Press Release

Facing the urgent need for user privacy to be protected, Sirdata makes its Consent Management Platform available for free to publishers who are victims of non-compliant CMPs.

Paris, 10th December 2019 : following INRIA's publication *"Do Cookie Banners Respect my choice?"*, in order to support the entire market in the collection and respect of user's choices towards trackers, Sirdata provides for a limited time its Consent Management Platform free of charge and without any commitment to publishers using non-compliant CMPs.

In their recent Report "***Do Cookie Banners Respect my Choice?"*** INRIA research scientists reveal how the IAB Transparency and Consent Framework's has been incorrectly implemented by poorly trained or uninformed Consent Management Platforms.

Despite the clarity of European GDPR Recital 32, "*Silence, pre-ticked boxes or inactivity should not therefore constitute consent*", the report states that **46.5% of CMPs are deployed with the use of a by default pre-selected boxes setting** and doing so they would record an invalid consent**.**

Even worse, a 7.7% of them would simply ignore the expression of user's choices and **12.3%** would store a consent before any choice had been expressed.

In all cases, an invalid *consent string* would be shared to advertisers and their partners, leading them to use trackers and process personal data without a **valid legal basis**.

Fortunately, however, this report also highlights the expertise of actors, including among those a digital Privacy European champion to whom **no violation has been attributed** : Sirdata.

CMP	Number of websites	Violations			
		Consent stored before choice	*No way to opt out*	*Pre-selected choices*	*Non-respect of choice*
Quantcast	174	3.4% (6/174)	5.2% (9/174)	37.8% (62/164)	0.6% (1/164)
OneTrust	50	74.0% (37/50)	4.0% (2/50)	83.3% (40/48)	8.3% (4/48)
Didomi	41	0.0% (0/41)	0.0% (0/41)	39.0% (16/41)	0.0% (0/41)
Sourcepoint	34	2.9% (1/34)	0.0% (0/34)	64.7% (22/34)	2.9% (1/34)
Evidon	22	4.5% (1/22)	22.7% (5/22)	25.0% (4/16)	25.0% (4/16)
iubenda	20	0.0% (0/20)	0.0% (0/20)	0.0% (0/20)	0.0% (0/20)
Clickio	14	0.0% (0/14)	0.0% (0/14)	0.0% (0/14)	0.0% (0/14)
Oath	12	0.0% (0/12)	0.0% (0/12)	16.7% (2/12)	0.0% (0/12)
Triboo Media	10	0.0% (0/10)	0.0% (0/10)	0.0% (0/10)	0.0% (0/10)
Commanders Act	10	40.0% (4/10)	0.0% (0/10)	80.0% (8/10)	0.0% (0/10)
Axel Springer	10	60.0% (6/10)	70.0% (7/10)	100.0% (3/3)	33.3% (1/3)
OneTag	9	0.0% (0/9)	0.0% (0/9)	100.0% (9/9)	0.0% (0/9)
Cookie Trust WG.	8	25.0% (2/8)	25.0% (2/8)	60.0% (3/5)	0.0% (0/5)
Conversant Europe	7	0.0% (0/7)	0.0% (0/7)	100.0% (7/7)	100.0% (7/7)
Ensighten	7	0.0% (0/7)	0.0% (0/7)	100.0% (7/7)	0.0% (0/7)
SIRDATA	5	0.0% (0/5)	0.0% (0/5)	0.0% (0/5)	0.0% (0/5)
Chandago	5	0.0% (0/5)	0.0% (0/5)	0.0% (0/5)	0.0% (0/5)
incorrect CMP ID	9	11.1% (1/9)	11.1% (1/9)	62.5% (5/8)	12.5% (1/8)
others	73	11.0% (8/73)	6.8% (5/73)	54.4% (37/68)	29.4% (20/68)
No consent string found	40	0.0% (0/40)	17.5% (7/40)	50.0% (11/22)	0.0% (0/22)
all	**560**	**11.8% (66/560)**	**6.8% (38/560)**	**46.5% (236/508)**	**7.7% (39/508)**

*** source: https://arxiv.org/pdf/1911.09964.pdf**

The report states that when an actor shares an invalid consent signal it has an impact on the whole chain by putting it under a non compliance risk, it violates the Transparency and Consent Framework Policies, but above all the European legislation. **Therefore, the INRIA research scientists urge those companies to change their settings and practices and respect the choices expressed by the user**.

As a consequence **the incriminated CMPs should quickly verify the foundations of the research and accordingly stop their service if they cannot upgrade it nor guarantee its compliance**.

As an answer to the need of the User privacy to be protected, and while waiting for the potential changes of the CMPs spotted in the research, Sirdata decided to provide its paid version of CMP **without any counterpart (licence, collection of data…) nor any commitment** until the launch of the TCF v2 to all publishers victims of incorrect settings of their current CMP and so under a risk of sanctions from the regulators. The websites lists have been published, Sirdata will seek to contact them, however, in the meantime invites them all to consult its website https://cmp.sirdata.com.

In December 2018, Sirdata mentioned the following : "The market will move towards the right direction, user's direction. To do so, it is a matter of respecting the choices he expressed, and not impacting other actors - publishers, brands, agencies, or Consent Management Platforms - which meet legislation and IAB Europe Framework specifications."

Nevertheless, Sirdata points out that these observations were written last September 2019 and that some mistakes and some shortcomings have already been corrected following IAB's actions such as the launch of the CMP Validator and the audit of existing and new solutions. Vendors and CMPs can also access to a dynamic list **of valid CMPs** enabling them to reject any unfounded *consent string* and therefore any invalid consent signal at https://cmplist.consensu.org/cmp-list.json.

Benoît Oberlé, Sirdata's founder **:** "***Some of the behaviours revealed in this report are an absolute lack of respect for the user and for the work provided by all the people deeply concerned by privacy matters and involved in the construction of the Transparency and Consent Framework. It is important to be clear that these results relate to private companies and not to the TCF itself. They are subject to laws, regulations, specifications and Policies, and it has now to be determined if they respect them. In the meantime and until the release of Transparency and Consent Framework V2, in order to protect the user and support the TCF Sirdata offers its Consent Management Platform and its technical know-how free of charge.***"

About Sirdata:
French independent Innovative company, Sirdata collects, aggregates, and processes - semantically and statistically - Internet users raw browsing data in the strictest respect of the regulatory framework.A unique know-how that enables it to create audience segments - interests, buying intentions, life moments, demographics, buyer personae - according to the targeting strategies or the use cases required by the Brands.

If the company has been natively integrated for several years into the major secure platforms (DSP, CRM, DMP, CDP...)used by agencies and brands, Sirdata also recently developed new services for the publishers to combine their premium inventory with the quality of its data and / or the benefits of its semantic tools directly in their Adserver or SSP. The solutions and services, Sirdata is providing enables its customers and partners to leverage their consumer understanding through a high quality and fresh data in a controlled governance and respect of the consent expressed by the end user.

In addition, Sirdata has always been supporting its partners in their steps of user consent management by providing personalized advice and support. Since summer 2018 and the entry into force of GDPR, Sirdata has been proposing its own Consent Management Platform (CMP) developed under the IAB Europe Transparency and Consent Framework specifications and already adopted by several thousand websites, mainly in France an the UK.

Appendix 1 –" INRIA research clarifications " Do Cookie Banners Respect my Choice"

- List of violations analysed by the report.

Detected GDPR and ePrivacy violations

During our September 2019 measurement of 22,949 websites from the EU domains, as well as `.org` and `.com`, with Cookinspect we first detected 1,426 websites containing cookie banners that implemented IAB Europe's TCF. After an automatic analysis of these websites, we proceeded to semi-automatic analysis of 560 websites from `.uk`, `.fr`, `.it`, `.be`, `.ie` and `.com` domains to detect violations that require human intervention.

We have detected four types of violations in cookie banners implemented by CMPs in 305 websites. We explain how such behavior violated GDPR and ePrivacy in Section III of our paper.

Violation	Description	Number of websites analysed	Number of websites with violation
Consent stored before choice	The cookie banner stores a positive consent before the user has made their choice in the banner. Therefore, when advertisers request for consent, the cookie banner responds with the positive consent even though the user has not clicked on a banner and has not made their choice yet.	1,426	175 (12.3%)
No way to opt out	The banner does not offer a way to refuse consent. The most common case is a banner simply informing the users about the site's use of cookies	560	38 (6.8%)
Pre-selected choices	The banner gives user a choice between one or more purposes or vendors, but some of the purposes or advertisers are pre-selected: pre-ticked boxes or sliders set to "accept".	508	236 (46.5%)
Non-respect of choice	The cookie banner stores a positive consent in the browser even though the user has explicitly refused consent.	508	39 (7.7%)

- The research conducted by three INRIA researchers, took place from September to October 2019 while the TCF V1.1 was in force and V2 in preparation.

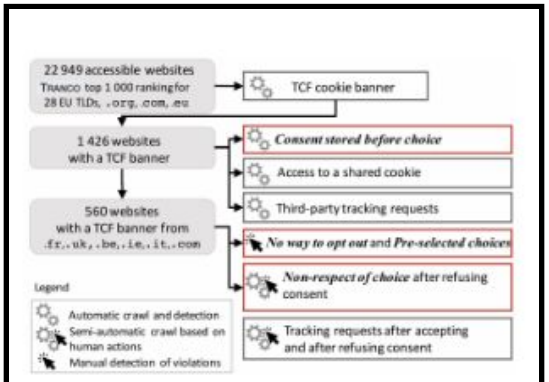


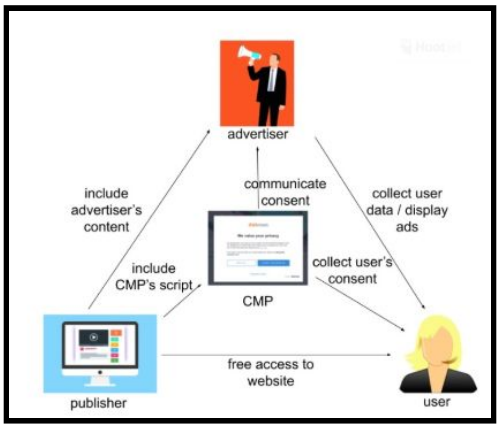
Fig. 6: Overview of the website-auditing process combining automatic crawling, semi-automatic crawling with human interaction and manual analysis to detect GDPR and ePD violations.

TABLE I: Overview of methods to detect the GDPR and the ePD violations in TCF banners.

Short name	Type of crawl	Analyzed component	Number of tested websites
Consent stored before choice	automatic	consent string	1 426
No way to opt out	semi-automatic	banner	560
Pre-selected choices	semi-automatic (when opting out is possible)	banner	508
Non-respect of choice	semi-automatic (when opting out is possible)	consent string	508

- According to the report, the INRIA developed a methodology, and tools on the one hand to detect the user information module (banner, pop up or any other integration) edited by the Consent Management Providers and operating under the Transparency and Consent Framework, and on the other hand to evaluate the validity of the consent transmitted according to two scores: GDPR and ePrivacy compliance.
- It allowed the research scientists to make a comparison between the choice expressed by the user and the consent stored by the CMPs.
- The report notes that it aims to "alert the user and the DPA about violations.".

- INRIA reminds how a Consent Management Platform is supposed to operate between publishers, users and brands within the IAB Europe Transparency & Consent Framework.



- Consent Management PLatforms mission is explained . They are “actors in charge of collecting consent from the end-user, and redistributing this consent to advertisers”meaning they are in charge of collecting the user’s consent, storing it and replying to requests from the advertiser (or its agency) who wishes to be sure the end user understood and gave his consent to the purposes addressed before it broadcasts him an advertisement or a content.

  - **The companies voluntary membership to the TCF is underlined** : The actors must respect the IAB Europe"policies".
  - Each member specifies the purposes it addresses for the collection of data (one to five in the TCF V1).
  - The report sheds light on the role of the Transparency and Consent Framework : the TCF puts in place an open standard for encoding the "*consent string*" (*encoded character string that transmits the signal | the vendor authorized to process the data | the processing purpose to which the user has consented as well as the identifier of the CMP*).
  - Consent signal proof is stored in a "*euconsent*" cookie.
  - The way the consent signal is shared (yes or no, for what purpose) and the opened technologies (API, Shared Cookie, ...) are described in the research.

Press Contact : Nathalie Harding nha@sirdata.fr Tel. 33 6 88 19 58 34