

Note interne

Date : 28/11/2022

Rédacteur	Pour information
Nacéra BEKHAT – Benjamin POILVE	Louis DUTHEILLET de LAMOTHE Mathias MOULIN Thomas DAUTIEU Bertrand PAILHES Aymeric PONTVIANNE

Object: TrustPID : presentation of the project and issues identified

1 Background

1.1 General context

Since September 2021, Vodafone has been in contact with the BfDI in the context of the creation of a new platform called TrustPid (the “project” or the “platform”), to be tested in Germany. In July 2022, Vodafone contacted both the Spanish DPA and the CNIL. Besides, it appears that they also presented the project to the ICO last June.

The overall goal of the project is to rely on the terminal identification provided by the network operator [REDACTED] to provide advertisers a persistent tracking identifier to be able to target users during their on-device navigation.

The existence of the plan has raised significant concerns amongst privacy experts, and has gained the nickname of “SuperCookie”¹ (a term that Vodafone disputes). The term “SuperCookie” has been used to described various methods of tracking, usually relying on a combination of fingerprinting, cache usage and other less known methods that differ from the technology used in the TrustPid project.

Since Vodafone does not operate in France, they wish to partner with local operator. On 6th of January 2023, Deutsche Telekom AG, Orange SA, Telefónica S.A. and Vodafone Group plc have notified to the Commission their intention to create a new joint venture.

1.2 Timeline of the future experimentations

[REDACTED]
[REDACTED] In any case, Vodafone committed to inform the CNIL before carrying the test in France.

We do not have at this stage a precise description of the test that will be run in France, Vodafone shared that the test will be of similar scale as the one run in Germany. [REDACTED]
[REDACTED]

¹ <https://www.wired.com/story/trustpid-digital-token-supercookie/>

1.3 Expectations from the CNIL

The services met with Vodafone and a local network operator in early October. Vodafone clarified that **this engagement with the CNIL does not constitute a formal request for a prior consultation (article 36 GDPR)**. They consider that they have been able to mitigate any risks and that the condition for such a consultation are not met. Rather, their initiative was to have an informal discussion with the services.

1.4 Ongoing work at national and European level

- ❖ **Ongoing exchanges at EDPB level: an informal “taskforce” with German and Spanish DPAs to ensure a coherent response at national level**

As a couple of DPAs were interested in having a more in-depth conversation about TrustPid (Member States were experimentations was taking place), **it has been decided to create an informal “task force” to discuss the project.**

The goal would be to address a letter to Vodafone pointing the issues identified by the services after having discussed the content of the letter with our European counterparts in the “task force”.

- ❖ **Request from the European Commission**

As part of their investigation, the European Commission (DG COMP) are currently in the process of gathering the views of market participants as well as other interested authorities.

The response would not be a “formal response”, but rather “an exchange of views” to determine whether the analysis of the proposed transaction from a data protection angle may feed into their analysis of the proposed transaction from a competition angle.

More specifically, the European Commission want to get our views on whether the Parties could combine their data with that of the joint venture, i.e., whether they could match personal information available to them with the anonymised information gathered by the joint-venture.

2 Explanation from a technical standpoint and challenges

2.1 Technical issues related to the proposed scheme

2.1.1 The involved entities

The heart of this project is to create a new platform called the “TrustPid Platform”. [REDACTED] while the data controller might be in a future iteration a joint venture of different network operators.

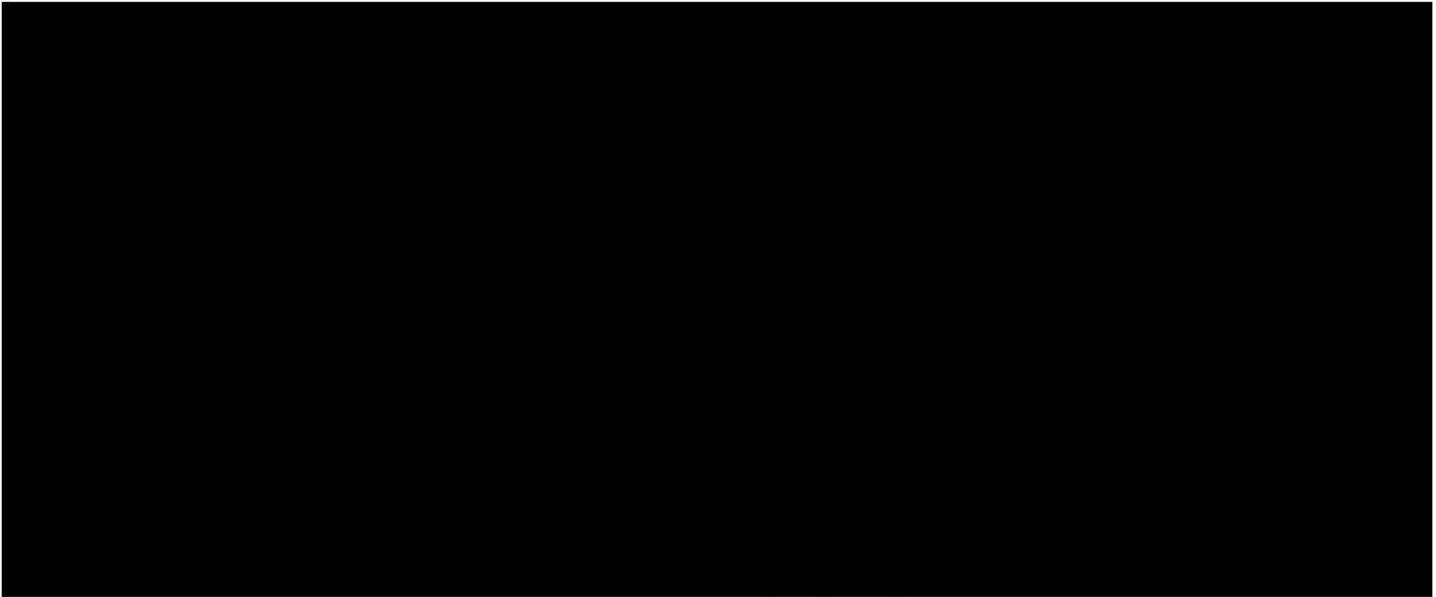
All the other participants to the proposed scheme are existing actors of the digital marketing ecosystem or network operators.

To list them:

- **The network operators** are providing the technical means for mobile users to connect to the internet. They use that technical operation to be able to identify each terminal and pass that information to the platform.
- **The advertisers and their DMP (data management platform)** are using the identifiers provided by the platform to collect navigation data and create targeting groups (ex. car company).
- **The publishers** are selling ad space, and include the identifiers in the bidding request (ex. website “le Monde”).
- **The SSP (supply-side platform)** are managing ad space to sell, and pass on the identifiers to organize the bidding.

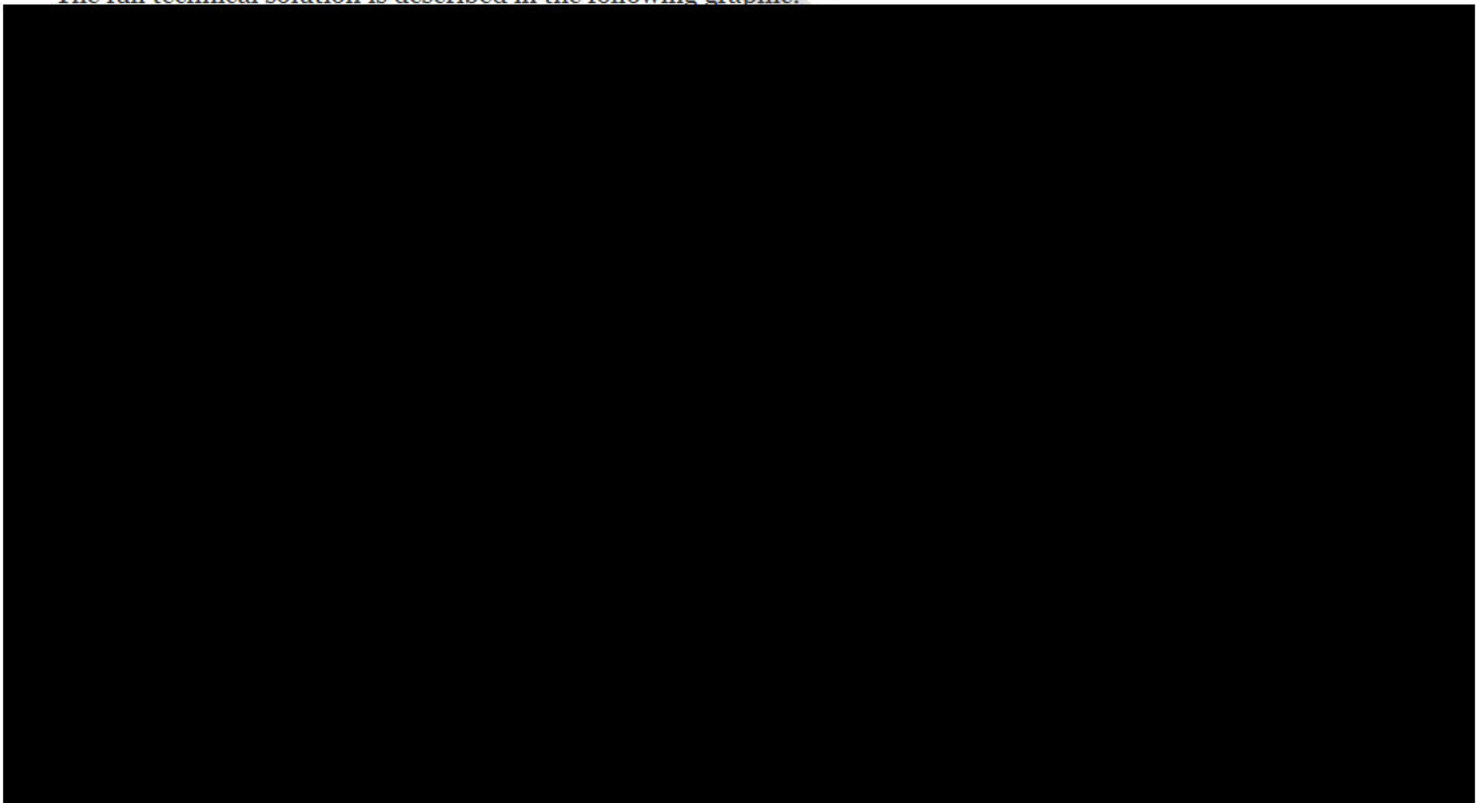
- **The DSP (demand-side platform)** are instructed to buy space for specific identifiers and do so during bidding based on the data provided by the SSP.

2.1.2 The proposed processing



2.1.3 Identifiers used

The full technical solution is described in the following graphic:



To go into further details, it should be noted that different levels of identifiers are used:



- **The MarTech ID** is a website-specific identifier [REDACTED] but not the website operator. This is the segment to locally follow a user and create segment for targeting. This ID is limited to a lifetime of 90 days. [REDACTED]
- **The AdTech ID** is a one time use identifier that is provided by TrustPID to websites wishing to engage in ad auction. [REDACTED]

The goal of this multi-identifier architecture is, according to Vodafone, to avoid having third parties collect excessive data in the use of this solution by introducing layers of de identification of the user.

3 Legal issues

3.1 On the possibility to rely on consent as a legal basis

3.1.1 On the applicability of Article 5(3) of the [ePrivacy directive](#)

As we see in the technical analysis, there are three steps when the Article 5(3) of the ePrivacy directive, regarding cookies storage on users' devices, might apply:

- **At the first step,** [REDACTED] the question of whether the IP address is subject to Art. 5(3) is still being discussed at the European level, but it is premature to rule it out.
- **At the third step,** [REDACTED]
- **At any further steps where the MarTech ID and AdTech ID are used.** [REDACTED] so the application of ePrivacy is quite obvious.

While Vodafone admits that Art. 5(3) is applicable, the applicability, according to them, of this provision is triggered solely by the storage of the MarTechId and AdTech ID on the user's device. They do not address the two other cases where Art. 5(3) might be applicable. While the end result is that consent is needed (and not disputed by Vodafone), we should ask them to clarify their position on all three cases in Vodafone's DPIA.

3.1.2 On the applicability of Article 6(3) of the [ePrivacy directive](#)

Vodafone considers that prior consent must be provided in light of article 6(3) of the ePrivacy directive. As a reminder, as per Article 6(3) of the ePrivacy directive, by principle, traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication **unless that data proves to be processed for the provision of value-added services to which the user has given consent.**

For Vodafone, as the IP is shared with mobile operators who will identify the user based on that address it qualifies as traffic data as it serves the purpose of the transmission of a communication. In addition, for Vodafone, the solution's reliance on the mobile network operator provision of hashed identifier based on IP address entails a service on top of the essential provision of communications therefore qualifying as a value-

added service. Specifically, the considered service is the provision of a one-stop-shop platform to the user enabling centralised management of consents and user data.

❖ **The first question to address is whether or not the IP address can rightfully be regarded as traffic data as Vodafone claims**

As per article 2(b) of the Directive, traffic data is defined “*data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing*”. In French law, various sources, such as articles R10-13 and R10-14 of the French Code of Post and Electronic Communications (“CPCE”) give a non-exhaustive list of traffic data which extend to information allowing to identify the user, data concerning the equipment used to get access to communication, data about additional services requested or used and its suppliers.

If it is true that the IP address can be qualified as traffic data *per se*, in the peculiar context at stake, there are doubts that the IP address could be qualified as traffic data as the purpose of the collection is targeted advertisement rather than the convenience of the communication. In other words, the data used for traffic allows to implement TrustPid which ultimate purpose is to allow targeted advertisement.

In the meantime, the term “communication” as a broad definition since it means “*any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information*” (article 2(d)).

The broad definition of a “communication” in article 2(d) could lead to consider that the IP address can be regarded as traffic data.

❖ **If the data has been qualified as traffic data, the second question to tackle is whether Vodafone is using traffic data for the purpose of marketing electronic communications services or for the provision of value added services**

The ePrivacy directive provides a few definitions of what encompasses this concept :

- As per 18 of the Directive “*Value added services may, for example, consist of advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and tourist information.*”
- Whereas 35 of the Directive provides additional examples “*the provision of value-added services such as services providing individualised traffic information and guidance to drivers*”.
- Article 2(g) of the directive “*value added service’ means any service which requires the processing of traffic data or “location data other than traffic data” beyond what is necessary for the transmission of a communication or the billing thereof*”.

The broad definition in article 2(g) would lead to consider that, in this case, traffic data is used for the provision of value-added services and requires consent. Furthermore, article 6 of the ePrivacy directive also allow the processing of traffic data for the purpose of “marketing electronic communications services”.

❖ **If the data cannot be qualified as traffic data, could it be qualified as content data and what consequences should be drawn?**

The concept of “content data” is used in the ePrivacy directive without being defined. In a word, to make a comparison with postal services, the envelope would be traffic data and the letter would be content data. Content data being about the substance of an information and traffic about the vehicle to provide that information.

In accordance with article 5(1) of the ePrivacy directive “*Member States shall ensure the confidentiality of communications*”.

Matching the IP address with the website visited in order to target an audience tends to fall for the qualification of content data. Indeed, knowing which website has been visited by a person could allow to know what the person reads/is interested in.

3.2 Consent as a legal basis applicable under the GDPR and related issues

❖ Relevance of this legal basis for onward processing

Vodafone understands that the onwards processing following the ePrivacy consent should be based on consent as per article 6(1)(a) of the GDPR. **We agree with the choice to rely on consent for processing operations under the GDPR.**

Indeed, in accordance with the EDPB doctrine and as reminded by the CNIL on its website², consent will most likely be the appropriate legal basis for onwards processing operations, following consent to place cookies on the terminal when the processing follows advertising purposes which are quite intrusive.

❖ Concerns about consent collection

Various issues surround the scope and extend of consent provided and understood by the user which, in result, implies issues to ensure informed and unambiguous consent as per article 4 (11) of the GDPR:

- [REDACTED]
- Besides, when a company owns different websites (like in the case of a media group), it is not clear if the consent extent only to the domain visited or to all the sites belonging to the group.

In addition, a user will most likely be confused by the fact that **TrustPID is only applicable when he/she accesses a website via the 4G**. The discrepancies while using the wifi or 4G can lead to difficulties in ensuring informed consent. In that regard, extra care should be given to the information of data subjects through enhanced pedagogical efforts.

❖ Concerns about withdrawal of consent

We understand that [REDACTED]
[REDACTED] in that respect, users might get confused regarding the respect of the withdrawal of their consent.

3.2 Excessive collection of data

As we see in the technical analysis, [REDACTED]
[REDACTED]
[REDACTED] While Vodafone might try to have contractual agreement to avoid that data collection, they will have a very limited capacity to enforce said agreement.

While the question of whether this “trade-off” is acceptable for the testing phase remains open, it is very clear that **the scheme should not be rolled out while this issue is not solved.**

3.3 Microtargeting of users

² <https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/FAQ>
(See Q/A 30)

[REDACTED] We consider that this would defeat the goal of the scheme (the introduction of layers of de identification of the user).

It is recommended, as a measure to enhance privacy by design, **to ensure that there is a minimum size in audience segmentation when segments are transmitted to DSP.**

3.4 On the qualification of stakeholders

Qualifications which can cause difficulties:

- For Vodafone, [REDACTED]
- For the operation of sharing the MarTech ID and Segment ID with the advertiser, [REDACTED]