

Avril - Septembre 2024

Synthèse rapport CMA

: SOMMAIRE

01 Topics

02 Protected Audience

03 Attribution Reporting

04 Trusted Execution Environments

05 Related Website Sets

06 Fenced Frames



Résumé

: Résumé

- Le rapport Q2 / Q3 2024 de la CMA se démarque de ses prédécesseurs par :
 - ❖ la définition par Google des contours de l'**organe de gouvernance** qui supervisera les évolutions futures de la Privacy Sandbox
 - ❖ une **délégation** importante de **responsabilité** de la CMA **vers ledit organe**, notamment en ce qui concerne la définition de l'**équilibre entre utilisabilité & privacy**
 - ❖ la **résolution** de nombreuses **inquiétudes**
 - ❖ des **arbitrages en faveur de l'utilisabilité** au détriment de la privacy
 - ❖ la collaboration rigoureuse de la CMA et l'ICO pour évaluer la compréhension des internautes face aux **interfaces de la Privacy Sandbox**
 - ❖ l'**absence** totale de **timeline** et un **flou** quant aux **prochaines étapes**
- Ce rapport contient **peu de références** aux résultats et enseignements de la phase de **market testing** laissant un vide quant à ses conclusions par rapport aux performances de la Privacy Sandbox et sa propension à répondre aux inquiétudes de distorsion de la compétition



: Résumé

- Le risque de **tracking cross-sites** reste une **inquiétude centrale pour l'ICO** qui semble considérer comme **illégaux le profiling excessif** des utilisateurs et le **détournement** des outils de la **Privacy Sandbox** à des fins de **tracking cross-sites** (car elle est présentée à l'utilisateur comme un mécanisme pour limiter le tracking cross-sites).
A cet égard, l'ICO a accueilli positivement la proposition de Google consistant à établir un **rapport annuel** à destination de la CMA& de l'ICO faisant état des **usages** faits **des APIs de la Privacy Sandbox** par les acteurs de l'écosystème et de l'évolution du risque de **tracking cross-sites que ces usages posent**
- Les outils de la **Privacy Sandbox** peuvent encore être utilisés d'une manière **non conforme à la législation** applicable en matière de protection des données. La résolution de ces risques de non-conformité par des modifications techniques des outils de la Privacy Sandbox a dû être mise en balance avec le risque de distorsion de la concurrence



: Résumé

- Dans ce rapport, de nombreuses **inquiétudes** ont été **résolues** ou sont en passe de l'être. **6 raisons** principales ont conduit à ces résolutions :
 - ❖ L'apport d'évolutions techniques de la Privacy Sandbox ou des mises à jour des interfaces utilisateurs associées
 - ❖ L'avènement du nouvel organe de gouvernance
 - ❖ La nouvelle expérience Chrome à venir
 - ❖ L'absence d'alimentation de certaines inquiétudes par l'écosystème
 - ❖ Le transfert de certaines inquiétudes vers d'autres dossiers de la CMA
 - ❖ Le partage par Google de contre-exemples aux inquiétudes levées



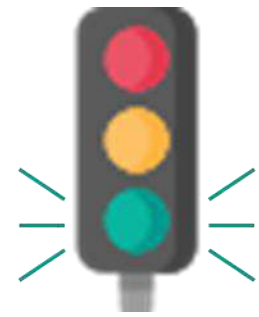
: Résumé

- Ce rapport met l'accent sur la **responsabilité légale** des acteurs exploitant les données utilisateurs issues des outils de la Privacy Sandbox : ils doivent **collecter leur consentement**. Le cadre légal de cette collecte n'est pas précisé
- La CMA et l'ICO ont porté une attention particulière à la **compréhension des internautes des interfaces utilisateurs** (CMP, paramètres, FAQ, documentation technique, ..) associées au fonctionnement de la Privacy Sandbox. Tout semble indiquer qu'ils porteront un niveau d'attention similaire lors de l'évaluation de la nouvelle expérience Chrome

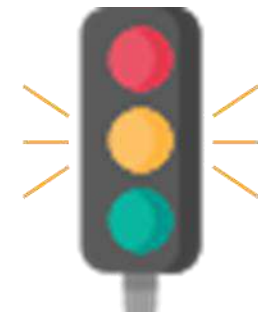


: Evaluation de la Privacy Sandbox

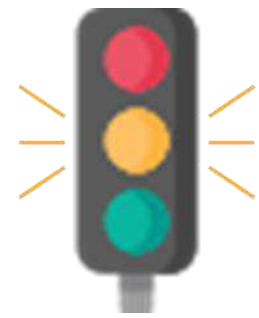
Au vu de la teneur actuelle des échanges entre la CMA, l'ICO, le marché, et Google au sujet des API de la Privacy Sandbox, du nombre d'inquiétudes restantes à lever pour chaque API, ainsi que la complexité de résolution de celles-ci, notre appréciation de leur état de validation par la CMA est la suivante :



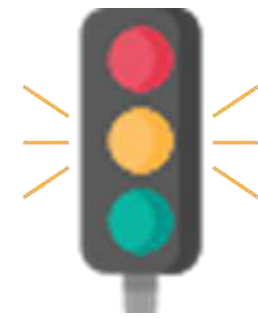
API Topics



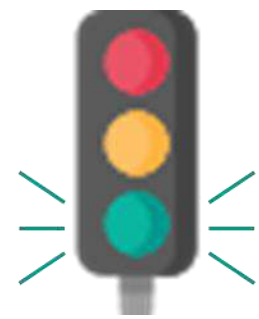
Trusted Execution Environments



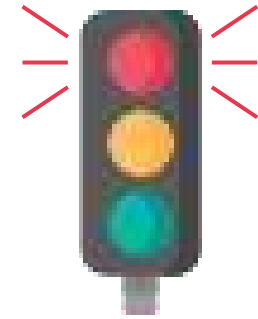
API Protected Audience



Related Website Sets



API Attribution Reporting

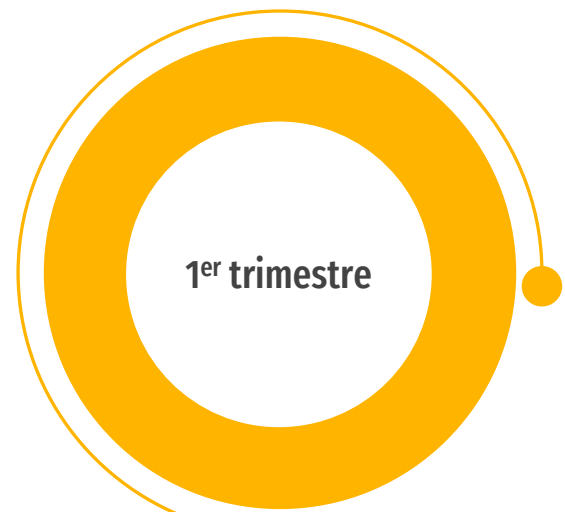


Fenced Frames

car non-compatibles avec formats Native & Vidéo

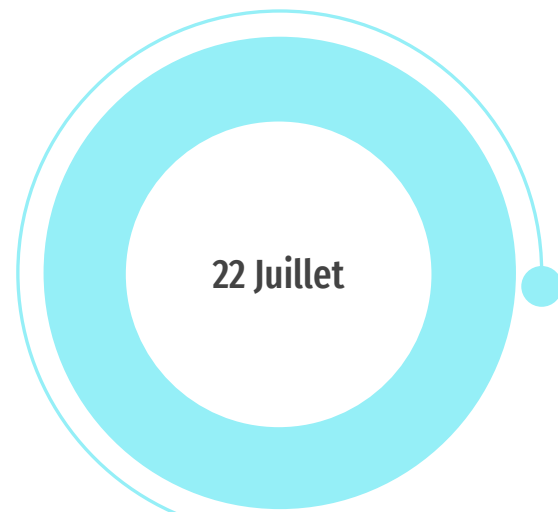


: Frise chronologique



1^{er} trimestre

Suppression des cookies tiers pour 1% des utilisateurs de Chrome



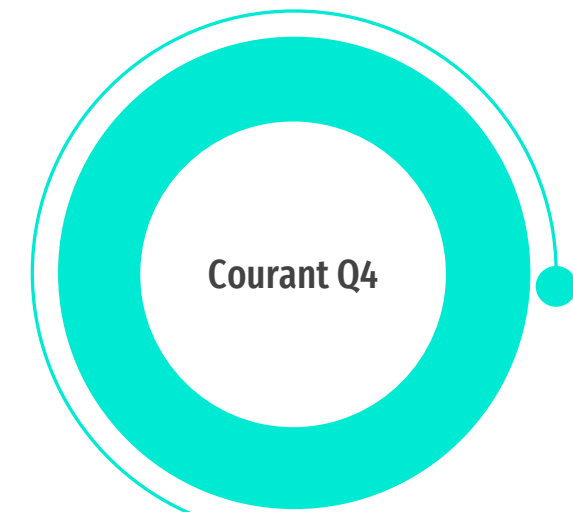
22 Juillet

Annonce de la nouvelle expérience Chrome



11 Novembre

Publication du rapport Q2/Q3 de la CMA



Courant Q4

Consultation publique nouvelle expérience Chrome

2025



2024





Focus Gouvernance

: Focus Gouvernance

Dans les rapports précédents, la CMA a indiqué que le pouvoir discrétionnaire de Google sur le fonctionnement, l'évolution, et les conditions d'utilisation de la Privacy Sandbox pouvait créer un risque de self-preferencing.

Pour limiter ce risque, Google a proposé la mise en place d'un organe de gouvernance dont les fondements reposent sur les principes suivants :

1. Une **période de consultation** formelle de 3 semaines sera tenue pour évaluer les modifications de la roadmap pouvant avoir un impact significatif sur la vie privée ou l'utilisabilité de la Privacy Sandbox. Les éléments suivants seront fournis lors de période de consultation :
 - ❖ Les détails concernant les modifications envisagées
 - ❖ Une évaluation des impacts sur les Commitments de Google
 - ❖ La durée de la consultation publique
 - ❖ Le résumé des éléments ayant abouti à la prise de décision



: Focus Gouvernance

2. Une **procédure d'appel gérée en externe**, permettant aux parties de faire appel de certaines décisions opérationnelles, c'est-à-dire des décisions binaires prises par Google sur la base de critères prédéfinis, qui concernent spécifiquement leur activité
3. Une **codification des principes de confidentialité et d'utilisabilité** permettant de mettre en balance simplement ces deux aspects, et faciliter la prise de décision
4. Un **rapport annuel** à destination de la CMA et de l'ICO **évaluant les risques de tracking cross-sites associés aux outils de la Privacy Sandbox**. Il contiendra notamment des éléments fournis par les parties prenantes (régulateurs, chercheurs, etc) et des métriques techniques telles que l'usage fait par l'écosystème des outils de la Privacy Sandbox

Aucun autre détail concernant cet organe de gouvernance n'a pour le moment été dévoilé (ex: ses membres, procédure d'élection, etc).

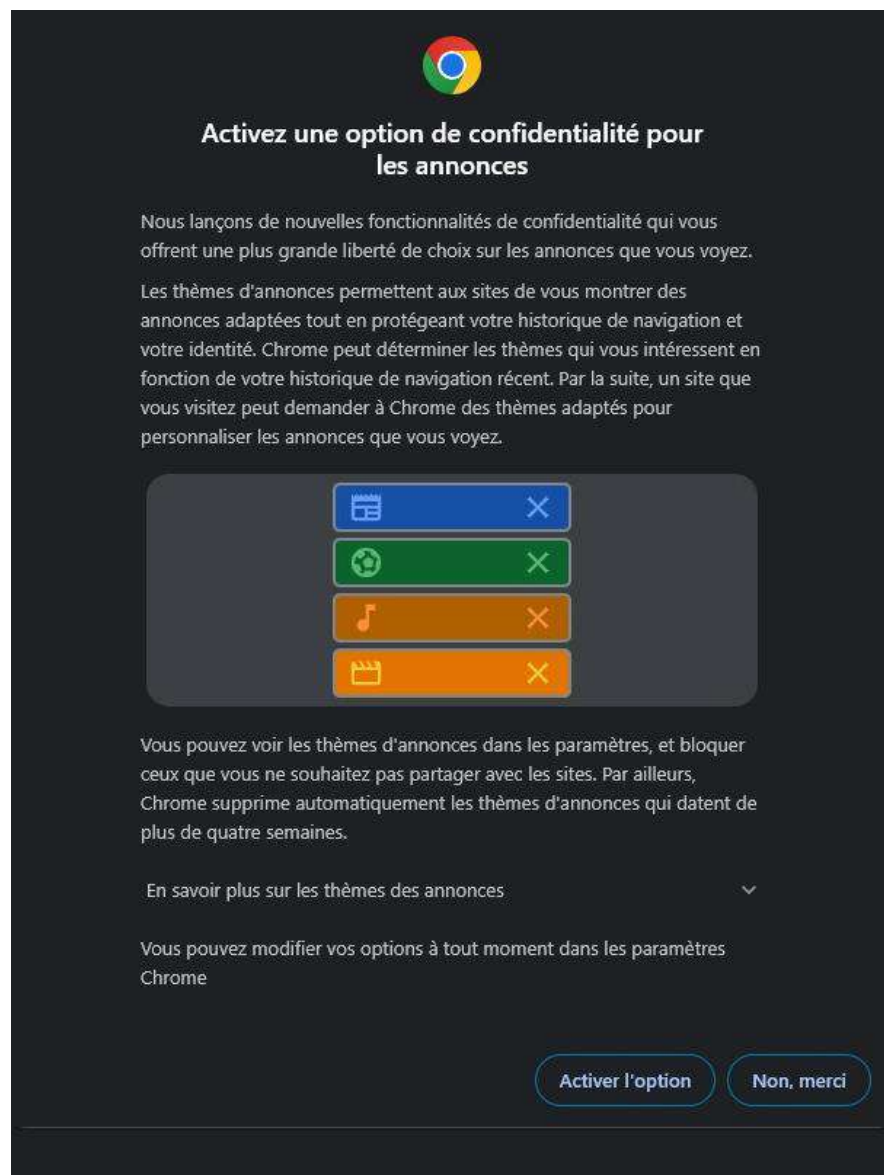




Visuels Privacy Sandbox

: Visuels “CMP”

Dans la suite du document, sont appelées « CMP » les interfaces de collecte du consentement de l'utilisateur pour l'activation des fonctionnalités suivantes de la Privacy Sandbox : Topics, Protected Audience, Aggregation Reporting. Ces interfaces sont affichées une seule fois à l'utilisateur, à l'installation de Chrome, mais ses choix restent modifiables via les paramètres de son navigateur



CMP Topics

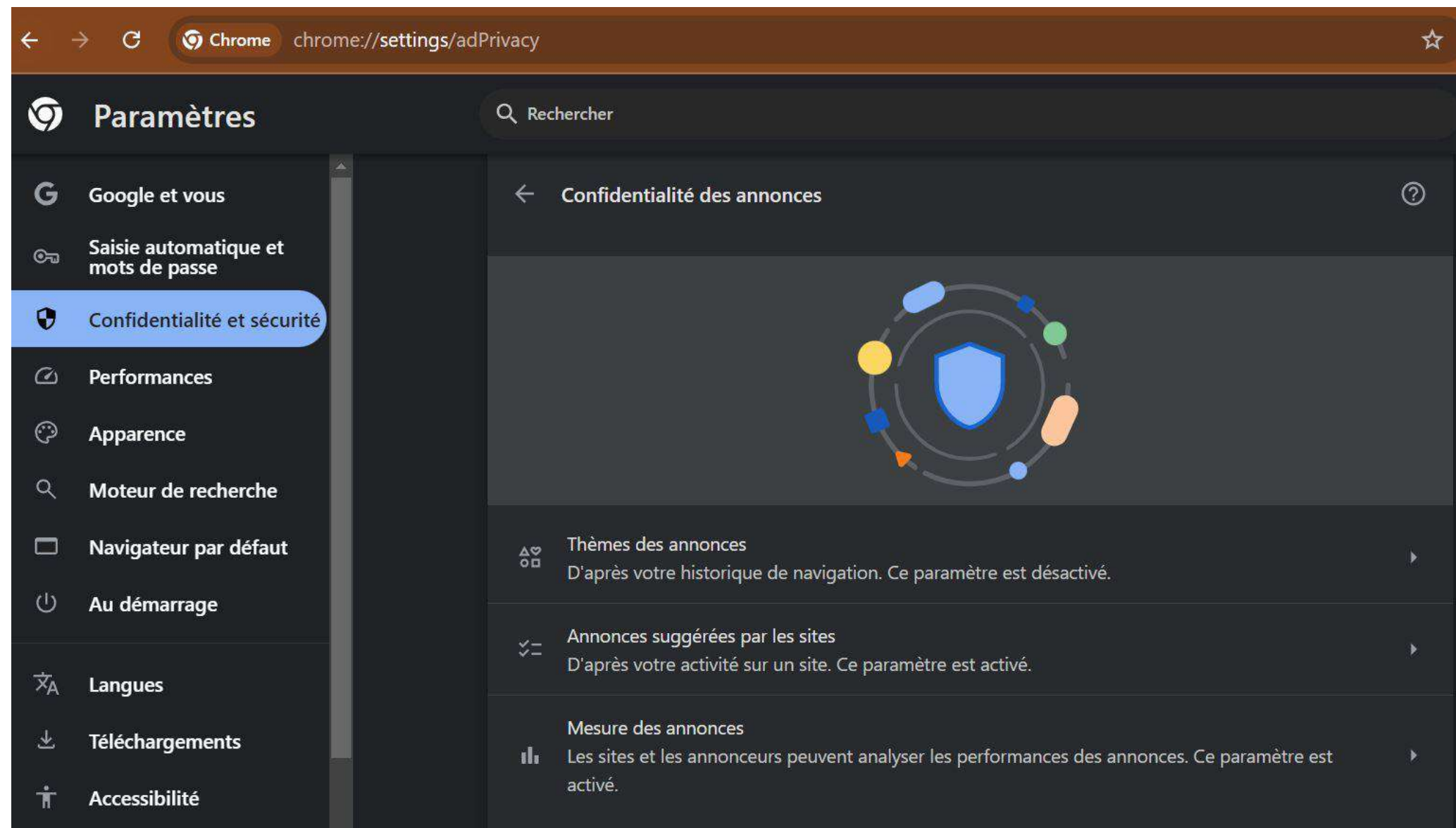


CMP PA-API & ARA



: Visuels paramètres Chrome

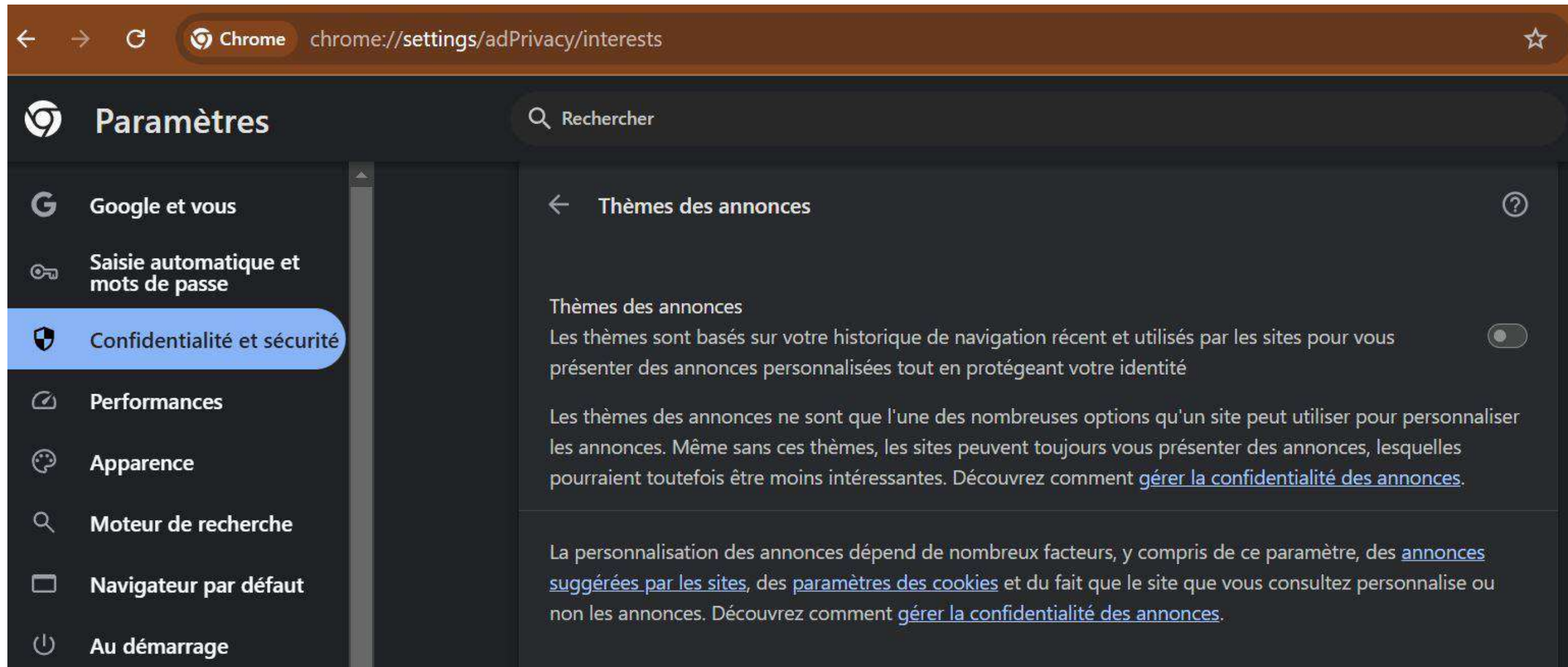
Dans la suite du document, sont évoquées à plusieurs reprises les interfaces de paramétrisation de la Privacy Sandbox permettant à l'utilisateur d'exercer un contrôle sur les données exploitées via les APIs de la Privacy Sandbox pour monétiser sa navigation sur les sites financés par la publicité



Paramètres Chrome ouvrant l'accès aux paramètres Privacy Sandbox



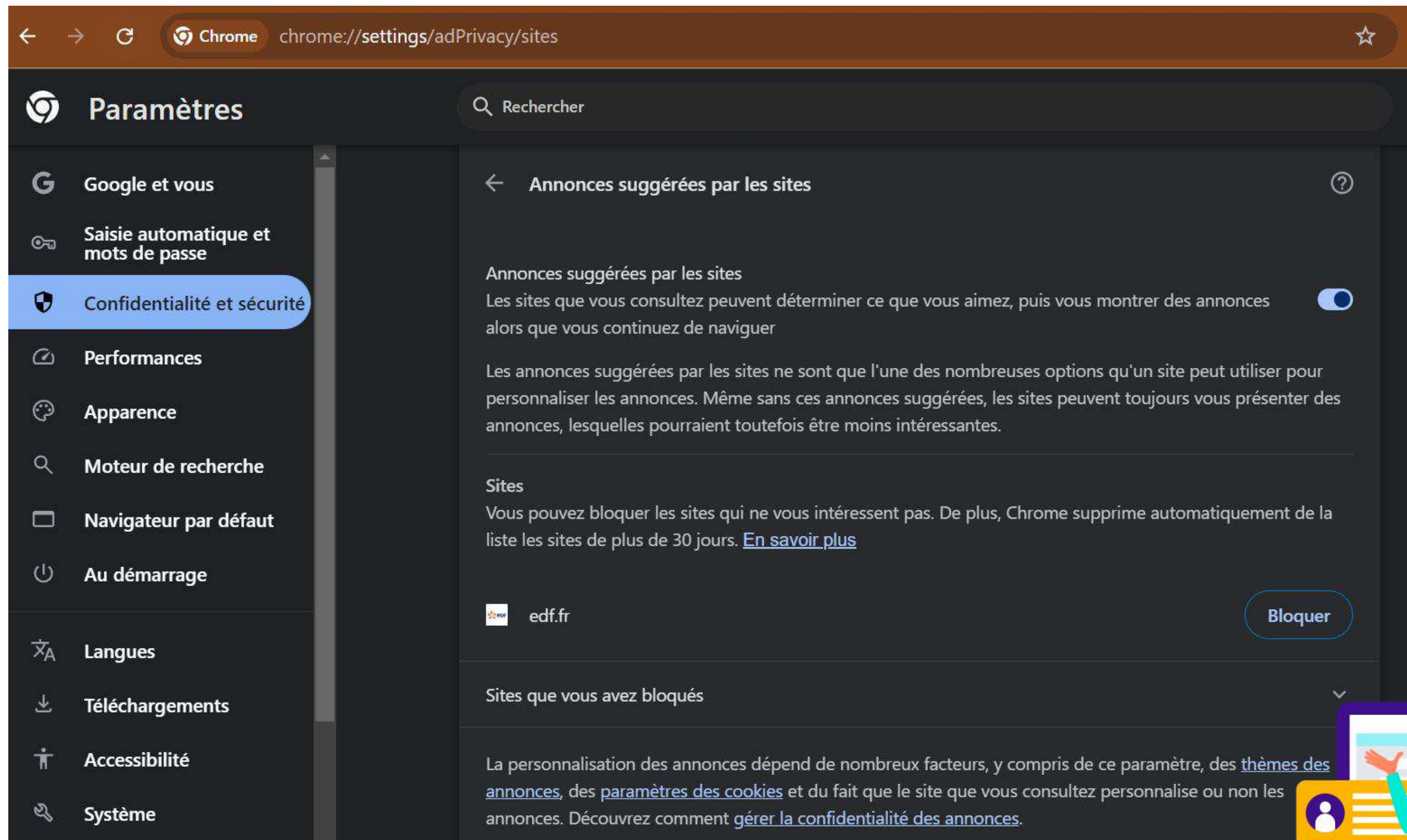
: Visuels paramètres Topics



Paramètres Chrome pour les Topics



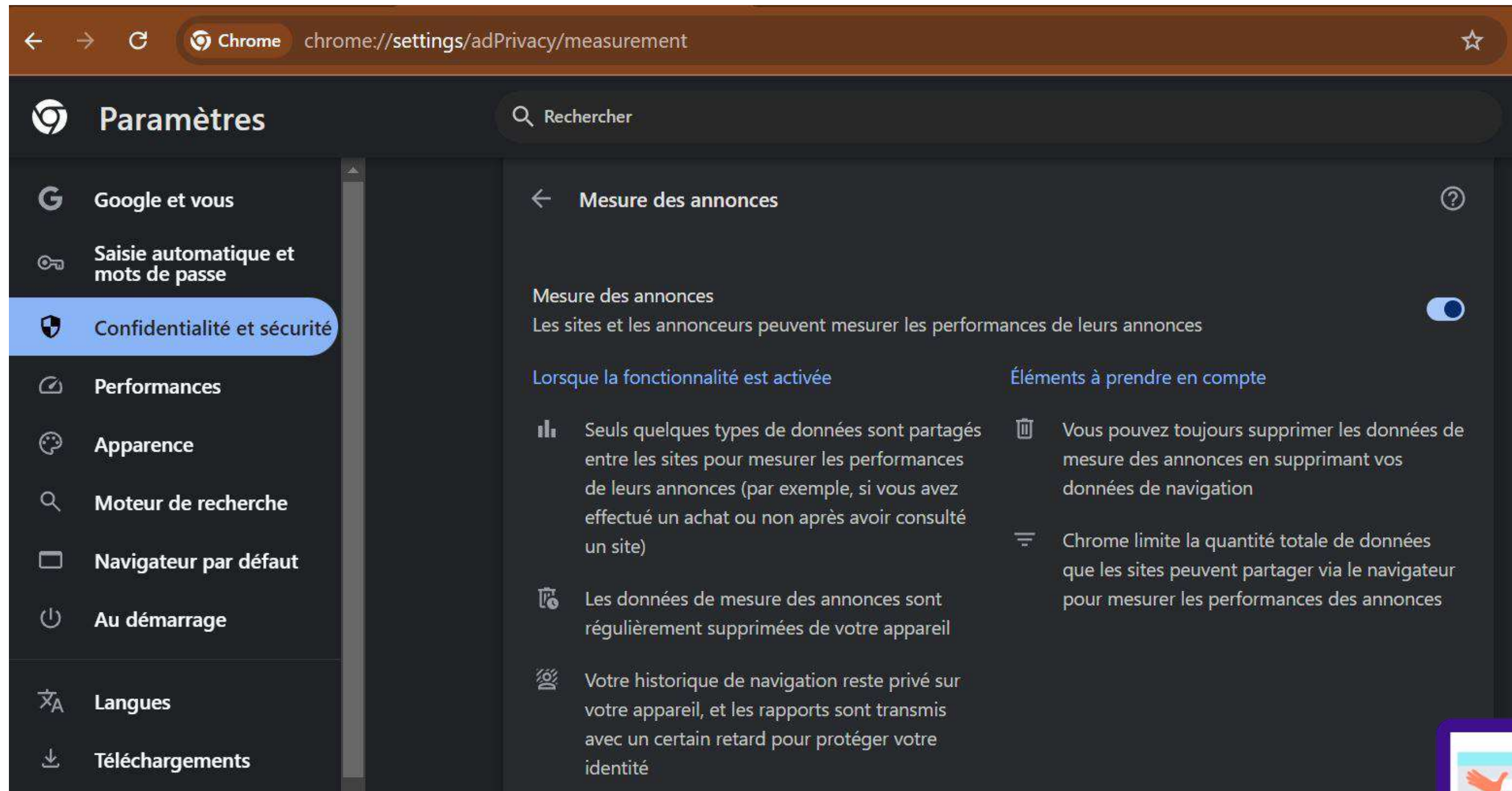
: Visuels paramètres Protected Audience



Paramètres Chrome pour Protected Audience



: Visuels paramètres Attribution Reporting



Paramètres Chrome pour Attribution Reporting



1



API Topics

7 / 19 inquiétudes restantes

: Résumé

Les principaux aspects qui ressortent du rapport de la CMA concernant l'API Topics sont les suivants :

- L'algorithme de classification Topics se rapproche de sa forme finale. Ses futures évolutions seront supervisées par l'organe de gouvernance proposé par Google. La CMP Topics ne sera affichée qu'une seule fois à l'utilisateur
- L'influence sur le référencement des sites d'un éditeur de sa décision de ne pas supporter (ou de supporter) l'API Topics est toujours sujet à discussion
- Le taux d'opt-in de la CMP Topics n'est pas une inquiétude pour la CMA : les éditeurs peuvent exploiter d'autres signaux contextuels pour limiter l'impact de l'absence de Topics sur le ciblage publicitaire, et donc une éventuelle baisse de leurs revenus



: Résumé

- **En l'état actuel de la Privacy Sandbox, les Topics peuvent servir à d'autres usages qu'à des fins publicitaires, et notamment à des usages malveillants**
- **De la même façon qu'ils l'ont toujours fait, les éditeurs et leurs Vendors devront collecter le consentement de l'utilisateur pour exploiter ses données personnelles issues de la Privacy Sandbox à des fins de ciblage publicitaire ou pour écrire dans son Local Storage. Ils sont responsables de traitement et passibles d'une saisine de l'ICO s'ils venaient à enfreindre à la loi**
- **Google a amélioré la clarté des interfaces détaillant l'usage faits des données issues des APIs de la Privacy Sandbox (dont Topics) résolvant la plupart des inquiétudes de la CMA concernant la capacité des utilisateurs à faire un choix éclairé et non-biaisé**
- **L'organe de gouvernance proposé par Google permettrait de lever les inquiétudes concernant son éventuel usage abusif des Topics si son fonctionnement venait à se montrer satisfaisant**



: API Topics

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Google ne fournit pas suffisamment de clarté aux individus sur la manière dont leurs données sont utilisées par l'API Topics	<ul style="list-style-type: none"> CMA : La CMP Topics ne permet pas aux internautes de comprendre précisément comment leurs données personnelles sont utilisées, ni comment les Topics qui leur sont attribués peuvent être utilisés à des fins dépassant le ciblage publicitaire basé sur leurs centres d'intérêt. De plus, Google devrait proposer régulièrement aux utilisateurs de revoir leurs préférences quant à l'utilisation qui est faite de leurs Topics 	<ul style="list-style-type: none"> Google : Nous avons fait évoluer la CMP Topics en ce sens, et avons mis à jour nos recommandations à destination des appelants de l'API afin qu'ils décrivent clairement aux utilisateurs à quelles fins leurs données vont être traitées CMA & ICO : Google a mis à jour la CMP Topics en suivant nos recommandations. Une enquête réalisée par Google sur la nouvelle interface montre que les utilisateurs font un choix éclairé lorsqu'ils interagissent avec 	<ul style="list-style-type: none"> Google doit mettre à jour son guide de confidentialité à destination des utilisateurs pour refléter les mises à jour apportées à la CMP Topics. Cette action permettrait de résoudre cette inquiétude
Certains aspects de la conception de la page des paramètres des Topics et de l'interface de consentement peuvent rendre plus difficile la prise de décisions éclairées par les individus concernant la collecte et l'utilisation de leurs données personnelles	<ul style="list-style-type: none"> N/A 	<ul style="list-style-type: none"> CMA & ICO : Nous avons demandé à Google d'apporter des modifications aux interfaces utilisateurs leur permettant de faire un choix éclairé quant à l'usage de leurs données personnelles. Ces modifications se sont avérées bénéfiques pour la compréhension des utilisateurs. Nous avons également souligné que ces interfaces pourraient influencer les utilisateurs à surestimer les protections de données à l'œuvre via l'API Topics (positive framing). Idem pour le guide de confidentialité à destination des utilisateurs. Google doit également préciser aux utilisateurs que les Topics peuvent être stockés de manière abusive par les appelants de l'API au-delà des 4 semaines prévues pour les Topics stockés dans Chrome 	<ul style="list-style-type: none"> Google doit remplacer les phrases induisant les utilisateurs en erreur par des formulations plus neutres (CMP Topics, Paramètres API Topics, guide utilisateur de confidentialité)



: API Topics

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Les utilisateurs peuvent avoir une connaissance limitée de leurs moyens de modifier leurs paramètres Topics dans Chrome car ils ne sont exposés qu'une seule fois à la CMP Topics	<ul style="list-style-type: none"> N/A 	<ul style="list-style-type: none"> Google : Afficher de multiples fois la CMP Topics conduirait à ce que les utilisateurs l'ignorent. Nous allons plutôt ajouter plus de détails dans notre guide de confidentialité à destination des utilisateurs quant aux paramètres à leur disposition 	<ul style="list-style-type: none"> Google doit indiquer clairement aux utilisateurs comment modifier leurs paramètres Topics. Cette action permettrait de résoudre cette inquiétude
Aucune restriction n'est imposée par Google aux appelants de l'API Topics, rendant cette dernière utilisable pour d'autres usages que celui du ciblage publicitaire basé sur les centres d'intérêt	<ul style="list-style-type: none"> CMA & ICO : Les Topics des utilisateurs sont accessibles sans restriction aux appelants de l'API, pouvant conduire à des utilisations abusives sortant du cadre originel fixé pour l'utilisation de ces informations, et donc nuire à l'utilisateur et enfreindre la RGPD Anglaise 	<ul style="list-style-type: none"> Google : Les éditeurs et leurs vendors devront décider de la signification du choix de l'utilisateur quant à l'utilisation ou non d'une API de la Privacy Sandbox et à la manière dont ils l'utilisent. Les éditeurs devront collecter le consentement de l'utilisateur (de la même façon qu'ils le font aujourd'hui) pour exploiter ses données personnelles issues de la Privacy Sandbox à des fins de ciblage publicitaire ou écriture dans le Local Storage. Nous avons modifié l'interface de la CMP Topics pour avertir l'utilisateur que les données de l'API Topics peuvent être utilisées pour d'autres usages que celui du ciblage publicitaire basé sur les centres d'intérêt CMA : Les risques de détournement de l'objet de l'API Topics demeurent. Les parties exploitant l'API Topics doivent se conformer à la régulation en matière de protection des données personnelles. Google reste un Data Controller (création des Topics) 	<ul style="list-style-type: none"> N/A



: API Topics

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Les Topics peuvent être stockés et accumulés par les appelants de l'API au-delà de la période de 3 epochs (3 semaines)	<ul style="list-style-type: none"> CMA & ICO : En général, les données collectées doivent être stockées uniquement pendant la durée où elles sont utilisées. Les données de l'API Topics peuvent être utilisées plus longtemps que les époques définies par les développeurs, ce qui peut conduire à l'infraction de la RGPD Anglaise 	<ul style="list-style-type: none"> Google : Les appelants de l'API Topics sont responsables des données extraites qu'ils stockent, et donc du droit à l'oubli qui leur est associé. Les Topics expirent au bout d'entre 26 et 28 jours afin de rendre plus difficile l'identification cross-sites d'un utilisateur lorsque ses Topics sont mis à jour CMA & ICO : Les précautions prises par Google sont de nature à réduire le risque de réidentification des utilisateurs, mais pas de le neutraliser. L'ICO pourra diligenter une action en justice contre les utilisateurs des APIs contrevenant à la réglementation en vigueur 	<ul style="list-style-type: none"> N/A
L'API Topics désavantage les plus petites Ad Tech (vs les plus importantes) du fait qu'elles présentent moins de reach et de données de ciblage que les Ad Tech les plus importantes	<ul style="list-style-type: none"> CMA : L'introduction de l'API Topics ne favorise pas davantage les plus larges acteurs (dont Google Ad Manager) en ce qui concerne l'accès aux données des internautes comparé au statu quo 	<ul style="list-style-type: none"> Marché : Il faut pouvoir exécuter du script sur les sites éditeurs si nous voulons pouvoir récupérer les Topics des internautes, développer davantage de partenariats entre sell et buy-sides le cas échéant. GAM et les Ad Tech prépondérantes sont moins concernés par cette limitation CMA : Les avantages cités par le marché pré-existaient avant la Privacy Sandbox et ne sont pas exacerbés par l'introduction de celle-ci. En l'absence de nouveaux éléments, nous considérons cette inquiétude comme résolue 	<ul style="list-style-type: none"> N/A



: API Topics

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Une même entité procédant à plusieurs enregistrements pour avoir droit d'appeler l'API Topics peut réidentifier un internaute en combinant les Topics récupérés par chaque sous-entité enregistrée	<ul style="list-style-type: none"> N/A 	<ul style="list-style-type: none"> CMA : Une même entité procédant à plusieurs enregistrements pour avoir droit d'appeler l'API Topics peut réidentifier un internaute en combinant les Topics récupérés par chaque sous-entité enregistrée Google : Les entités souhaitant enregistrer de multiples sous-entités à l'API Topics doivent le faire via un Multi Enrolment Request Process de façon à ce que nous en vérifions les raisons (ce motif sera refusé) 	<ul style="list-style-type: none"> La CMA est en attente d'une proposition plus robuste de la part de Google
Les modifications ultérieures apportées à la taxonomie des Topics pourraient introduire des risques en matière de protection des données personnelles des internautes si aucune précaution n'est prise	<ul style="list-style-type: none"> Google : La confidentialité des données des internautes est assurée par un nombre limité de Topics. Il faudrait cependant en accroître le nombre afin de rendre l'API plus utilisable et rémunératrice pour ses utilisateurs CMA & ICO : Plus il y a de Topics disponibles, plus la confidentialité des internautes est à risque. La confidentialité des internautes doit être la préoccupation numéro 1 de Google 	<ul style="list-style-type: none"> CMA : Toute évolution significative apportée à la taxonomie des Topics susceptible d'avoir un impact sur la confidentialité ou l'utilisabilité de l'API sera sujette à une validation de l'organe de gouvernance proposé par Google, ce qui pourrait permettre de résoudre cette inquiétude 	<ul style="list-style-type: none"> L'organe de gouvernance proposé par Google doit être testé pour valider si son fonctionnement permet de résoudre cette inquiétude
Le fait que les Topics soient assignés aux utilisateurs sur la base de leurs navigations durant la semaine écoulée peut aboutir à l'affichage de publicités à des utilisateurs qui ont déjà acheté le produit que l'annonceur, qui se baserait sur les Topics pour les cibler, souhaiterait leur proposer	<ul style="list-style-type: none"> CMA : La durée d'une semaine représente le bon compromis entre l'utilisabilité d'un Topic d'un utilisateur et la confidentialité de ses données 	<ul style="list-style-type: none"> CMA : Aucune évolution sur ce point-là. En l'absence de nouveaux éléments, nous considérons cette inquiétude comme résolue 	<ul style="list-style-type: none"> N/A




: API Topics

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Google ne dépendra pas autant de l'API Topics que le reste de l'industrie du fait de ses accès à la donnée first-party	<ul style="list-style-type: none"> CMA : Les Commitments imposés à Google limitent déjà l'usage de ses données 1st party par Google 	<ul style="list-style-type: none"> CMA : Aucune évolution sur ce point-là 	<ul style="list-style-type: none"> La CMA réfléchit à la nécessité de renforcer les restrictions imposées à Google pour répondre à cette inquiétude
Google pourrait manipuler à son avantage la taxonomie des Topics étant donné qu'il en est le seul gestionnaire	<ul style="list-style-type: none"> CMA : La mise en place d'une gouvernance de l'API Topics externe à Google permettrait de répondre à cette inquiétude L'amélioration de l'utilisabilité de l'API Topics ne doit pas être conduite au détriment de la confidentialité des internautes, et devra être compensée par la mise à disposition de ces derniers de nouveaux moyens de contrôle de la confidentialité de leurs données 	<ul style="list-style-type: none"> CMA : Toute évolution significative apportée à la taxonomie des Topics susceptible d'avoir un impact sur la confidentialité ou l'utilisabilité de l'API sera sujette à une validation de l'organe de gouvernance proposé par Google, ce qui pourrait permettre de résoudre cette inquiétude 	<ul style="list-style-type: none"> L'organe de gouvernance proposé par Google doit être testé pour valider si son fonctionnement permet de résoudre cette inquiétude
La décision d'un éditeur de ne pas supporter (ou de supporter) l'API Topics ne devrait pas influencer sur le référencement de ses sites	<ul style="list-style-type: none"> CMA : Le référencement des sites d'un éditeur ne doit en aucun cas dépendre de sa décision de ne pas supporter (ou de supporter) une <u>quelconque</u> API de la Privacy Sandbox 	<ul style="list-style-type: none"> CMA : Aucune évolution sur ce point-là 	<ul style="list-style-type: none"> En attente de la réponse de Google



: API Topics

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Le niveau de granularité de la taxonomie des Topics peut avoir un impact sur l'utilisabilité de l'API pour les éditeurs, les annonceurs, et sur les stratégies des éditeurs basées sur leurs données 1st party	<ul style="list-style-type: none"> CMA : Une des principales missions de la future gouvernance de l'API consistera à trouver le bon compromis entre la taille et le niveau de granularité de la taxonomie des Topics 	<ul style="list-style-type: none"> CMA : Toute évolution significative apportée à la taxonomie des Topics susceptible d'avoir un impact sur la confidentialité ou l'utilisabilité de l'API sera sujette à une validation de l'organe de gouvernance proposé par Google, ce qui pourrait permettre de résoudre cette inquiétude 	<ul style="list-style-type: none"> L'organe de gouvernance proposé par Google doit être testé pour valider si son fonctionnement permet de résoudre cette inquiétude
La classification des sites éditeurs basée sur l'hostname désavantage ceux qui couvrent différentes verticales vs les éditeurs de niche	<ul style="list-style-type: none"> CMA : Faute de contre-proposition plus privacy-oriented de la part des parties prenantes, la classification des sites en Topics basée sur leurs hostnames reste la solution retenue 	<ul style="list-style-type: none"> Marché : Le modèle de classification devrait également prendre en compte le titre ou le corps de la page en complément de l'hostname CMA : Le fonctionnement actuel de l'algorithme de classification des sites constitue un bon compromis entre la confidentialité et l'utilisabilité. S'il devait être modifié, les évolutions candidates devront être approuvées par l'organe de gouvernance proposé par Google 	<ul style="list-style-type: none"> En attente du dénouement des échanges entre le marché et Google sur ce sujet
Les éditeurs sont inquiets à l'idée que leurs sites puissent être mal ou non-classifiés par Google, et préféreraient pouvoir s'assigner leurs propres Topics	<ul style="list-style-type: none"> CMA : Permettre aux éditeurs de choisir leurs Topics pourraient en conduire certains à tricher Marché : La possibilité d'engager un recours en cas de mauvaise classification permettrait de résoudre cette inquiétude Google : Les données 1st party des éditeurs peuvent contrebalancer une mauvaise classification des Topics 	<ul style="list-style-type: none"> Google : Investir dans une solution à la mauvaise classification des sites serait trop coûteux (en ressources et en gestion des demandes d'appel abusifs). La classification actuelle, basée sur les avis de centaines d'être humains après avoir consulté 50 000 sites, est suffisamment robuste CMA : Le mécanisme de classification est suffisamment robuste et transparent. En l'absence de nouveaux éléments, nous considérons cette inquiétude comme résolue 	<ul style="list-style-type: none"> N/A 

: API Topics

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Si le taux d'opt-in de la CMP Topics est faible, cela peut impacter le ciblage publicitaire basé sur les centres d'intérêt des internautes, et donc les revenus des éditeurs	<ul style="list-style-type: none"> • CMA : Il n'est pas envisageable de proposer une API Topics sans CMP Topics 	<ul style="list-style-type: none"> • Google : La CMP Topics a été conçue pour permettre aux utilisateurs de faire un choix éclairé et libre quant au traitement de leurs données personnelles aboutissant à la création de leurs Topics. Depuis récemment, les utilisateurs bénéficient de contrôles supplémentaires sur les Topics qui leur sont associés • CMA : L'impact négatif sur les revenus des éditeurs peut être atténué en recourant à d'autres signaux de contexte 	<ul style="list-style-type: none"> • En attente des discussions entre la CMA et Google au sujet de l'UX de la CMP Topics. S'il s'avère qu'elle est satisfaisante, cette inquiétude pourrait être résolue par la CMA
L'API Topics est difficile à tester tant qu'elle n'a pas atteint sa forme finale	<ul style="list-style-type: none"> • Marché : L'API Topics a trop évolué dans le temps pour nous permettre de la tester convenablement • CMA : Le marché doit s'accoutumer au fait que les Topics évoluent dans le temps. La gouvernance qui sera proposée par Google pour la gestion des Topics devrait permettre au marché d'anticiper suffisamment en avance les évolutions à venir de la taxonomie des Topics 	<ul style="list-style-type: none"> • CMA : L'organe de gouvernance proposé par Google devrait résoudre les inquiétudes quant aux modifications apportées à la taxonomie Topics • Google : Nous continuerons de collaborer avec l'écosystème pour faire évoluer la Privacy Sandbox. Nous proposerons une période de consultation publique avant chaque changement pouvant impacter la confidentialité ou l'utilisabilité de l'API Topics 	<ul style="list-style-type: none"> • L'organe de gouvernance proposé par Google doit être testé pour valider si son fonctionnement permet de résoudre cette inquiétude



: API Topics

Sujet	Position Q3 2024	Prochaines étapes
Le séquençement des CMP Topics, Protected Audience et Attribution Reporting ne permettent pas aux utilisateurs de comprendre qu'ils expriment leur consentement pour 3 différentes API	<ul style="list-style-type: none">• Google : Notre recherche UX confirme cette hypothèse. Nous avons ajusté le parcours de consentement pour ces 3 APIs, ce qui a permis de porter la compréhension des utilisateurs à un niveau satisfaisant• CMA : Nous considérons cette inquiétude comme étant résolue	<ul style="list-style-type: none">• N/A
Les utilisateurs n'ont pas la possibilité d'accéder à l'intégralité de la hiérarchie des Topics lorsqu'ils consultent leurs Topics et cherchent à en bloquer certains	<ul style="list-style-type: none">• Google : Nous avons accordé cette possibilité aux utilisateurs à partir d'un article sur le centre d'aide de Chrome plutôt qu'à partir de l'interface de gestion des Topics dans les paramètres de Chrome afin de ne pas submerger l'utilisateur d'informations et car nos templates d'UX ne sont pas prévus pour afficher autant d'informations au même endroit• CMA : La solution proposée par Google permet de résoudre cette inquiétude	<ul style="list-style-type: none">• N/A



2



API Protected Audience

11 / 26 inquiétudes restantes

: Résumé

Les principaux aspects qui ressortent du rapport de la CMA concernant l'API Protected Audience (PAAPI) sont les suivants :

- Google ne participera pas aux enchères Protected Audience s'il n'est pas le top-level seller, ce qui lui confère un avantage concurrentiel conséquent. Prebid a proposé une alternative où il endosserait ce rôle à la place de Google Ad Manager
- Google a amélioré l'utilisabilité de Protected Audience (ajout de signaux aux enchères, baisse de leur latence, support du negative targeting) et poursuit dans cette voie en s'appuyant sur les retours de l'écosystème. La CMA rappelle que chaque nouvelle amélioration de l'utilisabilité doit être compensée par une précaution sur la confidentialité (ex: en informer l'utilisateur)
- L'écosystème déplore dépendre de Google pour la résolution de pannes survenant sur la Privacy Sandbox et affectant leurs revenus



: Résumé

- La latence induite par les enchères PA et leurs impacts sur les KPI de monétisation restent une inquiétude forte car non-résolue
- En l'état actuel de la Privacy Sandbox, l'API Protected Audience n'empêche toujours pas le tracking cross-sites des internautes
- L'API Protected Audience limite les informations dont disposent les éditeurs par rapport au statu quo (ex: identité des vainqueurs des enchères PA). Cette information sera uniquement connue de l'Ad Server de Google. Cette inégalité d'accès à l'information reste encore sujette à discussion entre Google et la CMA
- Les éditeurs peuvent à présent choisir quand déclencher une enchère PA sur leurs sites lorsque GAM est le top-level seller (avant, cette décision était prise par l'algorithme de Machine Learning de GAM). La CMA doit confirmer avec Google si cette possibilité sera pérenne dans le temps



: Résumé

- Google a rendu la majorité des usages de Protected Audience suffisamment explicites pour les internautes
- L'organe de gouvernance proposé par Google veillera à maintenir un bon équilibre entre la confidentialité et l'utilisabilité de PA-API
- De la même façon qu'ils l'ont toujours fait, les éditeurs et leurs Vendors devront collecter le consentement de l'utilisateur pour exploiter ses données personnelles issues de la Privacy Sandbox à des fins de ciblage publicitaire ou pour écrire dans son Local Storage. Ils sont responsables de traitement et passibles d'une saisine de l'ICO s'ils venaient à enfreindre à la loi



: API Protected Audience (PAAPI)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Lors de la dépréciation des cookies tiers, Protected Audience pourrait être déployée malgré l'absence d'un certain nombre de contrôles clés en matière de confidentialité	<ul style="list-style-type: none"> • CMA & ICO : La mise en place de PETs complémentaires au fonctionnement de l'API Protected Audience sont indispensables afin d'éviter que les utilisateurs de l'API ne puissent reconstituer les activités cross-sites des internautes • Google : L'introduction trop rapide de l'obligation d'utiliser des PETs en complément de l'API pour pouvoir l'utiliser peut nuire à son adoption 	<ul style="list-style-type: none"> • CMA : Il existe toujours des failles quant à la gestion de la confidentialité au sein de PAAPI. Le rapport annuel sur les risques de tracking cross-sites proposé par Google dans le cadre de la gouvernance qu'ils ont suggérée permettra d'intégrer des solutions à ces failles dans la roadmap de PAAPI. Si l'organe de gouvernance fonctionne correctement, alors cette inquiétude sera résolue 	<ul style="list-style-type: none"> • L'organe de gouvernance proposé par Google doit être testé pour valider si son fonctionnement permet de résoudre cette inquiétude
Le fait que les groupes d'intérêt soient créés par des tiers partis rend leur existence opaque pour l'utilisateur	<ul style="list-style-type: none"> • CMA & ICO : Les internautes ne sont ni en mesure de donner ou refuser de donner leur consentement pour que l'API soit utilisée, ni de comprendre l'usage qu'il est fait de leurs données personnelles, ni qui sont les acteurs les exploitant 	<ul style="list-style-type: none"> • Google : Nous avons mis en avant via les interfaces PAAPI (CMP, page des paramètres) les risques de collaboration entre les éditeurs et les Ad Tech lors de l'usage de PAAPI visant à enrichir les métadonnées des enchères avec des données déjà connues sur les internautes • CMA : Les précautions prises par Google sont de nature à résoudre cette inquiétude. Les risques restants en matière de privacy dépendent de la manière dont les sites informeront les utilisateurs que des tiers partis peuvent créer des groupes d'intérêt, et de s'ils les en informent 	<ul style="list-style-type: none"> • Google doit évaluer la compréhension des internautes suite à la dernière mise à jour de la CMP PAAPI



: API Protected Audience (PAAPI)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Le fait que la création des groupes d'intérêt soient opérés par des tiers sans consentement préalable de l'utilisateur peut avoir un impact sur la transparence, l'équité, et la légalité	<ul style="list-style-type: none"> • CMA & ICO : N'importe quel tiers parti peut créer et exploiter des groupes d'intérêt sur les sites des éditeurs sans que ces derniers ne puissent identifier lesdits tiers partis. Qui plus est, les données personnelles des utilisateurs sont exploitées sans base légale adéquate 	<ul style="list-style-type: none"> • CMA : Google a l'intention de faire passer les autorisations des tiers partis à créer des groupes d'intérêt sur les sites des éditeurs de « autoriser tout » (ce qui facilitait la période de test de PAAPI) à « bloquer tout » de façon à limiter le leakage des audiences des éditeurs vers des tiers partis opérant sans permission explicite. Cette autorisation peut être revue par l'éditeur. Une fois le calendrier de bascule publié, cette inquiétude sera résolue. 	<ul style="list-style-type: none"> • Google doit publier le calendrier de modification des autorisations par défaut des tiers partis à créer des groupes d'intérêt
L'utilisation des Fenced Frames limite les types de formats publicitaires qu'il est possible d'afficher. Elles ne prennent actuellement pas en charge (1) les formats Native, tels que le dimensionnement dynamique des publicités, et (2) les formats Video, tels que la transmission de signaux provenant de lecteurs vidéo (quartiles, etc)	<ul style="list-style-type: none"> • CMA : L'utilisation des Fenced Frames ne sera pas imposée avant 2026. Le marché veut pouvoir y afficher tous types de formats 	<ul style="list-style-type: none"> • Google : Les principaux formats publicitaires seront rendus utilisables avant l'entrée en vigueur de l'obligation d'utiliser les Fenced Frames • CMA : Le recours obligatoire aux Fenced Frames sera validé par l'organe de gouvernance proposé par Google. En l'absence de nouveaux éléments, nous considérons cette inquiétude comme résolue 	<ul style="list-style-type: none"> • Les discussions entre Google et l'écosystème concernant la conception des Fenced Frames sont toujours en cours



: API Protected Audience (PAAPI)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Les données cross-sites exploitables via l'API Protected Audience qui dépassent le champ d'application initial de l'API, le sont sans transparence suffisante	<ul style="list-style-type: none"> N/A 	<ul style="list-style-type: none"> Google : Basé sur les demandes de l'écosystème, nous avons autorisé les utilisateurs de PAAPI à utiliser les signaux de vue et de clic des internautes dans leur logique d'enchères. Nous avons mis à jour la CMP PAAPI en conséquence CMA : Cet ajout s'écarte de la proposition initiale visant à limiter le tracking cross-sites des internautes. La clarification de la CMP PAAPI est de nature à résoudre cette inquiétude 	<ul style="list-style-type: none"> Google doit informer les internautes que leur nombre total de vues des publicités (tous sites confondus) fait partie des données cross-sites exploitables lors de l'utilisation de PAAPI Le marché doit partager à Google ses retours quant à la disponibilité de ces deux nouveaux signaux
Les évolutions de l'API Protected Audience, visant à la rendre plus exploitable, ne prennent pas suffisamment en compte les impacts qu'elles peuvent avoir sur la confidentialité	<ul style="list-style-type: none"> CMA & ICO : Les évolutions apportées au fonctionnement même de l'API afin de rendre cette dernière plus utile à l'écosystème sont de nature à compromettre l'objet même de la dépréciation des cookies tiers, et plus particulièrement, de nature à rendre la Privacy Sandbox non-conforme aux réglementations en matière de protection des données personnelles des internautes 	<ul style="list-style-type: none"> CMA : Les futures évolutions apportées à PAAPI et qui impacteraient significativement sa confidentialité ou son utilisabilité devront au préalable être validées par l'organe de gouvernance proposé par Google. Si elles ne sont pas suffisamment impactantes pour être revues par cet organe, elles seront transmises pour révision à l'organe de contrôle, à la CMA et à l'ICO 	<ul style="list-style-type: none"> L'organe de gouvernance proposé par Google doit être testé pour valider si son fonctionnement permet de résoudre cette inquiétude



: API Protected Audience (PAAPI)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
En l'état, les groupes d'intérêt ne sont pas pensés pour permettre le traffic shaping	<ul style="list-style-type: none"> CMA : L'absence de traffic shaping lors des enchères PA favorise les Ad Tech ayant les plus grandes capacités de traitement des requêtes (ex: les DSPs de Google) 	<ul style="list-style-type: none"> Google : Permettre aux SSP de n'appeler que les DSP actifs sur un groupe d'intérêt présente un risque de fingerprinting. Il est possible à la place d'intuiter les préférences des DSP en recourant à la mise en cache, au filtrage basé sur le contexte, et à Private Aggregation CMA : L'absence de traffic shaping lors des enchères PAAPI ne distord pas la compétition car elle s'applique de la même manière pour tous 	<ul style="list-style-type: none"> En attente de nouvelles options de la part de Google et l'écosystème pour permettre le traffic shaping
L'API Protected Audience limite les informations dont disposent les éditeurs par rapport au statu quo. Les éditeurs n'auront aucune visibilité sur l'identité des vainqueurs des enchères Protected Audience, mais uniquement des informations sur l'identité de l'enchère gagnante	<ul style="list-style-type: none"> CMA : Le top-level seller bénéficie de plus d'informations que l'éditeur et les participants de l'enchère. Google ne doit pas pénaliser les autres acteurs des enchères vs son Ad Server. Google pourrait partager les données de view et de clic aux annonceurs 	<ul style="list-style-type: none"> N/A 	<ul style="list-style-type: none"> En attente des discussions entre la CMA et Google
L'identité des vainqueurs des enchères Protected Audience sera connue de l'Ad Server de Google, ce qui rend inégal l'accès aux informations des enchères	<ul style="list-style-type: none"> CMA : Google nous assure qu'aucune information liée aux enchères Protected Audience ne sort des processus des enchères. GAM a-t-il accès à des informations auxquelles les éditeurs n'ont pas accès ? 	<ul style="list-style-type: none"> N/A 	<ul style="list-style-type: none"> En attente des discussions entre la CMA et Google



: API Protected Audience (PAAPI)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Une fois l'évent-level reporting déprécié par Google en 2026, l'API Private Aggregation sera le seul mécanisme de reporting disponible	<ul style="list-style-type: none"> CMA : La fin de l'évent-level reporting peut limiter les capacités des Ad Techs à optimiser leurs stratégies d'enchère 	<ul style="list-style-type: none"> Google : Nous allons maintenir la disponibilité de l'évent-level reporting jusqu'à 2026 Marché : Nous souhaitons que la disponibilité de l'évent-level reporting soit prolongée, et avoir accès à des outils event-level de supervision et de débogage en temps réel CMA : Si l'organe de gouvernance fonctionne correctement, alors cette inquiétude sera résolue entre Google et l'écosystème 	<ul style="list-style-type: none"> En attente de la réponse de Google quant aux demandes formulées par l'écosystème
Le SSP de Google ne prendra pas part aux enchères Protected Audience à moins que GAM ne soit le top-level seller. Autrement dit, les éditeurs ne pourront pas accéder à la demande AdX via Protected Audience s'ils n'utilisent pas GAM comme Ad Server	<ul style="list-style-type: none"> Google : Nous ne reviendrons pas sur cette décision car cela limiterait les fonctionnalités de notre Ad Server (forecasting) CMA : Cette décision est de nature à renforcer la position dominante de Google sur le marché des solutions d'Ad Server et de top level-sellers 	<ul style="list-style-type: none"> Marché : Nous soutenons l'implémentation proposée par Prebid où ce dernier joue le rôle de top-level seller à la place de GAM. Elle s'avère être plus configurable que celle proposée par GAM 	<ul style="list-style-type: none"> En attente des discussions entre la CMA et Google quant à cette inquiétude
La gestion de l'exclusivité sectorielle au niveau d'une page n'est pas assurée en l'état actuel du fonctionnement de l'API car les enchères Protected Audience sont opérées séparément pour chaque emplacement publicitaire sur la page	<ul style="list-style-type: none"> Google : L'exclusivité sectorielle n'est pas gérée en l'état (i.e. sans Privacy Sandbox). Les solutions proposées peuvent nuire à la confidentialité ou sont trop complexes à mettre en œuvre 	<ul style="list-style-type: none"> Google : Nous n'avons pas changé d'avis mais restons ouverts à de nouvelles suggestions. La vente en direct permet de répondre à ce besoin CMA : Nous sommes alignés avec la position de Google. Si de nouvelles suggestions émergent, elles pourront être évaluées par l'organe de gouvernance proposé par Google tant qu'elles n'impactent pas négativement la confidentialité. En l'absence de nouveaux éléments, nous considérons cette inquiétude comme résolue 	<ul style="list-style-type: none"> N/A



: API Protected Audience (PAAPI)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Les enchères Protected Audience ne permettent pas d'opérer le negative targeting (faire en sorte que certains utilisateurs ne soient pas assujettis à une publicité en particulier)	<ul style="list-style-type: none"> • Google : Nous avons intégré la possibilité d'opérer le negative targeting via l'API 	<ul style="list-style-type: none"> • CMA : A en croire les échanges sur l'issue ouverte sur GitHub traitant du sujet, la proposition de Google semble répondre aux besoins du marché 	<ul style="list-style-type: none"> • En attente de la confirmation définitive de l'écosystème quant à la solution mise en place par Google
L'API Protected Audience ne permet aux annonceurs d'enchérir qu'au travers d'un seul groupe d'intérêt à la fois. Les annonceurs ne peuvent donc pas combiner plusieurs groupes d'intérêt (ex: enchérir si un internaute fait partie de 2 groupes d'intérêt à la fois)	<ul style="list-style-type: none"> • CMA : Combiner plusieurs groupes d'intérêt va à l'encontre des préceptes de confidentialité de la Privacy Sandbox • Marché : Il est possible pour les DSP et Ad Servers de contourner cette limitation en joignant leurs forces 	<ul style="list-style-type: none"> • CMA : Restreindre le remarketing à un seul groupe d'intérêt bénéficie à la confidentialité des internautes. En l'absence de nouveaux éléments, nous considérons cette inquiétude comme résolue. Microsoft & Prebid ont proposé une solution de combinaison des groupes d'intérêt respectueuse de la confidentialité. Elle pourra être évaluée par la gouvernance proposée par Google • Marché : Google, du fait de ses données first-party, est moins impacté par cette contrainte • Google : La combinaison de groupes d'intérêts ne sera pas possible dans PAAPI pour des raisons de confidentialité. L'ajout de données aux enchères PAAPI est limité pour tous de la même façon. Je suis contraint par mes Commitments à ne pas abuser de mes données first-party à mon avantage 	<ul style="list-style-type: none"> • N/A



: API Protected Audience (PAAPI)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Google envisage d'utiliser le Machine Learning pour décider des moments les plus opportuns où conduire les enchères Protected Audience. Les éditeurs manquent de transparence et de contrôle sur les décisions conduisant à la tenue de ces enchères	<ul style="list-style-type: none"> CMA : Les éditeurs peuvent désactiver le Machine Learning de Google dès lors qu'il existe un autre participant aux enchères que le SSP de Google. Mais les éditeurs ne peuvent pas décider quand déclencher une enchère PA 	<ul style="list-style-type: none"> Google : Nous avons rendu disponible aux éditeurs la possibilité d'override la décision de GAM portant sur la tenue des enchères PA CMA : La formulation de la présentation de cette nouvelle fonctionnalité suggère que sa disponibilité sert pour des tests temporaires et pas sur le long terme 	<ul style="list-style-type: none"> En attente des discussions entre la CMA et Google
La latence induite par la conduite des enchères Protected Audience peut affecter l'expérience de navigation ainsi que la monétisation des sites éditeurs	<ul style="list-style-type: none"> CMA : En attente des résultats des tests menés par les acteurs de l'écosystème depuis l'ouverture de la phase de test 	<ul style="list-style-type: none"> CMA : Les résultats des tests font état d'une augmentation de la durée d'affichage des publicités, une baisse des taux de visibilité des emplacements et du volume d'impressions diffusées Google : Afin de réduire les traitements on-device, il est désormais possible de répartir les traitements des enchères entre le terminal de l'utilisateur et le serveur Bidding & Auctions. L'exploitation des signaux de clickiness et la dépréciation partielle des cookies tiers sont de nature à compenser les pertes de revenus causées par la latence d'affichage des publicités 	<ul style="list-style-type: none"> En attente des résultats des tests des nouvelles propositions de Google pour limiter la latence (parallélisation des traitements, introduction de timeouts) pour valider la résolution de cette inquiétude
Conduire les enchères Protected Audience sur le device des internautes peut avoir un impact sur les performances des sites, des terminaux, et donc potentiellement sur l'expérience de navigation et le référencement desdits sites	<ul style="list-style-type: none"> CMA : Les enchères sont conduites séparément des processus permettant le rendu des pages. En attente des résultats des tests 	<ul style="list-style-type: none"> CMA : En l'absence de nouveaux éléments, nous considérons l'inquiétude portant sur le référencement des sites comme résolue 	<ul style="list-style-type: none"> N/A



: API Protected Audience (PAAPI)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Les données des tiers partis / cross-sites pourraient être combinées avec les données first-party au travers des groupes d'intérêt	<ul style="list-style-type: none"> • CMA & ICO : La possibilité nouvelle de combiner des données first & third-party dans le cadre des enchères Protected Audience peuvent conduire au non respect de la RGPD Anglaise et au sur-profilage des internautes dépassant alors les cas d'usage originels de remarketing définis pour l'API • Google : Le sur-profilage ne sera plus possible lors de l'entrée en vigueur des obligations d'utiliser des PETs pour faire fonctionner l'API 	<ul style="list-style-type: none"> • Google : Les utilisateurs de PAAPI (éditeurs, Ad Tech, etc) devront collecter le consentement de l'utilisateur de la même façon qu'ils le font aujourd'hui pour exploiter ses données personnelles issues de la Privacy Sandbox à des fins de ciblage publicitaire ou écriture dans le Local Storage. De plus, les éditeurs doivent informer les internautes lorsque des données de tiers sont impliquées lors de l'usage de PAAPI, et lorsqu'ils souhaitent créer des groupes d'intérêt exploitant des données cross-sites et en stocker les informations sur leurs navigateurs. Nous avons mis en avant via la CMP PAAPI les risques de combinaison des données des groupes d'intérêt par les Ad Tech • CMA : Nous considérons que la décision de Google d'assouplir les exigences en matière de k-anonymat est un bon compromis entre la confidentialité (car peut être assurée par des exigences en matière de protection des données imposées aux appelants de l'API) et l'utilisabilité (car réduit la latence des enchères PAAPI et permet aux Ad Techs d'opérer du microciblage) 	<ul style="list-style-type: none"> • Google doit continuer à faire évoluer la CMP PAAPI jusqu'à ce qu'elle fournisse un niveau de compréhension satisfaisant des traitements à l'œuvre aux internautes
L'API Protected Audience ne permet pas à un tiers-parti différent de celui ayant constitué le groupe d'intérêt de participer aux enchères pour ce groupe d'intérêt	<ul style="list-style-type: none"> • Google : La délégation de groupe d'intérêt est déjà possible en l'état via l'établissement de contrats 	<ul style="list-style-type: none"> • CMA : En l'absence de nouveaux éléments, nous considérons cette inquiétude comme résolue 	<ul style="list-style-type: none"> • N/A



: API Protected Audience (PAAPI)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Les traitements de données, à l'origine opérés server-side, se retrouvent effectués sur le terminal de l'utilisateur. Cela soulève des inquiétudes concernant l'opacité de ces traitements et la validité des contrats existants entre les entités opérant ces traitements de données	<ul style="list-style-type: none"> Google : Les acteurs souhaitant utiliser les outils de la Privacy Sandbox ne pourront nouer de contrat avec Google pour leur utilisation étant donné que ces outils font partie du navigateur et leur utilisation est à la discrétion de chacun 	<ul style="list-style-type: none"> Marché : Nous sommes dépendants de Google pour la résolution d'incidents intervenant sur PAAPI et impactant négativement notre fonds de commerce. Ce risque est exacerbé par l'absence de relations contractuelles avec Google. La panne des APIs de la Privacy Sandbox de Mai 2024 nous conforte dans notre inquiétude CMA : En l'absence de relation contractuelle, il est possible de superviser le code open-source de Chromium. L'organe de gouvernance proposé par Google tient pour responsable Google en cas de panne, et traitera les inquiétudes quant à l'aspect contractuel au cas par cas. Nous considérons cette inquiétude comme résolue 	<ul style="list-style-type: none"> N/A
L'obligation imposée par Google de recourir à des TEEs pour utiliser les composants server-side de l'API Protected Audience (Bidding & Auctions Services, Key/Value Server) soulève des inquiétudes	<ul style="list-style-type: none"> Google : Le recours aux TEEs de PAAPI ne sera obligatoire qu'à partir de Q3 2025 Marché : La plupart des Ad Techs ne peuvent pas se passer des services fournis par les composants server-side de Protected Audience 	<ul style="list-style-type: none"> Marché : La latence des enchères PAAPI augmentera lorsqu'elles seront résolues sur des TEEs. L'obligation de recourir à des TEEs pour conduire les enchères PAAPI limitera donc la portée de nos modèles d'enchère afin de réduire au maximum la latence d'affichage des publicités 	<ul style="list-style-type: none"> En attente des résultats des tests des TEEs de PAAPI par les acteurs de l'écosystème



: API Protected Audience (PAAPI)

Sujet	Position Q3 2024	Prochaines étapes
Le séquençement des CMP Topics, Protected Audience et Attribution Reporting rend obscur et contre-intuitif pour les utilisateurs qu'il s'agit de 3 API différentes	<ul style="list-style-type: none"> • CMA & ICO : La mise en évidence du bouton « Got it » sur les CMP PA & ARA incite les utilisateurs à les masquer sans lire ou comprendre les informations présentées • Google : Nous avons ajusté le parcours de consentement pour ces 3 APIs, ce qui a permis de porter la compréhension des utilisateurs qu'il s'agissait d'APIs distinctes à un niveau satisfaisant 	<ul style="list-style-type: none"> • Google doit harmoniser les couleurs des boutons « Got it » et « Settings » pour que cette inquiétude soit résolue
L'utilisateur ne sait pas clairement si un site a délégué des autorisations à un tiers	<ul style="list-style-type: none"> • CMA & ICO : Les utilisateurs ne voient que les noms de domaine des sites ayant délégué des permissions à des tiers partis sur l'interface de paramétrage de PAAPI, les portant à croire que seuls lesdits sites traitent leurs données, ce qui ne leur permet pas de réaliser des choix éclairés. Google n'a pas le moyen de savoir, et donc d'informer les internautes, que leurs données cross-sites sont exploitées dans le cadre d'enchères PAAPI. Il faut donc trouver un autre moyen de porter à leur attention cette information 	<ul style="list-style-type: none"> • Google doit rendre plus visible pour les utilisateurs la possibilité qu'ont les tiers partis à exploiter leurs données
Les objectifs des groupes d'intérêt ne sont pas clairement expliqués aux utilisateurs dans les paramètres Chrome de PAAPI	<ul style="list-style-type: none"> • CMA & ICO : Les utilisateurs n'ont pas la capacité de contrôler correctement leurs paramètres de confidentialité et à faire des choix efficaces pour bloquer certains groupes d'intérêt • Google : Nous explorons de nouvelles façons d'apporter aux utilisateurs de la clarté quant aux groupes d'intérêt, que ce soit via les interfaces Chrome ou celles des tiers partis les exploitant 	<ul style="list-style-type: none"> • Google doit rendre plus accessible aux utilisateurs les informations des groupes d'intérêts



: API Protected Audience (PAAPI)

Sujet	Position Q3 2024	Prochaines étapes
<p>Le positive framing de la CMP PAAPI peut rendre plus difficile pour les utilisateurs de faire des choix éclairés concernant leurs données</p>	<ul style="list-style-type: none"> • Google : Nous avons ajouté à l'écran de CMP PAAPI de nouvelles informations quant aux données qui y sont exploitables, ce qui a amélioré le niveau de compréhension des utilisateurs • CMA & ICO : La CMP PAAPI en son état actuel donne à l'utilisateur une fausse impression de surprotection de sa vie privée, d'autant que l'API va finalement être déployée sans un certain nombre de contrôles clés de la confidentialité des données des internautes 	<ul style="list-style-type: none"> • Google doit rendre plus neutres / moins exagérés les bénéfices en matière de confidentialité apportés par PAAPI
<p>Des données intersites supplémentaires dépassant le cadre initial de la proposition Privacy Sandbox sont traitées dans l'API Protected Audience sans transparence suffisante pour l'utilisateur</p>	<ul style="list-style-type: none"> • Google : Basé sur les demandes de l'écosystème, nous avons autorisé les utilisateurs de PAAPI à utiliser les signaux de vue et de clic des internautes dans leur logique d'enchères. Ces signaux peuvent d'ailleurs être utilisés comme source events via ARA. Nous avons mis à jour la CMP PAAPI en conséquence • CMA : Cet ajout s'écarte de la proposition initiale visant à limiter le tracking cross-sites des internautes. La clarification de la CMP PAAPI est de nature à résoudre cette inquiétude 	<ul style="list-style-type: none"> • Google doit informer les internautes que leur nombre total de vues des publicités (tous sites confondus) fait partie des données cross-sites exploitables lors de l'utilisation de PAAPI • Le marché doit partager à Google ses retours quant à la disponibilité de ces deux nouveaux signaux



3



API Attribution Reporting

2 / 17 inquiétudes restantes

: Résumé

Les principaux aspects qui ressortent du rapport de la CMA concernant l'API Attribution Reporting (ARA) sont les suivants :

- Google a amélioré l'utilisabilité de l'API Attribution Reporting (attribution multi-touch, augmentation du nombre d'ad events traçables, augmentation du nombre de contributions mesurées par rapport). La CMA rappelle qu'ARA n'a pas vocation à répondre exactement aux mêmes cas d'usage que les cookies tiers
- La CMA reconnaît qu'une mesure dégradée en Open Display peut conduire à la fuite de ses investissements au profit des inventaires O&O. Cependant, elle rappelle également que les Commitments de Google lui interdisent d'utiliser ses données 1st party en dehors de son inventaire O&O, ce qui est de nature à réduire les risques d'abus de position dominante



: Résumé

- Google considère qu'opérer la mesure via l'API Attribution Reporting n'aura qu'un impact limité sur les pratiques commerciales des acteurs de l'écosystème et qu'il n'a pas à nouer des contrats avec les utilisateurs des outils de la Privacy Sandbox
- En l'état actuel de la Privacy Sandbox, l'API Attribution Reporting n'empêche pas la ré-identification cross-sites des internautes si ses appelants décident d'en faire un usage malveillant. Cet usage sera suivi au travers du rapport annuel proposé par Google dans le cadre des activités de l'organe de gouvernance
- Avant toute utilisation, les appelants de l'Attribution Reporting API devront collecter le consentement de l'utilisateur pour l'accès et le stockage de données au sein de son navigateur



: API Attribution Reporting (ARA)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Les clés de contrôle, telles que la valeur d'épsilon et les taux limites d'usage de l'API Attribution Reporting, n'ont pas été testées	<ul style="list-style-type: none"> ICO : Sans tests préalables des clés de contrôle, il n'est pas possible d'identifier le bon compromis entre l'utilisabilité et la confidentialité. Qui plus est, le fait que l'API Attribution Reporting ne soit testable que par des acteurs ayant tout intérêt à privilégier son utilisabilité à la confidentialité des internautes pose problème 	<ul style="list-style-type: none"> CMA : Dans le cadre de l'organe de gouvernance proposé par Google, ce dernier suggère de suivre l'évolution des risques de tracking cross-sites au travers d'un rapport annuel. Ce rapport permettra d'évaluer la pertinence des précautions prises en matière de confidentialité 	<ul style="list-style-type: none"> L'organe de gouvernance proposé par Google doit être testé pour valider si son fonctionnement permet de résoudre cette inquiétude
Un produit de mesure permettant de relier des événements à un individu présentera toujours des risques de tracking cross-sites	<ul style="list-style-type: none"> CMA : La ré-identification des internautes est toujours possible, ce qui pourrait entrer en contradiction avec les préceptes de la RGPD Anglaise Google : La confidentialité des internautes est mieux préservée avec la Privacy Sandbox que sans, poursuivons dans cette direction 	<ul style="list-style-type: none"> CMA : Cette inquiétude ne peut être résolue tant que l'event-level reporting sera disponible, et dépendra de l'usage fait d'ARA par ses appelants. Le rapport annuel sur les risques de tracking cross-sites proposé par Google dans le cadre de la gouvernance qu'ils ont suggérée permettra de collecter des informations quant à cette inquiétude, et réagir en conséquence 	<ul style="list-style-type: none"> L'organe de gouvernance proposé par Google doit être testé pour valider si son fonctionnement permet de résoudre cette inquiétude



: API Attribution Reporting (ARA)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Le navigation tracking permettra de contourner les principales limites de l'API Attribution Reporting imposées aux événements de clic	<ul style="list-style-type: none"> CMA : La Privacy Sandbox ne limite pas la possibilité d'un tiers à opérer du fingerprinting ou du navigation tracking, et donc à traquer l'utilisateur cross-sites 	<ul style="list-style-type: none"> Google : Le navigation tracking n'est pas la technique de tracking cross-sites la plus prioritaire à adresser et complexe à bloquer. Nous n'allons pas non plus empêcher l'enrichissement des URLs lors des clics CMA : Pour nous, cette inquiétude est résolue 	<ul style="list-style-type: none"> N/A
Les documents publics partagés par Google quant à l'API Attribution Reporting ne permettent pas de savoir avec certitude si la collecte du consentement de l'utilisateur est requise au sens du PECR	<ul style="list-style-type: none"> ICO & CMA : Le stockage et l'accès à des informations servant d'autres besoins que des finalités essentielles devraient être soumis au consentement de l'utilisateur 	<ul style="list-style-type: none"> Google : Nous allons mettre à jour notre EU Consent Policy FAQ et notre Privacy Sandbox Privacy-related Compliance FAQ pour refléter l'obligation des appelants de l'API ARA à collecter le consentement de l'utilisateur avant tout appel CMA : Une fois les FAQs publiées, cette inquiétude pourra être résolue 	<ul style="list-style-type: none"> En attente de la publication des mises à jour des FAQs par Google
ARA ne prend pas en charge certains mécanismes d'attribution qui sont actuellement disponibles avec les cookies de tiers (ex: multi-touch attribution)	<ul style="list-style-type: none"> CMA : Le marché considère que la disparition du multi-touch attribution au profit du single-touch attribution avantage Google car celui-ci présente plus de chances d'être le last touch, et donc de tirer le plus de valeur de la conversion 	<ul style="list-style-type: none"> Google : L'attribution multi-touch n'est utilisée que rarement pour attribuer les conversions. La disparition du multi-touch affectera donc peu les éditeurs et les annonceurs. Il est tout de même possible de procéder à l'attribution multi-touch en combinant Shared Storage & Private Aggregation 	<ul style="list-style-type: none"> En attente de retours de la part de l'écosystème pour mesurer l'importance de l'attribution multi-touch pour l'industrie et de retours quant à la procédure pour procéder à cette mesure proposée par Google



: API Attribution Reporting (ARA)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Une mesure plus grossière (i.e. pas de tracking cross-sites en temps réel) peut rendre plus difficile pour les éditeurs l'évaluation de la valeur de leurs inventaires publicitaires	<ul style="list-style-type: none"> CMA : La réduction de l'accès aux données de tracking cross-sites en temps réel peut empêcher d'évaluer la valeur des inventaires publicitaires 	<ul style="list-style-type: none"> CMA : Les résultats des market testings mettent en évidence que sans cookies tiers la valorisation de l'inventaire publicitaire sera impactée, mais qu'avec ARA elle le sera moins que sans rien du tout. ARA n'a pas vocation à remplacer parfaitement les cookies tiers 	<ul style="list-style-type: none"> N/A
La proposition de « 20 événements minimum » par rapport semble arbitraire et compromet l'utilité de l'ARA	<ul style="list-style-type: none"> CMA : 20 semble une valeur raisonnable permettant une utilisation satisfaisante d'ARA 	<ul style="list-style-type: none"> Google : Il est désormais possible de modifier le nombre de contributions mesurées par rapport, et le nombre de contributions par défaut par rapport a été augmenté dans certains cas CMA : Toute évolution significative apportée au fonctionnement d'ARA et susceptible d'avoir un impact sur la confidentialité ou l'utilisabilité de l'API sera sujette à une validation de l'organe de gouvernance proposé par Google 	<ul style="list-style-type: none"> L'organe de gouvernance proposé par Google doit être testé pour valider si son fonctionnement permet de résoudre cette inquiétude
Les annonceurs sont actuellement en mesure d'ajuster leurs dépenses pour les campagnes publicitaires en temps réel. L'ARA impose des délais de reporting et pourrait entraîner un gaspillage de dépenses qui auraient pu être réaffectées	<ul style="list-style-type: none"> CMA : Il est maintenant possible de générer des rapports couvrant des périodes flexibles depuis ARA Marché : Il manque certains champs essentiels dans les rapports flexibles 	<ul style="list-style-type: none"> Google : Nous n'ajouterons pas les champs demandés (currency & OrderID) dans les rapports car les besoins associés sont couverts par l'event-level reporting en déduisant de la localisation de l'utilisateur sa devise CMA : ARA n'a pas vocation à remplacer parfaitement les cookies tiers. En l'absence de nouveaux éléments, nous considérons cette inquiétude comme résolue 	<ul style="list-style-type: none"> N/A



: API Attribution Reporting (ARA)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
ARA dégrade la mesure de l'Ad Serving Display en Open par rapport aux capacités de mesure des inventaires propriétaires (Owned & Operated), ce qui pourrait leur permettre d'attirer davantage de budgets	<ul style="list-style-type: none"> CMA : Nous avons conscience des impacts potentiels de la Privacy Sandbox sur les investissements en Open Display au profit des inventaires Owned & Operated. Nous allons y réfléchir avec Google 	<ul style="list-style-type: none"> CMA : Les Commitments de Google cantonnent son usage de ses données 1st party à son inventaire O&O. Google peut donc utiliser ses données 1st party pour opérer la mesure sur son inventaire O&O. Nous considérons cette inquiétude résolue d'autant qu'ARA améliore globalement la confidentialité des internautes, ce qui est une bonne chose. 	<ul style="list-style-type: none"> N/A
La mesure reposera à terme exclusivement sur ARA, ce qui présuppose la nécessité de pouvoir auditer et vérifier les résultats produits par l'API	<ul style="list-style-type: none"> Marché : ARA ne prévoit pas la possibilité de contrôler ses traces (logs), ce qui rend impossible la vérification de la mesure qu'elle permet d'opérer et que Google applique les traitements qu'il indique appliquer aux données collectées, ce qui peut nuire aux contrats commerciaux 	<ul style="list-style-type: none"> Google : Les acteurs de la mesure n'offrent pas plus de possibilité d'auditer leurs services de conversion, ni des traitements appliqués aux données. Il est tout de même possible de vérifier le fonctionnement des conversions opérées par ARA via les outils déjà disponibles. ARA n'est pas un service, et Google n'est pas co-responsable des traitements de données qui y sont opérés. Si contrat commercial il doit y avoir, alors il doit être passé entre l'éditeur ou l'annonceur et son fournisseur de services de mesure ou de vérification CMA : Les contraintes liées à ARA s'appliqueront de la même façon aux services publicitaires de Google. Nous considérons cette inquiétude résolue 	<ul style="list-style-type: none"> N/A



: API Attribution Reporting (ARA)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
L'approche de l'attribution proposée par Google étant différente de celles proposées par les autres navigateurs, cela limite l'interopérabilité d'ARA	<ul style="list-style-type: none"> CMA : Le manque d'interopérabilité pénalise le business des entreprises proposant des services de mesure à cause des coûts supplémentaires qu'elle entraîne, ce qui renforce la position de Google sur le marché publicitaire 	<ul style="list-style-type: none"> Google : Notre objectif reste de convenir d'un standard interopérable de mesure supporté par la majorité des navigateurs Web CMA : Trouver un consensus ne dépend pas uniquement de Google. En l'absence de nouveaux éléments, nous considérons cette inquiétude comme résolue 	<ul style="list-style-type: none"> N/A
La limite imposée par Google à 8 (2 ³) types de mécanismes de conversion au maximum pénalise les annonceurs ayant recours à davantage de mécanismes de conversion	<ul style="list-style-type: none"> CMA : Google devrait augmenter cette limite à 32. Google devrait également permettre d'attribuer une conversion à plus de 3 domaines 	<ul style="list-style-type: none"> Google : Nous avons augmenté cette limite à 32, mais plus il y a de types de mécanismes de conversion configurés, plus nous ajouterons du bruit dans les rapports issus d'ARA CMA : En l'absence de nouveaux éléments, nous considérons cette inquiétude comme résolue 	<ul style="list-style-type: none"> N/A
Il est nécessaire de laisser transiter un transaction ID entre les buy et sell sides pour assurer le reporting de l'attribution	<ul style="list-style-type: none"> CMA : Le transaction ID pourrait nuire à la confidentialité apportée par ARA 	<ul style="list-style-type: none"> Google : Nous ne soutiendrons pas l'ajout d'un transaction ID pour des raisons de confidentialité CMA : En l'absence de nouveaux éléments, nous considérons cette inquiétude comme résolue 	<ul style="list-style-type: none"> N/A
Les annonceurs pourraient vouloir revoir leurs contrats commerciaux à cause des changements liés à l'anonymisation de l'agrégation et de l'attribution	<ul style="list-style-type: none"> Marché : Google doit s'entretenir avec les annonceurs afin de comprendre s'ils sont enclins à être facturés sur la base de reporting agrégés et brouillés. L'ajout du bruit et de la latence apportée par ARA ont un impact sur la facturation au CPM ou au CPC 	<ul style="list-style-type: none"> Google : La facturation repose essentiellement sur les CPM et CPC, tous deux supportés par l'évent-level reporting de PAAPI. Les cookies 1st party ou ARA peuvent être utilisés pour le marketing d'affiliation. Les inquiétudes quant à la latence imposée par ARA pour la facturation au CPA sont résolues CMA : En l'absence de nouveaux éléments, nous considérons cette inquiétude comme résolue 	<ul style="list-style-type: none"> N/A



: API Attribution Reporting (ARA)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Les rapports agrégés d'ARA ne permettent pas de répondre à tous les cas d'usage du marché	<ul style="list-style-type: none"> • CMA : Google a proposé de rendre plus exploitables les rapports agrégés 	<ul style="list-style-type: none"> • CMA : Google n'a reçu aucun retour de l'écosystème concernant les problèmes posés par la présence de bruit dans les rapports. En l'absence de nouveaux éléments, nous considérons cette inquiétude comme résolue 	<ul style="list-style-type: none"> • N/A
L'ajout de bruit dans les rapports aura un impact important sur les petites Ad Techs	<ul style="list-style-type: none"> • Marché : La limite à 20 événements minimum par rapport peut rendre les rapports longs à obtenir pour les Ad Techs générant peu d'affichages publicitaires • CMA : Google indique que cette limite n'existe pas 	<ul style="list-style-type: none"> • CMA : En l'absence de nouveaux éléments, nous considérons cette inquiétude comme résolue 	<ul style="list-style-type: none"> • N/A
La conception actuelle d'ARA ne permet l'optimisation manuelle des campagnes	<ul style="list-style-type: none"> • Marché : Des rapports plus granulaires sont nécessaires pour optimiser manuellement les campagnes • CMA : Google a proposé un mode d'emploi d'ARA permettant de limiter l'impact du bruit sur les rapports, rendant ces derniers suffisamment exploitables pour répondre à tous les besoins formulés d'optimisation des campagnes 	<ul style="list-style-type: none"> • CMA : En l'absence de nouveaux éléments, nous considérons cette inquiétude comme résolue 	<ul style="list-style-type: none"> • N/A



4



Trusted Execution Environments

5 / 6 inquiétudes restantes

: Résumé

Les principaux aspects qui ressortent du rapport de la CMA concernant les Trusted Execution Environments (TEEs) sont les suivants :

- Les premières fonctionnalités basées sur des TEEs seront disponibles courant Q4 2024 avec des capacités limitées, et en leurs formes finales début 2025
- Google ne prévoit pas avant Q3 2025 l'entrée en vigueur de l'obligation de recourir aux TEEs pour traiter les données issues des APIs de la Privacy Sandbox
- La CMA et certains acteurs de l'écosystème s'accordent sur leurs inquiétudes quant à la viabilité des solutions basées sur les TEEs, surtout à grande échelle, par rapport aux coûts qu'ils impliquent. Certains acteurs considèrent que les TEEs doivent toujours faire leurs preuves



: Résumé

- Google encourage l'écosystème à tester au plus vite les services de la Privacy Sandbox hébergés sur des TEEs et à leur partager les résultats associés
- La CMA estime que l'organe de gouvernance de la Privacy Sandbox proposé par Google est le bon canal pour les Ad Tech pour faire valoir leurs demandes et inquiétudes au sujet des TEEs (calendrier trop court, rejet de candidature des cloud providers, roadmap et demandes d'évolution)
- Les Ad Tech recourant aux outils de la Privacy Sandbox restent responsables de leur propre conformité réglementaire en matière de protection des données personnelles



: Trusted Execution Environments (TEEs)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
L'adoption et la maintenance des TEEs requis pour faire fonctionner la Privacy Sandbox sont trop coûteuses et complexes à mettre en œuvre	<ul style="list-style-type: none"> CMA : Google doit aider l'écosystème à estimer les coûts de la mise en place des TEEs. Nous craignons que l'adoption des TEEs impliquera des coûts supplémentaires pour les Ad Tech en dehors de l'écosystème Google 	<ul style="list-style-type: none"> Google : Nous avons publié un playbook et une aide pour estimer les coûts du TEE K/V Server. Nous invitons l'écosystème à participer à notre programme bêta pour les K/V & B&A servers Marché : Remplacer nos infrastructures existantes par des TEEs représente des coûts supplémentaires et nous empêche d'amortir nos récents investissements en serveurs. Qui plus est, les TEEs ne représentent pas une technologie éprouvée à grande échelle CMA : L'évaluation globale des coûts et de la viabilité des solutions basées sur les TEEs est encore incertaine, en particulier à grande échelle, et lorsque l'on met en balance les coûts vs les bénéfices. De plus, les changements apportés à la roadmap prévue par Google pour imposer le recours obligatoire aux TEEs devraient être évalués par l'organe de gouvernance de la Privacy Sandbox proposé par Google 	<ul style="list-style-type: none"> Google : Les premières fonctionnalités basées sur des TEEs seront disponibles en test début 2025. Nous fournirons aux Ad Tech un préavis substantiel pour commencer les tests des serveurs K/V dans les TEEs avant d'en imposer le recours



: Trusted Execution Environments (TEEs)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Les TEEs requis pour faire fonctionner la Privacy Sandbox ne sont compatibles qu'avec la Google Cloud Platform et Amazon Web Services	<ul style="list-style-type: none"> • Google : Les TEEs ayant vocation à accéder aux données issues des API de la Privacy Sandbox doivent être sécurisés, privés, isolés, et auditables à distance. Nous nous assurerons du respect des standards industriels de sécurité du cloud par les TEEs. Nous onboarderons d'autres hébergeurs cloud • CMA : Google n'a pas l'intention d'onboarder d'autres fournisseurs de cloud publics d'ici la dépréciation des cookies tiers. Google a publié son protocole d'onboarding de nouveaux hébergeurs clouds 	<ul style="list-style-type: none"> • CMA : La candidature de Microsoft Azure afin de pouvoir accéder aux données de la Privacy Sandbox est toujours en cours de validation par Google. Nous ne sommes pas au fait de candidatures d'autres cloud providers. La procédure d'appel proposée par Google dans le cadre de la gouvernance qu'ils ont suggérée pourra vraisemblablement s'appliquer aux décisions de rejet des candidatures des fournisseurs de cloud 	<ul style="list-style-type: none"> • N/A



: Trusted Execution Environments (TEEs)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
<p>Google a limité le support de ses services server-side au cloud public (K/V server, etc) Les Ad Techs ne peuvent donc pas opérer de TEEs sur leurs infrastructures privées de cloud</p>	<ul style="list-style-type: none"> • Google : Nous réfléchissons à étendre la liste des solutions autorisées à traiter les données issues de la Privacy Sandbox, et à ouvrir l'utilisation de ces données à des solutions qui ne sont pas hébergées sur le cloud public • CMA : Le coût de l'adoption des TEE par les Ad Techs se répercutera sur les annonceurs et les éditeurs 	<ul style="list-style-type: none"> • Google : Nous recueillons les réactions de l'écosystème sur les aspects techniques et opérationnels de l'exploitation d'une infrastructure de traitement confidentielle dans des clouds privés. Nous recueillons également les commentaires sur les exigences techniques proposées pour le déploiement du TEE sur les clouds privés. A ce stade, nous ne pouvons garantir l'autorisation d'opérer des TEEs sur des infrastructures privées de cloud 	<ul style="list-style-type: none"> • Les Ad Tech souhaitant opérer des TEEs sur leurs infrastructures privées de cloud sont invitées à conduire et partager les résultats de leurs tests d'intégration à l'organe de gouvernance de façon à ce que les exigences de Google portant sur les TEEs soient ré-évaluées
<p>Google pourrait privilégier les requêtes de Google Ads à destination des TEEs hébergés sur leur plateforme cloud au détriment des requêtes des autres acteurs de l'écosystème</p>	<ul style="list-style-type: none"> • CMA : Le marché propose l'utilisation de TEEs open-source transparents et auditables. Google Ads pourrait bénéficier d'une efficacité accrue et de coûts plus bas par rapport à ses concurrents du fait de l'utilisation de la plateforme cloud de Google 	<ul style="list-style-type: none"> • CMA : Ce sujet n'entre pas dans le champ de l'enquête Privacy Sandbox de la CMA. La CMA n'exclut cependant pas d'enquêter sur cette question à l'avenir, notamment dans le cadre du Digital Markets, Competition and Consumer Act 2024 	<ul style="list-style-type: none"> • N/A



: Trusted Execution Environments (TEEs)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Dégradation de la performance et de la scalabilité due au recours imposé aux TEEs	<ul style="list-style-type: none">• Marché : Devoir recourir à des TEEs hébergés sur le cloud public lors de la conduite des enchères pose des problèmes de performance, et soulève la question de la scalabilité de ces TEEs le moment venu	<ul style="list-style-type: none">• Google : Les Ad Techs ne sont pas obligés d'attendre 2025 pour tester le service d'agrégation sur un TEE. Les tests sont disponibles depuis Octobre 2022 sur AWS et Novembre 2023 sur GCP. Le service Bidding & Auctions est ouvert aux tests depuis Novembre 2023, et le service K/V depuis Avril 2023. Tous ces services seront disponibles pour tout le monde courant Q4 2024. Le recours aux TEEs ne sera pas rendu obligatoire avant Q3 2025• CMA : Nous ne pensons cependant pas que tester les versions non-finalisées des services de la Privacy Sandbox réponde aux préoccupations soulevées, en particulier celles concernant les performances des opérations réalisées sur le terminal de l'utilisateur et le fait que ces services ne se seront pas disponibles en leurs formes finales avant début 2025	<ul style="list-style-type: none">• Google va poursuivre ses travaux avec les Ad Techs pour améliorer la scalabilité du service Bidding & Auctions



: Trusted Execution Environments (TEEs)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Google Chrome limite le périmètre de l'innovation via son implémentation des TEEs	<ul style="list-style-type: none">• Marché : Au lieu de nous forcer à utiliser les TEEs de Google, ce dernier devrait plutôt nous laisser implémenter nos composants comme nous l'entendons tout en respectant les critères qu'il aura définis concernant la confidentialité des données. Nous sommes bridés dans notre capacité à différencier nos services par rapport à ceux de Google• Google : L'ouverture souhaitée par le marché nous forcera à contrôler chaque solution, ainsi que les évolutions qui y seront apportées. Les mêmes limitations s'appliquent à Google Ads	<ul style="list-style-type: none">• CMA : Le fonctionnement de la Privacy Sandbox ne saurait être défini sans l'intervention de Google. Cependant, les parties prenantes pourront toujours soumettre pour révision leurs remarques par rapport à l'implémentation que Google fait des TEEs dans la Privacy Sandbox, ou proposer des implémentations alternatives	<ul style="list-style-type: none">• N/A



: Trusted Execution Environments (TEEs)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Calendrier des TEEs	<ul style="list-style-type: none">• Marché : Le calendrier d'imposition des TEEs proposé par Google n'est pas tenable. Qui plus est, pour être pertinents, les tests d'ARA doivent être conduits une fois que la Privacy Sandbox est disponible sur Android pour tester le cas d'usage de l'attribution cross-devices	<ul style="list-style-type: none">• Google : ARA sur Android est ouvert aux tests depuis Février 2023, et l'attribution app-to-web entre Android et Chrome depuis Mai 2023. Nous estimons que les délais de mise à disposition des API concernées sont suffisants• CMA : La durée nécessaire à l'écosystème pour ajuster son fonctionnement à celui de la Privacy Sandbox est différente pour chaque acteur. Il est donc difficile de proposer une durée de préavis qui satisfasse toutes les parties. L'organe de gouvernance proposé par Google sera le bon canal pour demander une extension des délais d'imposition des TEEs si besoin. Nous considérons cette inquiétude comme étant résolue	<ul style="list-style-type: none">• N/A



5



Related Website Sets

6 / 9 inquiétudes restantes

: Résumé

Les principaux aspects qui ressortent du rapport de la CMA concernant les Related Website Sets (RWS) sont les suivants :

- Les éditeurs se voyant refuser une demande de constitution de RWS peuvent à présent faire appel de cette décision
- En l'état, le but ainsi que les usages faits des RWS ne sont pas suffisamment explicites pour les internautes. Idem pour leurs contrôles sur les données des RWS. Google y travaille
- Il n'existe aucun processus permettant d'adresser les abus potentiels faits des RWS si ça n'est le rapport annuel sur les risques de tracking cross-sites proposé par Google



: Résumé

- Les restrictions imposées par Google via la mise en place des RWS peuvent pénaliser les éditeurs présentant une faible base d'utilisateurs logués et avantager Google. La CMA réfléchit à la nécessité de restreindre davantage le recours de Google à ses données 1st party
- De la même façon qu'ils l'ont toujours été avec les cookies tiers, les éditeurs sont responsables de la collecte du consentement de l'utilisateur pour stocker et lire les cookies sur son terminal, ainsi que l'informer des objectifs des traitements liés aux RWS



: Related Website Sets (RWS)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Les raisons pour lesquelles les éditeurs constituent des sets ne sont pas correctement renseignées	<ul style="list-style-type: none"> • CMA : Les éditeurs peuvent outrepasser les cas prévus par Google pour la création de RWS, ce qui nuit à la transparence vis-à-vis des utilisateurs 	<ul style="list-style-type: none"> • Google : Les déclarants doivent choisir un motif de constitution des RWS dans une liste prédéfinie de motifs. Les retours sont bienvenus • CMA : Les propriétaires de RWS doivent collecter le consentement de l'utilisateur pour stocker et lire les cookies sur son terminal, ainsi que l'informer des objectifs des traitements liés 	<ul style="list-style-type: none"> • En attente des discussions entre la CMA et Google au sujet de la validation de la liste des motifs disponibles
Les raisons pour lesquelles les domaines constituant un RWS s'échangent des données ne sont pas partagées aux internautes de manière explicite	<ul style="list-style-type: none"> • CMA & ICO : L'interface de Google Chrome ne donne aucune information aux internautes leur permettant de comprendre pourquoi certains sites peuvent s'échanger leurs données 	<ul style="list-style-type: none"> • CMA : La liste des motifs renseignés par les éditeurs pour la création de RWS apparaît plus clairement sur l'interface de gestion des RWS des internautes, ce qui améliore la transparence 	<ul style="list-style-type: none"> • En attente des discussions entre la CMA et Google
Les abus d'utilisation des RWS à large échelle par les éditeurs ne seront pas traités	<ul style="list-style-type: none"> • CMA & ICO : Il n'existe aucune démarche ni gouvernance permettant d'adresser les abus d'utilisation des RWS • Google : Nous considérons que le design même des RWS en l'état limite les mauvais usages qui peuvent en être faits 	<ul style="list-style-type: none"> • CMA : Cette inquiétude n'est pas résolue et dépendra de l'usage fait des RWS par les éditeurs. Le rapport annuel sur les risques de tracking cross-sites proposé par Google dans le cadre de la gouvernance qu'ils ont suggérée permettra de collecter des informations quant à cette inquiétude, et réagir en conséquence. Si l'organe de gouvernance fonctionne correctement, alors cette inquiétude sera résolue 	<ul style="list-style-type: none"> • N/A



: Related Website Sets (RWS)

Sujet	Position Q1 2024	Position Q3 2024	Prochaines étapes
Le processus de validation des RWS opéré par Google peut être sujet à des décisions arbitraires de sa part	<ul style="list-style-type: none"> CMA : La nécessité de l'intervention humaine lors de la validation des demandes de constitution des RWS crée un risque de décision arbitraire. Les candidats aux RWS ne peuvent faire appel de la décision de Google 	<ul style="list-style-type: none"> Google : La validation des demandes de constitution des RWS va être automatisée. Nous suggérons, dans le cadre de l'organe de gouvernance proposé, la mise en place d'un processus indépendant pour faire appel CMA : Si cet organe fonctionne correctement, alors cette inquiétude sera résolue 	<ul style="list-style-type: none"> N/A
Le partage de données cross-sites entre sites faisant partie d'un RWS n'est limité qu'aux 5 premiers domaines déclarés dans le RWS	<ul style="list-style-type: none"> CMA : La limite de 5 permet de réduire le risque d'abus de partage de données inter-domaines comparé aux cookies tiers. Le marché souhaite étendre cette limite et partager les données RWS avec des tiers partis 	<ul style="list-style-type: none"> CMA : Nous considérons cette inquiétude comme étant résolue. Si le marché souhaite améliorer l'utilisabilité de RWS, il doit soumettre ses demandes à l'organe de gouvernance proposé par Google pour validation 	<ul style="list-style-type: none"> N/A
Les éditeurs présentant une importante base d'utilisateurs logués seront moins impactés par les restrictions imposées aux RWS que les éditeurs n'en présentant pas (i.e pour la constitution de segments d'audience 1st party)	<ul style="list-style-type: none"> CMA : Nous comprenons ces inquiétudes que nous considérons avérées et échangeons avec Google sur ce point 	<ul style="list-style-type: none"> CMA : Nous nous interrogeons sur la nécessité de restreindre davantage l'utilisation par Google de ses données 1st party concernant l'activité des utilisateurs sur des sites autres que ceux de l'éditeur et de l'annonceur concernés 	<ul style="list-style-type: none"> En attente des discussions entre la CMA et Google



: Related Website Sets (RWS)

Sujet	Position Q3 2024	Prochaines étapes
Les utilisateurs ne comprennent pas suffisamment l'objectif et le champ d'application du RWS	<ul style="list-style-type: none">• CMA & ICO : La maîtrise limitée des concepts associés aux cookies tiers par les internautes compromet leur capacité à exercer un contrôle sur les paramètres RWS. Les études utilisateur conduites par Google démontrent une compréhension lacunaire des motifs de constitution des RWS	<ul style="list-style-type: none">• Google va rendre la liste des motifs de constitution des RWS plus compréhensible pour les utilisateurs
Le parcours de l'utilisateur pour savoir quels sites font partie d'un RWS n'est pas toujours intuitif	<ul style="list-style-type: none">• CMA & ICO : Le parcours de l'utilisateur pour savoir quels sites font partie d'un RWS (via ses paramètres Chrome ou la barre de recherche) n'est pas intuitif. La transparence de cette information est primordiale pour nous• Google : Nous sommes en train de reconcevoir l'accès des utilisateurs à cette information	<ul style="list-style-type: none">• En attente des résultats du nouveau parcours utilisateur imaginé par Google
Il n'est pas toujours intuitif pour les utilisateurs de comprendre comment effacer des données pour des RWS spécifiques	<ul style="list-style-type: none">• CMA : La suppression des données RWS à partir du bouton à côté de la barre de recherches n'est pas intuitif pour l'utilisateur, ce qui compromet sa capacité à faire ce qu'il veut• Google : Nous sommes en train de reconcevoir la page des paramètres Chrome pour répondre à cette inquiétude	<ul style="list-style-type: none">• En attente des résultats du nouveau parcours utilisateur imaginé par Google



6



Fenced Frames

0 / 4 inquiétudes restantes

: Résumé

Les principaux aspects qui ressortent du rapport de la CMA concernant les Fenced Frames sont les suivants :

- **Afficher les publicités au sein de Fenced Frames dans le contexte d'utilisation de PA-API ne sera pas rendu obligatoire avant 2026**
- **En l'état, les Fenced Frames ne sont pas compatibles avec les formats Native, Vidéo. Google ne prévoit pas de rendre compatible les Expandable Ads avec les Fenced Frames pour des raisons de confidentialité**
- **En l'état, le recours aux Fenced Frames n'empêche pas le tracking cross-sites mais Google y travaille sans pouvoir communiquer de timeline associée. Le bon fonctionnement de l'organe de gouvernance proposé par Google est de nature à permettre de résoudre cette inquiétude**
- **Les Fenced Frames ne constituent pas un frein à la Brand Safety contrairement à ce que certains acteurs ont évoqué**





Merci !

contact@alliancedigitale.org
<https://www.alliancedigitale.org>
97 Bd Malesherbes, 75008 Paris



@Alliance_Dgtle



@Alliance Digitale