Identity Special Report

ad exchanger

Insights | Analysis | Benchmarks

Survey of Ad Tech Companies, Agencies, Publishers and Brands on Digital Marketing Identity and Privacy in Digital Marketing

Table of Contents

Introduction

AdExchanger's Identity Report: Taking the pulse of leading digital marketing executives on identity, privacy and the end of the third-party cookie

Welcome to AdExchanger's *2021 Identity Special Report*. You'd be hard pressed to find two issues that are more top of mind for our industry right now than identity and privacy. There's a lot of angst – but also a good deal of hope.

And in AdExchanger's Q2 research report, digital marketing professionals express both emotions while sharing their perspectives on the end of third-party cookies, their opinions on proposed alternatives and candid insights on what they're doing to plan for the future.

We surveyed ad tech providers, agencies, publishers and brands to get the lowdown on how they're approaching today's most urgent digital marketing challenges and issues. This report includes insights and benchmarks on:

- Identity and privacy
- Preparing for the loss of third-party cookies
- Alternative identity solutions, including first- and second-party data, email-based identifiers and the Privacy Sandbox proposals
- How identity and privacy challenges will impact connected TV

This report provides a mix of quantitative survey data and write-in comments in response to open-ended questions. The analysis is based on survey responses from 190 digital marketing professionals representing a wide cross-section covering all segments of the industry. The survey was conducted in April 2021. Note: In some of the data tables, the totals may not add up to 100% due to multiple-choice options or rounding.

AdExchanger thanks all respondents for their invaluable contribution to this study.

Executive Summary

The digital marketing industry is experiencing a period of transformational change.

The foundations of identity, understood through third-party cookies and app IDs, are crumbling.

Safari and Firefox block third-party cookies by default. Chrome, the world's most penetrated browser, will soon follow – albeit in 2023.

But the industry is divided as to whether or not the new solutions that are emerging to replace this core building block of digital advertising will actually improve consumer privacy.

Meanwhile the identity picture is impacted by two other macro trends: Linear TV advertising budgets are shifting to CTV (connected TV), which offers advertisers digital-like targeting and measurement capabilities. And walled gardens have continued to capture even more consumer attention and advertising investment.

Closely tied to these important changes and shifts are the twin challenges of consumer privacy protection and proliferating data regulations. As a result, we're seeing a new identity ecosystem emerge. The promise of digital marketing and advertising is bound to an understanding of end-user identity – or, at least, detailed and unique cohorts.

Yet, there are still many unknowns and unanswered questions about the future of identity that are still only in the early stages of being addressed – and, as demonstrated in this study, there's not agreement on what the outcome will be. Our readers hold divergent opinions on what these changes will mean for the industry.

But most are well aware of and actively pursuing options that aim to solve for the loss of third-party cookies. Solid majorities, as illustrated by our survey data, are collecting more first-party data, testing new identity resolution solutions and using contextual data more frequently. Just over half of digital marketers are tapping into second-party data and participating in industry data partnerships.

The one thing everyone agrees on is that how identity is determined and used in digital advertising is in the midst of being wholly redefined. New identity and privacy standards will be set over the next few years at the same time we're likely to see continued rapid shifts in consumer digital media consumption and innovation by technology providers and media companies.

Below are some of the key insights from our new research.

Insight #1 – The industry is moving forward with email-based replacements to third-party cookies – yet, digital marketing pros are split on whether these solutions improve privacy

The digital marketing industry is split in half on the question whether email-based identifiers are more privacy-safe than third-party cookies.

Forty-four percent feel email is more privacy-safe than third-party cookies, but another 44% disagree. Twelve percent simply don't know.

Survey respondents were also asked to provide write-in comments (provided later in the report). Some of their comments mentioned that how privacy-safe these solutions are depends on how data is handled, shared and stored.

Are Email-based Identifiers More Privacy-Safe than Third-Party Cookies?


UNSURE
12%

YES
44%

NO
44%
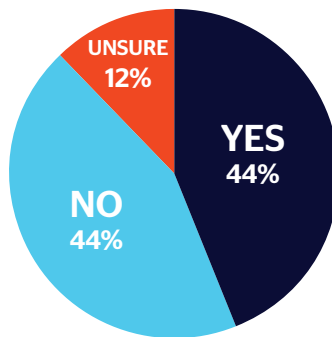
Insight #2 – Nearly half of digital marketers believe Privacy Sandbox proposals are more privacy-safe than third-party cookies

Forty-nine percent of the respondents believe Privacy Sandbox proposals are more privacy-safe than third-party cookies. This finding suggests another industry split as 29% say they disagree and a sizable 22% indicate they don't know yet.

Themes in some of the write-in comments include that Sandbox proposals are likely an improvement, but many privacy issues remain as data will still be grouped by personal attributes, and a number of others mentioned that there are still many unknowns.

Are Privacy Sandbox Proposals More Privacy-safe than Third-Party Cookies?
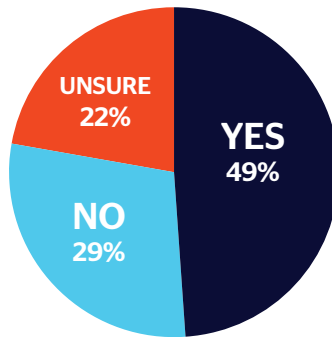
Insight #3 – A large majority of digital marketers believe first- and second-party data is an improvement over third-party data

Is the use of first- and second-party data considered a privacy improvement over third-party data? Seventy-three percent of digital marketing pros say first- and second-party data provides a privacy improvement compared to third-party data. Sixteen percent of the respondents disagree, and 11% are unsure/don't know.

Is First- and Second-Party Data a Privacy Improvement Over Third-Party Cookies?
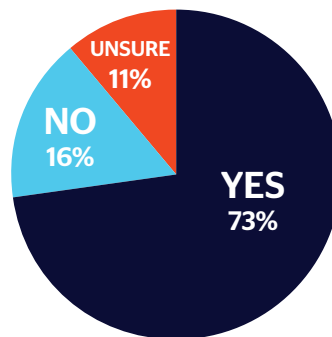
Insight #4 – Forty percent of digital marketing groups expect the loss of third-party cookies to negatively impact their advertising effectiveness – yet, the majority say the change will actually make their advertising better or will have no effect

The survey asked a fundamental question: Will the loss of the third-party cookie ultimately make your advertising better or worse?

While 40% say third-party cookies going away will negatively impact their advertising effectiveness, 35% expect to see better advertising outcomes, and 25% expect their results to be the same.

How Digital Advertising Overall Will Be Impacted by Loss of Third-Party Cookies

SAME
25%

BETTER
35%

WORSE
40%
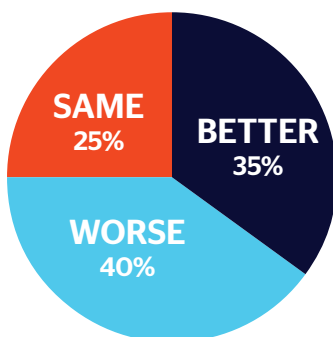
Insight #5 – Collecting first-party data, testing new identity solutions, and using contextual data are the top three ways digital marketing groups are preparing for the loss of third-party cookies

To deal with the loss of third-party cookies, 70% of respondents are collecting first-party data. Sixty-six percent are testing new identity resolution solutions and 61% are using more contextual data. Just over half are using other organizations' first-party data – a more advanced use case. Half participate in industry groups.

How Digital Marketers are Preparing for the Loss of Third-Party Cookies

70%	66%	61%	52%	51%
Collecting first-party data	Testing new identity resolution solutions	Using contextual data	Using others' first-perty data	Participating in industry groups
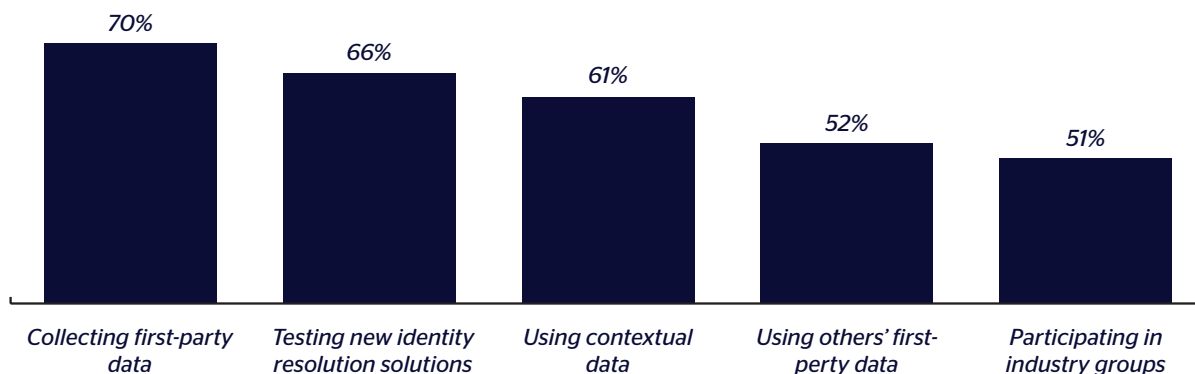
About the Survey Respondents

The respondents are primarily digital marketing executives and managers with ad tech providers, agencies, publishers and brands. A diverse range of job titles and roles are also represented as seen in the chart below.

Respondents' Job Titles/Roles
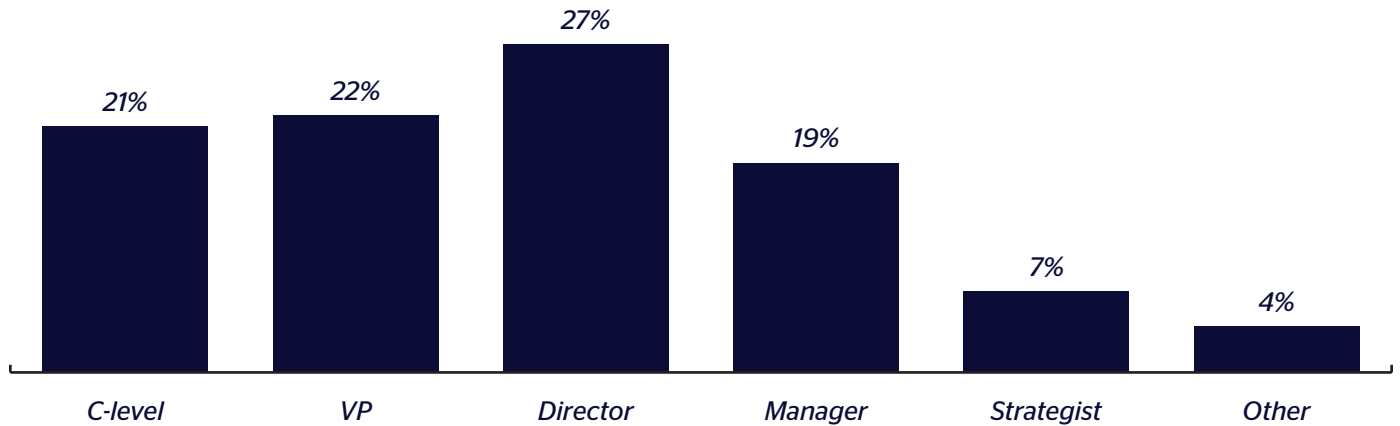
The findings in this Executive Summary offer a high-level view into the study's insights. The upcoming sections offer additional specific and actionable data, analytics and benchmarks.

I. Identity and Privacy

There is no one solution that replaces third-party cookies. This important section covers how the industry feels about the different solutions available: email-identifiers, Privacy Sandbox proposals, first- and second-party data as an alternative to third-party data. Plus, with so many identity solutions entering the market, we assess confidence levels with evaluating identity partners.

Are Email-based Identifiers More Privacy-safe Compared to Third-Party Cookies?

Survey Question: Do you believe email-based identifiers are more privacy-safe than third-party cookies?

Email-based identifiers divided the industry. Respondents were split on whether these solutions actually improve privacy.

Forty-four percent feel email is more privacy-safe then third-party cookies, but another 44% disagree. Twelve percent indicated they simply don't know at this stage.
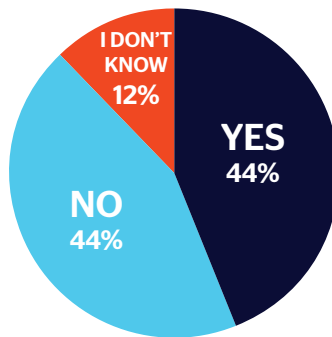
We asked respondents to offer context for their answers. Those in favor of email-based identifers said they were more privacy-safe if hashed, anonymized, and handled prudently. Others felt email was personally identifiable information (PII), making it less safe (and under more scrutiny from privacy laws). The issue of consent also factored prominently.

Select respondent comments in favor:

Yes:

- "Yes, if they are hashed/anonymized."
- "Assuming they are hashed properly (e.g., SHA-256)."
- "Email-based IDs guarantee more secure level of identification and opt-in/out possibilities."

> 66 **"They are opt-in, put the user in control, allow for transparency."**

- "Slightly safer, but not a long-term solution."
- "They are opt-in, put the user in control, allow for transparency."
- "They can be if they are anonymized like TTD Unified ID 2.0."
- "But there are still issues around email-based identifiers if you have enough contextual information 'reasonably identify'."

No:

- "99% of people who provide emails don't expect them to be shared for third-party targeting purposes."
- "Emails are directly PII (Personal Identifiable Information). How can circulating this around the internet as a signifier possibly be considered 'privacy-safe'."?
- "A tracking ID is a tracking ID. These will only vary by scope and consent."
- "Cookies are more transitory and do not refer back to any element of a user's identity."
- "Having multiple parties manage email, then use the same hashing algorithm to match them to create scale is an invitation for a bad actor to capture and un-hash emails. Plus email has no truth set to authenticate against, opening the door wide open to even more fraud."

> 66 **"Emails are directly PII (Personal Identifiable Information). How can circulating this around the internet as a signifier possibly be considered 'privacy-safe'."?**

- "Email is a direct unambiguous piece of PII (Personal Identifiable Information)."
- "Email IDs are based on implicit consent signals and far closer to personal identification then third-party cookies."
- "I appreciate that email-based IDs are most often going to be based on a user's consent, I worry about the management of the ID if a user opts-out."

Unsure:

- "At this point it is difficult to tell as not sufficient information has been shared on the email-based approach."
- "Depends on how they are collected and stored."
- "They give users more control, but you need clean rooms."

Are Privacy Sandbox Proposals Considered More Privacy-Safe than Third-Party Cookies?

Survey Question: Do you believe the Privacy Sandbox proposals are more privacy-safe than third-party cookies?

Just under half of respondents say they believe the Privacy Sandbox proposals are more privacy-safe than third-party cookies, slightly more than email-based identifiers. Twenty-nine percent say no. Yet, a sizable 22% are unsure still at this stage, larger than any of the other solutions we asked about. Many respondents also voiced objections to Google's control of the Privacy Sandbox, concerned about what this would mean for the broader industry.
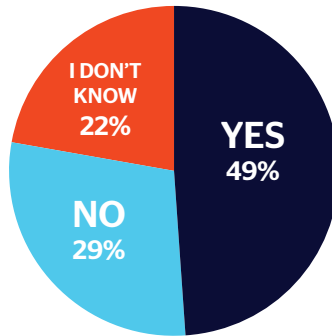
Key themes in the write-in responses include:

- With consolidated data, privacy issues become more concentrated
- Privacy Sandbox is likely a privacy improvement, but it is still early in the process with many unknowns
- How does Privacy Sandbox ask for consumer content?
- Maintains/gives leverage to Google

Select comments:

Yes:

- "Yes, but I am not confident in Google as the main gatekeeper and potential impact on UX."
- "The end result will likely be an improvement but will still leave potential for intentional and unintentional learning about users."
- "Yes, but there are increased issues around 'church and state' for some providers/enablers."

> **"The end result will likely be an improvement but will still leave potential for intentional and unintentional learning about users."**

- "Yes. It's nowhere near perfect, but it doesn't look like there is much of a choice left."

No:

- "A group of 25 niche people is still niche. The issue isn't that you've named me, it's that you grouped me by some personal attribute. Sandboxing doesn't change the fact that you are still targeting me based on my drug usage or sexual bias."
- "Actually they are less privacy-safe and of course lacking one of the most important concepts of consent!"
- "FLoCs can still be drilled down to an individual user over time through their dynamic building."
- "They are very clearly a mechanism Google are leveraging to continue to build their monopoly."
- "Just puts Google in the driver's seat."
- "Privacy sandbox moves too much stuff towards the one big company."
- "The privacy sandboxes just provide certain large parties with power and ownership over users' data. But I don't see how they equate to 'more privacy-safe'."

> **"FLoCs can still be drilled down to an individual user over time through their dynamic building."**

- "They just concentrate the private data (browsing history, etc.) into Google's hands. They become the purveyor of 'privacy'."
- "This is kind of fake as Google owns a substantial first-party universe with Search, GDN, Gmail and Maps, and so forth."

Unsure:

- "Again, there are still many unanswered questions and if this has not yet been approved by the GDPR laws, then something is still not right."
- "I agree that some of the proposals provide more privacy and user choice than exists today, but I worry about the impact to the overall industry."
- "It's hard to tell, honestly. It seems to be more protective of the tracking of an actual individual, but it's still tracking, just by a different party who aggregates it."

Is First- and Second-Party Data an Improvement Over Third-Party Data?

Survey Question: Is the use of first-party data or second-party data (e.g., publisher data if you are a brand) a privacy improvement over use of third-party data?

Seventy-three percent of digital marketers say first- and second-party data offers a privacy improvement over third-party data, the strongest positive response of the group. Sixteen percent disagree, and 11% percent are unsure.

The write-in comments mainly focus on issues around end-user consent, and how data is collected, matched, stored and used.
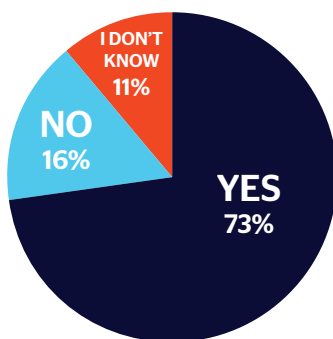
Industry Sector Break-Outs: First-Party and Second-Party vs. Third-Party Data as a Privacy Improvement

This data table below breaks out the findings to the question above by the respondents' industry sectors. Publishers, followed by agencies, are the groups with the highest percentage of respondents agreeing that first- and second-party data offers improved privacy compared to third-party data.

	Brand/In-House Marketer	Agency	Ad Tech Company	Publisher
Yes	64%	73%	69%	77%
No	27%	17%	20%	8%
I don't know	9%	10%	11%	15%

Among the respondents, both those who answered "yes" and "no" were often in agreement. They both felt that first-party data becomes shared widely or part of a profile, it loses its privacy advantage. So whether they answered "yes" or "no" depended on if they viewed this data sharing as an inevitability ("no"), or something that could be tightly controlled ("yes").

Yes:

- "It's an improvement given that the tradeoff between the consumer/end-user and the publisher is more direct and explicit."

- "If transparently permissioned."

- "In so far that there is no overall [user] profile this is true. The profile is only constructed with first-party data."

- "Only if [the data] is not shared across websites. The more it is shared, the less private the data becomes."

> **"[First-party and second-party] data provides clearer ownership and audit trails. And [brands] can better inform their customers about how their data will be used in marketing so they can provide informed consent."**

- "Yes, provided consent is provided and the end-user understands the value-exchange."

No:

- "It all depends as to how the data will be used. If the objective is to continue to follow consumers, then the answer is no."

- It's not about what data is shared, it's about the controls to break persistent tracking that will create a privacy improvement."

- "First-party data is being stitched together with second parties to create faux third-party data."

- "Possibly, but depends on how the data is being collected. First-party data is more deterministic than third-party data, but is only a privacy improvement if such terms are agreed upon with the consumer."

- "How is using actual PII [Personal Identifiable Information] more privacy protective than the anonymous nature of a cookie?"

- "Third-party data was hardly precise, and therefore not privacy intruding."

I don't know:

- "Depends on data collection and choice/notice methodologies."

Multi-Question/Issue Comparison: Which Areas are Considered More Privacy-safe than Third-Party Cookies?

The most privacy-safe alternative to third-party cookies is first-party data, according to our respondents. In second was Privacy Sandbox, and last was email-based identifiers.

Alternatives Digital Marketing Professionals Consider Safer than Third-Party Cookies

73% — First/Second-Party Data

49% — Privacy Sandbox

44% — Email IDs
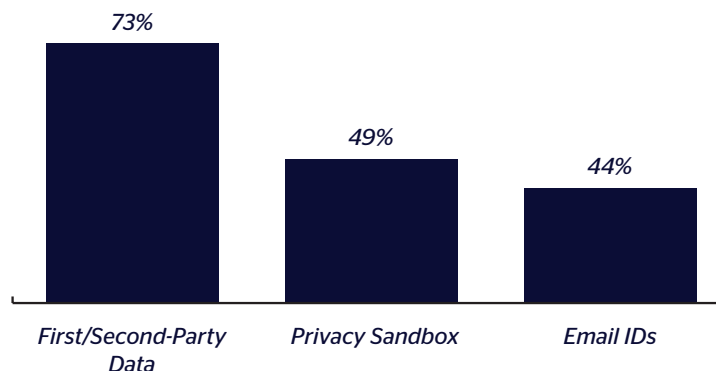
Confidence Level When Evaluating Identity Partners

Survey Question: How confident do you feel in your ability to evaluate identity partners?

A total of 62% of the respondents are very or somewhat confident in their ability to evaluate identity partners.

A number of the survey respondents offered tips for evaluating partners on claims, but also pointed out that there are often a number of unknowns and uncertainties related to new services that cannot be verified – yet.
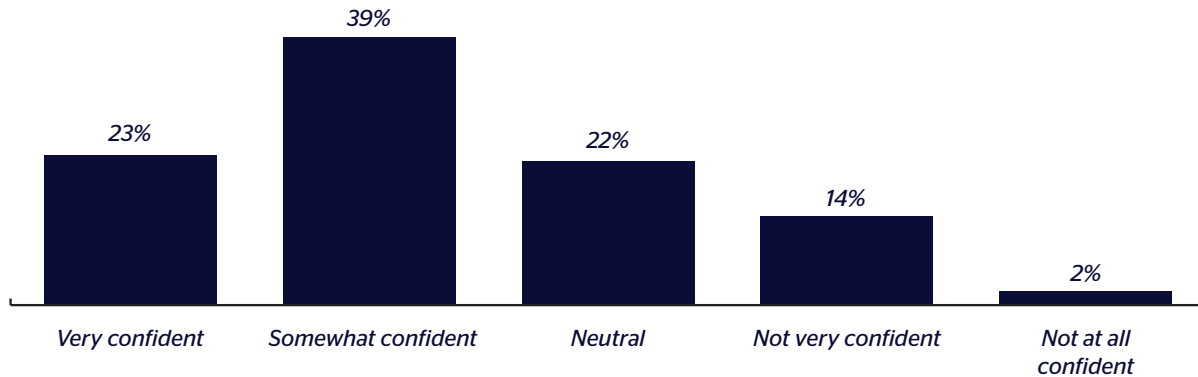
Comments on evaluating identify partners.

Concerns about their compliance with browser rules and industry regulation:

- "Even if I like their data, who's to say that it will continue being allowed in the browser or the exchange?"

Does the technology do what it says it does?

- "There is a lot of smoke and mirrors right now in this space. It's hard to parse through reality and fact vs. unverified claims."
- "Companies have very good marketing, but little transparency as to how they produced the results in their materials. This requires a significant amount of analysis, testing and interrogation for each solution."
- "Challenge is how to verify what is being said vs. what is actually done. I think that for the big name companies (LiveRamp, TTD, etc.) this is much less of an issue than for smaller companies."

> **"Companies have very good marketing, but little transparency as to how they produced the results in their materials. This requires a significant amount of analysis, testing and interrogation for each solution."**

- "There is so much murkiness and a history in digital of murkiness equally fraud; no clue how we will all come to any decisions."

Scale and adoption will matter – but it's too early to pick a winter when evaluating partners:

- "Evaluation should consist of technology stack and algo as well as reach, the latter is easier to evaluate."

> **"It's hard to assess which ones will have long-term value in the ecosystem."**

- "It's hard for partners to prove value without adoption from both sell/buy side at scale. We also don't have authenticated users at scale right now, although that is something we plan on addressing."

- "It's hard to assess which ones will have long-term value in the ecosystem."

II. Preparing for the Loss of Third-Party Cookies

Marketers have many options to test as replacements for third-party cookies. This section gauges the popularity of the alternatives. We also ask about what parts of digital marketing will be most affected by the transition.
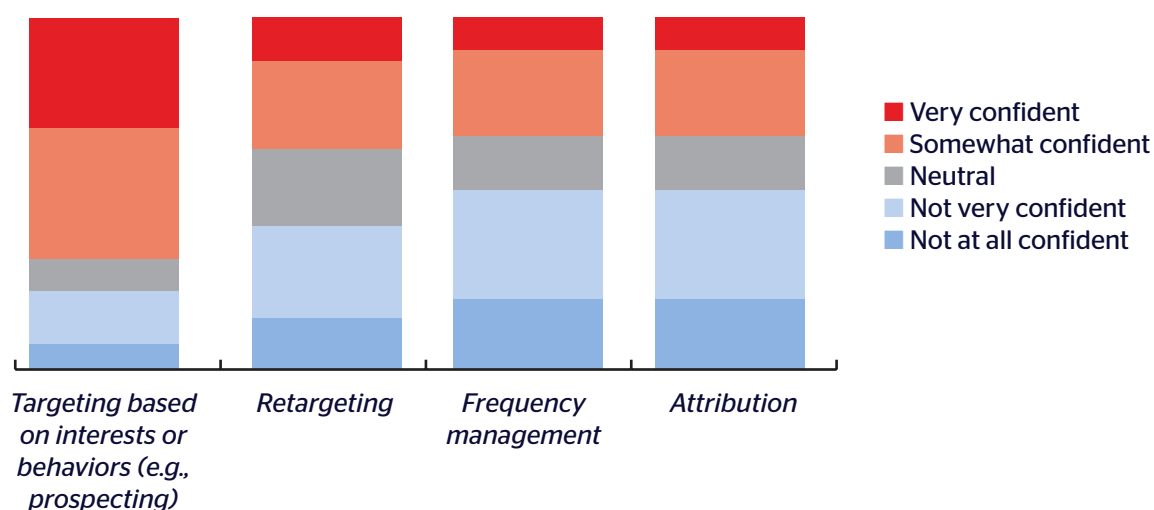
Confidence There Will be Satisfactory Use Case Replacements for Third-Party Cookies

Survey Question: How confident do you feel that there will be satisfactory replacements for the following use cases for third-party cookies?

Prospecting will be least affected, according to our respondents. They were less bullish on alternatives for retargeting, attribution and frequency management.

Complete Data Set	Very / Somewhat confident together	Very confident	Somewhat confident	Neutral	Not very confident	Not at all confident
Targeting based on interests or behavior (e.g., Prospecting)	67%	32%	35%	13%	15%	5%
Retargeting	39%	15%	24%	18%	31%	12%
Frequency management	35%	10%	25%	13%	39%	13%
Attribution	35%	11%	24%	15%	36%	14%

Confidence There Will be Satisfactory Use Case Replacements for Third-Party Cookies

Legend:
- ■ Very confident
- ■ Somewhat confident
- ■ Neutral
- ■ Not very confident
- ■ Not at all confident

Categories: Targeting based on interests or behaviors (e.g., prospecting) | Retargeting | Frequency management | Attribution

Where Digital Marketers are Most Confident About Use Case Alternatives to Third-Party Cookies

Digital marketing pros are most confident that, post-third party cookies, solutions will be provided that will allow for targeting based on interests or behavior. (This data is based on the table directly above.)

67%
39%
35%
35%

Targeting based on interests or behavior (e.g., Prospecting) | Retargeting | Frequency management | Attribution
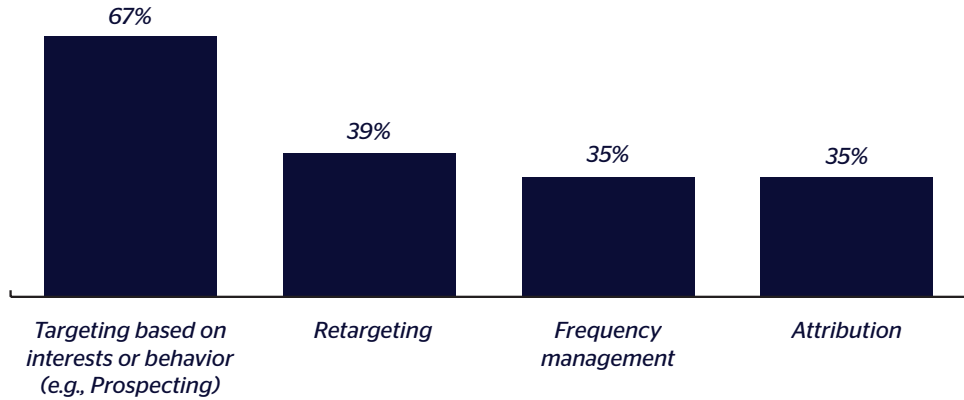
Where Digital Marketers are Least Confident About Use Case Alternatives to Third-Party Cookies

The respondents are least confident about effectively replacing frequency management, attribution and retargeting capabilities.

52%
49%
44%
20%

Frequency management | Attribution | Retargeting | Targeting based on interests or behavior (e.g. Prospecting)
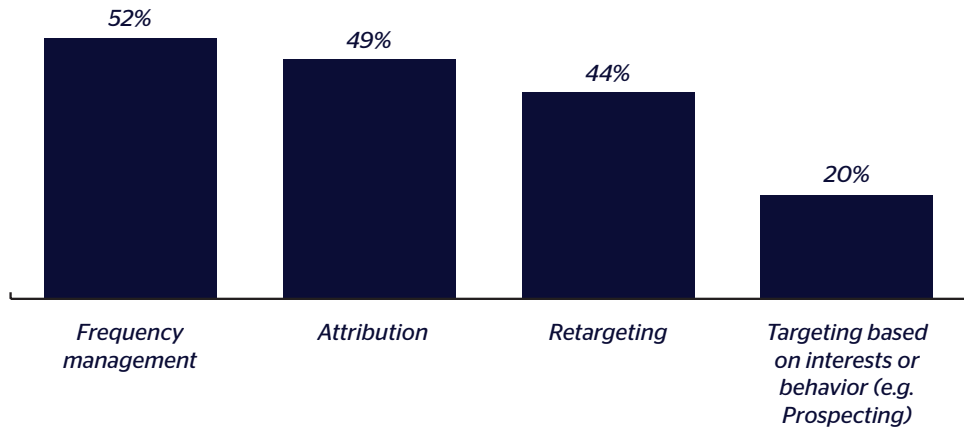
Actions Taking to Prepare for the Loss of Third-Party Cookies

Survey Question: What actions have you been taking to deal with the upcoming loss of the third-party cookie?
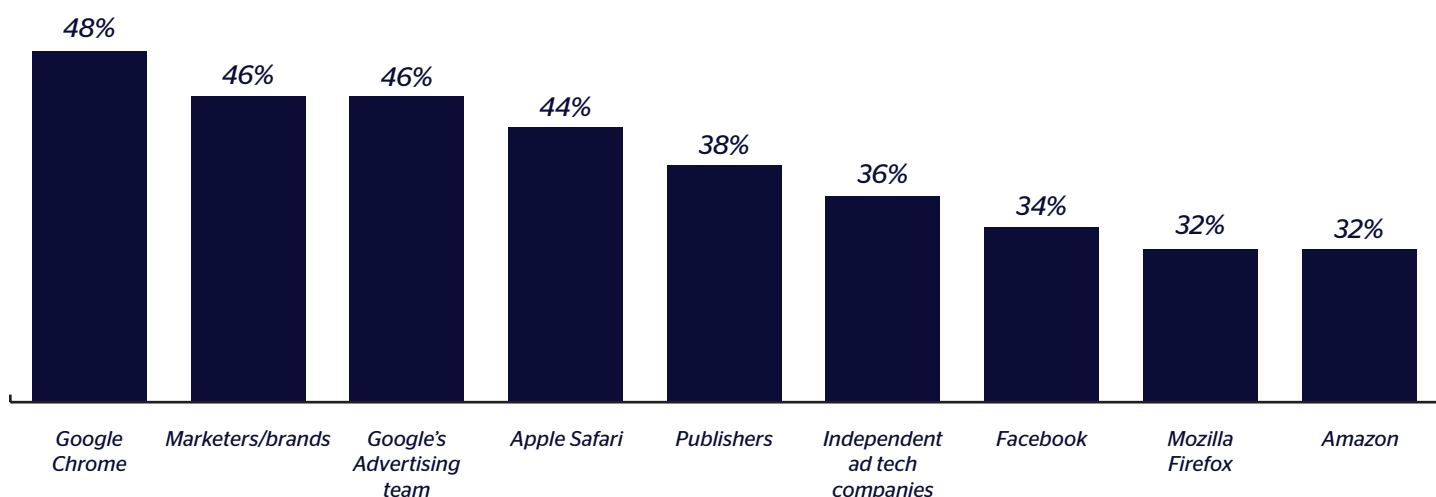
To deal with the loss of third-party cookies, 70% of respondents are collecting first-party data, 66% are testing new identity resolution solutions, and 61% are using more contextual data. Just over half are using others' first-party data or participating in industry groups. Clean rooms and pushing on partners to come up with solutions were both less common steps.

	%
Collecting first-party data	70%
Testing new identity resolution solutions (e.g. UnifiedID 2.0, LiveRamp, BritePool, Neustar)	66%
Using contextual data	61%
Using others' first-party data (e.g. working with publisher data if you are a brand, or using a brand's data if you are a publisher)	52%
Participating in industry groups (e.g. W3C's Improving Web Advertising business group, IAB Tech Lab)	51%
Testing Privacy Sandbox items	36%
Using clean rooms to analyze data with media partners	34%
Requesting partners come up with solutions	31%
Other	8%

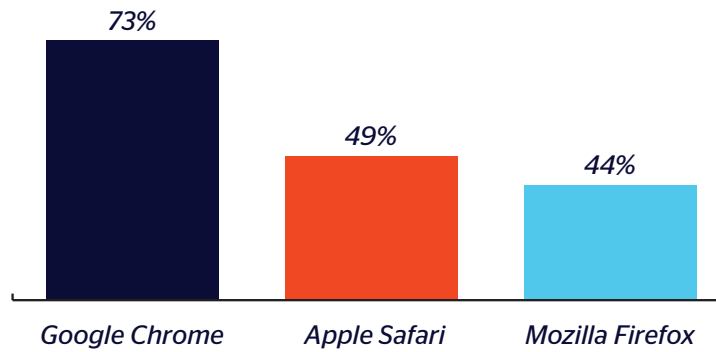**Industry Players that Need to Do More to Support Third-Party Cookie Alternatives**

Survey Question: Who are the "slackers" who need to do more to support alternatives for third-party cookies?

Based on the total base of respondents, Google Chrome – at the center of the change – came up as a common target as a "slacker." Marketers and brands, who control the advertising dollars, also ranked highly, followed by Apple Safari, another initiator of change, ranked as groups that need to do more to support alternatives for third-party cookies.

| Google Chrome	Marketers/brands	Google's Advertising team	Apple Safari	Publishers	Independent ad tech companies	Facebook	Mozilla Firefox	Amazon
48%	46%	46%	44%	38%	36%	34%	32%	32%

The charts below provide the same data in the table above but are broken-out by key industry segments: browsers, tech cos./walled gardens, and other parts of the industry ecosystem.
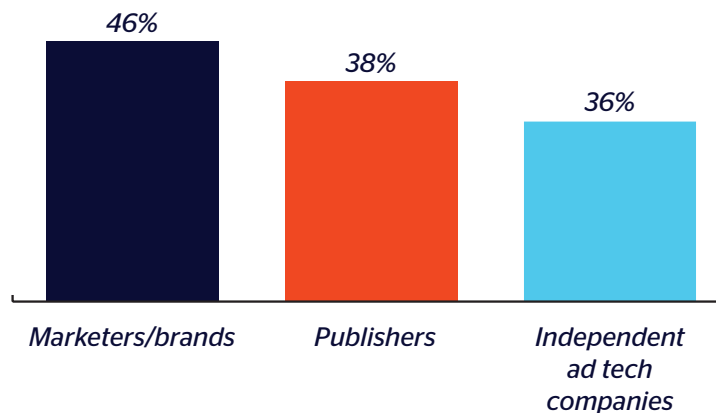
Browsers that Need to Do More to Support Third-Party Cookie Alternatives

- 73% Google Chrome
- 49% Apple Safari
- 44% Mozilla Firefox

Tech Cos. / Walled Gardens that Need to Do More to Support Third-Party Cookie Alternatives

- 46% Google's Advertising team
- 34% Facebook
- 32% Amazon
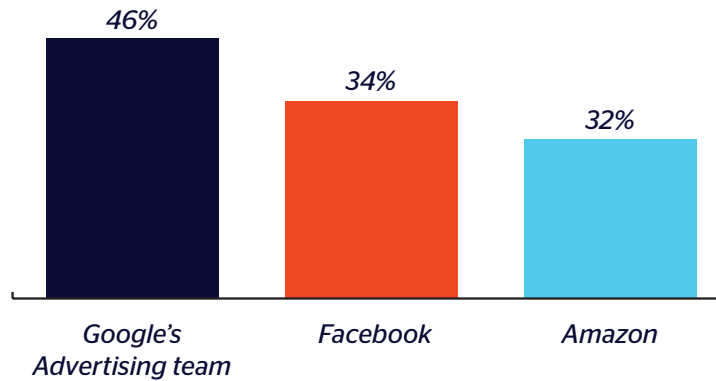
Other Parts of the Ecosystem that Need to Do More to Support Third-Party Cookie Alternatives

- 46% Marketers/brands
- 38% Publishers
- 36% Independent ad tech companies

Below are comments in response to the question about which groups are considered the "slackers" who need to do more to support alternatives to third-party cookies:

Marketers and publishers aren't slackers – their hands are tied by ad tech companies:

- "Vendors put us into this spot, they better get us out, or my dollars go elsewhere." Director at a Brand

- "Publishers and brands for the most part are reliant upon ad tech companies for targeting." – VP with Publishing Company

> **"Companies have very good marketing, but little transparency as to how they produced the results in their materials. This requires a significant amount of analysis, testing and interrogation for each solution."**

But some ad tech companies are clamoring for marketers to test their solutions:

- "There hasn't been significant marketer testing of unified IDs." – Manager with Ad Tech Company

There is resentment that browsers caused the problem, but aren't building the solution:

- "The browsers are forcing this and allowed it to happen. Causing a stir without an appropriate solution is dumb." – Agency C-Level

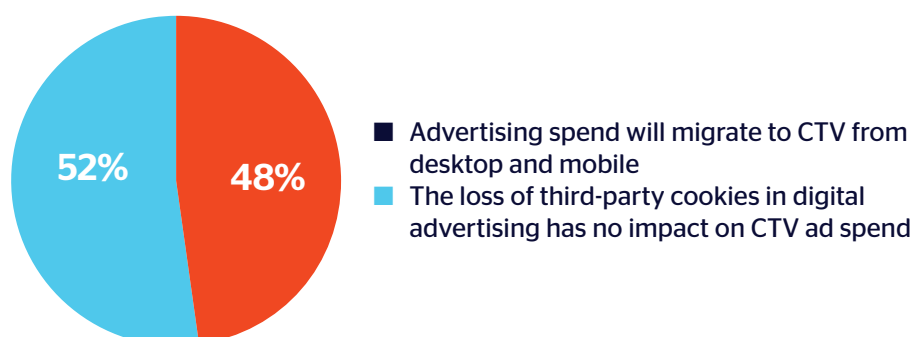# III. Connected TV Investment and Identity Challenges

This section provides findings on CTV investments and identity issues.

How Identity Challenges Will Affect Connected TV Ad Investments

Survey Question: How do you think identity challenges will affect CTV (Connected TV) ad investments?

Here is another issue that splits the industry basically down the middle. Forty-eight percent feel that advertising spend will migrate to CTV from desktop and mobile, while 52% hold the opinion that the loss of third-party cookies in digital advertising has little to no impact on CTV ad spend.

Some confounding factors may be at play: CTV has been growing rapidly anyway, making it harder to tease out the impact. Plus, CTV spending can come out of different marketing budgets than online channels using third-party cookies.

- Advertising spend will migrate to CTV from desktop and mobile
- The loss of third-party cookies in digital advertising has no impact on CTV ad spend

Respondent's Job Function Break-Out: How Identity Challenges Will Affect Connected TV Ad Investments

This question's findings are broken out below by job function. VPs and Strategists are most likely to expect advertising spend will migrate to CTV from desktop and mobile compared to the other job titles/roles.

	C-Level	VP	Strategist	Director	Manager
Advertising spend will migrate to CTV from desktop and mobile	50%	55%	54%	48%	44%
The loss of third-party cookies in digital advertising has no impact on CTV ad spend	50%	45%	46%	52%	56%

Key themes in the comments include:

CTV will benefit from third-party cookie loss:

- "Perfect use case for a post cookie world, it should accelerate the shift."

...But maybe the money won't move so easily:

- "Channel decisions are driven by incremental reach, which will be measurable without cookies."
- "These are entirely separate budgets."
- "Price-conscious advertisers will not be able to move to CTV."
- "Loss of third-party cookies may not impact CTV spend immediately, but over time may accelerate existing trends."
- "Spend on CTV will continue to grow, but there will be only incremental growth as a result of the loss of third-party cookies."

Plus, CTV measurement is evolving/innovating anyway:

- "CTV spend will increase naturally anyways, because that is where the growth opportunity is. It will not be a causation from identity challenges. It's just a correlation."

Technical nuances – around IP address, IDFAs and more – matter:

- "IP address is a household level ID and not comparable to an Identity unless associated with a login or device level identifier."
- "I feel like there's a bit of an informational void on negative impacts data deprecation will have on CTV as this question points out. For example, Apple ATT also applies to TV OS the OTT Apple TV box runs on."
- "Current CTV tracking is bad, lack of cookies will not make it worse or better."
- "It will effect targeting, but the attribution part won't be affected as we aren't measuring site actions against CTV."

How Identity Challenges on Browsers and Apps Will Migrate to Connected TV

Survey Question: Do you think identity challenges on browsers and apps will migrate to CTV (Connected TV)?

There's more agreement throughout the industry on this question. Over two-thirds believe that CTV will face similar identity challenges for privacy reasons in coming years.

48%

52%

- CTV is insulated from privacy-related identity challenges (e.g., regulation, consumer privacy concerns, loss of features due to privacy concerns)
- CTV will face similar identity challenges for privacy reasons in coming years

Select comments.

CTV's privacy reckoning is coming:

- "It will be faster than what happened on the web and mobile."
- "The potential loss of IP address will put CTV in the same place as the web."
- "IP address will be removed from bidstream."
- "The current state of addressability using household ID's and IP addresses may be challenged at some point, by consumers or government."
- "ATT is already going to impact CTV."
- "Consumers will need assurances from smart TV companies and device manufacturers (e.g., Roku) that their data is protected, and they are able to exercise control over how it is being used, including opt-out."

> **"The current state of addressability using household ID's and IP addresses may be challenged at some point, by consumers or government."**

- "CTV already has complicated identity issues."
- "CTV isn't insulated from privacy regulations. But again, because these platforms require authentication, they have a better method to provide accurate scale and attribution."
- "CTV relies on a billing relationship which requires identity disclosure."

CTV won't face privacy challenges:

- "Most CTV is based on already logged-in users, so the value-exchange is explicit."
- "CTV is household-level."

Conclusion: There's No Consensus on the Impact of the Loss of the Third-Party Cookie

As the industry pursues different options to find a new foundation for identity, the question remains: How will advertising performance – and investments -- change?

With Third-Party Loss Will Advertising Results be Better or Worse?

Survey Question: Will the loss of the third-party cookie ultimately make your advertising better or worse?

These findings suggest that there are basically three groups in the industry today. While 40% say third-party cookies going away will have a negative impact on their advertising effectiveness, 35% expect to see better advertising performance, and 25% expect their results to be the same. That means a full 75% of respondents think digital advertising will be the same or better, while the remaining quarter foresee a decline.

How Digital Advertising Overall Will Be Impacted by Loss of Third-Party Cookies
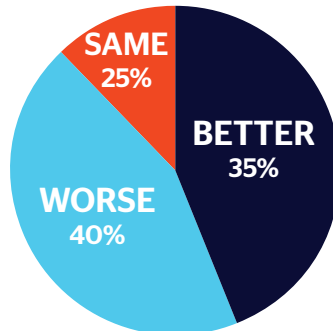
Here are select write-in comments grouped by sentiment on what the impact of the loss of third-party cookies will mean for advertising results:

Digital advertising will suffer – including the consumer experience:

- "Ads will be even more annoying."
- "We used to target really well, and eliminated waste. Now, we'll target like the 70s, buying contextual pages based on some hope of content interest synchrony. What a waste."
- "At the least it will put digital on par with less measurable media such as TV. The loss of RFM (Recency/Frequency/ Monetary Value) analysis and holistic attribution will definitely hurt."
- "In the short term, the loss of advertising scale for targeted audiences will be tremendous. I think this will be addressed eventually, but realistically, there will be a dramatic impact to scale."
- "Will have to overcompensate due to targeting fidelity loss, driving up costs, time and resources."

The loss of third-party cookies will create new areas of opportunity:

- "Audio, specifically podcasts, have been functioning without cookies from the start. Contextual targeting is key."
- "CTV is a major focus."
- "Will force publishers to create more unique value."

> **"Worse in the near term. Innovation will likely make it better in the long run."**

- "Initially worse, but then gravitate to acceptable."
- "Worse in the near term. Innovation will likely make it better in the long run."
- "The more things focus on (permissioned) identity and addressability, the better."

Methodology and About the Respondents

In April 2021, AdExchanger conducted a survey of a wide cross-section of leading digital advertising and marketing companies throughout the industry. The survey received 190 responses. The respondents are primarily digital marketing executives and managers with Ad Tech providers, agencies and publishers. Brands and consultants were also surveyed. Twenty-one percent of the respondents are C-Levels, 22% are VPs, and a total of 34% hold the titles of Strategist or Director.

Respondents' Company Type

	%
Ad Tech Company	53%
Agency	17%
Publisher	15%
Brand/In-House Marketer	7%
Consultant	6%
Other	3%

Respondents' Job Title

	%
C-level	21%
VP	22%
Strategist	7%
Director	27%
Manager	19%
Other	4%

Conclusion

What are we in for when the dust settles after the loss of the third-party cookie on Chrome in 2023?

It's hard to argue that the industry doesn't face unprecedented challenges from the loss of third-party identifiers –and yet a full 75% of respondents believe that digital advertising will either be the same or better after third-party cookies go away. The remaining quarter is far less sanguine. Twenty-five percent of our respondents foresee that advertising will get worse.

Regardless of who will be proven right, the only sane thing to do is hope for the best and prepare for the worst – and there are a lot of prospective solutions out there that claim to be a viable alternative to the third-party cookie.

By far the most popular approach is to focus on first-party data. It's the most widely tested post-cookie tactic and the one that most industry experts consider to be more privacy-safe than cookies.

Digital marketing pros are also feeling pretty good about their ability to evaluate identity solutions. Although most acknowledge the confusing claims made by many identity vendors, the vast majority of respondents – 72% – feel up to the task of assessing the identity vendor landscape.

Industry respondents were also largely bullish at 67% that the prospecting use case remain effective and intact.

But, still, confusion reigns in quite a few ways. For example, nearly one in four respondents said they were "unsure" about whether the Privacy Sandbox would be more privacy-safe than cookies, reflecting the fact that all the technologies within are still in the process of being built.

The answer is ongoing industry collaboration – but many parties feel that other constituents aren't doing enough. Criticism was leveled at Google and Apple in particular as the architects behind many of these seismic changes for not doing more to come up with solutions for the problems they caused by their platform-wide identity-related changes.

There is also an unfortunate lack of participation and action on the part of marketers. Although they are control the ad budgets, they are more removed from the urgency of this challenge. Nearly half – 46% – of those surveyed called marketers "slackers" who need to do more.

Our industry is also split on whether CTV will be the beneficiary as advertisers seek cookieless investment vehicles for their ad dollars. Among C-level respondents, half say they plan to spend the same amount on CTV, while the other half say CTV investment will increase as a result of the loss of third-party cookies on the web.

But here's a web blanket for the CTV bulls: 77% of our respondents believe that CTV will receive privacy-related scrutiny in coming years, and we're talking sooner rather than later.

In the words of one respondent, "It will be faster than what happened on the web and mobile."

40 Wall Street
New York, NY 10005
www.adexchanger.com