CONTRIBUTION OF ID side to EDPB PUBLIC CONSULTATION ON

"Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive"

SUMMARY OF OUR CORE COMMENT

We understand the scope assessed by the EDPB in the frame of "Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive" currently focuses on "*the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user*", that is to say on all techniques that can be used in 2023-2024 to "track" people's activity online.

However, because of the brand-new technical approach our solution offers regarding the way each individual is enabled to "*[give] his or her consent, having been provided with clear and comprehensive information*", we respectfully invite EDPB members and Secretariat to consider whether part of the scope of the "Technical Scope of Art. 5(3) of ePrivacy Directive "remains uncovered in the current draft of Guidelines 2/2023.

Such observation stems from the fact that not only "tracking technologies" changed since a decade and the adoption of "Opinion 9/2014 of the Article 29 Working Party on the application of ePrivacy Directive". Ways in which consent Could be requested, which are a central part of article 5(3) of the ePrivacy Directive, evolved substantially and, to our view, also deserve being reassessed based on state-of-the-art technologies rendered available.

Our contribution relies on ID side solution (plugin + API), architected to empower individuals:

1. to automatically share their individual Privacy reasonable expectations wherever they browse,
2. to receive a reduced number of consent requests[1] from first-party and third-party cookie providers (and from providers using URL and pixel tracking, local processing, tracking based on IP only, intermittent and mediated Internet of Things (IoT) reporting and unique Identifiers),
3. to assess, whenever they have time and interest to do so, each consent request, based on specific, intelligible and relevant information, shared by providers in a dedicated "contact box".

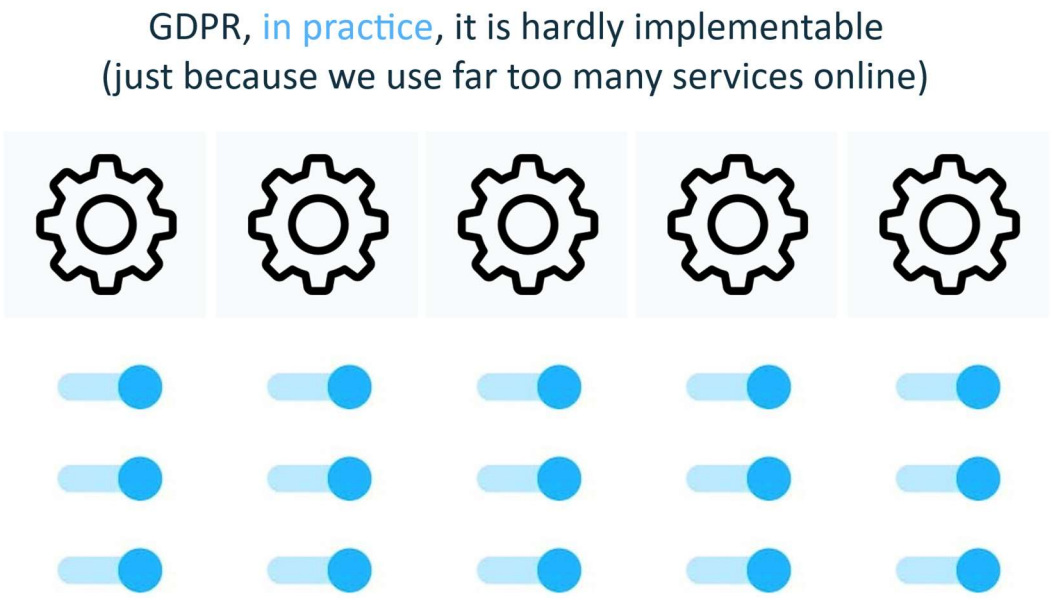
Of course, should such contribution not be related to EDPB's ongoing reflection, we respectfully invite EDPB members to clarify the scope of Guidelines 2/2023 - stating precisely the specific focus of such guidelines on "tracking technologies" state-of-the-art rather than the full scope of article 5(3) in extenso -which would entail reassessing **state-of-the-art techniques that could be used to provide a valid consent** as per recital 32 of the GDPR.

[1] Within the framework of the Cookie Pledge, we count among those contributors that inspired the drafting of Principle H of the Pledge: "*Signals from applications providing consumers with the possibility to record their cookie preferences in advance with at least the same principles as described above will be accepted*". As suggested by some public stakeholders in this frame, our solution might also be relevant to EDPB's work on the Technical Scope of Art5(3) of ePrivacy Directive. Hence our contribution.

BRIEF DESCRIPTION OF ID side's TECHNOLOGY (IN CASE RELEVANT)

With the hope that it can contribute to the EDPB's ongoing refection on article 5(3) ePrivacy directive technical scope, we take the liberty to share here-below a brief description of ID Side's technology.

I - The Problem we address today



Because they wanted to make rec. 32 GDPR consent definition ("a clear affirmative act establishing a freely given, **specific**, **informed** and unambiguous indication of the data subject's agreement") applicable in practice, two former legal and security experts from CNIL created ID side in 2019, along with an UX & data visualisation expert. The core objective of ID side is to give individuals real control over the way their (meta)data gets collected online, specifically because:

- consent collection would be substantially streamlined (individuals would receive targeted information, only when relevant to them),
- individuals would freely consent after reading such information and assessing whether they are willing to agree or not.

We started from the observation that, actually today, no one **validly** consents for 3 reasons in addition to the issue of power imbalance and "Pay or ok".

1/ **Privacy policies** (2012 Carnegie Mellon Research: 76 Working days to read privacy policies) and targeted Privacy information reading is just impossible.

2**/ Cookie banners bombing**, requiring endless/complex validation and repetition of individuals' basic choices often triggers "systematic acceptance" of any term & condition or privacy specification, just to "get rid of it" and be able to access content (consent fatigue).

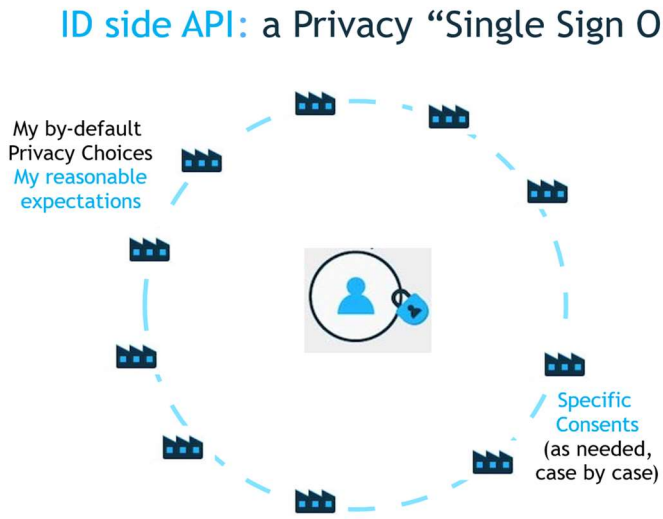
3/ It is really difficult to **find appropriate and effective privacy settings** online: where are they? What controls are actually given (potentially accessing also a binary Accept/Decline option or dark patterns' requests)?

II- Our Proof of Concept (PoC) and Consent online

ID side is about making privacy setting/monitoring possible, based on a tool or mechanism that is **user-centric and cross-platform**. Let's take the example of cookie banners. In addition to dealing with the issues we highlighted previously (too many privacy policies to read, too many settings, not enough time), ID side's proposal is to start from the existing online business environment and help individuals:

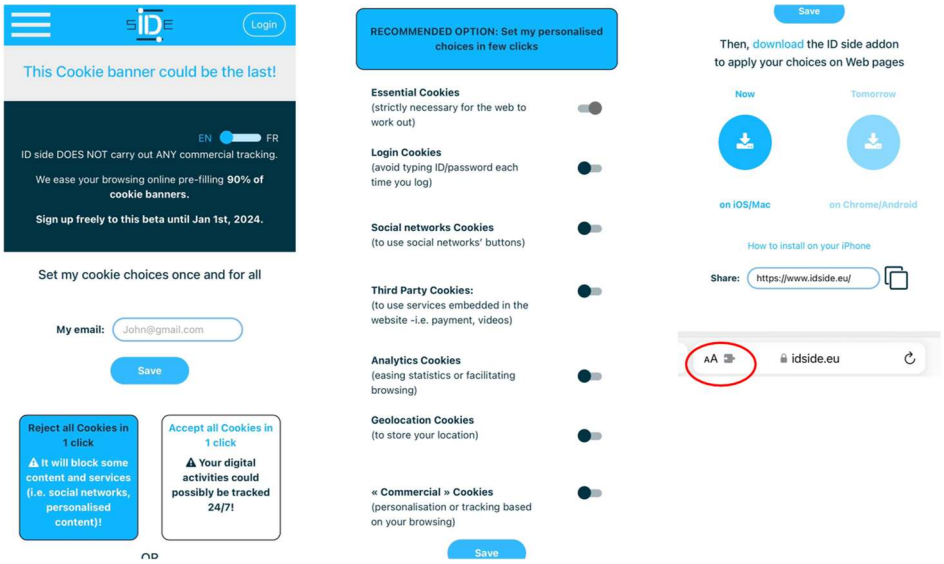
1. set their **Privacy Choices by-default** (that is to say their **individual reasonable expectations**);
2. **automatically & seamlessly share those choices**, wherever they browse;
3. **decide, when they are ready to do so, and based on their personal interests at a t time, to consent to specific data processing**.

In a nutshell, ID side puts users in control because it provides them with a **Privacy "Single Sign On"**.



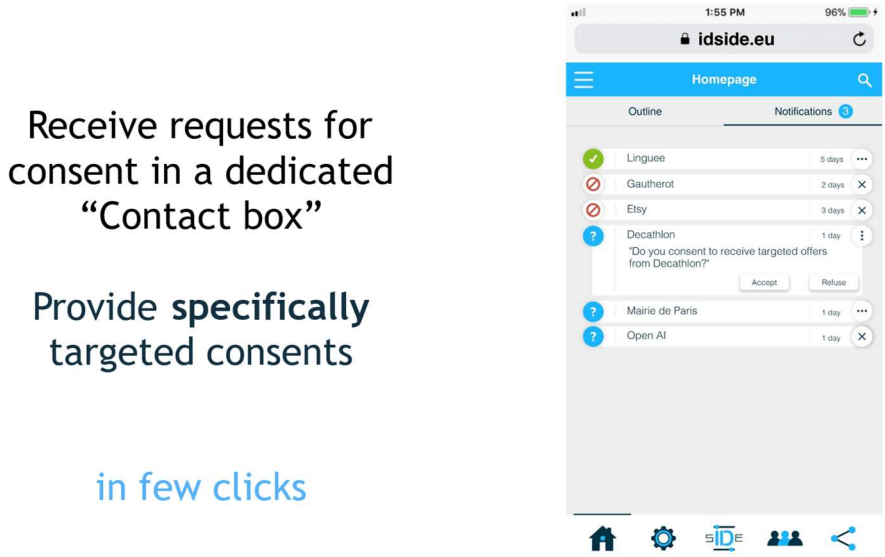
To do so, ID side PoC is two-folded:

Step 1 is about automatically sharing (using ID side plugin) internet users' individual reasonable expectations seamlessly and wherever they browse (individuals' by-default privacy choices –i.e. only analytics cookies are ok). *Our PoC available on idside.eu demonstrates that it is technically feasible.*



Step 2 is about enabling third parties to share with individuals (using ID side API) targeted, informed and specific consent requests whenever relevant, that is to say only if it makes sense based on individuals' reasonable expectations (i.e. if I store in ID side plugin my choice to decline any tracking online -without exception, it does not make sense that each company asks me to specifically consent to being tracked using ID side API). It aligns with the GDPR legal framework and the "specific and informed" requirement overseen by DPAs/EDPB).

We already developed a second version of our PoC with a dedicated "contact inbox" (or "spambox") in which each individual can go back using a dedicated email address (i.e. marie@idside.eu), whenever they have time or interest to do so, in order to assess consent requests they received.



Using ID side solution, individuals receive requests for specific consent in a targeted "**Contact box**" on ID side (separated from other private mailboxes) in which companies can ask whether individuals are interested in their brand/service/product/communication. They will in fact, ask in a simplified, intelligible and timely way (individuals will look at this contact box when they have time!) for being provided with a specific consent.

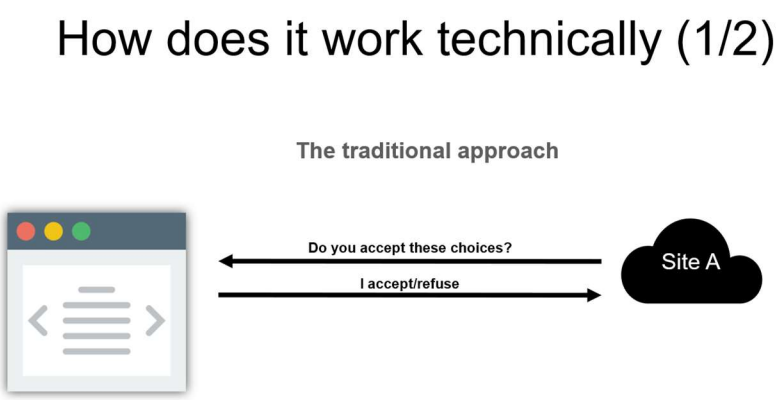
Based on their interests, individuals will provide targeted consents to certain entities, as best pleases them. For instance, a person whose reasonable expectation is to avoid being commercially targeted could grant a specific authorisation to company C (but not companies A, B, D…) to be targeted for at least 15% discounts on Product Z.

III- Potential impact on the technical scope of Art. 5(3) of ePrivacy Directive

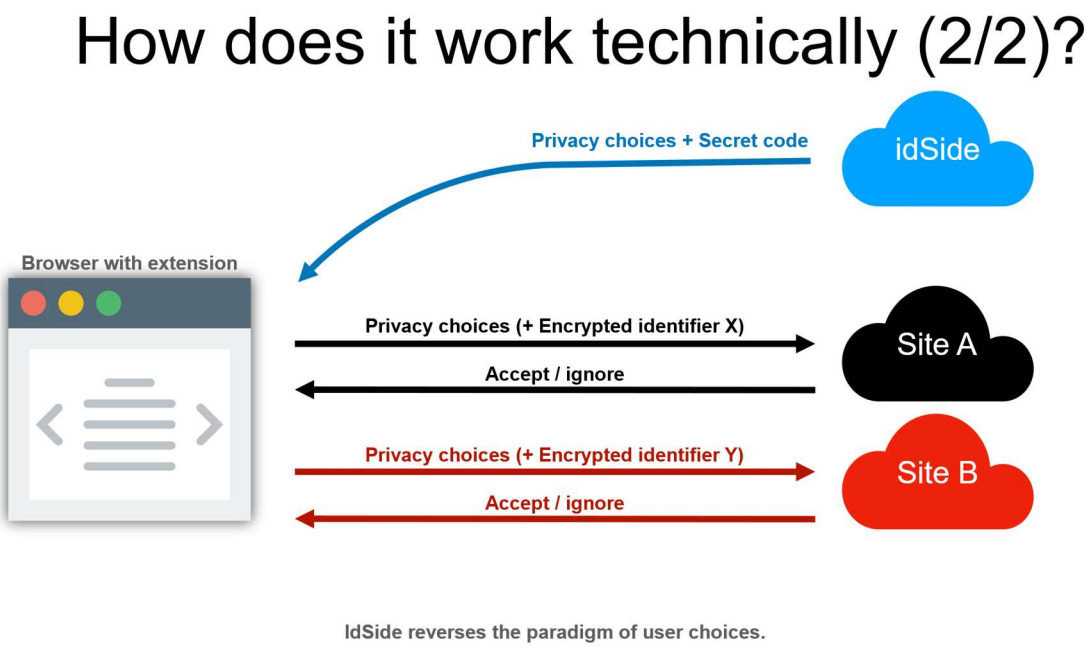
How does ID side work for users today?

ID side plugin allows users to set their by-default Privacy choices regarding cookie banners once and for all, in a granular way, and share those automatically online wherever they browse. For instance, it currently automatically fills potentially all, and so far most, cookie banners. **ID side API** monitors their Privacy choices, update them and helps Users manage targeted consent requests.

How does ID side work technically today?



The current & traditional approach is summarised above -in summary: far too many websites, policies, settings along with potentially limited choices (accept/refuse) or dark patterns.



ID side approach is summarised above (see section IV here-below). ID side team stands ready to explain our technical approach in more details if needed.

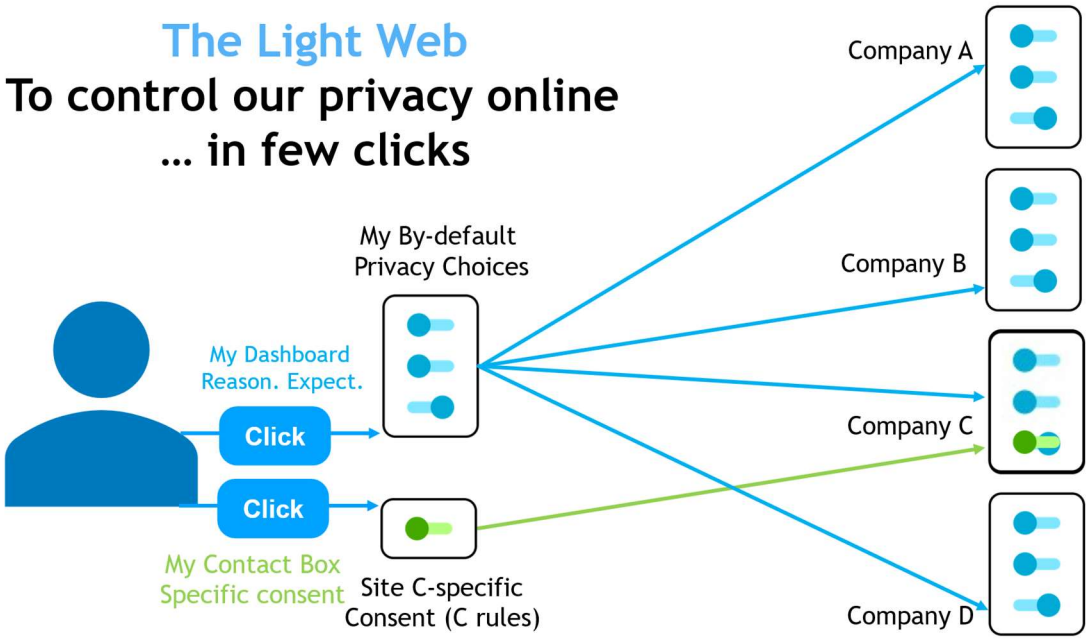
What potential impact on article 5(3) e-privacy's implementation in practice?

A major impact ID side model could have on consent collection online, notably regarding cookies, is that:

1- **it would substantially reduce the number of consent requests** that individuals will receive (they actually now can manage those);
2- **All consent requests would be sent along with targeted and intelligible information** in a dedicated email;

3- **individuals would review such consent requests accessing their dedicated "spambox" whenever they are ready to read and "pay attention"**, that is to say when they are in capacity to freely consent;
4- **consent would become an act under the control of users** and create "trusted relations" with few companies/entities rather than massive and indiscriminate "consent fatigue".

This approach, which is based on a "Personal data choice management platform" (like ID side) rather than a "Consent management platform" is what we call the "Light Web" project. The way it works is summarised here-below.



A potentially relevant distinction to consider:
The difference between a "**Personal data choice management platform**" (like ID side)
and a "Consent management platform" [2]

"***Consent management platforms***" are a mechanism allowing people to consent at a t-time, that is to say when individuals browse a website and are willing to access content. Consent is requested at a t-time, potentially as a take-it or leave-it choice, as a pre-condition for individuals to access the content or service they are interested in. Such mechanisms are widely spread across the web to demonstrate consent has been provided, but not that people did "freely consent".

They do not allow users to share their individual reasonable expectations in advance, nor to update those -or to have those automatically and seamlessly shared as they browse.

[2] Based on the reading of EDPB's letter commenting EU Commission DG Connect's initial draft of the Cookie Pledge -see EDPB comments on Principle H of the Cookie Pledge, we take the opportunity to clarify the difference between "**Personal data choice management platforms**" (like ID side) **and "Consent management platforms**".

Most of all, they do not reduce the number of consent requests shared by first-party and third-party cookie providers, do not increase the quality of information provided nor give more time to individuals to assess whether they want to consent (consent should be provided immediately).

Therefore, such mechanisms do not empower individuals, nor address the consent fatigue problem.

"***Personal data choice management platforms***" (like ID side) allow users to automatically share their by-default preferences regarding Privacy (i.e. by-default cookie choices) or commercial interests (i.e. flagging agreement to be tracked by company C or sector (c) -and not A, B or D- because they like Company C or sector (c) products and ads from this Company/sector could be relevant to them).

In Step 1 (based on the use of **ID side plugin**), **personal data choice management platforms do NOT allow to collect consent** (rec 32 GDPR) **but they do allow users to share their individual reasonable expectations**. If an individual's reasonable expectation is to avoid being targeted online except by Company C or for products and services of sector (c), only Company C or providers of products and services of sector (c) are entitled to send a consent request to said individual. Of course, users of personal data choice management platforms are empowered to change and update their individual reasonable expectations over time, in few clicks (allowing for instance Company E or sector (e) to target them).

In Step 2 (based on the use of **ID side API**), **first-party and third-party providers are entitled to ask for a GDPR-valid consent** (that is to say freely given, informed, specific and explicit) to be targeted. This 2-steps mechanism is the core feature that helps substantially reduce consent requests and drastically reduces "consent fatigue". In our example, for instance, such consent requests would be sent only by Company C or sector (c) providers in the individual's "contact inbox" (or individual "spambox").

IV- The technical scope of Art. 5(3) of ePrivacy Directive & ID side patent

ID Side patented technology

ID Side's technology allows internet users to broadcast their default privacy choices to information technology providers. Conversely, it also allows these information technology providers to ask specific internet users to grant them an exception to these default privacy choices, through the "Contact Box" mechanism we described earlier. To enable this to work, information technology providers need a way to indirectly identify a specific internet user within the ID side system, so that these requests for an exception are routed to the correct individual. ID Side's technology relies on a pseudonymous identifier to make this possible in API calls. This approach creates a potentially unexpected privacy risk: this pseudonymous identifier could be used by information technology providers to indirectly track users, somewhat like using a device address. ID Side counters this risk by using cryptographic mechanisms that make the pseudonymous identifier change continuously, rendering it useless as a tracking tool.

In the interest of transparency, we wanted to note that, since 2021, ID Side holds a WIPO-PCT patent on the technology that covers the creation of the "Personal Data Choice Management Platform" described in this documents, including notably the use of "privacy-preserving" pseudonymous identifiers mentioned above.

ID side WIPO patent

DESCRIPTION

TITLE: PERSONAL DATA CHOICE MANAGEMENT PLATFORM

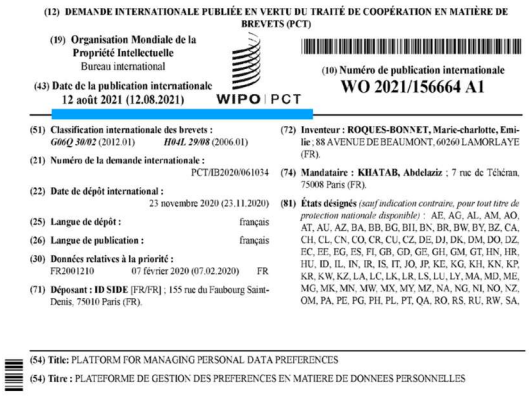
TECHNICAL FIELD OF THE INVENTION

[0001] The present invention relates to the field of online communications. More particularly, it relates to the protection of personal data of users of communication networks such as the Internet for example.

TECHNICAL BACKGROUND

[0002] When a user accesses online services, for example on the Internet, he or she is faced with the difficulty of controlling the use that these services make of his or her personal data.

[0003] The control of this data comes up against the tedious task of expressing choices in this matter for each service used (for example on each website visited). The



(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(10) Numéro de publication internationale
WO 2021/156664 A1

(43) Date de la publication internationale
12 août 2021 (12.08.2021)

WIPO | PCT

(51) Classification internationale des brevets :
G06Q 30/02 (2012.01) *H04L 29/08* (2006.01)

(21) Numéro de la demande internationale :
PCT/IB2020/061034

(22) Date de dépôt international :
23 novembre 2020 (23.11.2020)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
FR2001210 07 février 2020 (07.02.2020) FR

(71) Déposant : **ID SIDE** [FR/FR] ; 155 rue du Faubourg Saint-Denis, 75010 Paris (FR).

(72) Inventeur : **ROQUES-BONNET, Marie-charlotte, Emilie** ; 88 AVENUE DE BEAUMONT, 60260 LAMORLAYE (FR).

(74) Mandataire : **KHATAB, Abdelaziz** ; 7 rue de Téhéran, 75008 Paris (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,

(54) Title: PLATFORM FOR MANAGING PERSONAL DATA PREFERENCES

(54) Titre : PLATEFORME DE GESTION DES PREFERENCES EN MATIERE DE DONNEES PERSONNELLES

A NON-BINARY APPROACH
THAT COULD HELP ADDRESSING THE "PAY OR OK" DEADLOCK?

Tracking online is not a black or white assessment.

Individuals might be interested by few companies/products/services/public content. But not all.

They might be willing to share some interests to conclude the best deals, get the latest intel or grab a unique commercial opportunity –but not all their interests.

If they are empowered to share about their interests & privacy choices, and to consent to meaningful specific data processing –as best suits them, tracking individuals 24/7 might be pointless.

Both companies/public bodies and individuals can now TECHNICALLY freely agree to build a trusted & long-term relationship online –instead of setting 24/7 tracking online as the default standard.