GUIDE

Pourquoi l'identification échoue :

La vérité sur les Cookies « First Party »

celebrus

La plupart des CDP utilisent des Cookies pseudo « first party » - et c'est pourquoi l'identification échoue.

Principaux enseignements

- Comprendre les cookies pseudo « first party »
- Comment ces cookies pseudo « first party » impactent le marketing et la publicité
- La solution aux cookies pseudo « first party », aux restrictions de suivi et aux bloqueurs de cookies
- Pourquoi les cookies « first party » sont la clé d'une identification efficace
- Pourquoi Celebrus est la seule véritable solution de capture de données « first party »

Introduction

Les cookies sont de petits fichiers de données créés par un serveur Web pendant qu'un utilisateur navigue en ligne. Les cookies sont déposés sur l'appareil utilisé pour accéder à un site Web ou à une application mobile, et plusieurs cookies peuvent être déposés par le navigateur sur l'appareil d'un utilisateur pendant une session.

Les cookies sont déposés par de nombreuses applications logicielles, y compris celles qui capturent des données d'interaction et de comportement. Bien que l'essentiel du battage médiatique concerne les technologies publicitaires et les DMP qui reposent sur des cookies tiers, les restrictions croissantes perturbent tout autant la construction et la persistance de l'identité des clients. Les CDP, l'analyse du parcours client et les outils de Web Analytics utilisent tous des cookies pour suivre les interactions des clients et aider à identifier les visiteurs qui ne sont pas encore connectés ou authentifiés.

Mais la façon dont leur infrastructure de capture de données est déployée et accédée par leurs clients les rendent vulnérables aux bloqueurs de cookies, aux restrictions de suivi et à la fraude potentielle.

Que sont les cookies pseudo « first party » ?

Également appelés cookies fantômes ou cookies externes, les cookies pseudo « first party » sont considérablement affectés par le rejet des cookies et les restrictions telles que l'ITP.

Comme le définit cet article commun de la North Carolina State University et de la Stony Book University : « Les pseudo cookies « first party » sont ceux qui sont définis par un code tiers... » et « Si le destinataire du cookie n'est pas le même que l'auteur, ce n'est pas un vrai cookie « first party ». »

Bien qu'il soit courant pour les fournisseurs de CDP et de Marketing Cloud de définir des cookies tiers à l'aide de CNAME pour les faire paraître comme « first party », pour contourner la technologie inhibant les cookies telle qu'Apple ITP, cela reste une échappatoire. Avec cette solution de contournement, les fournisseurs tiers placent un code sur votre page à l'aide de JavaScript (JS) pour définir un CNAME qui masque la balise JS pour donner l'impression qu'elle se trouve sur votre domaine. Il est important de noter que ce n'est pas le CNAME qui pose problème – Le problème c'est de cacher le caractère tiers derrière une étiquette first-party. C'est une solution médiocre.

Représentez-le-vous ainsi : quand une solution de tierce partie met du code sur vos pages, vous pouvez

avoir l'impression de tout contrôler, mais finalement, peu importe comment vous l'avez architecturée, elle doit se connecter ailleurs. Cela commence sur votre domaine et cela abouti invariablement sur l'application de votre fournisseur.

Apple a depuis comblé cette faille, et les navigateurs axés sur la confidentialité tels que DuckDuckGo et Brave sont des options bien connues pour bloquer les trackers publicitaires et les requêtes CNAME. Bien que l'accent soit actuellement mis sur le bloqueur de cookies tiers de Google, il est fort probable que ces cookies pseudo first-party seront la prochaine cible des initiatives de protection de la vie privée dans le monde entier.

L'ITP (Intelligent Tracking Prevention) d'Apple est le bloqueur le plus connu. Conçu pour empêcher les annonceurs de suivre à leur insu et sans leur consentement les clients qui cliquent sur leurs annonces, il empêche désormais également les cookies « first party » d'être définis côté client via JavaScript, limitant leur durée de vie à 7 jours. Pourquoi ? Parce qu'ils considèrent ce type de cookie comme tiers puisqu'ils communiquent avec un serveur externe. Bien que conçu pour cibler le monde de la publicité, cela a également un impact sur les systèmes de capture de données tiers, y compris de nombreux grands noms de MarTech qui utilisent des cookies définis de cette manière pour reconnaître et capturer les données et les préférences des visiteurs anonymes pour créer un profil d'identité. En fait, presque tous les fournisseurs de solutions CDP et Marketing Cloud définissent des cookies qui sont considérés comme tiers par des navigateurs tels que Safari.

Étant donné que la plupart des navigateurs bloquent désormais complètement les cookies tiers ou les suppriment après une courte période, les solutions de capture de données traditionnelles ne peuvent pas identifier un client anonyme qui revient. Les restrictions du suivi empêchent les fournisseurs de CDP, d'analyse et de capture de données de personnaliser les interactions pour les visiteurs anonymes qui reviennent sur un site après plus de 7 jours. Toutes les données de navigations précédentes sont perdues et il est impossible de relier ces sessions à une seule identité complète.

Les spécialistes du marketing savent qu'une personnalisation efficace en temps réel entraîne une augmentation substantielle des ventes et des conversions, mais des dispositifs tels que l'ITP et la perte de personnalisation qui en résulte sapent la croissance des revenus et rebutent les clients qui reviennent et qui s'attendent à ce que vous les reconnaissiez !

Qu'est-ce que cela signifie pour le marketing et la publicité ?

Avec la perte de données de valeur due aux restrictions du suivi, beaucoup moins de données analytiques sont disponibles pour l'organisation. Moins de données signifie moins de décisions éclairées et une perte de personnalisation en temps réel. Sans personnalisation en temps réel, l'expérience client devient moins pertinente et des indicateurs tels que la conversion, le coût d'acquisition et le retour sur investissement en sont impactés significativement.

Les fournisseurs qui utilisent une technique de masquage des cookies pour capturer des données (CNAME pour configurer le JS pour définir des cookies) n'ont aucun moyen d'assurer une visibilité complète du comportement des clients, sont incapables de créer des profils d'identité complets et ne peuvent pas adresser avec précision et fiabilité les problématiques d'attribution.

L'utilisation de CNAME est également intrinsèquement risquée car elle expose les consommateurs à la fraude, en effet les sous-domaines créés dans le cadre du processus CNAME sont vulnérables aux attaques s'ils ne sont pas gérés correctement.

Alors que les fournisseurs et les clients de l'industrie

MarTech et AdTech cherchent désespérément une solution de contournement, la réalité est que les gouvernements et les fournisseurs de navigateurs sont déterminés à rendre la prévention du suivi absolue... C'est une situation sans issue.

La majorité des solutions MarTech et AdTech sur le marché ne seront jamais à l'abri de la mort des cookies tiers, car leur modèle commercial consiste à capturer des données à partir d'un emplacement distant et centralisé. Si vous utilisez des solutions de l'un de ces fournisseurs, vous ne pourrez jamais exécuter la technologie sur votre propre infrastructure « first party ».

Non seulement les configurations MarTech nécessitent des compromis de sécurité risqués, mais la définition d'un cookie de première partie via JS nécessite du code et doit être correctement implémenté – ce qui est rarement le cas. Il faut que la configuration du client, le paramétrage réseau, etc. fonctionnent ensemble. En cas d'échec, par défaut le cookie est automatiquement défini comme tiers et immédiatement bloqué.

Lorsque vous essayez d'adapter votre offre à un individu, de faire évoluer votre publicité ou de déclencher une campagne marketing sur la base d'évènements, vous DEVEZ connaître votre public. Un graphique d'identité complet est le meilleur moyen de savoir qui est quelqu'un lorsqu'il arrive sur le site de manière anonyme, et de rappeler et réconcilier instantanément cette personne et ce profil lorsqu'ils s'authentifient afin que vous puissiez personnaliser leur expérience. Vous ne pouvez pas le faire si vous perdez cette connaissance tous les quelques jours.

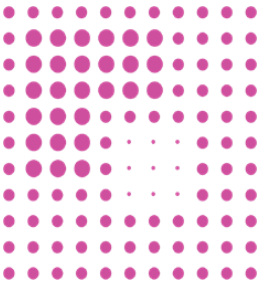
La réalité est qu'il n'y a pas de solution de contournement aux dispositifs contre les cookies tiers et le tracking. Pour garantir qu'une capture de données précise, conforme et à l'épreuve du temps alimente des profils d'identité complets, les organisations doivent abandonner les méthodologies de suivi par des tiers et les technologies MarTech qui utilisent des solutions de contournement pour la capture des données et le tracking.

Quelle est la solution ?

La seule façon pour les organisations de maintenir une vision complète de leurs interactions avec les clients et une compréhension précise de l'attribution est de gérer et d'orchestrer cela via un système véritablement « first party » – une solution installée au sein des environnements contrôlés par le client, qui utilise des cookies propriétaires légitimes et qui n'est pas affecté par ITP et d'autres restrictions de navigateur. Cette solution réside à l'intérieur du pare-feu, dans des centres de données sur site ou dans des infrastructures de cloud privé sécurisées, et les données ne sont jamais envoyées à l'extérieur.

Les organisations doivent s'assurer que pour définir les cookies de captures de données et d'identification des clients, elles n'utilisent que des solutions véritablement « first party ». Pour qu'une solution soit légitimement « first party » (plutôt que d'essayer de se faire passer pour telle via l'une des solutions de contournement discutées), toute la technologie et l'infrastructure de capture et de stockage de données doivent être entièrement détenues et exclusivement gérées par votre organisation. Elles doivent être contrôlées et exploitées par le propriétaire du canal digital à partir duquel la collecte a lieu.

Pour réussir dans un monde post cookies tiers et offrir une personnalisation en temps réel, les organisations doivent éviter les solutions de contournement alambiquées telles que les redirections CNAME ou les modifications d'infrastructure impliquant la communication avec un serveur externe. Les investissements considérables et les perturbations causés par ces approches ne valent pas les résultats limités et incertains qu'elles permettent. Les fournisseurs de navigateurs sont tout aussi déterminés à faire respecter leurs restrictions que le Martech à les contourner.



Pourquoi Celebrus est la seule solution vraiment « first party » de capture de données, non affectée par les restrictions de suivi

Celebrus est une solution « first party » installée dans l'environnement sous contrôle de ses clients, 100% non affectée par ITP. Notre bibliothèque JS va directement sur les pages (ou SDK dans les applications mobiles) et ne définit pas d'identité ou de cookies, elle active simplement le suivi. Les cookies sont définis côté serveur dans le cadre de la communication entre le site web de nos clients et leur instance privée de Celebrus.

Les identifiants Celebrus n'expirent jamais. Ils persistent sur cet appareil pour chaque session et chaque visite, avec une continuité inter-domaines. Chaque ID est mappé dans le graphe d'identité, avec la possibilité d'ajouter d'autres identifiants à ce graphe à chaque étape du parcours. Au fur et à mesure que les identifiants sont ajoutés et appariés, Celebrus les réconcilie instantanément afin que vous vous retrouviez avec un profil individuel construit au fil du temps et pouvant avoir de nombreux identifiants tous connectés au sein d'un même graphe d'identité. Celebrus se souvient de cette personne et de ce profil en temps réel pour l'hyperpersonnalisation, le re-ciblage, la satisfaction client et bien plus encore.

Celebrus est la seule solution pour une identité VERITABLEMENT « first party ». Alors que d'autres solutions prétendent définir des cookies propriétaires, elles présentent trois défauts majeurs :

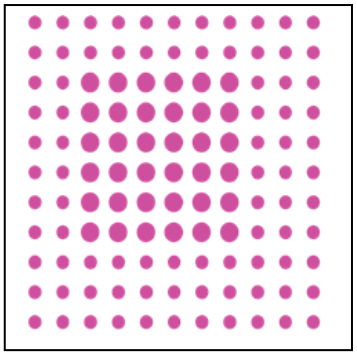
1. Elles ne peuvent pas conserver les identifiants au fil du temps, de sorte que l'identité est massivement fragmentée avec plusieurs photos du même client. Ce ne sera jamais exact et vous ne pourrez jamais les réconcilier en une seule identité.

2. Il n'y a pas de suivi cross-canal, cross-device ou cross-domain - ce qui signifie qu'il n'y a jamais de vision holistique d'un individu.

3. Les identifiants doivent être rapprochés avec l'ID du fournisseur, ce qui signifie qu'ils ne font rien en temps réel et que vous vous retrouvez avec plusieurs ID pour une même personne.

Comme l'a si bien dit un grand client bancaire mondial : « Vous ne pouvez pas avoir une vision client avec l'analyse Web. » Les autres CDP sont des solutions orientées session – Celebrus est une solution orientée client.

Celebrus vous permet d'identifier vos clients facilement et en toute conformité, quel que soit l'appareil, le canal ou le navigateur qu'ils utilisent. Que vos clients se soient connectés ou non, qu'ils reviennent sur votre site Web après 7 jours ou 7 semaines, Celebrus résout le problème de l'identité afin que vous puissiez maximiser vos investissements marketing.



Boostez votre expérience client avec Celebrus

De nombreuses entreprises à travers le monde utilisent Celebrus de D4t4 Solutions comme partie intégrante de leur infrastructure CX orientée données en raison de la facilité de déploiement de la solution – une seule ligne de code pour être exact. Celebrus se concentre à 100% sur la capture de données, innove constamment et garde une longueur d'avance. Les données capturées par Celebrus sont conformes aux réglementations en matière de confidentialité, y compris RGPD, CCPA et plus encore, offrant ainsi une tranquillité d'esprit aux entreprises mondiales. Les gains de nos clients atteignent souvent des centaines de millions d'Euros en raison de la fourniture d'expériences client hautement personnalisées à grande échelle.

Celebrus a été la première solution de capture de données à combiner l'apprentissage automatique avancé (ML) avec le traitement du langage naturel (NLP) et la capture de données en temps réel. Ces technologies permettent aux entreprises clientes d'avoir une visibilité totale du comportement des clients, ce qui leur permet d'obtenir un aperçu puissant de l'intention du client. Ces institutions pionnières offrent une personnalisation authentique et individuelle, dans l'instant. Grâce à des fonctionnalités d'apprentissage automatique prêtes à l'emploi, Celebrus élimine les maux de tête et les coûts de configuration généralement associés à la capture de signaux comportementaux. Offrant des capacités brevetées, telles que la continuité inter-domaines et CX Vault, Celebrus offre des avantages exceptionnels aux organisations de premier plan qui souhaitent sérieusement offrir des expériences client de classe mondiale en faisant passer les activités marketing de réactives à « dans le moment ».

Prêt à voir comment une véritable solution « first-party » de capture de données peut résoudre les défis de l'identification ?

PRENEZ CONTACT MAINTENANT