GUIDE

Why identity fails:

The truth about first-party cookies

celebrus

Most CDPs use fake first-party cookies - and that's why identity is failing.

Key takeaways

- Understanding fake first-party cookies
- How fake first-party cookies impact marketing and advertising
- The solution to fake first-party cookies, tracking restrictions, and cookie blockers
- Why first-party cookies are the key to identity
- Why Celebrus is the only true first-party data capture solution

Introduction

Cookies are small blocks of data created by a web server while a user is browsing online. Cookies are placed on the device used to access a website or mobile application, and more than one cookie may be placed by the browser on a user's device during a session.

Cookies are set by many software applications, including those which capture interaction and behavioral data. Although most of the hype is around AdTech and DMPs which rely on third-party cookies, growing restrictions are just as disruptive to building and persisting customer identity. CDPs, Customer Journey Analytics, and Web Analytics tools all set cookies to track customer interactions and help identify visitors who aren't yet logged in or authenticated. But the way their data capture infrastructure is deployed and accessed by their clients makes them vulnerable to cookie blockers, tracking prevention, and potential fraud.

What are fake first-party cookies?

Also referred to as ghost cookies or external cookies, fake first-party cookies are drastically affected by cookie deprecation and restrictions like ITP.

As this combined paper from North Carolina State University and Stony Book University defines it: "Fake first-party cookies are those which are set by third-party code…" and "If the recipient of the cookie isn't the same as the originator, it's not a true first-party cookie."

While it's common practice for CDP and Marketing Cloud vendors to set third-party cookies using CNAME to mask them as first-party, often as a workaround to cookie-inhibiting technology such as Apple ITP, it's a loophole. With this workaround, third-party vendors put a code on your page using JavaScript (JS) to set a CNAME which masks the JS tag to make it look like it's on your domain. It's important to note, the CNAME isn't the issue here – masking the third-party tag as first-party is. It's a subpar solution.

Think of it like this: When a 3rd party solution puts code on your pages you may feel like you control it, but eventually, no matter how you architect it, it must go to another location. It starts on your domain and

eventually gets sent to your vendor's application.

Apple has since closed this loophole, and privacy-focused browsers such as DuckDuckGo and Brave are well-known options for blocking advertising trackers and CNAME requests. Although the current focus is on Google's impending third-party cookie blocker, it's highly likely these fake first-party cookies will be the next target for privacy-first initiatives worldwide.

Apple's ITP (Intelligent Tracking Prevention) is the most widely known blocker. Designed to prevent advertisers from tracking customers who click on their ads without their knowledge and consent, it now also restricts first-party cookies from being set client-side via JavaScript, limiting their life to 7 days. Why? Because they regard this type of cookie as third-party since it communicates with an external server. Although designed to target the advertising world, this also impacts third-party data capture systems, including many of the leading names in MarTech who use cookies set in this way to recognize and capture the data and preferences of anonymous visitors to build an identity profile. In fact, almost all CDP and Marketing Cloud solution vendors set cookies that are deemed to be third-party by browsers such as Safari.

Since most browsers now either block third-party cookies entirely or delete them after a short period of time, traditional data capture solutions can't identify a returning, anonymous customer. Tracking prevention stops CDP, analytics, and data capture vendors from personalizing interactions for anonymous visitors who return to a site after more than 7 days. All the previous browsing data is lost, and it's impossible to stitch these sessions into a single, comprehensive identity.

Marketers know that effective, real-time personalization leads to substantial increases in sales and conversions, but restrictions like ITP, and the resulting loss of personalization, undermines revenue growth and alienates returning customers who expect you to recognize them!

What does this mean for marketing and advertising?

The loss of valuable data due to tracking prevention results in far less analytics data being available to the organization. Less data means less informed decisions, and loss of real-time personalization. Without real-time personalization the customer experience becomes less relevant and metrics such as conversion, acquisition cost, and ROI take a huge hit.

Vendors who use a cookie masking technique to capture data (CNAME to set JS to set cookies) have no way to ensure complete visibility of customer behavior, are unable to build comprehensive identity profiles, and can't accurately determine attribution from advertising.

The use of CNAME is also inherently risky as it leaves consumers open to fraud since the subdomains created as part of the CNAME process are vulnerable to attack if not managed properly.

While MarTech and AdTech industry vendors and clients desperately search for another work-around, the reality is governments and browser vendors are determined to make tracking prevention airtight… it's a no-win situation.

The majority of MarTech and AdTech solutions on the market will never be immune from third-party cookie death because their business model is to capture data from a remote, centralized location. If you're using solutions from one of these vendors, you'll never be able to run the technology on your own, first-party infrastructure.

Not only do MarTech configurations require risky security compromises, setting a first-party cookie via JS requires code and it must be implemented properly – which it rarely is. It requires client configuration, networking, etc. to all work in tandem. When it fails, it automatically defaults to set a third-party cookie and gets blocked immediately.

When you're trying to market to an individual, update your advertising, or trigger a marketing campaign, you MUST know your audience. A comprehensive identity graph is the best way to know who someone is when they arrive on the site anonymously, and to recall and reconcile that person and profile instantly when they log in so you can personalize their experience. You can't do this if you lose the insights every few days.

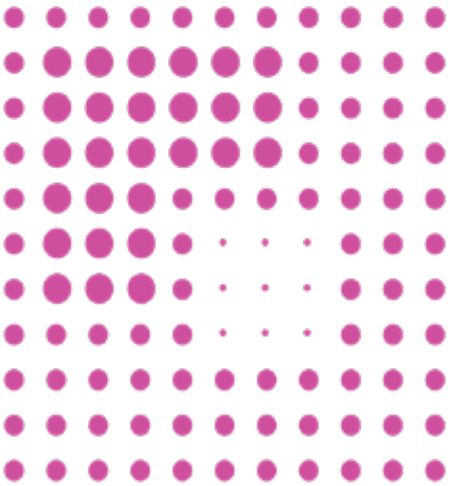
The reality is there's no workaround to third-party cookies and tracking prevention. To ensure accurate, compliant, future-proof data capture that feeds complete identity profiles, organizations must transition away from third-party tracking methodologies and MarTech solutions that use indirect data capture and tracking workarounds.

What's the solution?

The only way organizations can maintain complete visibility of their customer interactions and an accurate understanding of attribution is to manage and orchestrate this through a true first-party system – a solution installed within the clients' controlled environment that uses legitimate first-party cookies and is unaffected by ITP and other browser restrictions. This solution lives inside the firewall, in on-premises data centers, or in secure private cloud infrastructures - and the data is never sent to an external location.

Organizations must ensure they only use real first-party data capture and customer tracking solutions to set cookies for all data capture and customer identification. For a solution to be legitimately first-party (rather than trying to pass itself off as first-party via one of the workarounds discussed), all the data capture and data storage technology and infrastructure needs to be fully owned and exclusively managed by your organization. It needs to be controlled and operated by the owner of the digital channel from which collection is taking place.

To succeed in a post third-party cookie world and deliver real-time personalization, organizations must avoid convoluted workarounds like CNAME redirects or infrastructure changes that involve communicating with an external server. The considerable investment and disruption caused by these approaches isn't worth the limited and uncertain rewards. As determined as MarTech is to overcome browser restrictions, browser vendors are equally determined to make their restrictions stick.



Why Celebrus is the only true first-party data capture solution, unaffected by tracking restrictions

Celebrus is a first- party solution installed within the clients' controlled environment, 100% unaffected by ITP. Our JS library goes directly on the pages (or SDK in mobile apps) and doesn't set identity or cookies, it simply enables the tracking. Cookies are set server-side as part of the communication between the client's website and their private instance of Celebrus.

Celebrus identifiers never expire. They persist on that device for every session and every visit, with cross-domain continuance. Every ID is mapped in the identity graph, with opportunities to add more identifiers to the graph at every step of the journey. As identifiers are added and matched, Celebrus reconciles them instantly so you end up with an individual profile built over time that may have many identifiers all connected within a single identity graph. Celebrus recalls that person and profile in real-time for hyper-personalization, retargeting, customer success, and so much more.

Celebrus is the only solution for REAL first-party identity. While other solutions claim to set first-party cookies, they have three major flaws:

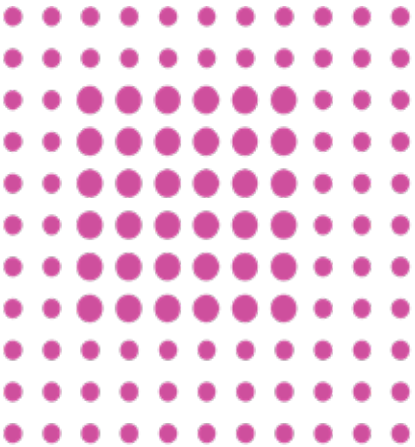
1. They can't persist identifiers over time, so the identity gets massively fragmented with multiple pictures of the same customer. It will never be accurate, and you can never reconcile them into a single identity.

2. There's no cross-channel, cross-device, or cross-domain tracking – which means there's never a wholistic view of an individual.

3. The identifiers have to route to the vendor's ID, which means they do nothing in real-time and you end up with multiple IDs for one person.

As a large global banking client so accurately put it: "You can't do customer with web analytics." Other CDPs are session solutions – Celebrus is a customer solution.

Celebrus empowers you to identify your customers easily and compliantly - no matter the device, channel, or browser they're using. Regardless of whether your customers have logged in, whether they're returning to your website after 7 days or 7 weeks, Celebrus solves the identity challenge so that you can maximize your marketing investments.



Supercharge your CX with Celebrus

Many enterprise organizations around the world use Celebrus from D4t4 Solutions as an integral part of their data driven CX infrastructure because of how easy the solution is to deploy – a single line of code to be exact. Celebrus is 100% laser-focused on data capture and is constantly innovating and staying ahead of the curve. Data captured by Celebrus satisfies privacy regulations including GDPR, CCPA, and more, providing peace of mind across global businesses. Client revenues often run into the hundreds of millions of dollars as a result of delivering highly personalized customer experiences at scale.

Celebrus was the first data capture solution to combine advanced machine learning (ML) with natural language processing (NLP) and real-time data capture. These technologies enable enterprise clients to have total visibility of customer behavior, arming them with powerful insight into customer intent. These pioneering institutions deliver genuine, individual level personalization, in-the-moment. With out-of-the-box machine learning features, Celebrus removes the configuration headaches and costs typically associated with capturing behavioral signals. Offering patented capabilities, like cross-domain continuance and CX Vault, Celebrus delivers outstanding benefits for leading organizations that are serious about providing world-class customer experiences by shifting marketing activities from reactive to 'in-the-moment'.

Ready to see how a genuine first-party data capture solution can solve YOUR identity challenges?

CONNECT NOW