



Universiteit Utrecht



Web tracking, consent pop-ups and dark patterns: legal and technical perspectives

Nataliia Bielova

Researcher in Online Privacy
PRIVATICS team Inria



Cristiana Santos

Assist. Prof. in Law&Tech
Utrecht University



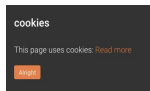
CIF Seminars @ KU Leuven
6th May 2021



Joint work with
Célestin Matte
Colin Gray
Damian Clifford
Michael Toth
Midas Nouwens
Vincent Roca



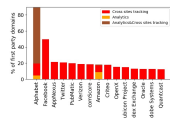
Outline of this talk



Why do we see consent pop-ups at all ?



How can we understand when a pop-up is compliant?



When does Web tracking violate the law?



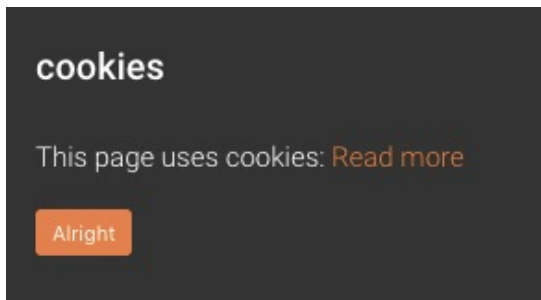
Analysis of **grey design choices** potentially violating legal requirements for consent



Future Work



Why do we see consent pop-ups at all ?!



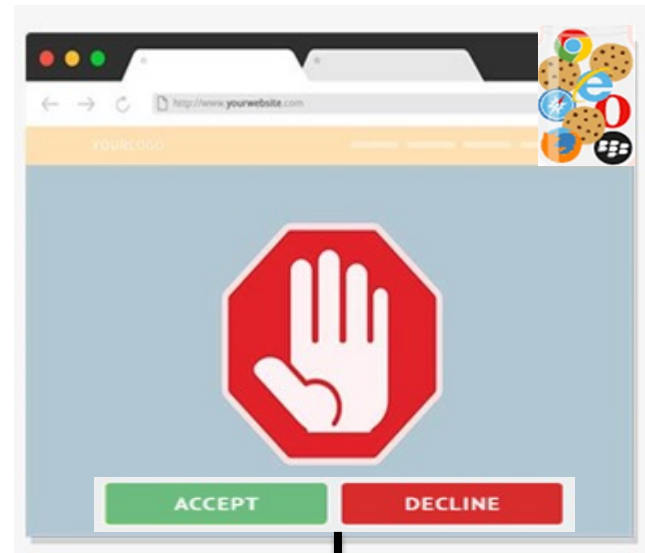
Why do we see consent pop-ups at all ?!



Applies to any form of web tracking
(such as cookies and similar technologies)
that collect/store data of users



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



consent pop-ups
common method to
collect consent



How can we understand when a pop-up is compliant?

It is easy, read the GDPR!



Requirements for consent pop-ups



Consent must be:

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

• How to audit for compliance?

- Detect all Web tracking technologies
- Manual, technical 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@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 Directive¹ 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. 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^{5, 6} that lead to nudging users to consent, data subjects are

¹ 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 GDPR related WPag Guidelines, for simplicity purposes, we only mention Article 29 Working Party.

² Article 29 Working Party, "Guidelines on consent under Regulation 2016/679" (WP29 rev. 01, 10 April 2018).

³ For example, the French DPA (henceforth named CNIL) decided to remove its cookie banner and to leave no trace 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.

⁴ Harry Brignull, "What are Dark Patterns?" (2018) <https://darkpatterns.org> accessed 7 May 2020.







⁵ Colin M. Gray, Yubo Kou, Bryan Batties, 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.

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

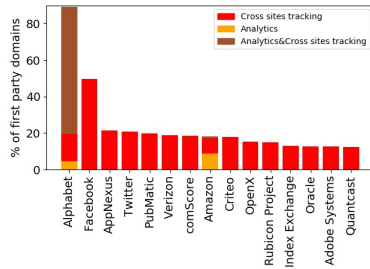


22 requirements for consent pop-up compliance!

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				
	R6 Accessibility of information page				
Informed	T (partial)	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)	✓	✓	-
	Combination of M and T (partially)	✓	✓	-	-
Unambiguous	R11 Affirmative action design	M or T (partially)	-	✓	L
	R12 Configurable banner	M (fully)	-	✓	L
	R13 Balanced choice	T (partially)	-	✓	CS
	R14 Post-consent registration	Combination of M and T (partially)	-	✓	CS
	R15 Correct consent registration	M (fully) or T (partially)	✓	✓	-
Readable and accessible	R16 Distinguishable	U	✓	✓	-
	R17 Intelligible	U	✓	✓	-
	R18 Accessible	U	✓	✓	-
	R19 Clear and plain language	M (fully) or T (partially)	-	✓	L
	R20 No consent wall	M (fully)	✓	✓	-
Revocable	R21 Possible to change in the future	Not possible	-	-	CS
	R22 Delete "consent cookie" and communicate to third parties				

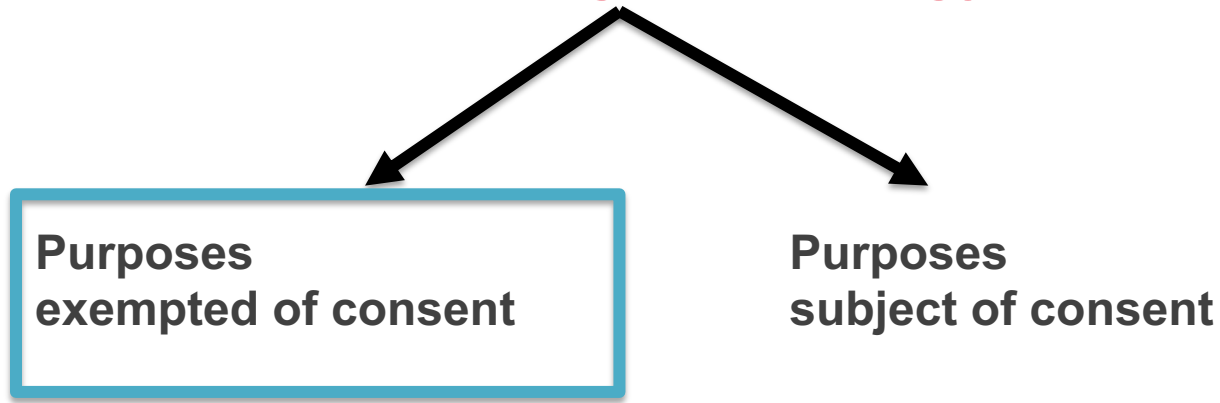


When does Web tracking violate the law?





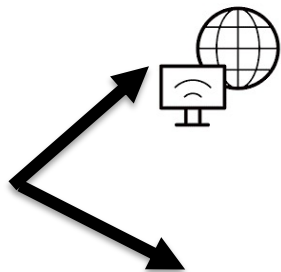
To answer this question, we need to know the purpose of each tracking technology!





Exempted purposes (Article 5(3) ePD)

“necessary”

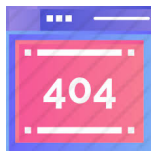


transmit a communication over an electronic communications network

cookies used to help web pages to load faster and to route information over a network (load balancing)



provide a service, requested by the user, to access content



Exempted purposes: necessary for providing a service ... because without it, no service!



e-commerce websites: for keeping track of my **shopping cart**

authentication: keeping me logged in, so users don't have to remember my login password, eg. email services, eBanking service

user interface (UI) preferences (customization): language, display format (nr of results), personalized services



web audience measuring of a website, without profiling users by third parties, e.g. nr users, click/person



user-security cookies: protect login system from abuses



multimedia session cookies: render image, audio/video content

> Necessary

Always Enabled

> Non-necessary

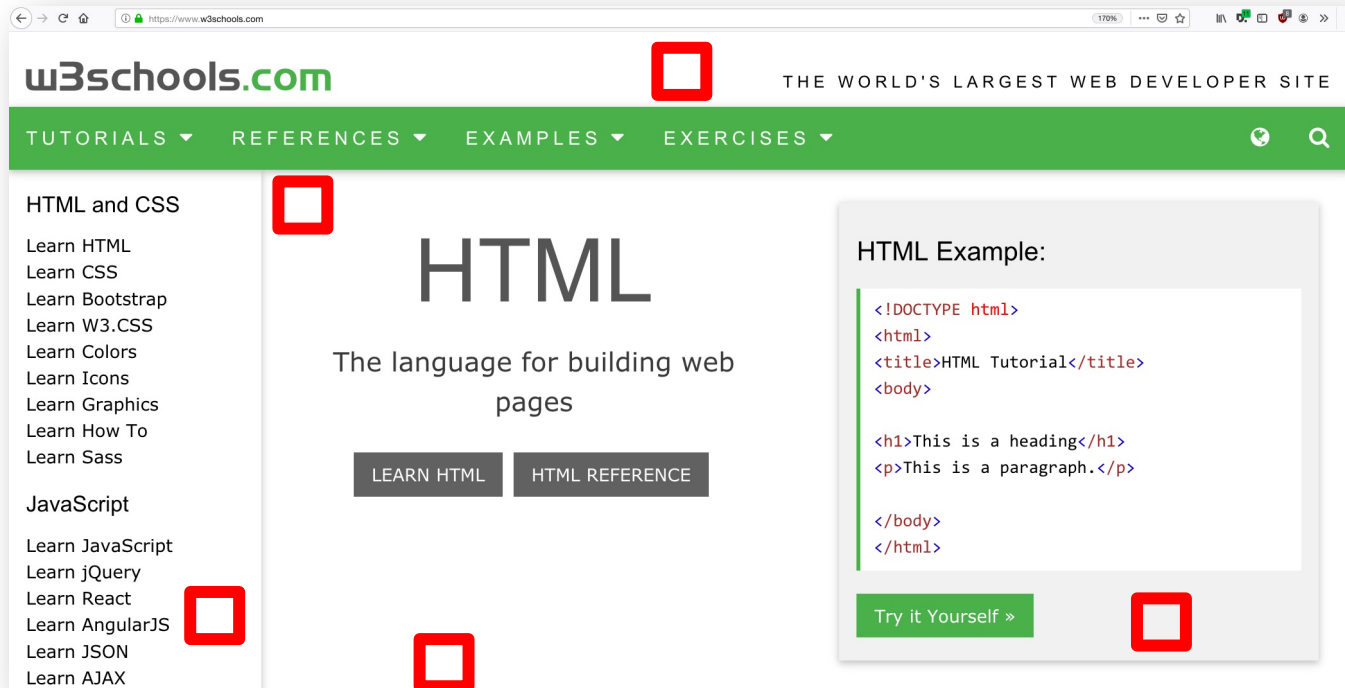
Disabled





But how to detect tracking with certainty?

Invisible pixels

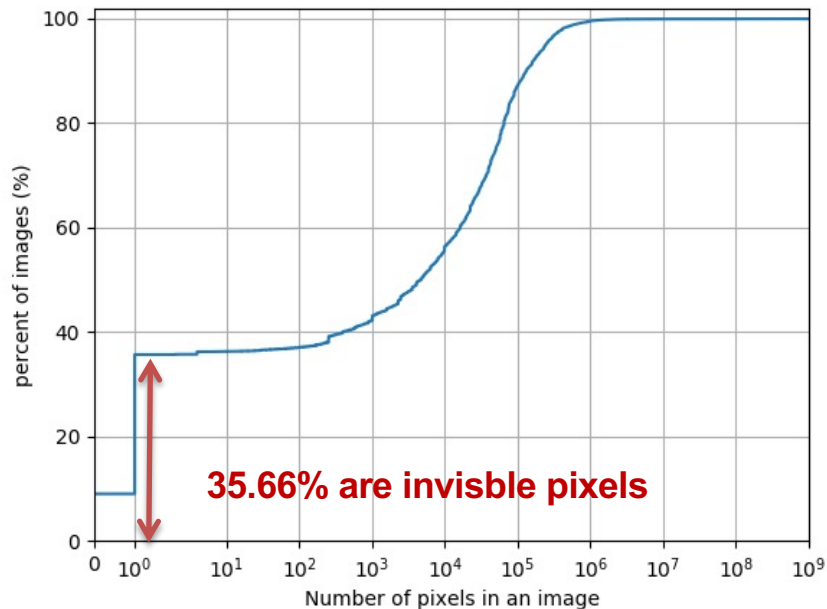


Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels. Imane Fouad, Nataliia Bielova, Arnaud Legout, Natasa Sarafijanovic-Djukic. Privacy Enhancing Technologies Symposium (PETS 2020).



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**

However all types of content track users!



What content is tracking users with cookies?

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

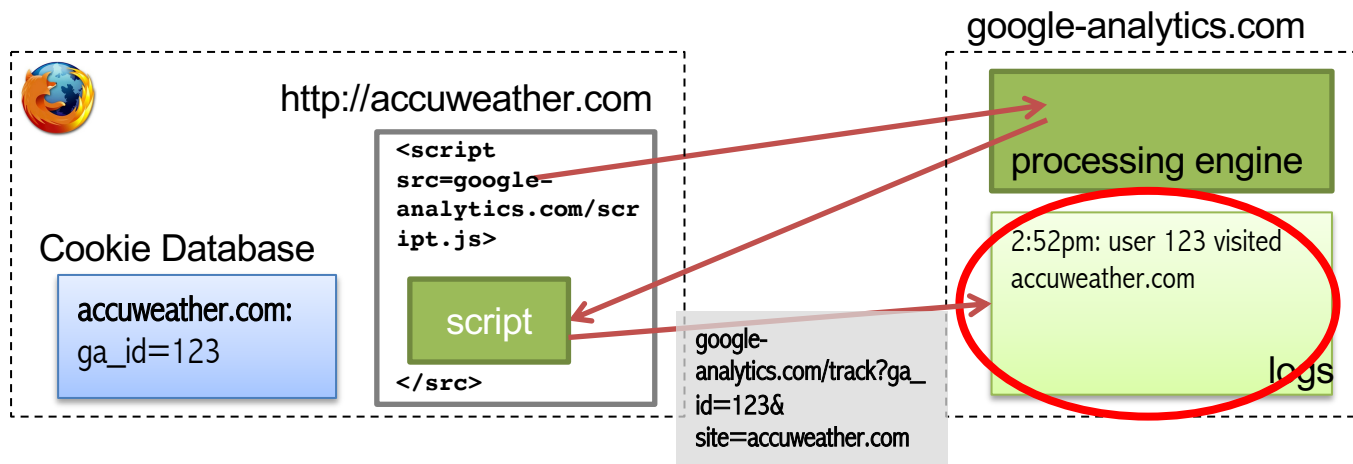
Content type	% requests
Script	34.36%
Invisible images	23.34 %
Text/html	20.01%
Big images	8.54 %
Application/json	4.32%

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

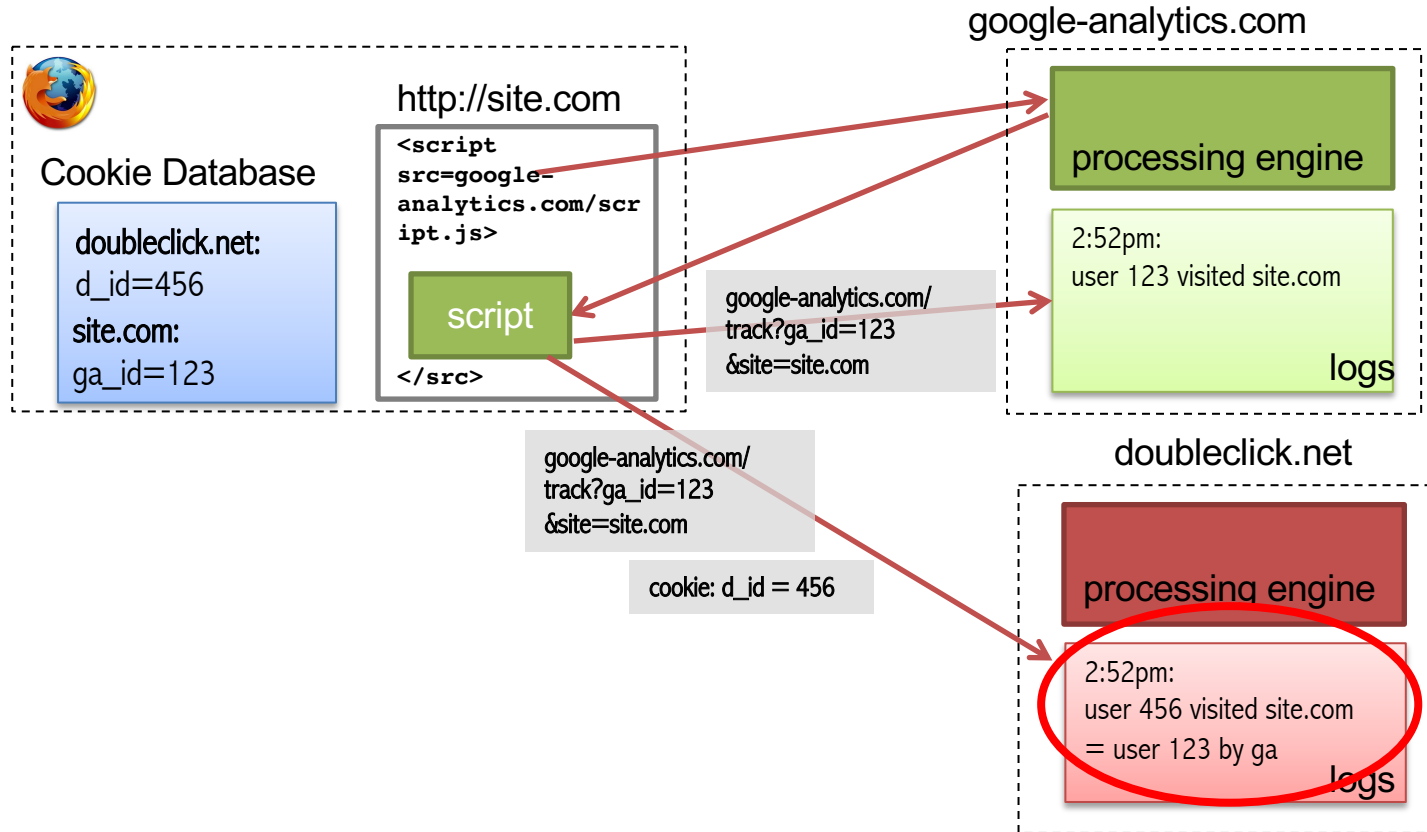


Analytics (within-site tracking only)

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



First party analytics cookies synchronized with third party cookies





First party analytics cookies synchronized with third party cookies

- 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](#)

Get the guide

Learn how Google Analytics can improve your Google Ads results.



CNIL sanction against CARREFOUR FRANCE (18 November 2020)

First party Google Analytics cookies detected

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 conséquences. [Les annonceurs peuvent] également combiner les produits afin d'identifier [leurs] segments et susciter l'intérêt de ces utilisateurs à l'aide de messages personnalisés.*

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

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

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



Computer scientists and DPAs detect tracking...

But how to know the purposes of trackers?



How to define purposes?



Principle of Purpose Specification (art. 5(1)(b) GDPR, WP203)



Specific

Precisely and clearly defined



Explicit

Unambiguous; no doubt in their meaning or intent; expressed, not hidden



Legitimate

Conform to a legal basis, e.g. consent for using cookies and similar technologies

We analysed cookie policies for 20,000 cookies...



Available

- **only 13% cookies** are described in cookie policies
- cookie policies should be available on all websites



Explicit

- **only 5% cookies** are explicit



Specific

- common cookies purposes are not specific!



EDPB, DPAs should pre-define and standardize purposes



Analysis of grey design choices potentially violating legal requirements for consent





DARK PATTERNS

applied to consent banners

Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective

Colin M. Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, Damian Clifford

User engagement with data privacy and security through consent banners has become a ubiquitous part of interacting with internet services. While previous work has addressed consent banners from either interaction design, legal, and ethics-focused perspectives, little research addresses the connections among multiple disciplinary approaches, including tensions and opportunities that transcend disciplinary boundaries. In this paper, we draw together perspectives and commentary from HCI, design, privacy and data protection, and legal research communities, using the language and strategies of "dark patterns" to perform an interaction criticism reading of three different types of consent banners. Our analysis builds upon designer, interface, user, and social context lenses to raise tensions and synergies that arise together in complex, contingent, and conflicting ways in the act of designing consent banners. We conclude with opportunities for transdisciplinary dialogue across legal, ethical, computer science, and interactive systems scholarship to translate matters of ethical concern into public policy.



Designer: Colin M. Gray
expertise in UX, UI, ethics, dark patterns



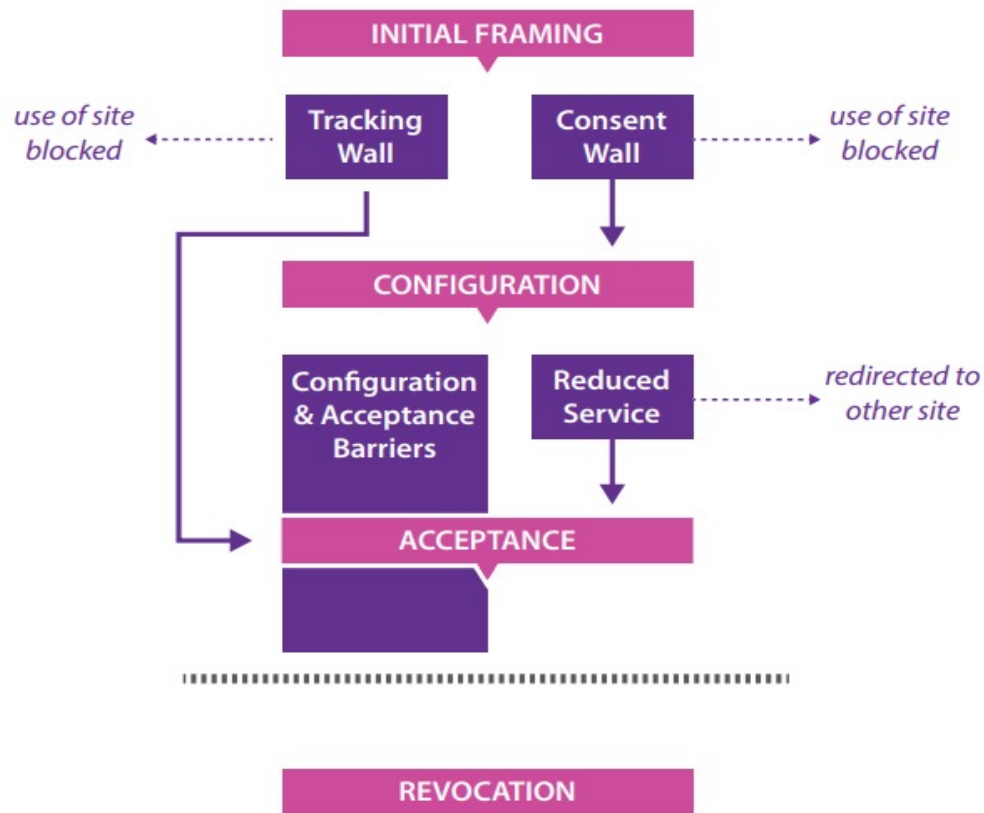
Legal scholars: Cristiana Santos, Damian Clifford
expertise in EU Data Protection law



Computer Scientists: Nataliia Bielova, Michael Toth
expertise in web privacy measurement



Best of ACM CHI Honorable mention, accepted at ACM CHI 2021 <https://arxiv.org/abs/2009.10194>

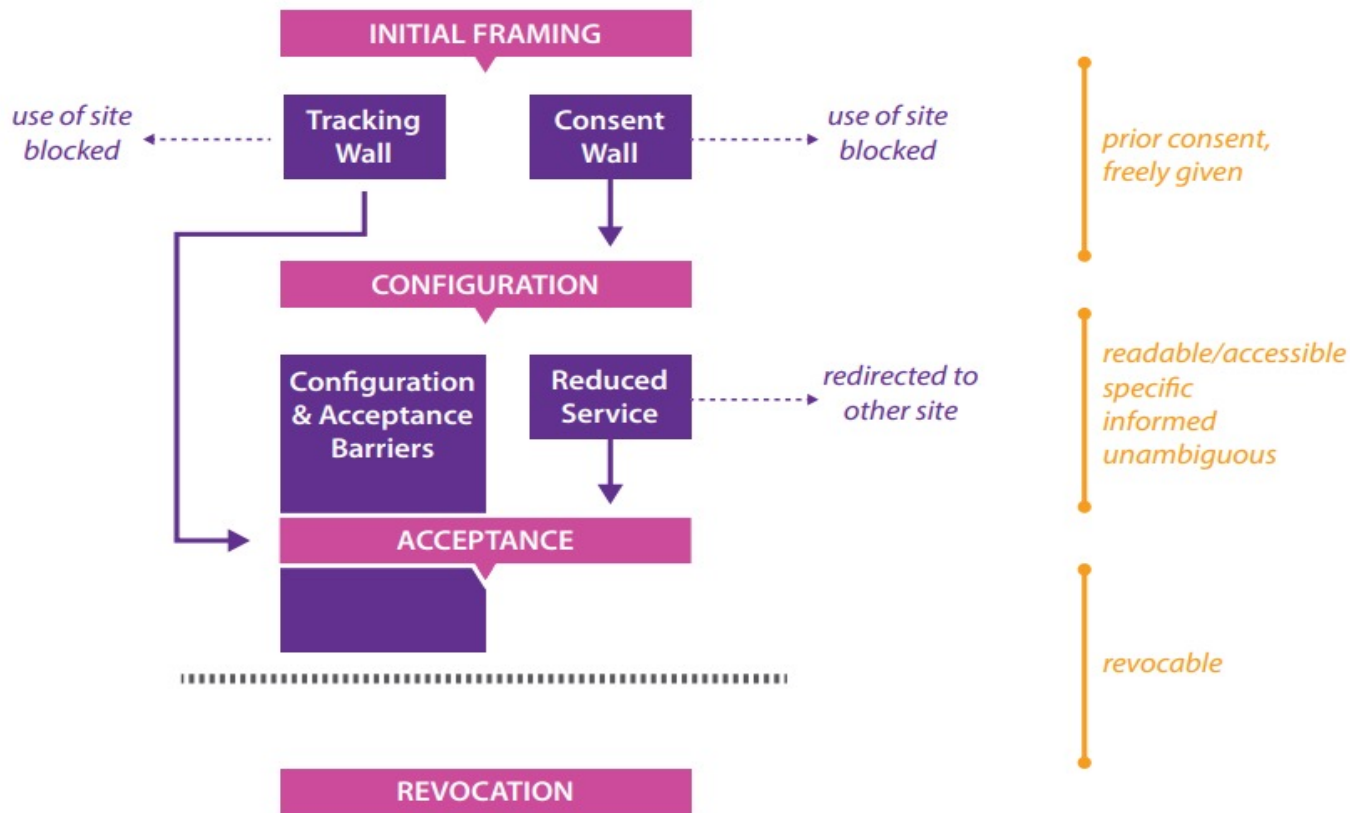




FORMS OF MANIPULATION

CONSENT TASK FLOW

CONSENT REQUIREMENTS

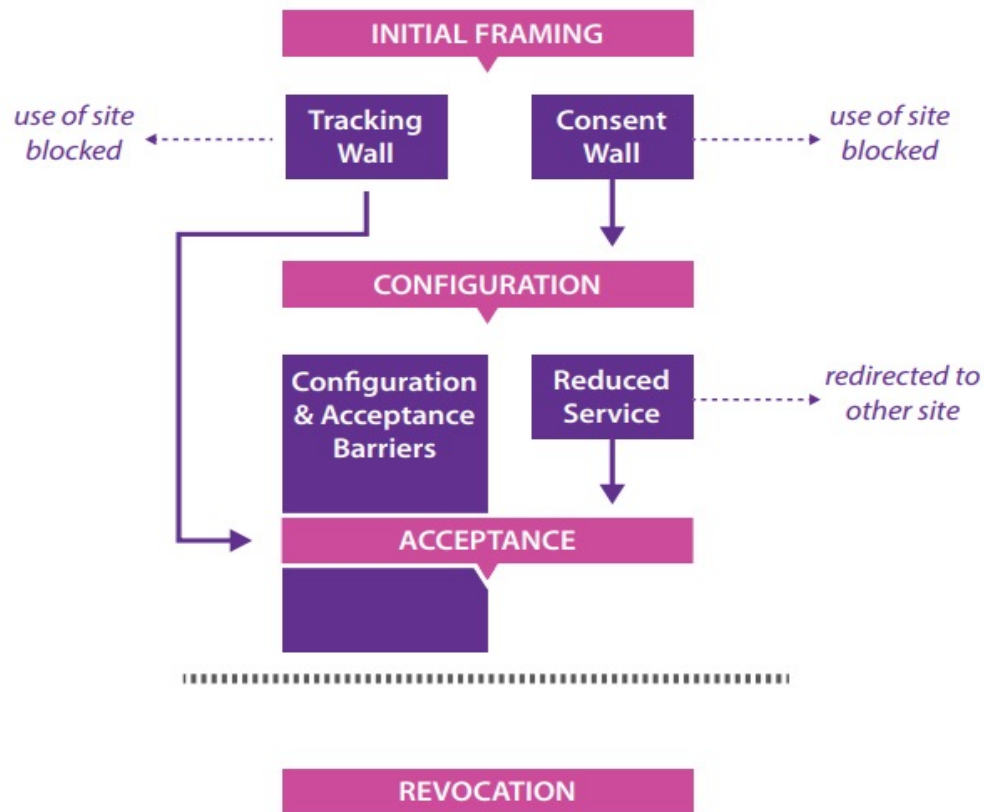


FORMS OF MANIPULATION

CONSENT TASK FLOW

CONSENT REQUIREMENTS

DARK PATTERN STRATEGIES



prior consent,
freely given

forced action

readable/accessible
specific
informed
unambiguous

interface interference
obstruction
sneaking

revocable

Grey design choices – grey zone



Consent Wall

Reduced Service

Grey design choices – grey zone



Consent Wall

Reduced Service



What is a 'Consent wall'?



The user can indeed select between acceptance and refusal;
BUT the use of the website is blocked until a choice is made

Your choices regarding cookies on this site

You can exercise choice and determine how your personal information is used by switching the consent toggles on or off. Each page on this site and our partners use your information. Please consent to process your personal information.

Service	Consent
Select personalised content	<input type="checkbox"/>
Select personalised ads	<input type="checkbox"/>
Select basic ads	<input type="checkbox"/>
Create a personalised ads profile	<input type="checkbox"/>
Create a personalised content profile	<input type="checkbox"/>
Measure ad performance	<input type="checkbox"/>
Measure content performance	<input type="checkbox"/>

Save & Close **Accept All** **Reject All**

What does the law say about 'consent wall'?



Art. 7(2) - request for consent shall be presented in a (...) **easily accessible form**

Recital 32 - consent request should not be **unnecessarily disruptive** to the use of the service for which it is provided



- Confusing, unnecessarily disruptive of the user experience
- The website should be accessible even if the user didn't respond to request for consent



Tension between user interaction and easily accessible consent request: **how enforceable/illegal is this design choice?**



Dark patterns related to 'consent wall'



The user can select between acceptance and refusal; however, the **use of the website is blocked** until a choice is made

Save & Close **Accept All** **Reject All**

The screenshot shows a Bloomberg website with a consent wall overlay. The consent wall has a title 'Your choices regarding cookies on this site' and a paragraph explaining that users can exercise choice and determine how their information is used. Below the text are several toggle switches for different cookie categories: 'Select personalised content', 'Select personalised ads', 'Select basic ads', 'Create a personalised ads profile', 'Create a personalised content profile', 'Measure ad performance', and 'Measure content performance'. At the bottom of the consent wall are three buttons: 'Save & Close', 'Accept All', and 'Reject All'. A red callout box with a red border contains the text 'The user can select between acceptance and refusal; however, the use of the website is blocked until a choice is made'. Two red arrows point from the callout box to the 'Accept All' and 'Reject All' buttons, which are also highlighted with red boxes.

DARK PATTERNS

- **Forced Action**
- **Obstruction**

Grey design choices – grey zone



Consent Wall

Reduced Service



What is 'Reduced Service'?



If the user refuses consent, she is redirected to a different website
<https://anon.healthline.com/>,

It is a reduced version of the original website, with only **10 pre-selected pages** available to the user

healthline

medicalnewstoday.com/privacy-settings

Privacy Settings

You can opt-out or change your preferences at any time by clicking on "Privacy Settings" in the footer at the bottom of the page.

This page explains how we and our partners use and process your personal data. We use cookies to enhance your browsing experience, to analyze site usage, and to assist in our marketing efforts. For more information about our cookies and data practices, please see our [Privacy Policy](#).

processing by our partners. However, because we need to collect and process your data to support our business, we request that you allow cookies in order to access all features and services on our site. If you do not allow cookies, you may not be able to use all of the features and services on our site. We will not share your data with any third parties without your consent.

provide you the full site experience if you disallow any purposes, features, or partners. If you do not allow cookies, you may not be able to use all of the features and services on our site. We will not share your data with any third parties without your consent.

that shows 10 of our most popular articles without ads, cookies, or tracking technology.

Partners

IAB TCF Partner

DISALLOW ALL

ALLOW ALL AND CONTINUE TO SITE

anon.healthline.com

You're seeing this version because you disallowed cookies. [Update your privacy settings.](#)

Welcome to our ad-free, tracking-free version of Healthline

We detect that you are in one of the member countries of the EU/EEA, which is now subject to the General Data Protection Regulation (GDPR). Unfortunately, a tracking-free version of our full website is currently unavailable in these countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market.

While we continue to identify technical compliance solutions that will allow all readers to experience our content, we are providing you with 10 articles that highlight the breadth and quality of our content. You are on this page because you disallowed the purposes listed in the "How we use your data" section of our Privacy Settings page.

We believe that health information should be free to everyone and we rely on advertising to make this possible on our family of websites: Healthline, Medical News Today, Greatist, and Everyday Family. Providing the best health information in the world is expensive. We spend up to thousands of dollars per article to ensure it is accurate and precise with quality review by a doctor or other certified, trained medical professional.



What is 'Reduced Service'?



DARK PATTERNS

- Forced Action
- Obstruction
- Interface interference
- Sneaking

If the user refuses consent, she is redirected to a different website
<https://anon.healthline.com/>,

It is a reduced version of the original website, with only **10 pre-selected pages** available to the user

healthline

You're seeing this version because you disallowed cookies. [Update your privacy settings.](#)

Welcome to our ad-free, tracking-free version of Healthline

We detect that you are in one of the member countries of the EU/EEA, which is now subject to the General Data Protection Regulation (GDPR). Unfortunately, a tracking-free version of our full website is currently unavailable in these countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market.

While we continue to identify technical compliance solutions that will allow all readers to experience our content, we are providing you with 10 articles that highlight the breadth and quality of our content. You are on this page because you disallowed the purposes listed in the "How we use your data" section of our Privacy Settings page.

We believe that health information should be free to everyone and we rely on advertising to make this possible on our family of websites Healthline, Medical News Today, Greatist, and Everyday Family. Providing the best health information in the world is expensive. We spend up to thousands of dollars per article to ensure it is accurate and precise with quality review by a doctor or other certified, trained medical professional.



Is 'Reduced Service' illegal or acceptable?



Arts. 4(11), 7(4): consent freely given
Rec. 42: 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, persuasion coercion



• Freedom to reject non-necessary cookies without detriment



“Certain cases may exist where lack of acceptance of the use of cookies prevents (...) partial or full use of the service, provided that users are **adequately informed** on it, an **alternative** of access to the service without the need to accept the use of cookies is provided. (...) the services of both alternatives **must be genuinely equivalent**, and equivalent services offered by an external entity with regard to the editor will not be accepted”

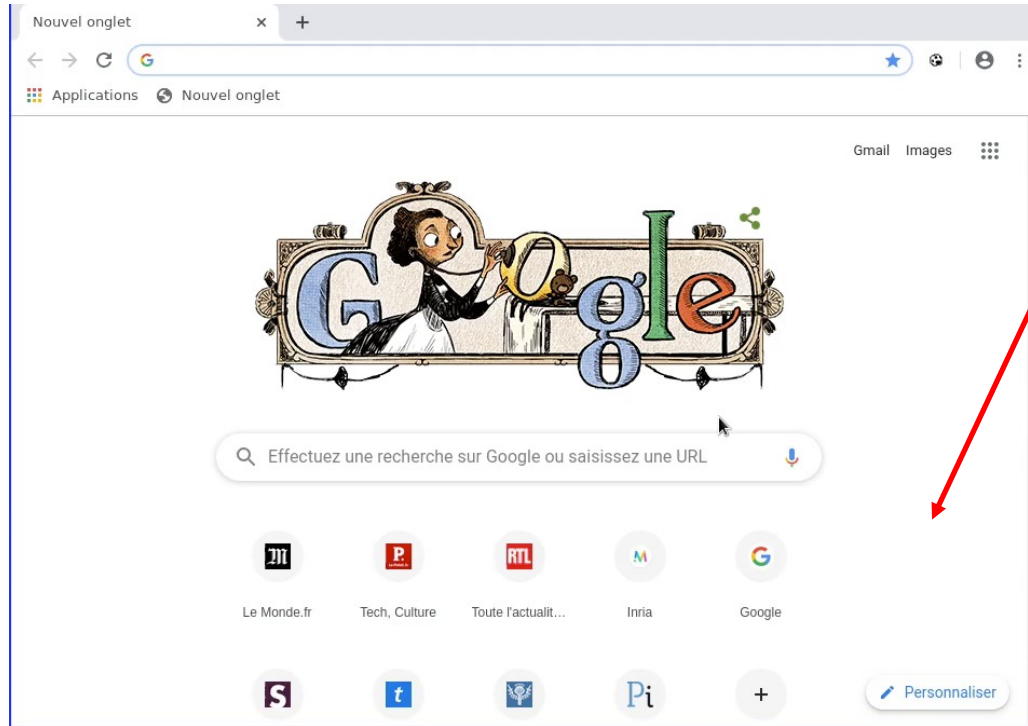


Is it enough to look at the design of a banner?

What happens behind the interface of a cookie banner?



Violation of '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!

Video availbale at https://www-sop.inria.fr/members/Nataliia.Bielova/cookiebanners/vid/nonrespect_flashscore_com.mp4



Violations found on websites with TCF banners

- 27 websites register your **acceptance even if you said “no”**
- 141 websites store your consent **before you made your choice**
- 38 websites **do not allow to say “no”**
- 236 websites nudge users by **pre-selecting options**



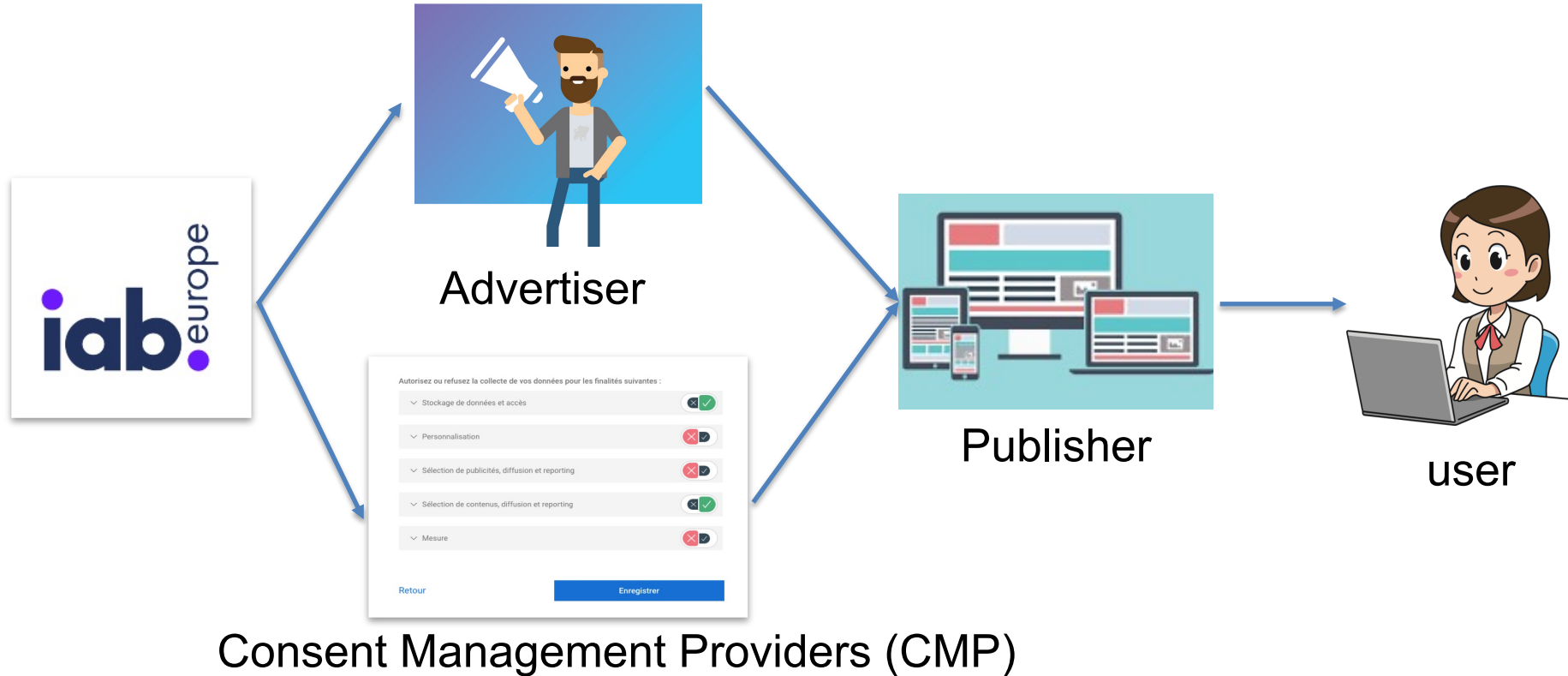
- **NOYB** filed 3 complaints to the **CNIL** based on our research!



We have impact!

- Most popular websites have fixed their practices
- See historical videos here: <https://www-sop.inria.fr/members/Nataliia.Bielova/cookiebanners/>

IAB Europe Transparency & Consent Framework





IAB Europe TCF: Consent Management Providers provide banners with dark patterns by default

OneTrust is the most popular CMP on top global 10,000 websites

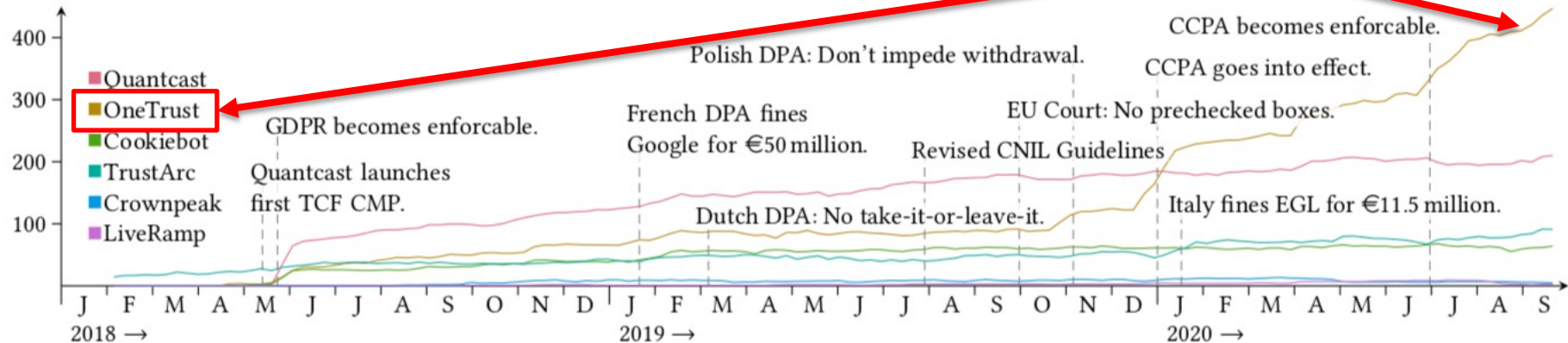


Figure 6: Number of websites in the Tranco 10k toplist that embed a CMP. We include a non-exhaustive timeline of events with relevance to the GDPR and the CCPA.

OneTrust

Top level of the page:
easily accessible
“Allow All”

Bottom of the screen:
hardly accessible
“Reject All” and
“Confirm My Choices”

CookiePro
by OneTrust

About Your Privacy

We process your data to deliver content or advertisements and measure the delivery of such content or advertisements to extract insights about our website. We share this information with our partners on the basis of consent and legitimate interest. You may exercise your right to consent or object to a legitimate interest, based on a specific purpose below or at a partner level in the link under each purpose. These choices will be signaled to our vendors participating in the Transparency and Consent Framework. [More information](#)

Allow All

Manage Preferences

Create a personalised ads profile

A profile can be built about you and your interests to show you personalised ads that are relevant to you.

Object to Legitimate Interests

[List of IAB Vendors](#) | [View Full Legal Text](#)

Measure content performance

The performance and effectiveness of content that you see or interact with can be measured.

Object to Legitimate Interests

[List of IAB Vendors](#) | [View Full Legal Text](#)

Apply market research to generate audience insights

Market research can be used to learn more about the audiences who visit sites/apps and view ads.

Object to Legitimate Interests

[List of IAB Vendors](#) | [View Full Legal Text](#)

Select personalised content

Personalised content can be shown to you based on a profile about you

identification

Your device can be identified based on a scan of your device's unique combination of characteristics.

[List of IAB Vendors](#) | [View Full Legal Text](#)

Match and combine offline data sources

Always Active

Data from offline data sources can be combined with your online activity in support of one or more purposes

[List of IAB Vendors](#) | [View Full Legal Text](#)

Ensure security, prevent fraud, and debug

Always Active

Your data can be used to monitor for and prevent fraudulent activity, and ensure systems and processes work properly and securely.

[List of IAB Vendors](#) | [View Full Legal Text](#)

Receive and use automatically-sent device characteristics for identification

Always Active

Your device might be distinguished from other devices based on information it automatically sends, such as IP address or browser type.

[List of IAB Vendors](#) | [View Full Legal Text](#)

Link different devices

Always Active

Different devices can be determined as belonging to you or your household in support of one or more of purposes.

[List of IAB Vendors](#) | [View Full Legal Text](#)

Technically deliver ads or content

Always Active

Your device can receive and send information that allows you to see and interact with ads and content.

[List of IAB Vendors](#) | [View Full Legal Text](#)

Reject All

Confirm My Choices

Powered by OneTrust

OneTrust default banner, captured on 13 Jan. 2021

OneTrust

Top level of the page:
easily accessible
“Allow All”

Bottom of the screen:
hardly accessible
“Reject All” and
“Confirm My Choices”

DARK PATTERNS

- Obstruction
- False Hierarchy
- Sneaking

CookiePro
by OneTrust

About Your Privacy

We process your data to deliver content or advertisements and measure the delivery of such content or advertisements to extract insights about our website. We share this information with our partners on the basis of consent and legitimate interest. You may exercise your right to consent or object to a legitimate interest, based on a specific purpose below or at a partner level in the link under each purpose. These choices will be signaled to our vendors participating in the Transparency and Consent Framework. [More information](#)

Allow All

Manage Preferences

Create a personalised ads profile

A profile can be built about you and your interests to show you personalised ads that are relevant to you.

Object to Legitimate Interests

[List of IAB Vendors](#) | [View Full Legal Text](#)

Measure content performance

The performance and effectiveness of content that you see or interact with can be measured.

Object to Legitimate Interests

[List of IAB Vendors](#) | [View Full Legal Text](#)

Apply market research to generate audience insights

Market research can be used to learn more about the audiences who visit sites/apps and view ads.

Object to Legitimate Interests

[List of IAB Vendors](#) | [View Full Legal Text](#)

Select personalised content

Personalised content can be shown to you based on a profile about you

identification

Your device can be identified based on a scan of your device's unique combination of characteristics.

[List of IAB Vendors](#) | [View Full Legal Text](#)

Match and combine offline data sources

Always Active

Data from offline data sources can be combined with your online activity in support of one or more purposes

[List of IAB Vendors](#) | [View Full Legal Text](#)

Ensure security, prevent fraud, and debug

Always Active

Your data can be used to monitor for and prevent fraudulent activity, and ensure systems and processes work properly and securely.

[List of IAB Vendors](#) | [View Full Legal Text](#)

Receive and use automatically-sent device characteristics for identification

Always Active

Your device might be distinguished from other devices based on information it automatically sends, such as IP address or browser type.

[List of IAB Vendors](#) | [View Full Legal Text](#)

Link different devices

Always Active

Different devices can be determined as belonging to you or your household in support of one or more of purposes.

[List of IAB Vendors](#) | [View Full Legal Text](#)

Technically deliver ads or content

Always Active

Your device can receive and send information that allows you to see and interact with ads and content.

[List of IAB Vendors](#) | [View Full Legal Text](#)

Reject All

Confirm My Choices

Powered by OneTrust

OneTrust default banner, captured on 13 Jan. 2021

Consent Management Platforms under the GDPR: processors or controllers? Cristiana Santos, Michael Toth, Nataliia Bielova, Midas Nouwens, Vincent Roca. Soon to be discussed at **ConPro'21**, accepted for publication at **Annual Privacy Forum (APF'21)**.



What's next? 

Auditing legal compliance of websites



Data
controllers

need to declare all the third parties and the **purposes of all the tracking technologies** they use



DPOs

want **scalable auditing** to ensure compliance



DPAs

need precise and scalable auditing to enable enforcement, and to react towards complaints they receive daily

How can we improve the situation?



Collaborate!

embrace interdisciplinary research between Law, Computer Science, Design and other fields



Contribute to public consultations!

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

Talk to DPAs!

researchers and DPAs should collaborate – check our interview at the LINC of the **CNIL** on consent pop-ups!

Share ideas & contacts: help us change the consent pop-ups practices in the EU and the world!

Thank you!

Nataliia Bielova

Researcher in Online Privacy
PRIVATICS team, Inria



nataliia.bielova@inria.fr



@nataliabelova

Cristiana Santos

Lecturer and Researcher in Law&Tech
Utrecht University



cristianasantos@protonmail.com



@cristianapt