PERSOSA

Closing the Consumer Experience Gap with connected journeys.

NEW VISITOR, WHO 'DIS?

HOW COMPANIES NEED TO OWN THEIR CONSUMER DATA IN A HUMAN PRIVACY-FOCUSED WAY

Modern day consumers interact with technology at every turn. At Persosa, we have a vision of what a *connected consumer experience* would look like throughout a single day with our platform, compared to how we currently interact with media and technology.

Research shows that over half of our days are consumed by media intake. The reality is that much of that activity involves creepy ads that follow us around the internet, fueled by large companies capturing as much data as possible about us. Unfortunately, these companies aren't using that data to deliver value to the consumer.

Platforms such as Facebook, Google, and online retailers gather data around all of our actions and use it to predict what we want, how we feel and what we're going to do next without us actively consenting to that level of data collection. Let's look at that underlying data and how it is being impacted by changes in user privacy and regulations.

THE DEMAND FOR MORE HUMANE TECHNOLOGY

As technology evolves, the type of data we collect and how it can be used becomes more advanced. In many ways, the data creates better consumer experiences. This is seen in more personalized ads and content recommendations. But as time goes on, we're seeing some of the reasons for concern when platforms are able to gather and manipulate data without user knowledge or regulatory oversight.

As a result, users and creators alike are calling for technology platforms to evaluate how they collect and use data. There has also been a growing call from within the industry itself for a change to more humane technology as seen in the 2020 documentary, *The Social Dilemma*.

During the documentary, experts explain how these platforms are designed to engage and keep people interacting with their content. This constant state of engagement allows them to sell advertising with certainty about their ability to deliver ads, which requires greater predictions. This is done by tracking user data and recommending similar content.

This predictive cycle of feeding content to continue engagement is referred to in the documentary as "surveillance capitalism." This type of business model effectively trades in human attention and actions, fueled by more and more user data.

Technology has developed an "opt-out" culture as a solution to user privacy, which puts the burden on the user to understand how to turn off the data capture. This creates friction because it incentivizes brands to be less transparent about how they capture and use data.

These growing concerns are why, over the last couple of decades, we've seen more calls for improved user privacy and regulations around how businesses can collect, store and use data. Some of the major responses to these growing concerns include:

General Data Protection Regulation (GDPR)

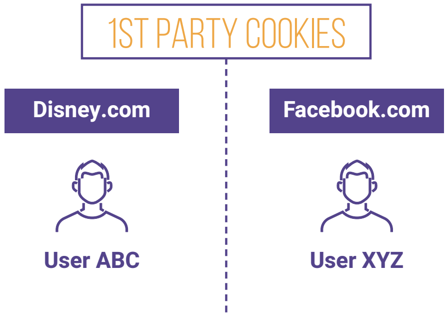
This regulation came out of the EU that was implemented in May of 2018. The GDPR primarily addressed the need for transparency, and required organizations to permanently remove consumer data if requested.

California Consumer Privacy Act (CCPA)

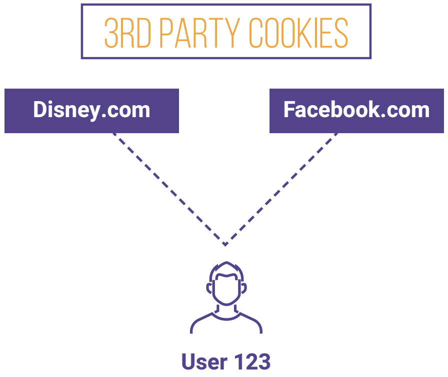
This was the first privacy regulation passed in the United States and was signed into law in June of 2018. Other countries are following suit by developing their own set of privacy regulations.

The most recent and wide-spread change to the world of user privacy will effectively stop the flow of broad user data. This change is due to happen in 2022, when Google will stop supporting 3rd party cookies (something Safari has already done). This is essentially pulling the plug on what has been the backbone of the marketing and advertising world for so long.

THE TECHNOLOGY THAT FUELS USER TRACKING



Sites are siloed and can't tell that user ABC & XYZ are the same visitor.



Sites can share information and create a single identity for users across sites.

Every technology company has their own "secret sauce" that allows them to have an edge on competitors. They each build models and algorithms that predict our actions, and whoever has the best model wins. For platforms that make their revenue from advertising, this is especially true.

The majority of these algorithms depend heavily on one key piece that ties the user data together: 3rd party cookies. 3rd party cookies allow platforms to collect, store and use user data across any website without the user ever knowing. Let's look at the difference between 3rd party cookies and 1st party cookies, and how they power the advertising industry.

1ST PARTY COOKIES

These are files that are set on a website that a user is currently visiting. For example, if a user visits Disney.com and navigates to the young girls clothing section of the website, Disney can set a cookie to indicate that the visitor likely has a young daughter. From there, it can recommend products that are more appropriate for young girls.

Because it's a 1st party cookie, this cookie and its data can only be accessed by Disney.com. 3rd party sites (for example, the Facebook pixel) are not able to read this cookie data. This makes it more secure as any data stored about the user in the context of the brand they're interacting with can not be automatically shared with other sites across any website on which they have a pixel installed without them knowing.

3RD PARTY COOKIES

These are files that are set while a user is on one website, but feeding information to another website or application. Let's look at the previous example. Disney.com has the Facebook tracking pixel on their site, which means that when a user visits Disney.com, Facebook is able to read and write its own cookies. This allows Facebook to track the user's activity on Disney.com and serve them ads and retargeting accordingly when they're back on the Facebook platform

Since the user is visiting Disney.com, but has a cookie for Facebook, that makes it "3rd party". This 3rd party cookie can then be accessed by Facebook on any other site that loads the Facebook pixel. Using this 3rd party cookie, brands can then track users uniquely across any website on which they have a pixel installed without them knowing.

In both cases, data is being tracked and stored. In the case of 3rd party cookies, the user is unaware of the 3rd party platforms that are tracking their data behind the scenes. Retargeting, and the feeling of being "followed around the internet" has brought to light just how much information is being tracked without users' knowledge.

THE NEW DATA COLLECTION LANDSCAPE

Chrome will be phasing out 3rd party cookies in 2022. Meanwhile, Safari and Firefox both already limit or don't support 3rd party cookies entirely, fueling the urgency for the advertising world to find a solution. The goal is to create a more humane and transparent way for platforms to gather and use user data.

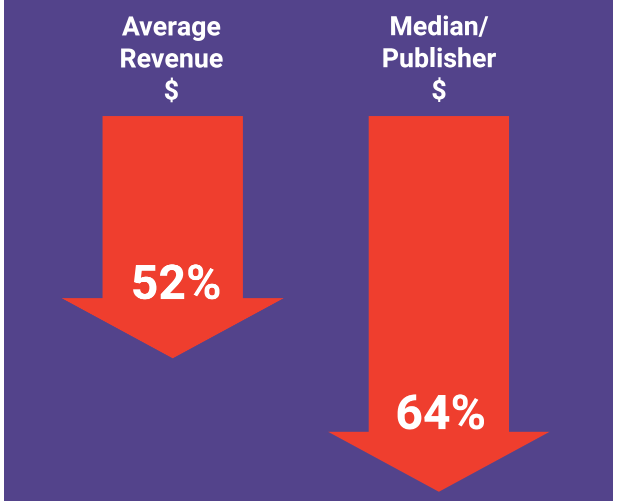
This means that brands who rely on services from platforms using 3rd party cookies are at risk of losing revenue and web analytics capabilities. In fact, Google ran an experiment to try and predict the impact 3rd party cookies going away will have on web publishers. Out of a group of 500 publishers, there was an overwhelming drop in revenue.

As a response to the impending change, key technology players are all trying to find new, innovative ways to gather data and create personalized user experiences. Research has shown that when brands are transparent, 73% of consumers are willing to share their data. This is an opportunity for brands to collect the data they need to continue to deliver value to their consumers.

Opt-in networks are one key piece to the new data collection process. This means that users will have the ability to give brands permission to collect and use their data across sites to create more personalized recommendations and experiences. This will provide a trust-based solution for when 3rd party cookies go away altogether.

The reality is that many of the solutions that platforms will use as a response to the changing data privacy landscape are being built now, or have yet to be built. Fortunately, Persosa developed a solution that balances user privacy and humane data management.

Google predicts that the average [publisher] revenue will decrease by 52%, with the median per publisher decreasing by 64%.



PERSOSA'S GROUNDBREAKING TECHNOLOGY

Persosa prides itself on being on the forefront of the disruption of the traditional data collection industry, and we understand the need for more humane and transparent data management.

Persosa's Identity Network solves for the deprecation of 3rd party cookies by using secure 1st party cookies and providing a trust-based opt-in network for cross-domain tracking without relying on 3rd party cookies.

This means our partners can track and own 1st party user data in a secure, privacy-first manner. That data can then be evaluated and streamed in real time as well as warehoused for insights and reporting and is not implicitly shared with outside vendors.

Some of the key differentiating features of our solution include:

COMPATIBLE WITH ALL BROWSERS

- Uses strict, secure, HTTP-only 1st party cookies by default
- Safari ITP support

PROVIDES MULTI-CHANNEL SUPPORT

- Installs on web with simple JavaScript snippet
- Track across devices with native SDK's **(iOS, Android, Apple TV, Android TV)**
- Track any other channel via restful API

EASY, SECURE SETUP

- No server-side scripts required
- Tracking performed in secure 1st party context *(e.g., persosa.yourdomain.com)* via CNAME

OPT-IN NETWORK

- Privacy-first, trust-focused network
- Enables cross-domain tracking without 3rd party cookies
- Safari ITP support

HOW BRANDS & USERS BENEFIT FROM PERSOSA'S TECHNOLOGY

Persosa's Identity Network creates a transparent and humane relationship between brands and consumers. By creating a foundation of opt-in, privacy-first networks, users can feel confident that the data they choose to share is being used to create a world class immersive consumer experience.

For brands, they can rebuild their reputation around responsible data usage by capturing data in a privacy-focused manner. Instead of relying on 3rd party platforms to capture and provide data, brands can now own their own data among a number of other important benefits. This includes:

- Use your 1st party data in real time for segmentation
- Emulate website analytics products (e.g., GA)
- Tap into real-time data event streams (see and react to user activity in real time)
- Data warehousing, insights, and reporting
- Own the user data and create an independent 1st party data set

Let's revisit the example of the user that visits Disney.com. With Persosa's new Identity Network, the user will be able to opt-in when they first interact with either Disney.com to elect if they would like to share certain data to create a better user experience.

Disney then has the ability to implement cross-domain tracking between their own portfolio of domains. For example, Disney and Hulu are both part of the Disney conglomerate, so they could use Persosa's Identity Network to implement cross-domain tracking using 1st party cookies in a secure, trustworthy manner. This gives them more specific user insights that Disney owns, which are not implicitly shared with 3rd party vendors. This allows them to serve great customer experiences across their entire brand portfolio.

As more platforms stop supporting 3rd party cookies, it's imperative that brands, advertisers and publishers implement new and innovative ways to capture and store user data. The brands that succeed in this, will lead the way in the next phase of media and advertising.

Learn how your business can get ahead of the data revolution.

Visit *persosa.com* or contact us at (877) 488-8502.