universität innsbruck
Institut für Informatik

1st International Workshop on Consent Management in Online Services, Networks and Things (COnSeNT 2021), co-located with 6th IEEE Euro S&P, 7 September 2021

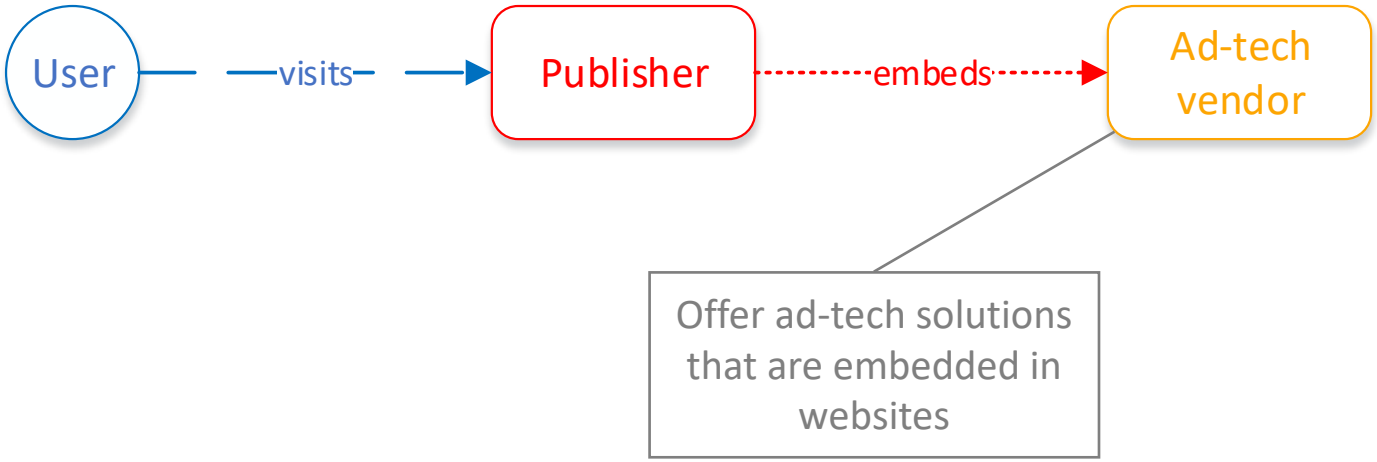
Drivers and Obstacles for the Adoption of Consent Management Solutions by Ad-Tech Providers

Paulina Jo Pesch

Image: Tiia Monto, Wikimedia Commons, Image License: CC Attribution-Share Alike 3.0 Unported

universität innsbruck
Institut für Informatik

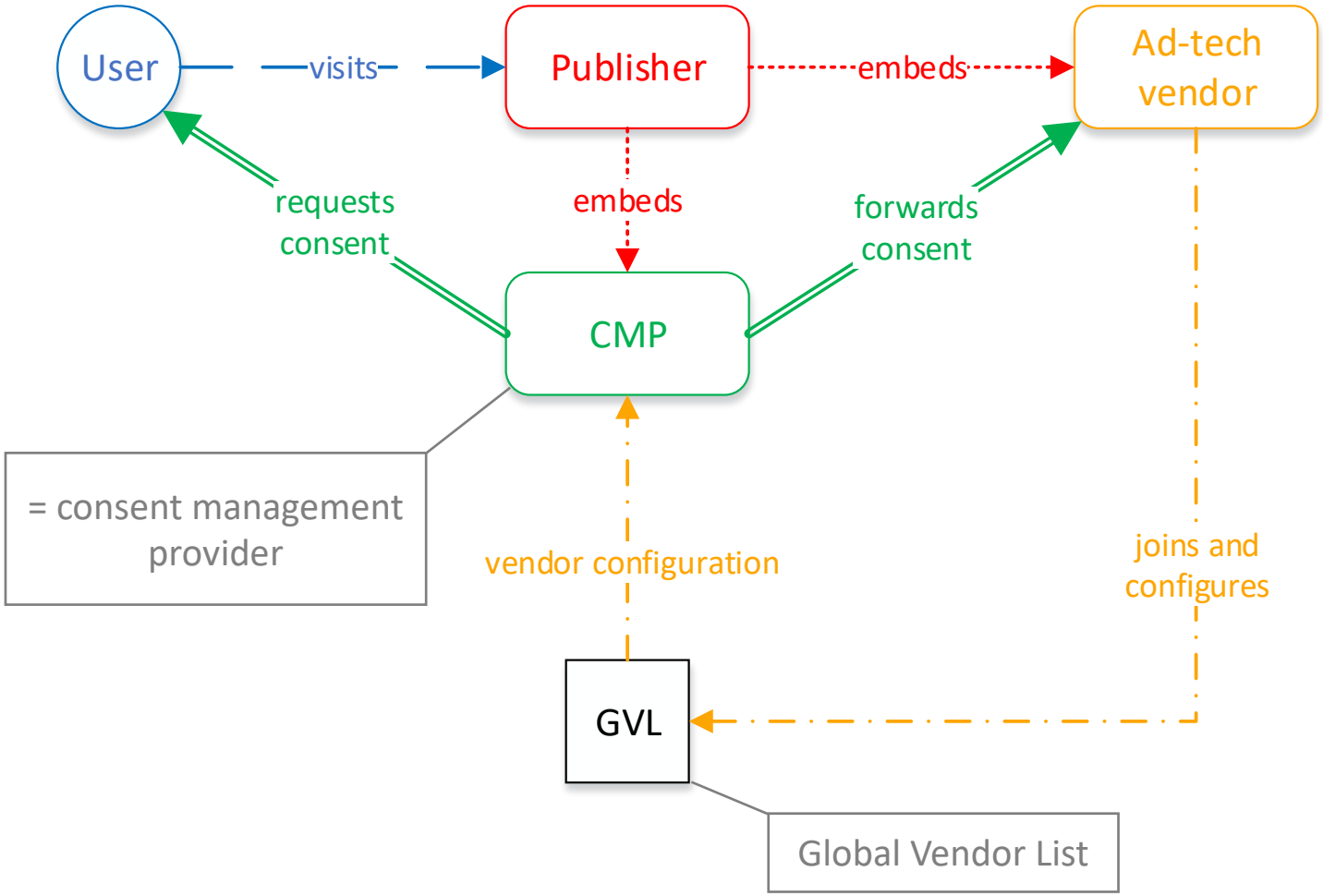
1. Introduction: embedding “ad-tech”



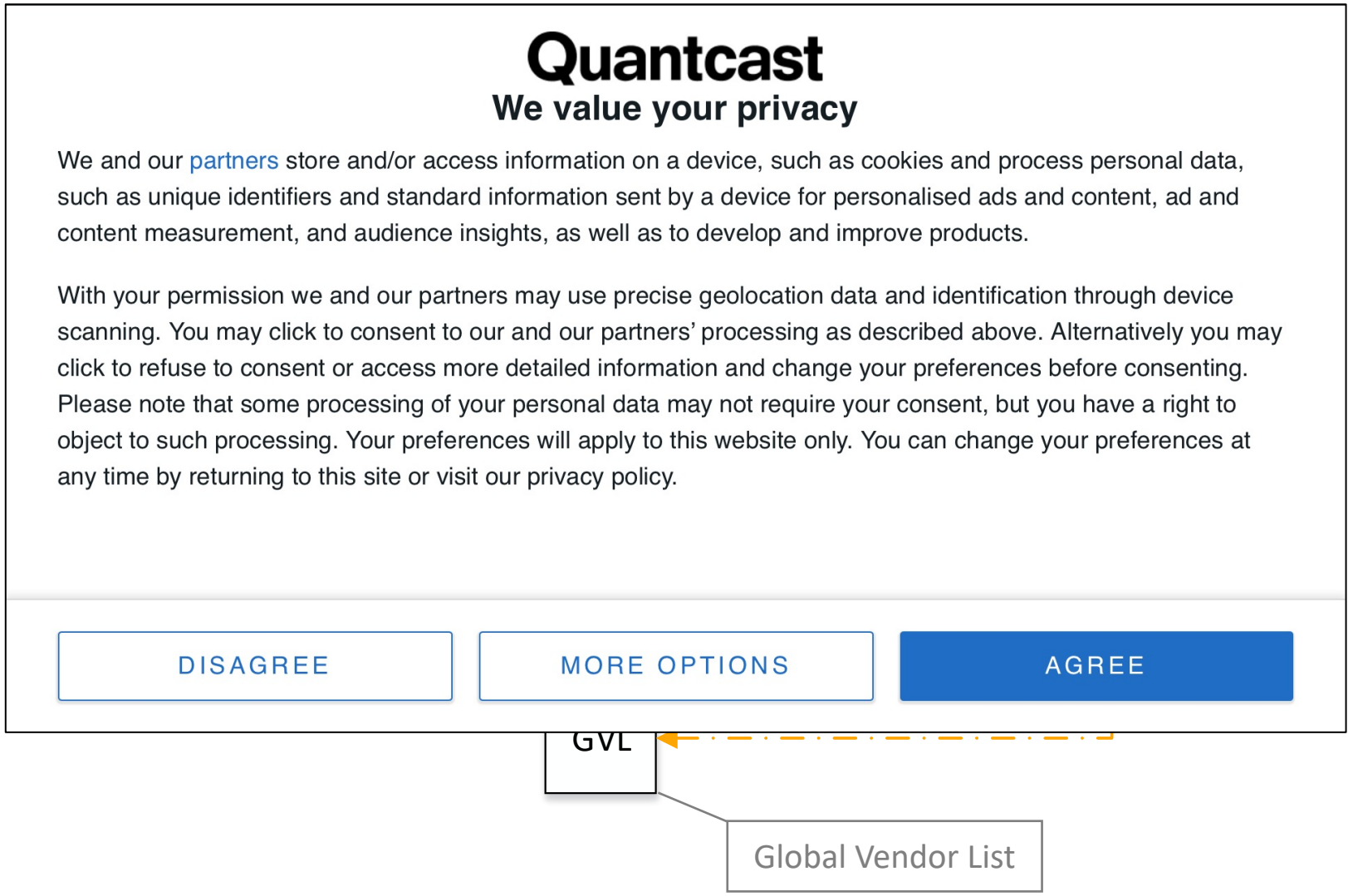
universität innsbruck
Institut für Informatik

1. Introduction: embedding “ad-tech”

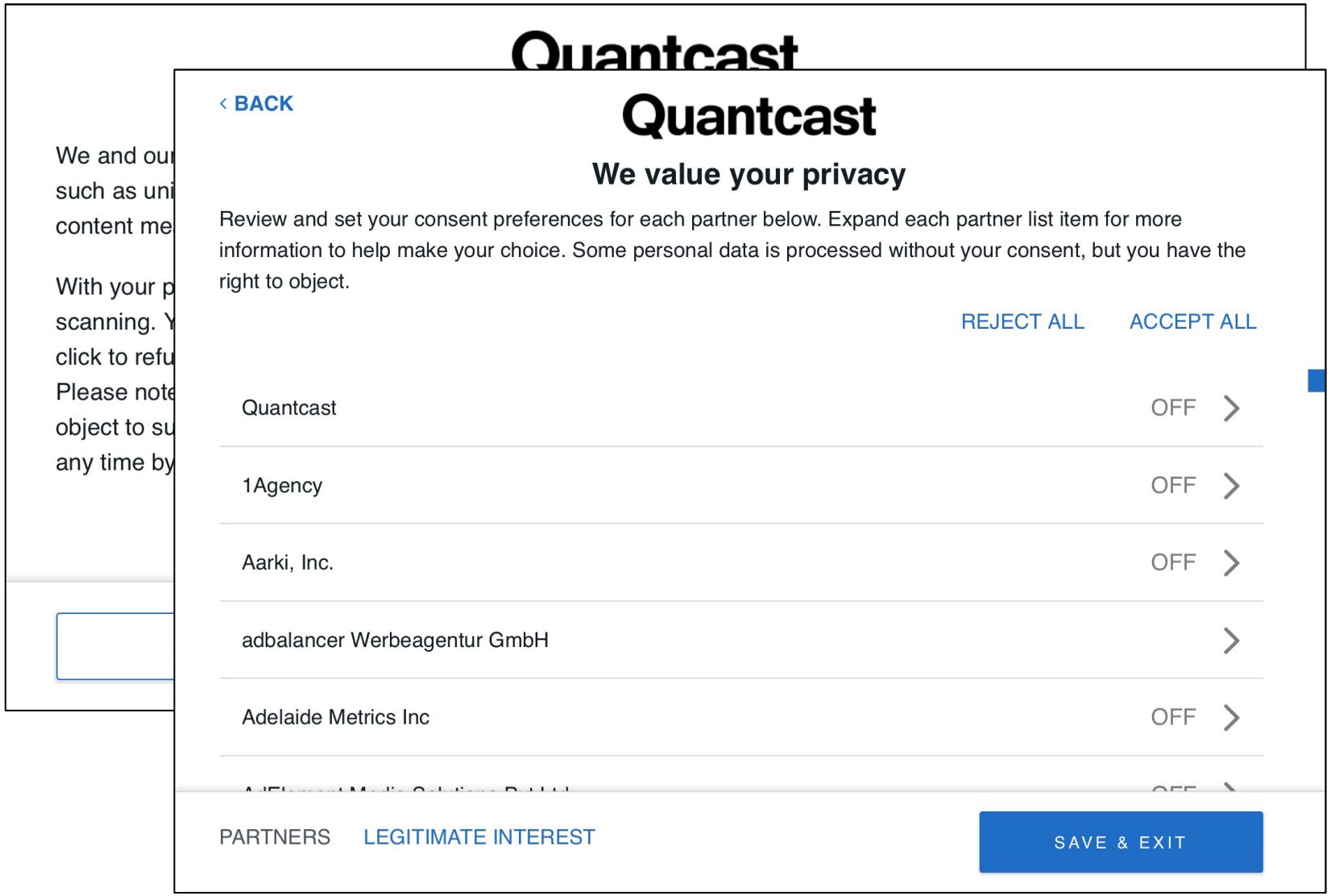
1. Introduction: involving a CMP



1. Introduction: involving a CMP



1. Introduction: involving a CMP



1. Introduction: the TCF

universität innsbruck
Institut für Informatik

TCF = Transparency and Consent Framework

Industry standard by the Interactive Advertising Bureau (IAB)

Comprising technical specifications and policies for *CMPs*, *ad-tech vendors* and *publishers*

In order to collect consent through *CMPs, ad-tech vendors* have to

(1.) join the GVL and

(2.) set their config, i.e.

(a) choose which purposes they process personal data for, and

(b) which legal basis they base the data processing on

1. Introduction: the TCF

TCF = Transparency and Consent Framewo

Industry standard by the Interactive Adver

Comprising technical specifications and po
and *publishers*

In order to collect consent through *CMPs,*

(1.) join the GVL and

(2.) set their config, i.e.

(a) choose which **purposes** they process personal data for, and

(b) which legal basis they base the data processing on

- Appendix A: Purposes and Features Definitions
  - A. Purposes
  - Purpose 1 - Store and/or access information on a device
  - Purpose 2 - Select basic ads
  - Purpose 3 - Create a personalised ads profile
  - Purpose 4 - Select personalised ads
  - Purpose 5 - Create a personalised content profile
  - Purpose 6 - Select personalised content
  - Purpose 7 - Measure ad performance
  - Purpose 8 - Measure content performance
  - Purpose 9 - Apply market research to generate audience insights
  - Purpose 10 - Develop and improve products

1. Introduction: the TCF

TCF = Transparency and Consent Framework

Industry standard by the Interactive Advertising Bureau (IAB)

Comprising technical specifications and policies for *CMPs*, *ad-tech vendors* and *publishers*

In order to collect consent through *CMPs, ad-tech vendors* have to

(1.) join the GVL and

(2.) set their config, i.e.

(a) choose which pur
process personal

(b) which **legal basis** they base the data processing on

i. consent as its sole legal base

ii. legitimate interest as its sole legal base

iii. consent or legitimate interest as its Legal Bases, selected in accordance with the Policy and Specifications

1. Introduction: the TCF

TCF = Transparency and Consent Framework

Industry standard by the Interactive Advertising Bureau (IAB)

Comprising technical specifications and policies for *CMPs*, *ad-tech vendors* and *publishers*

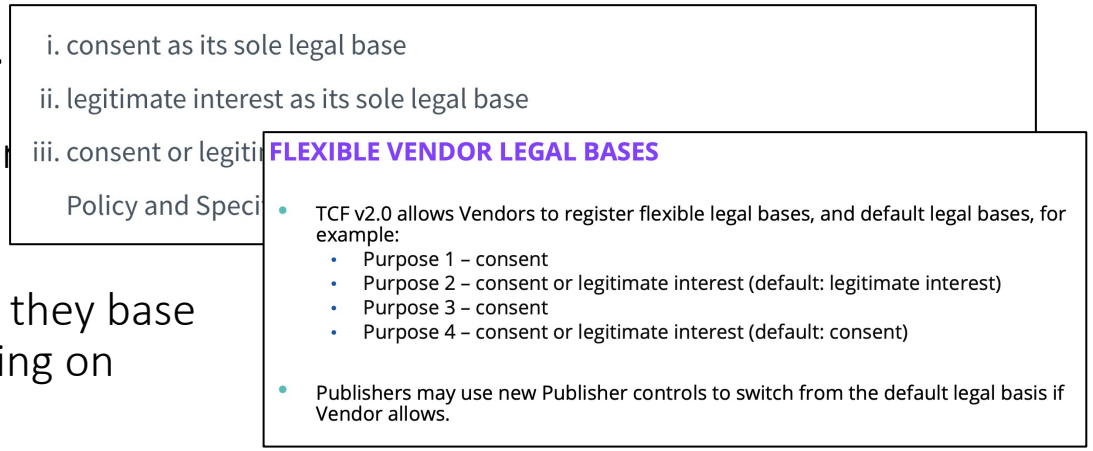
In order to collect consent through *CMPs, ad-tech vendors* have to

(1.) join the GVL and

(2.) set their config, i.e.

(a) choose which pur
process personal

(b) which **legal basis** they base the data processing on



1. Introduction: the TCF

The TCF purpose definitions are too unclear to base informed consent on.
CNIL, 2018

Often the option to refuse consent is hidden, or refusing consent requires more clicks than giving unrestricted consent. In these cases users' consent is not valid.
CNIL, 2019; Nouwens et. al., 2020

Often cookies are stored on the user's computer without them having given consent. In these cases there is no consent.
Matte et. al., 2020

2. High-level research questions

a) What drives GVL adoption and configuration?

- Why do ad-tech vendors join the GVL?

2. High-level research questions

a) What drives GVL adoption and configuration?

- Why do ad-tech vendors join the GVL?
- What drives ad-tech vendors' configuration decisions?

2. High-level research questions

a) What drives GVL adoption and configuration?
   - Why do ad-tech vendors join the GVL?
   - What drives ad-tech vendors' configuration decisions?

b) Do ad-tech vendors see compliance risks of the GVL membership?

3. Empirical approach: measurement basis

Hils et. al., Measuring the Emergence of Consent Management on the Web, IMC'20

Longitudinal measurements of the consent management ecosystem:

> 160 Mio. browser-crawls (toplist- and social media based selection of URLs)

Systematic download of all versions of the GVL, i.e. the list of all GVL members and their configurations

Source: https://vendor-list.consensu.org/v2/vendor-list.json
and for historical versions Internet Archive, https://archive.org/web/

Field experiment measuring user behaviour

Measuring the Emergence of Consent Management on the Web

Maximilian Hils
University of Innsbruck
maximilian.hils@uibk.ac.at

Daniel W. Woods
University of Innsbruck
daniel.woods@uibk.ac.at

Rainer Böhme
University of Innsbruck
rainer.boehme@uibk.ac.at

ABSTRACT

Privacy laws like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have pushed internet firms processing personal data to obtain user consent. Uncertainty around sanctions for non-compliance led many websites to embed a Consent Management Provider (CMP), which collects users' consent and shares it with third-party vendors and other websites. Our paper maps the formation of this ecosystem using longitudinal measurements. Primary and secondary data sources are used to measure each actor within the ecosystem. Using 161 million browser crawls, we estimate that CMP adoption doubled from June 2018 to June 2019 and then doubled again until June 2020. Sampling 4.2 million unique domains, we observe that CMP adoption is most prevalent among moderately popular websites (Tranco top 50-10k) but a long tail exists. Using APIs from the ad-tech industry, we quantify the purposes and lawful bases used to justify processing personal data. A controlled experiment on a public website provides novel insights into how the time-to-complete of two leading CMPs' consent dialogues varies with the preferences expressed, showing how privacy aware users incur a significant time cost.

CCS CONCEPTS

• Networks → Network measurement; • Information systems → Online advertising; • Security and privacy → Privacy protections; Usability in security and privacy.

KEYWORDS

GDPR, CCPA, consent, privacy, web measurement

ACM Reference Format:

Maximilian Hils, Daniel W. Woods, and Rainer Böhme. 2020. Measuring the Emergence of Consent Management on the Web. In *ACM Internet Measurement Conference (IMC '20), October 27–29, 2020, Virtual Event, USA.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3419394.3423647

1 INTRODUCTION

Vendors harvesting personal data prefer operating beyond the user's attention as evidenced by the use of secret tracking technologies [1, 29, 38]. This was tolerated by websites who rely on advertising revenues [51]. Sanctions associated with recent privacy laws threaten this state of affairs. In the EU, the General Data Protection Regulation (GDPR) requires firms processing personal data to establish a legal basis, such as by obtaining user consent. In the US, the California Consumer Privacy Act (CCPA) requires websites to collect the consent of minors and also to allow users to opt-out of the sale of their personal data. To comply with both laws, an infrastructure of consent must be designed so that users can consent to the privacy practices of websites and Ad-tech vendors.

In the past, each website offered a unique privacy policy and dialogue. This diversity overwhelmed users who could not commit hundreds of hours to reading each privacy policy [6, 36] nor navigate novel interface designs without making errors [2]. Privacy advocates argued that users should set preferences in the browser to avoid such problems [9, 27, 34], whereas Ad-tech companies lobbied against standardized privacy. However, the new imperative to obtain consent creates problems for Ad-tech vendors who must manage and document heterogeneous forms of consent collected across multiple websites.

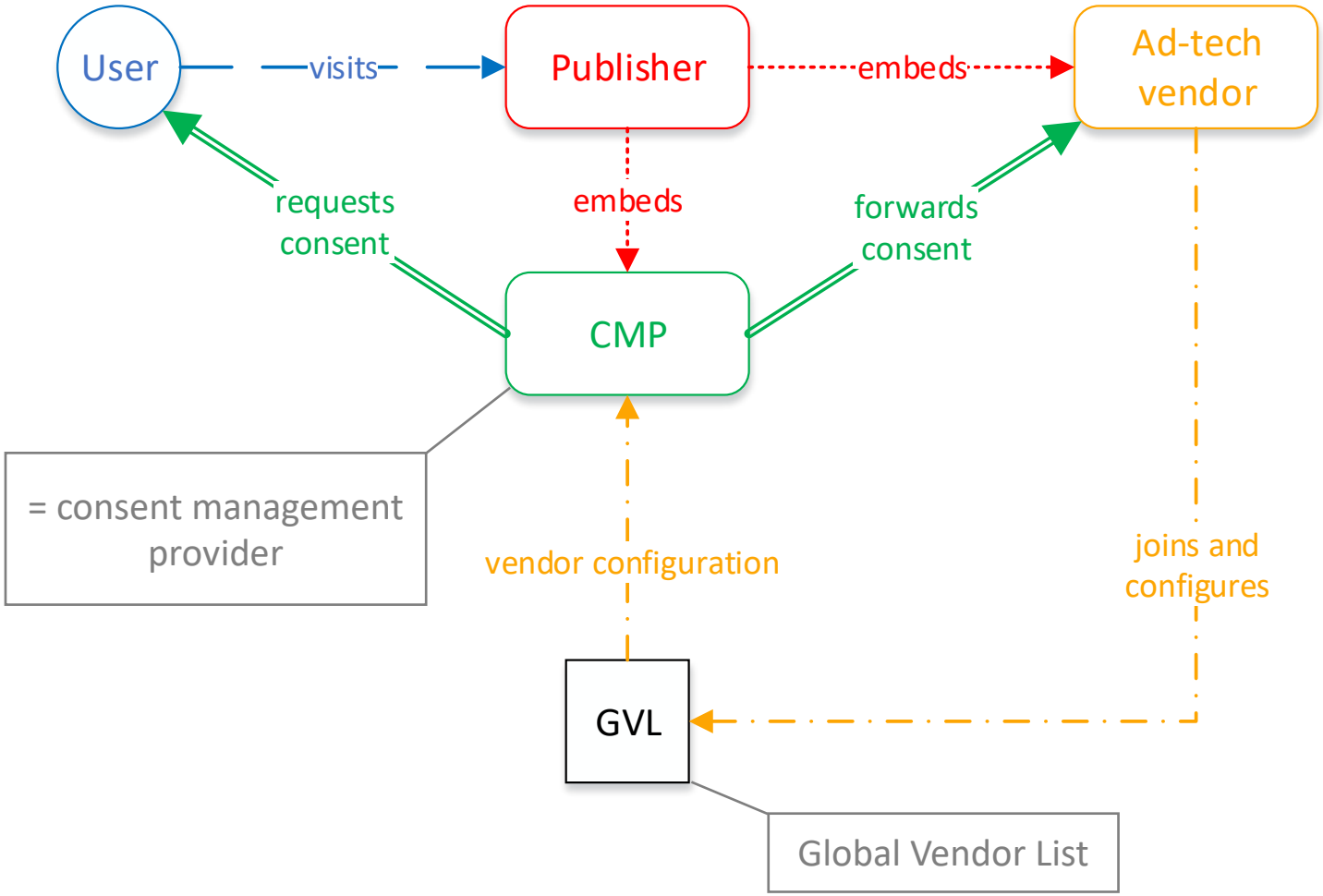
Consent management providers (CMPs) emerged in the last three years to standardize the collection of online consent. These intermediaries define legal terms and conditions, present those to users via an embedded consent dialogue, store the resulting signal, and share it with third-parties. In essence, CMPs have created a consent ecosystem involving users, websites, and third-party vendors. For example, one CMP allows websites to collect consent for a 'Global Vendor List' with a membership fee of 1200 €, which was termed the commodification of consent [60].

The rise of CMPs represents a new stage in how privacy preferences are communicated, with previous stages including cookies settings in browsers [37] or custom cookie banners on websites [53]. This paper offers a longitudinal study of the formation of a consent ecosystem orchestrated by CMPs. We introduce the notion of a consent flow—from users through consent dialogues to a website and then onto third-parties—and make measurements at each interface. This complements post-GDPR related work relying on snapshots of relatively small samples of domains, which is shown in Figure 1.

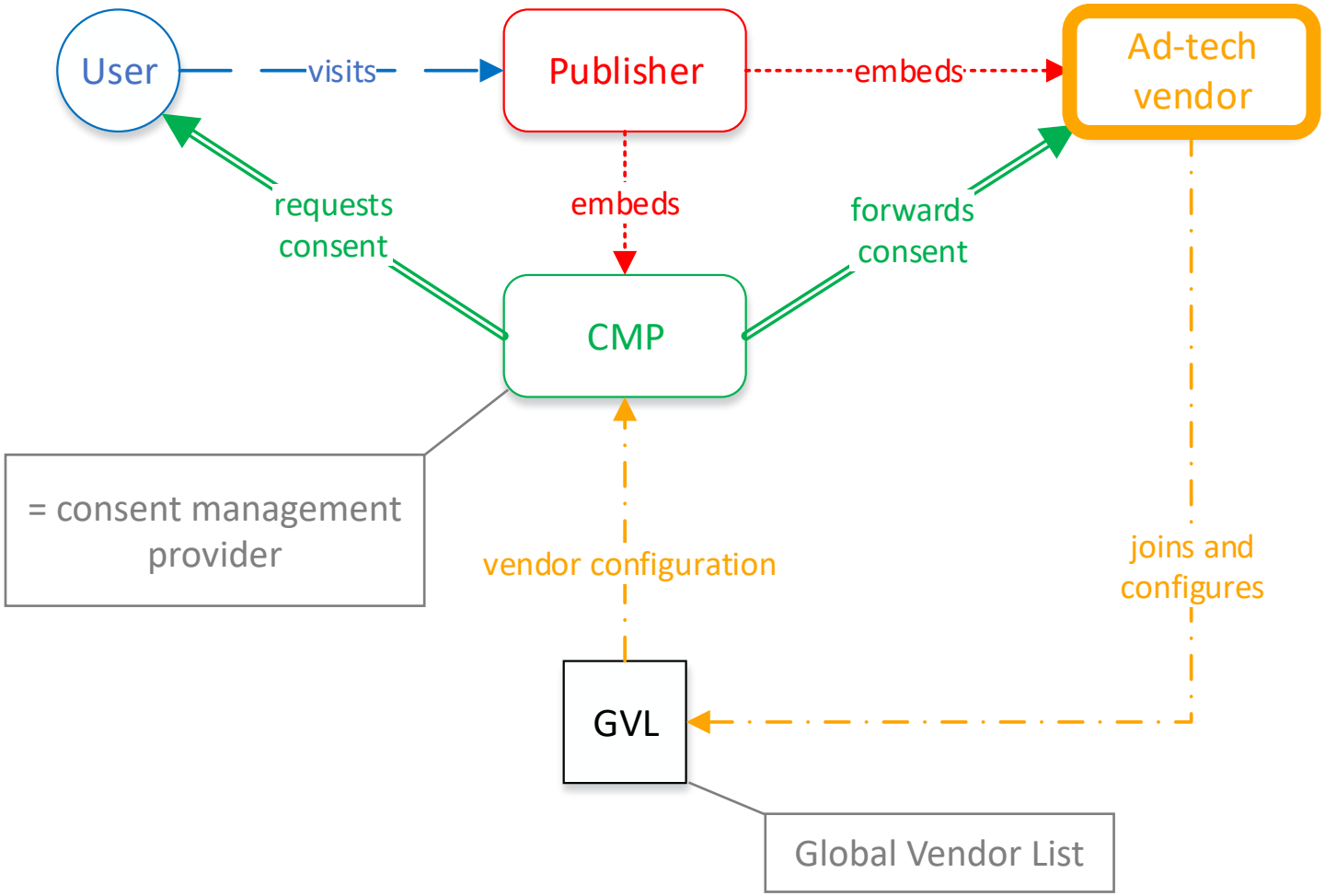
Our insights include:

- Using 161 million browser crawls, we measure CMP adoption over time and by website popularity. We show that uptake is most prevalent among 'mid-market' sites ($50^{th} - 10,000^{th}$), although this varies between CMPs. We also show the winners and losers of inter-CMP competition in the form of websites switching CMPs.
- In terms of methodology, we introduce a novel URL sampling approach seeded by social media shares, which improves subsite coverage. This is complemented by a traditional toplist sample.

3. Empirical approach: vendor interviews



3. Empirical approach: vendor interviews



3. Empirical approach: vendor interviews

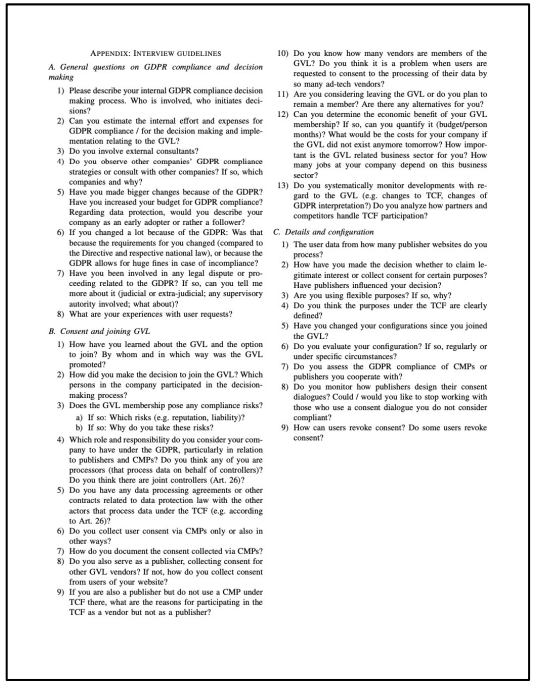
Semi-structured interviews

Interview guidelines with questions concerning…

… **GDPR compliance** in general

… **GVL membership**

… **GVL configuration** and the **behaviour of others** under the TCF



APPENDIX: INTERVIEW GUIDELINES

A. General questions on GDPR compliance and decision making

1) Please describe your internal GDPR compliance decision making process. Who is involved, who initiates decisions?
2) Can you estimate the internal effort and expenses for GDPR compliance / for the decision making and implementation relating to the GVL?
3) Do you involve external consultants?
4) Do you observe other companies' GDPR compliance strategies or consult with other companies? If so, which companies and why?
5) Have you made bigger changes because of the GDPR? Have you increased your budget for GDPR compliance? Regarding data protection, would you describe your company as an early adopter or rather a follower?
6) If you changed a lot because of the GDPR: Was that because the requirements for you changed (compared to the Directive and respective national law), or because the GDPR allows for huge fines in case of incompliance?
7) Have you been involved in any legal dispute or proceeding related to the GDPR? If so, can you tell me more about it (judicial or extra-judicial; any supervisory autority involved; what about)?
8) What are your experiences with user requests?

B. Consent and joining GVL

1) How have you learned about the GVL and the option to join? By whom and in which way was the GVL promoted?
2) How did you make the decision to join the GVL? Which persons in the company participated in the decision-making process?
3) Does the GVL membership pose any compliance risks?
   a) If so: Which risks (e.g. reputation, liability)?
   b) If so: Why do you take these risks?
4) Which role and responsibility do you consider your company to have under the GDPR, particularly in relation to publishers and CMPs? Do you think any of you are processors (that process data on behalf of controllers)? Do you think there are joint controllers (Art. 26)?
5) Do you have any data processing agreements or other contracts related to data protection law with the other actors that process data under the TCF (e.g. according to Art. 26)?
6) Do you collect user consent via CMPs only or also in other ways?
7) How do you document the consent collected via CMPs?
8) Do you also serve as a publisher, collecting consent for other GVL vendors? If not, how do you collect consent from users of your website?
9) If you are also a publisher but do not use a CMP under TCF there, what are the reasons for participating in the TCF as a vendor but not as a publisher?
10) Do you know how many vendors are members of the GVL? Do you think it is a problem when users are requested to consent to the processing of their data by so many ad-tech vendors?
11) Are you considering leaving the GVL or do you plan to remain a member? Are there any alternatives for you?
12) Can you determine the economic benefit of your GVL membership? If so, can you quantify it (budget/person months)? What would be the costs for your company if the GVL did not exist anymore tomorrow? How important is the GVL related business sector for you? How many jobs at your company depend on this business sector?
13) Do you systematically monitor developments with regard to the GVL (e.g. changes to TCF, changes of GDPR interpretation?) Do you analyze how partners and competitors handle TCF participation?

C. Details and configuration

1) The user data from how many publisher websites do you process?
2) How have you made the decision whether to claim legitimate interest or collect consent for certain purposes? Have publishers influenced your decision?
3) Are you using flexible purposes? If so, why?
4) Do you think the purposes under the TCF are clearly defined?
5) Have you changed your configurations since you joined the GVL?
6) Do you evaluate your configuration? If so, regularly or under specific circumstances?
7) Do you assess the GDPR compliance of CMPs or publishers you cooperate with?
8) Do you monitor how publishers design their consent dialogues? Could / would you like to stop working with those who use a consent dialogue you do not consider compliant?
9) How can users revoke consent? Do some users revoke consent?

3. Empirical approach: vendor interviews

universität innsbruck
Institut für Informatik

Semi-structured interviews

Round 1: **German-based** *ad-tech vendors*

Round 2: **International** *ad-tech vendors* that met the following **4 criteria**

(1) Picked **at least seven purposes**

(2) Claim **legitimate interest** for at least one purpose

(3) Use the **"flexible purpose" option**

(4) „flexible purposes" are **not identical** with those that the vendor, **by default, claims legitimate interest for**

3. Empirical approach: vendor interviews

universität innsbruck
Institut für Informatik

Semi-structured interviews

Round 1: **German-based** *ad-tech vendors*
21 contacted, 4 interviewed

Round 2: **International** *ad-tech vendors*
37 contacted, 3 interviewed

Seven *ad-tech vendors* = ca. 1 %

4. Results

GDPR compliance and use of CMPs	
High relevance for the company	7/7
≥ 3 persons in GDPR-related decision-making	6/7
Lawyers involved in the decision-making	5/7
External lawyers or DPOs involved in the decision-making	4/7
Name CMPs as the reason for joining the GVL	0/7
State that they do not obtain any consent via CMPs Actually, CMPs collect consent for both.	2/7

We obtain consent via CMPs, but that was not our reason to join the GVL.

We do not need any consent and we do not use CMPs.

4. Results

Market pressure	
Do not consider their GVL membership a free choice	4/7
Feel market pressure regarding their configurations	3/7
State that publishers would want „flexible purposes“	2/7
Have not had significant problems with data subjects/authorities	7/7

The GVL is business critical. We are forced to collect personal data, even though that does not increase revenues.

Some publishers want to collect consent for everything.

Many advertisers co-operate with GVL members only.

4. Results

Compliance risks	
See compliance risks in the GVL membership itself	1/7
Consider the TCF purpose definitions unclear	4/7
Stated others under the TCF would act unlawful	4/7

We interpret the purpose definitions in our favour.

Many publishers design consent dialogues unlawfully.

We are to small to take action against unlawful practices of others under the framework.

5. Conclusion and outlook

Consent collection via CMPs is not a main driver of TCF adoption.

Even data protection friendly *ad-tech vendors* join the GVL.

Big awareness of GDPR violations, but no awareness of compliance risks.

Particularly *publishers* pressurize *ad-tech vendors.*

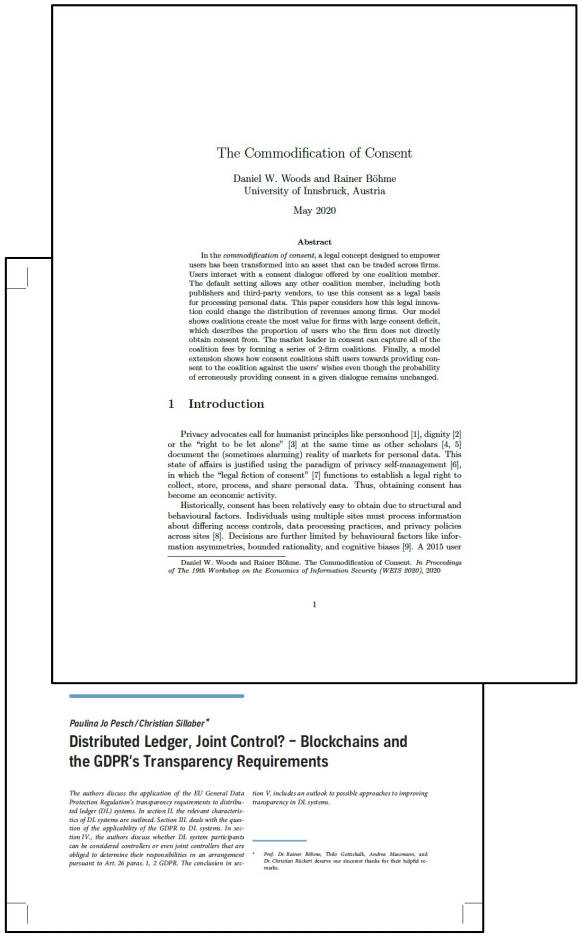
5. Conclusion and outlook

Broader application of the empirical method (interviews with *publishers*, *CMPs*, *advertisers*)

Woods/*Böhme*, The Commodification of Consent, WEIS 2020

In-depth legal analysis, particularly regarding the the question of joint controllership (Art. 26 GDPR)

On Art. 26 in the context of blockchain systems:
Pesch/*Sillaber*, Distributed Ledger, Joint Control? (2016)



The Commodification of Consent

Daniel W. Woods and Rainer Böhme
University of Innsbruck, Austria

May 2020

Abstract

In the *commodification of consent*, a legal concept designed to empower users has been transformed into an asset that can be traded across firms. Users interact with a consent dialogue offered by one coalition member. The default setting allows any other coalition member, including both publishers and third-party vendors, to use this consent as a legal basis for processing personal data. This paper considers how this legal innovation could change the distribution of revenues among firms. Our model shows coalitions create the most value for firms with large consent deficit, which describes the proportion of users who the firm does not directly obtain consent from. The market leader in consent can capture all of the coalition fees by forming a series of 2-firm coalitions. Finally, a model extension shows how consent coalitions shift users towards providing consent to the coalition against the users' wishes even though the probability of erroneously providing consent in a given dialogue remains unchanged.

1 Introduction

Privacy advocates call for humanist principles like personhood [1], dignity [2] or the "right to be let alone" [3] at the same time as other scholars [4, 5] document the (sometimes alarming) reality of markets for personal data. This state of affairs is justified using the paradigm of privacy self-management [6], in which the "legal fiction of consent" [7] functions to establish a legal right to collect, store, process, and share personal data. Thus, obtaining consent has become an economic activity.

Historically, consent has been relatively easy to obtain due to structural and behavioural factors. Individuals using multiple sites must process information about differing access controls, data processing practices, and privacy policies across sites [8]. Decisions are further limited by behavioural factors like information asymmetries, bounded rationality, and cognitive biases [9]. A 2015 user

Daniel W. Woods and Rainer Böhme. The Commodification of Consent. *In Proceedings of The 19th Workshop on the Economics of Information Security (WEIS 2020)*, 2020

1

*Paulina Jo Pesch / Christian Sillaber**

Distributed Ledger, Joint Control? – Blockchains and the GDPR's Transparency Requirements

The authors discuss the application of the EU General Data Protection Regulation's transparency requirements to distributed ledger (DL) systems. In section II. the relevant characteristics of DL systems are outlined. Section III. deals with the question of the applicability of the GDPR to DL systems. In section IV., the authors discuss whether DL system participants can be considered controllers or even joint controllers that are obliged to determine their responsibilities in an arrangement pursuant to Art. 26 paras. 1, 2 GDPR. The conclusion in section V. includes an outlook to possible approaches to improving transparency in DL systems.

* Prof. Dr. Rainer Böhme, Thiki Gottschalk, Andrea Maccarone, and Dr. Christian Rückert deserve our sincerest thanks for their helpful remarks.

universität innsbruck
Institut für Informatik

Thank you!

Dr. Paulina Jo Pesch
Security and Privacy Lab
Department of Computer Science
University of Innsbruck, Austria
paulina.pesch@uibk.ac.at