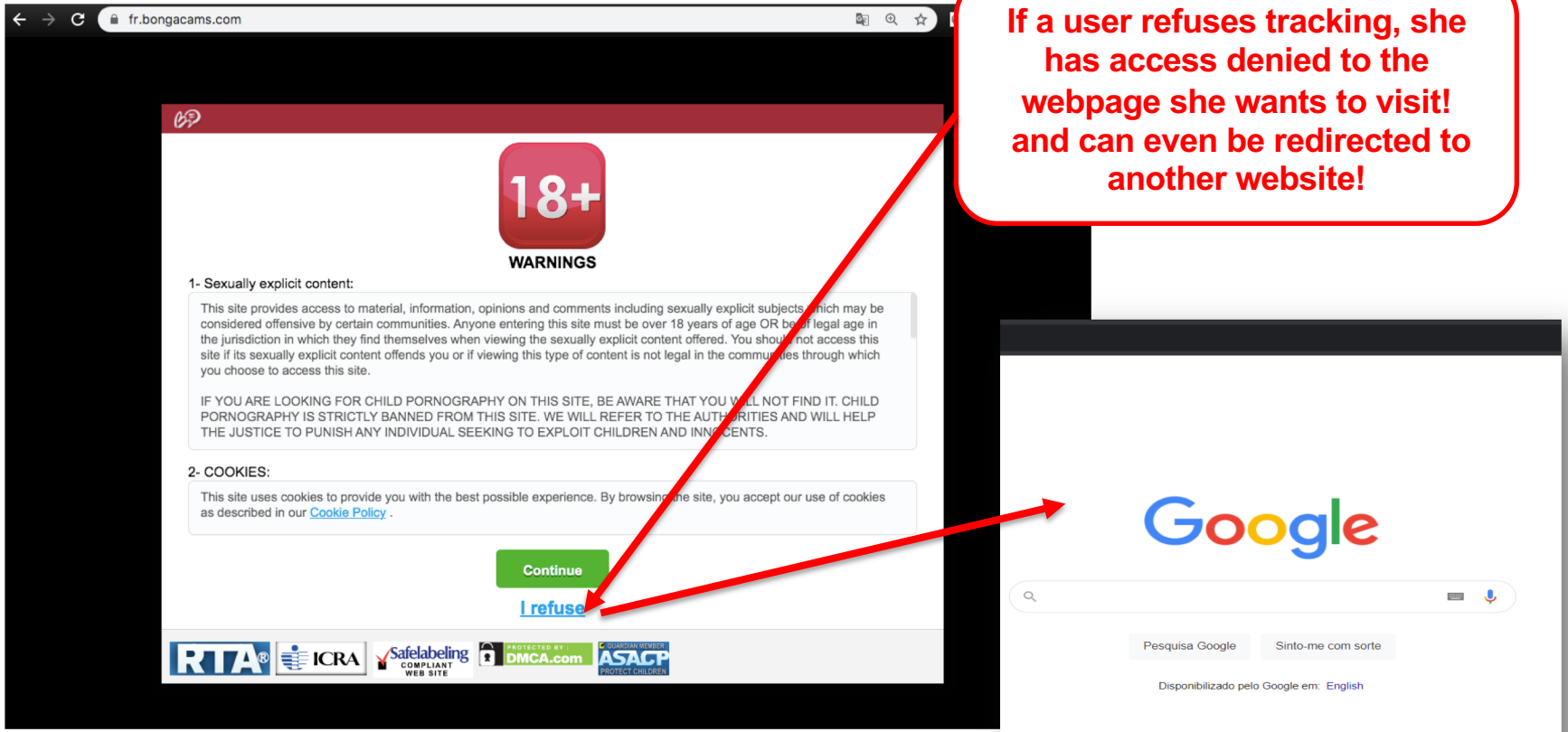
Arts. 4(11), 7(4): consent freely given; Rec. 42: without detriment

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

- No pressure, persuasion on user's free will
- Freedom to reject non-necessary cookies without detriment

Stakeholders	Positioning on tracking wall
EDPB, EDPS, BEUC, EU Parliament, DPAs: Dutch, French, German, Danish, Greek, Irish, Belgian, Spanish	Violation of a freely given consent
UK DPA	Not clear
Austrian DPA	Valid consent

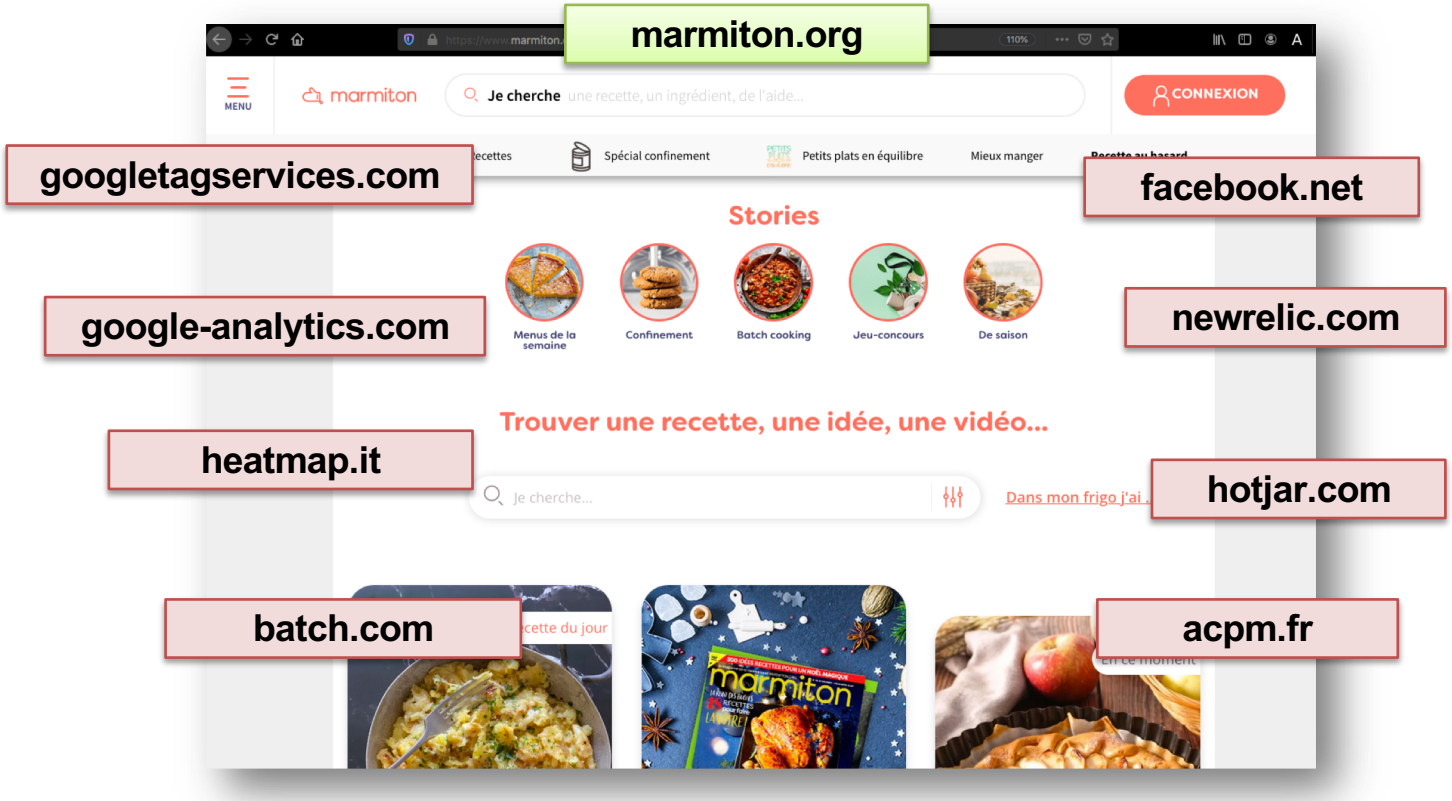
Violation of R4: No tracking walls



If a user refuses tracking, she has access denied to the webpage she wants to visit! and can even be redirected to another website!

What actually happens on websites?

Third-party content



*Website visited on 10 November, 2020

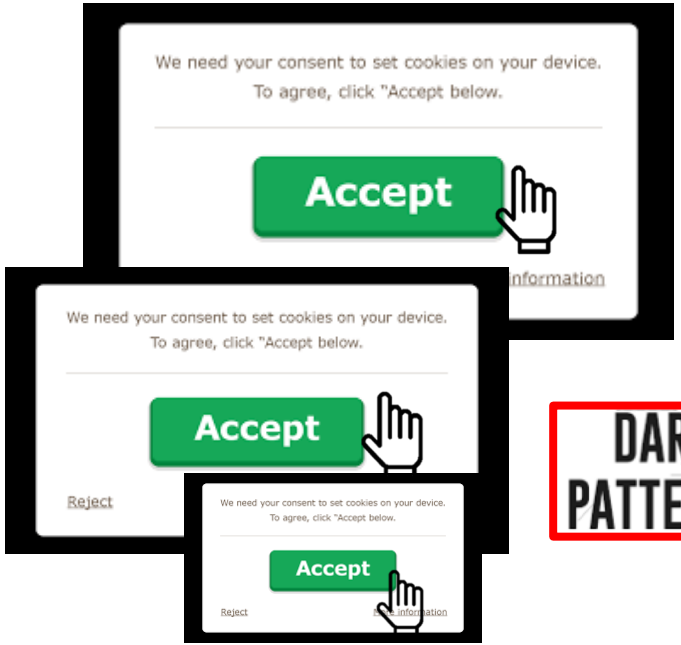
What are the requirements on cookie banners that are more technical?

22 requirements for cookie banners compliance!

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

R15 Correct consent registration

- Art. 7(1), Rec. 42: websites obligation to demonstrate the user consented to tracking
- Art. 30: record of processing activities
- Art. 5(2): principle of accountability



- User's choice made in the banner interface (acceptance/refusal) = decision that gets registered/stored in the browser
- Correct registration => user not nagged to face another banner by the same website!

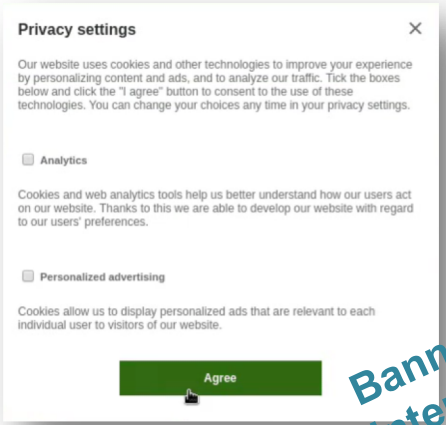
Violation of R15: Correct consent registration

Consent banner has registered user's consent for 5 purposes and 544 vendors even when the user refused everything in the cookie banner interface!

https://www.flashscore.com/ accessed on 25 November 2019

How to detect violations of “correct consent registration” (R15)?

- Only possible for standardized and open storage of consent
  - ✓ Manually compare options in the interface vs. options in consent storage
  - ✓ **Hard to analyse all possible combinations**

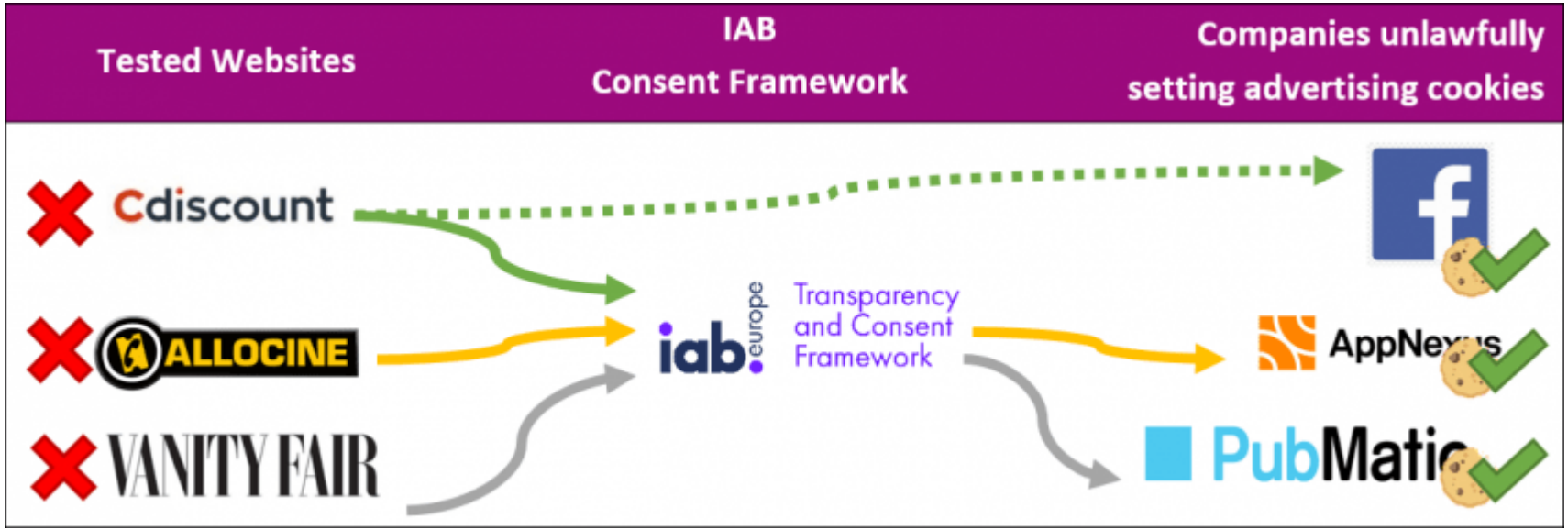


Banner interface

Are the purposes selected the same in the interface and in the stored consent?

Stored consent

Complaints to the CNIL on “fake consent”



Cookie banners of large French webpages turn a clear “NO” into “fake consent” *noyb.eu* files three GDPR complaints with the French Data Protection Regulator (CNIL).

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**).*

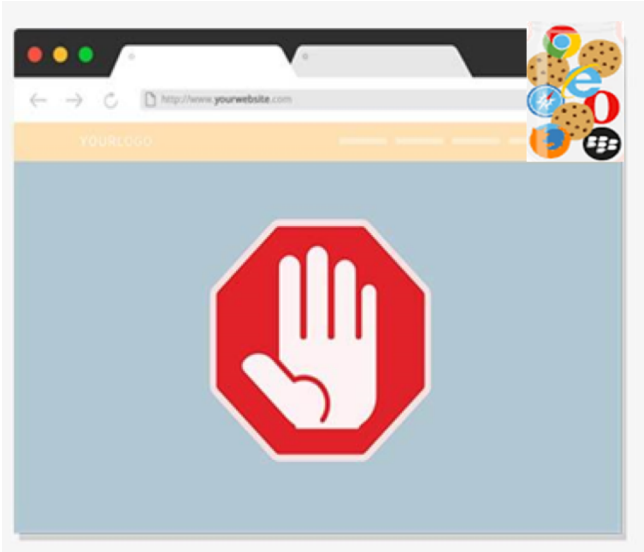
22 requirements for cookie banners compliance!

Requirements		Assessment	Sources at low-level requirement		
High-Level Requirements	Low-Level Requirements	Manual (M), Technical (T) or User study (U)	Binding	Non-binding	Interpretation: Legal (L) or Computer Science (CS)
Prior	R1 Prior to storing an identifier	M (partially) or T (partially)			-
					CS
Free		T (partially)			-
	R4 No tracking walls	M (fully)	-	√	-
Specific	R5 Separate consent per purpose	M (fully)	√	√	-
Informed	R6 Accessibility of information page	M (fully) or T (partially) together with U	-	√	-
	R7 Necessary information on BTT	M (fully) or T (partially)	√	√	-
	R8 Information on consent banner configuration	M (fully) or T (partially)	-	√	-
	R9 Information on the data controller	M (fully) or T (partially)	√	√	-
	R10 Information on rights	M (fully) or T (partially)	√	√	-
Unambiguous	R11 Affirmative action design	Combination of M and T (partially)	√	√	-
	R12 Configurable banner	M or T (partially)	-	√	L
	R13 Balanced choice	M (fully)	-	√	L
	R14 Post-consent registration	T (partially)	-	√	CS
	R15 Correct consent registration	Combination of M and T (partially)	-	√	CS
Readable and accessible	R16 Distinguishable	M (fully) or T (partially)	√	√	-
	R17 Intelligible	U	√	√	-
	R18 Accessible	U	√	√	
	R19 Clear and plain language	U	√	√	-
	R20 No consent wall	M (fully) or T (partially)	-	√	L
Revocable	R21 Possible to change in the future	M (fully)	√	√	-
	R22 Delete "consent cookie" and communicate to third parties	Not possible	-	-	CS

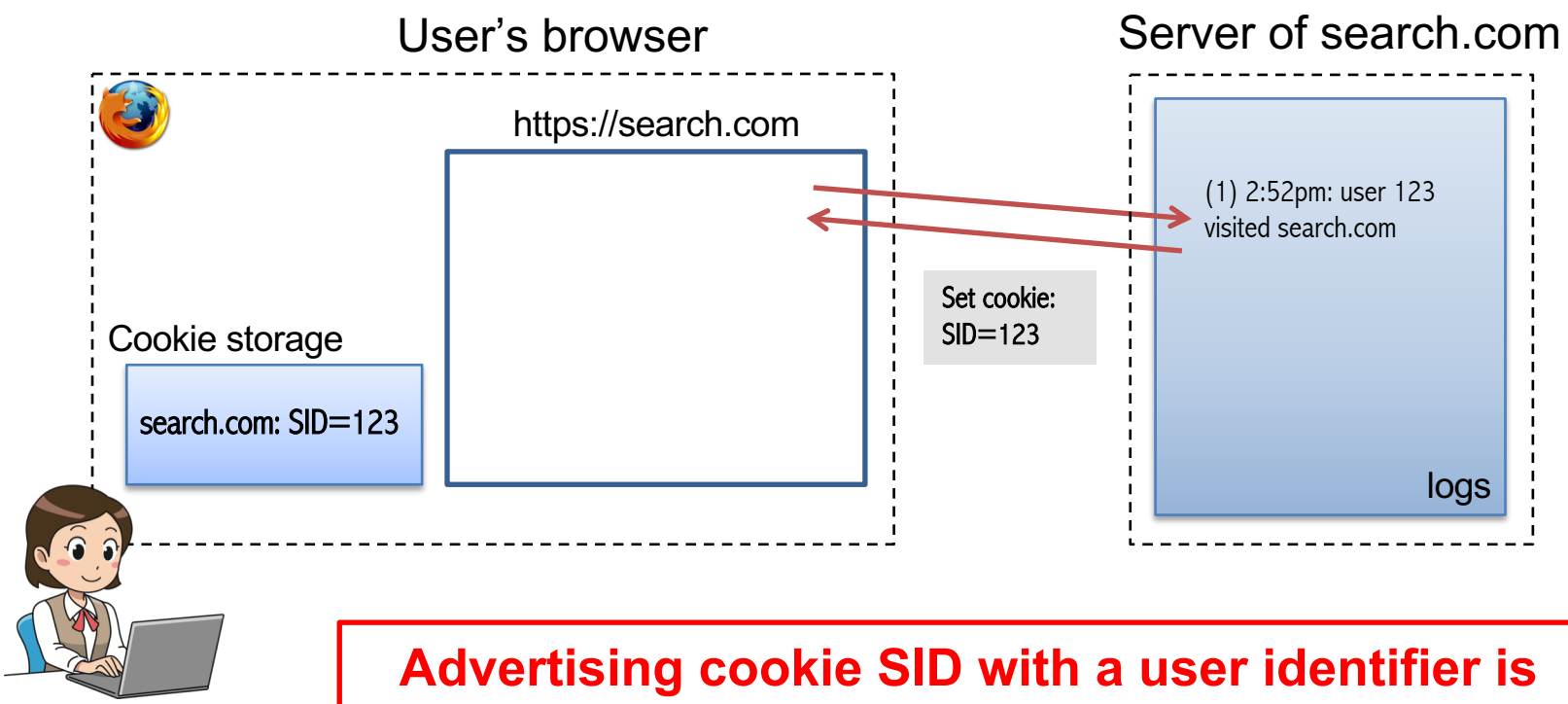
R1: Prior to storing an identifier

Art. 6: data subject “has given” consent

Consent should be collected before cookies are set/stored in the user’s device (those requiring consent)



Violation of R1: Prior to storing an identifier



Advertising cookie SID with a user identifier is stored in her browser

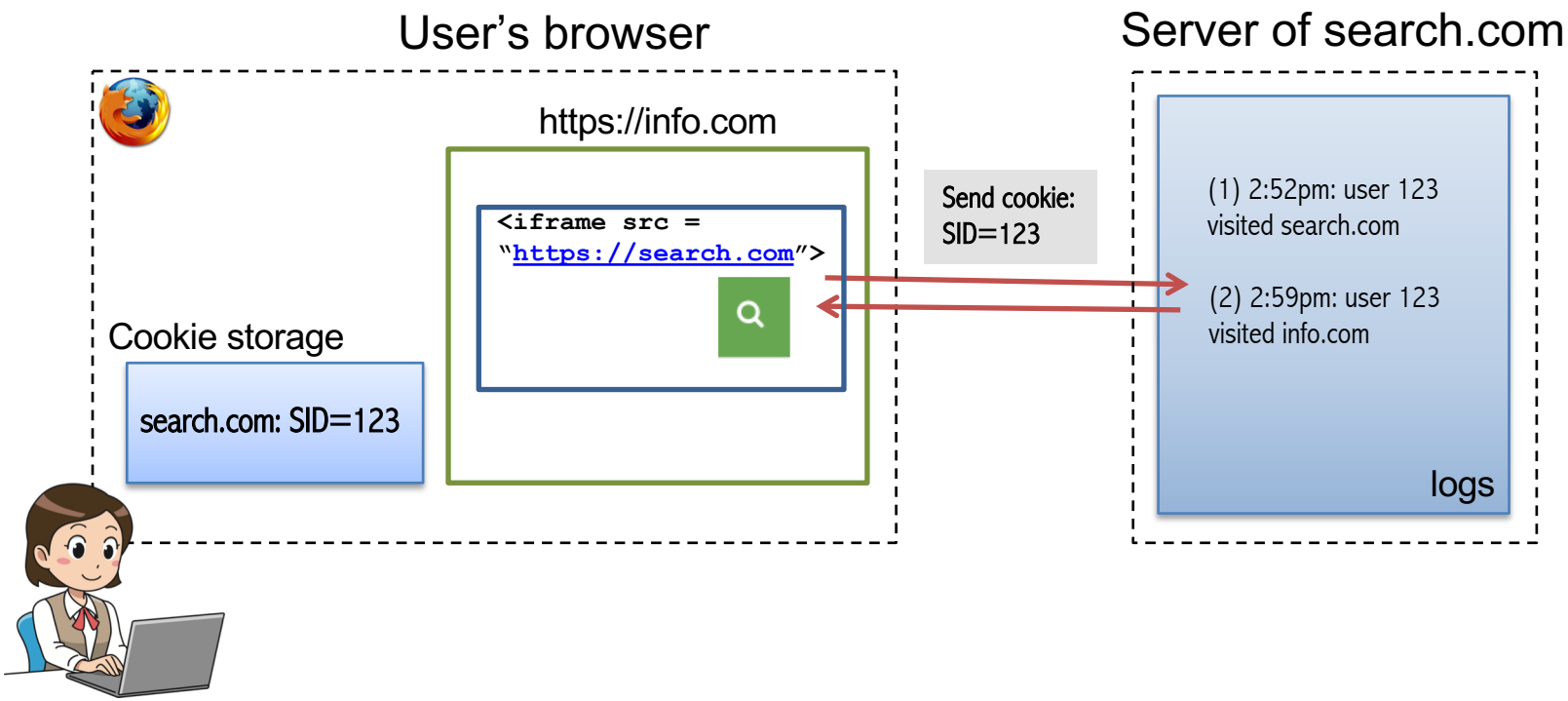
How to detect violations?

R1 Prior to storing an identifier	M (partially) or T (partially)

- **Detecting whether a stored element is a user identifier**
  - it's not possible to know with certainty that an element is an identifier
- **Analyzing all possible browser storages**
  - all combinations of storages are impossible to analyse (also HSTS)
- **Identifying the purpose of an identifier**
  - **impossible to know purposes of all stored elements***
    - ✓ **only 13% cookies** are available in cookie policies
    - ✓ **only 5% cookie purposes** are explicit

On Compliance of Cookie Purposes with the Purpose Specification Principle. Imane Fouad, Cristiana Santos, Feras Al Kassar, Nataliia Bielova and Stefano Calzavara. *International Workshop on Privacy Engineering (IWPE 2020).* https://hal.inria.fr/hal-02567022

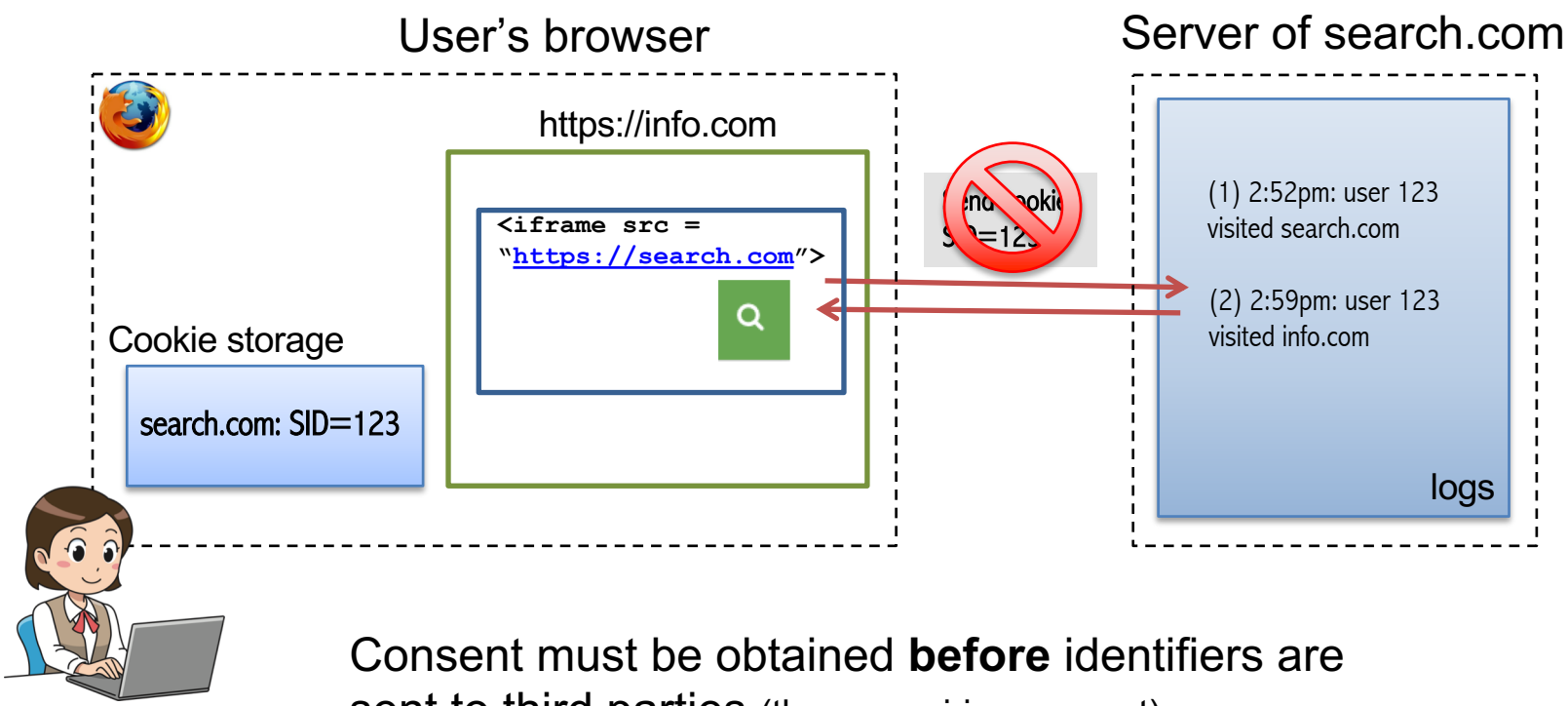
What if the user visits a different website…



22 requirements for cookie banners compliance!

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

R2: Prior to sending an identifier



Consent must be obtained **before** identifiers are sent to third parties (those requiring consent)

How to detect violations?

R2 Prior to sending an identifier	T (partially)	CS

- **Same difficulties as for R1: Prior to setting an identifier**
- **Extensive testing**
  - hard to detect all identifiers in the browser
  - can't detect encrypted identifiers in the traffic
  - sophisticated analysis of JavaScript needed
- **Detection of browser fingerprinting***
  - no precise technique to detect fingerprinting exists
  - impossible to identify a purpose of fingerprinting

Browser Fingerprinting: A survey. Pierre Laperdrix, Nataliia Bielova, Benoit Baudry and Gildas Avoine. *ACM Transactions on the Web (ACM TWEB), 2020.* https://hal.inria.fr/hal-02864872

How to comply when consent is shared among website publishers?

Can consent be shared?

When a website publisher receives the user consent, it can **share the consent with other controllers**, insofar:

- further data processing operations pursue the same purposes
- user informed

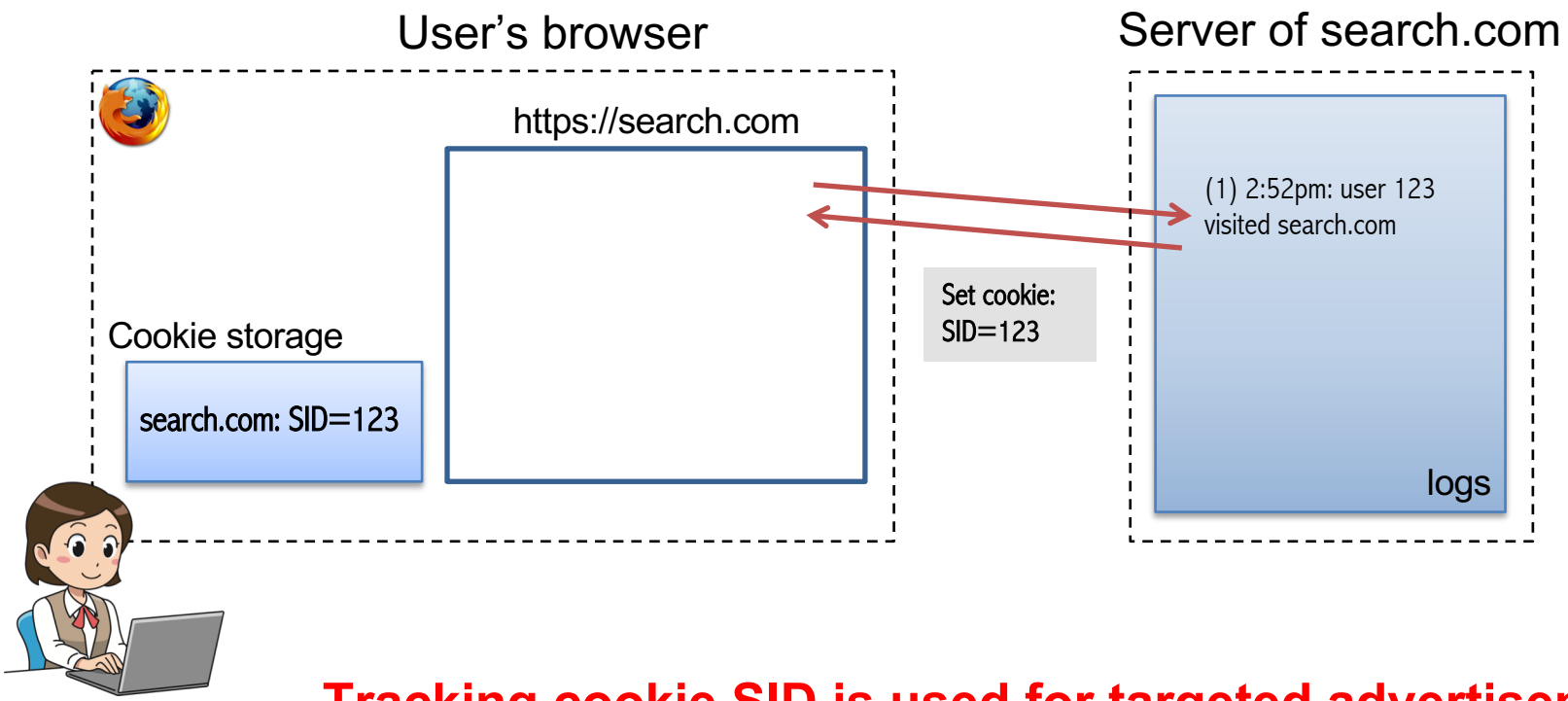
"user will generally not have a selective opinion to object to the sharing of the same data through another, yet similar, provider"

In practice this raises 2 issues:

shared responsibility between data controllers

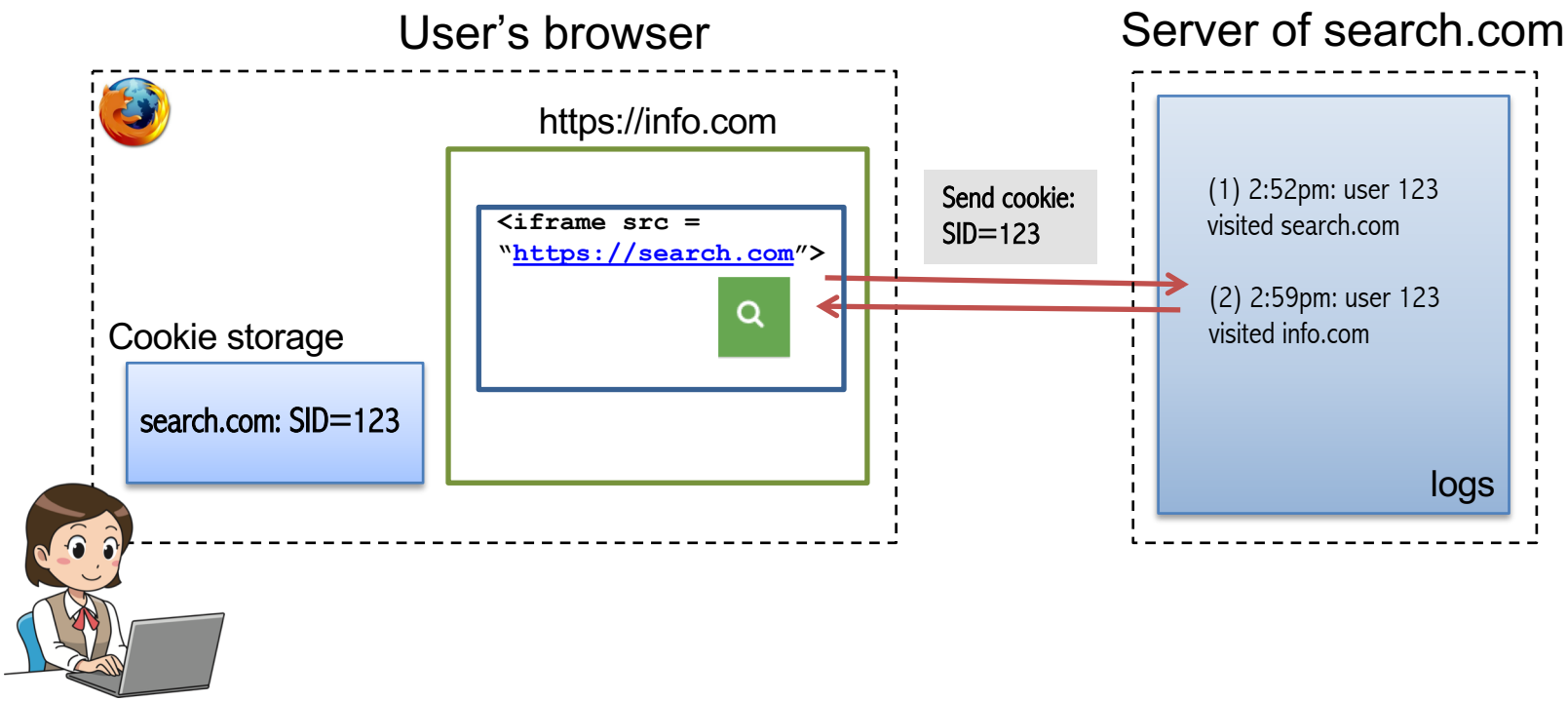
implies trust **on the way** consent was collected by other publishers or providers of third-party content?

Shared consent: example



Tracking cookie SID is used for targeted advertisement.

Shared consent: example



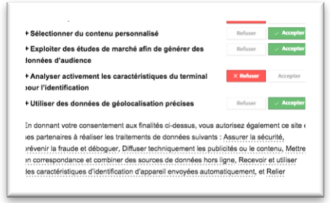
https://info.com

How can publisher of info.com be compliant?

OPTION 1: info.com collects consent itself

OPTION 2: info.com relies on consent already collected by a third party search.com

How can publisher of info.com be compliant?



OPTION 1: info.com collects consent itself

- Consent must be collected "**Prior to sending an identifier" (R2)**

https://info.com

https://info.com

How can publisher of info.com be compliant?

OPTION 1: info.com collects consent itself

- Consent must be collected "**Prior to sending an identifier" (R2)**

Refusal of consent makes website not working

- Prevents loading of third-party content (search widget)
- Access to website functionality is conditional to consent (tracking wall)
- Consent is not freely given

https://info.com

=> Publisher info.com is not compliant!

How can publisher be compliant?

OPTION 2: info.com relies on consent already collected by a third party search.com

- If consent on search.com is not valid, then **publisher is jointly responsible for non-compliance**!
- But publisher “includes” many third parties (often unaware of all because of “inclusion chain”)

=> Publisher cannot safely rely on all (unknown) third-parties!

How can a publisher be compliant?

OPTION 2: info.com relies on consent already collected by a third party search.com

- **Publisher can rely only on "negative consent"** (refusal) because no personal data processing is allowed

- **=> In general, publisher in today's Web cannot be compliant…**
- **Can the Web rely on shared consent at all?**

Consent expressed in technical settings?

- "Gatekeepers": mediate much of what occurs between user and the website, helps user to control the information to and from the equipment
- Could **technical browser settings** solve the challenges of shared consent? The choice expressed in the browser settings would be binding and enforceable against third-parties
- Art. 9 draft of the ePReg, Germany's last version excluded

~~*Article 9*~~

~~*Consent*~~

~~1. The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.~~

~~2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.~~

4 November 2020, German Presidency

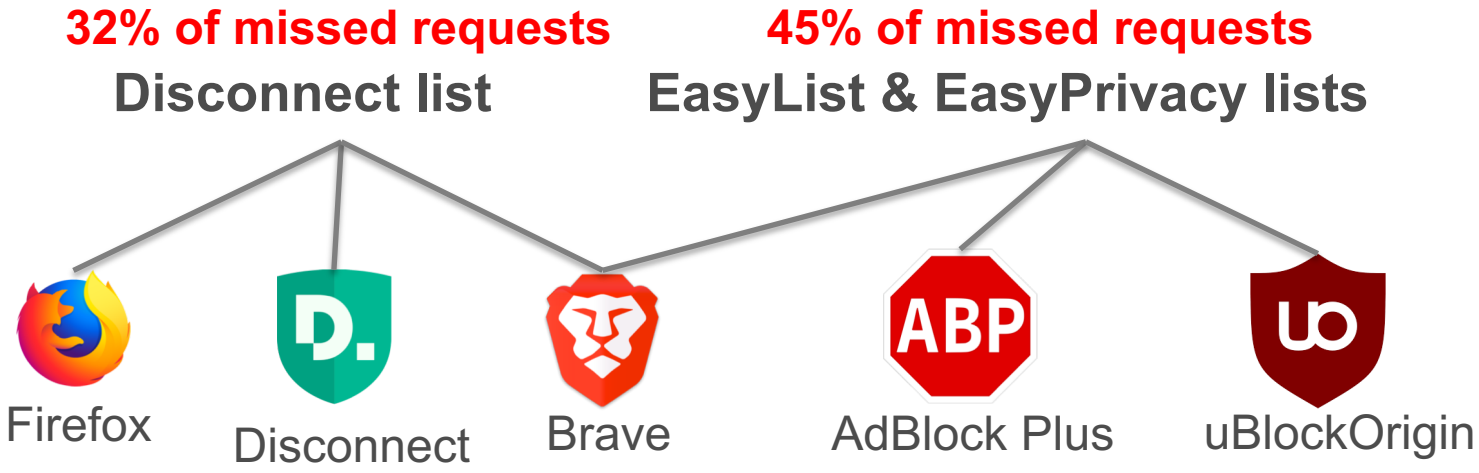
Remaining problem of the Web

Functional content is mixed with trackers that require consent!

- “Customized Search Engine” of Google (cse.google.com) receives google.com targeting cookies with functional content
- Content Delivery Network (CDN) Cloudflare inserts tracking cookies when delivering functional jQuery library (code.jquery.com)
- Tag managers Tealium (tags.tiqcdn.com) and Adobe (assets.adobedtm.com) insert tracking cookies into their tags

Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels. Imane Fouad, Nataliia Bielova, Arnaud Legout, Natasa Sarafijanovic-Djukic. *Privacy Enhancing Technologies (PoPETS 2020)*.

Can Web browsers block such sending?



No, because tracking cookies are sent with requests to fetch (functional) third-party content

Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels. Imane Fouad, Nataliia Bielova, Arnaud Legout, Natasa Sarafijanovic-Djukic. *Privacy Enhancing Technologies (PoPETS 2020)*.

Takeaway: browser vendors and Web developers

- **Web developers** can't really control what they include!

- **How to improve tracking detection?**
  - More fine-grained approaches than filter lists
  - Detect scripts responsible for sharing & syncing cookies
  - Detect fingerprinting scripts
  - Detect when functional content contains tracking

Takeaway: Data Protection Authorities

- **Most tech requirements are impossible to assess with technical means** because:
  - lack of standards on consent interfaces
  - lack of standards on consent collection and technical storage
  - lack of specification of purposes
  - lack of mapping purposes to legal basis

  ⇒ time-consuming, not scalable for automatic auditing of compliance

- **Update their guidelines on cookies and other trackers**
  - our contribution* to the CNIL (French DPA)
  - upcoming contribution to the Italian DPA

References

- **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. Accepted for publication at *International Journal on Technology and Regulation, 2020.* [PDF]
- **Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers?** Célestin Matte, Cristiana Santos, Nataliia Bielova. Annual Privacy Forum (APF 2020). [PDF]
- **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).* [PDF] [Video]
- **On Compliance of Cookie Purposes with the Purpose Specification Principle.** Imane Fouad, Cristiana Santos, Feras Al Kassar, Nataliia Bielova and Stefano Calzavara. International Workshop on Privacy Engineering (IWPE 2020). [PDF] [Video]
- **Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels.** Imane Fouad, Nataliia Bielova, Arnaud Legout, Natasa Sarafijanovic-Djukic. *Privacy Enhancing Technologies (PoPETS 2020)*. [PDF] [Video]
- **Browser Fingerprinting: A survey.** Pierre Laperdrix, Nataliia Bielova, Benoit Baudry and Gildas Avoine. *ACM Transactions on the Web (ACM TWEB), 2020.* [PDF]
- **Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective.** Colin Gray, Cristiana Santos, Nataliia Bielova, Michael Toth and Damian Clifford. *Accepted for publication at ACM CHI 2020.* [PDF]
- **Feedback to the EDPB regarding Guidelines 07/2020** on the concepts of controller and processor in the IAB Europe Transparency and Consent Framework, 2020, Nataliia Bielova, Cristiana Santos. [PDF]
- **Contribution to the public consultation on the CNIL's draft recommendation** on "cookies and other trackers", Michael Toth, Nataliia Bielova, Cristiana Santos, Vincent Roca, Célestin Matte. [PDF]