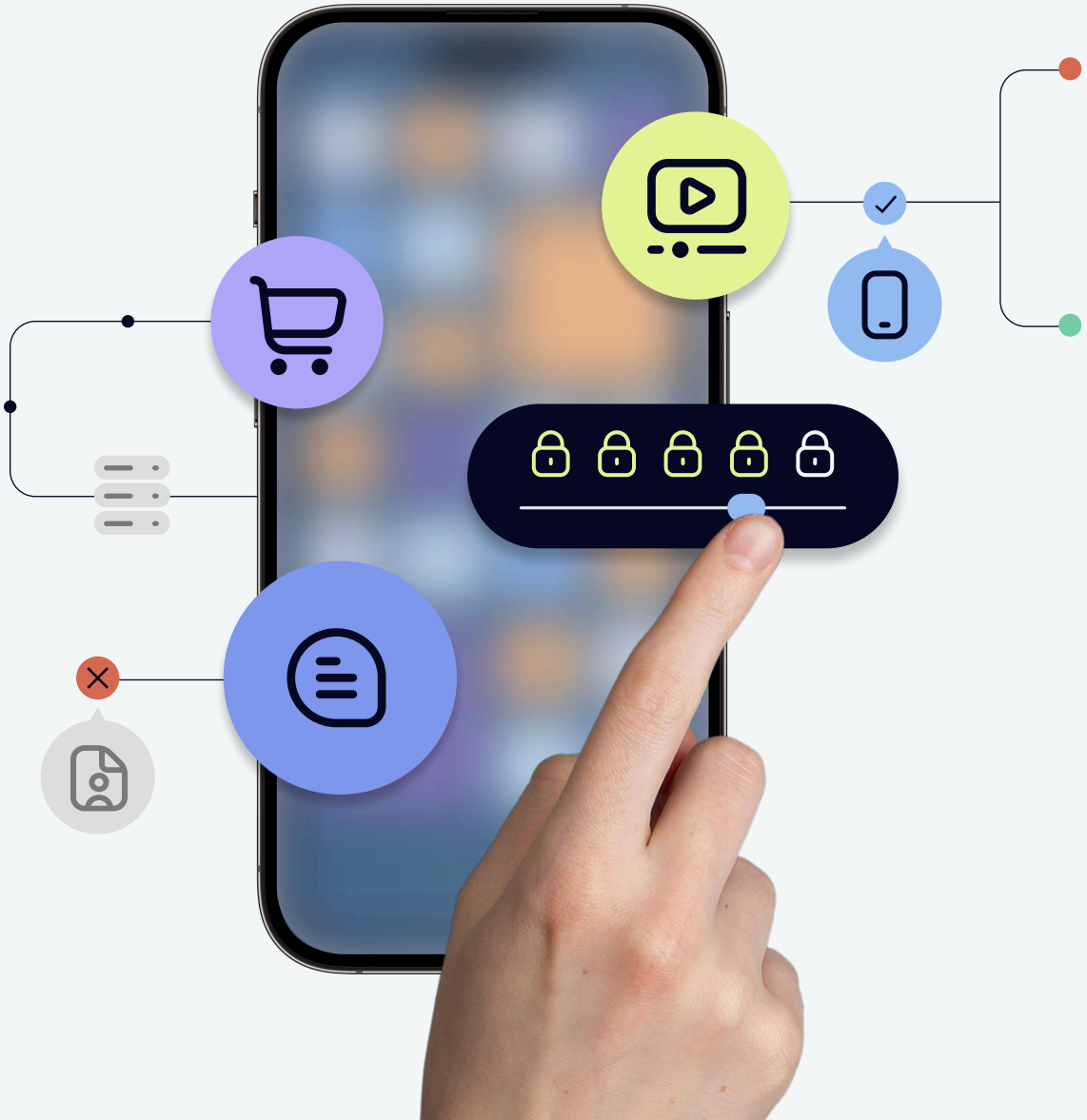
verve

2025 In-app User Privacy Report



Key findings

This study aims to answer a fundamental question: How can we build trust between consumers and publishers?

To find out, we surveyed 4,000 mobile users across the US and UK about the factors shaping willingness to share data, how they view their data's value, the impact of personalization — and how their attitudes have changed over time. The survey also explored specific levers for trust and the value exchange with regard to different app categories, devices, and platforms.

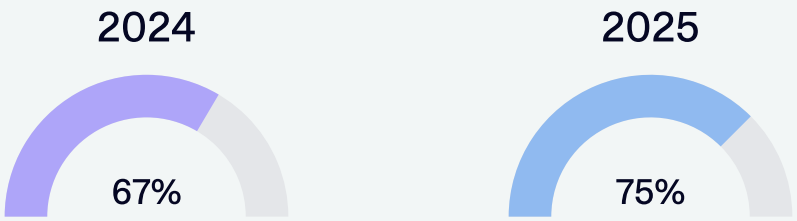
More worried about privacy — but still willing to share data

Data privacy concerns are climbing across all categories we measured, yet consumers remain open to sharing data with publishers — under the right circumstances. Importantly, the increase in willingness to share data did not keep pace with the jump in fears about data privacy. This is a clear call to action for the industry to address consumers' concerns directly.

From 2024 to 2025, consumers pulled back on sharing highly identifying information like names and contact details, while showing more openness to sharing demographic and contextual information like region, health data, and personal characteristics.

Accepting ads in exchange for free content

Of those who shared an opinion, three in four consumers now say they're more willing to watch ads in exchange for free content than they were two years ago. That's up from two in three in the last 12 months. Amid global economic uncertainties and growing subscription fatigue, this shift creates new opportunities for advertisers and publishers.[1]



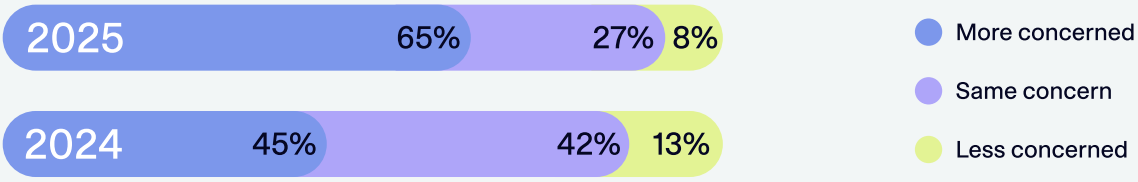
Agree (net)[2]: "I am more willing to watch/receive advertisements in exchange for free content than I was two years ago."

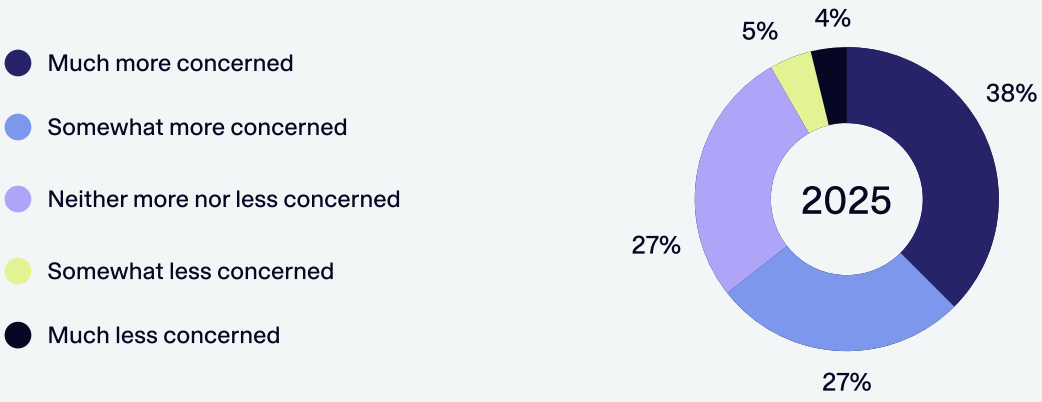
This preference for ads over in-app purchases was consistent across demographics, though its strength varies depending on the incentive. You'll find a detailed breakdown on page 18.

[1] MarketWatch: Subscription Fatigue Survey: 1 in 3 Americans are canceling subscriptions to save money (2025)
[2] Agree (net) combines "Strongly agree" and "Somewhat agree" responses.

Consumers crave transparency as concerns over AI skyrocket

One of the most dramatic changes from 2024 to 2025 was consumer concern over publishers using their data to train AI. Two-thirds of consumers surveyed are more concerned than they were two years ago (65%). This segment of respondents more concerned about their data being used to train AI grew by over 40% in the past 12 months.[3] The majority of this group is “much more concerned.”





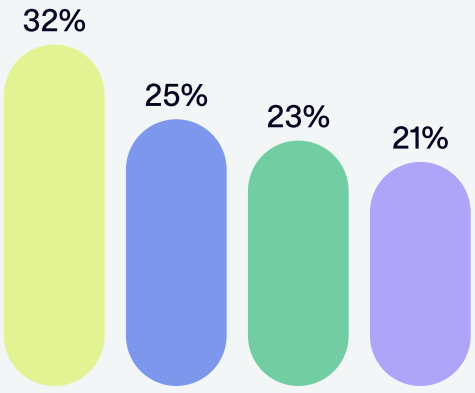
Beyond AI and data usage, a striking 97% of respondents agreed with the statement that “app publishers and platforms need to do more to be transparent with how consumer data is used and handled." To earn consumer trust, publishers’ communication about AI and data usage must be transparent and proactive.

[3] 2024 “Same concern” data combines responses for “Same concern” (32.78%) and “Was never and am still not concerned about this” (9.26%). Excluded “Not sure” responses for year-over-year consistency.

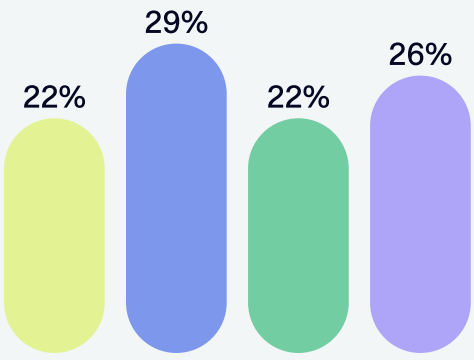
Personalized, relevant ads are critical for brand-building and product discovery

The survey reveals that three in four consumers are more likely to pay attention to an ad if it's relevant to them (76%). Additionally, two in three respondents said that relevant, personalized ads could help them discover products they didn't know existed.

Where are you most likely to pay attention to an advertisement, if it is relevant to you? (Select up to 2.)



On which platforms, if any, do you feel your personal data is most protected? (Select up to 2.)



On a CTV · On mobile apps · On mobile websites · On desktop websites

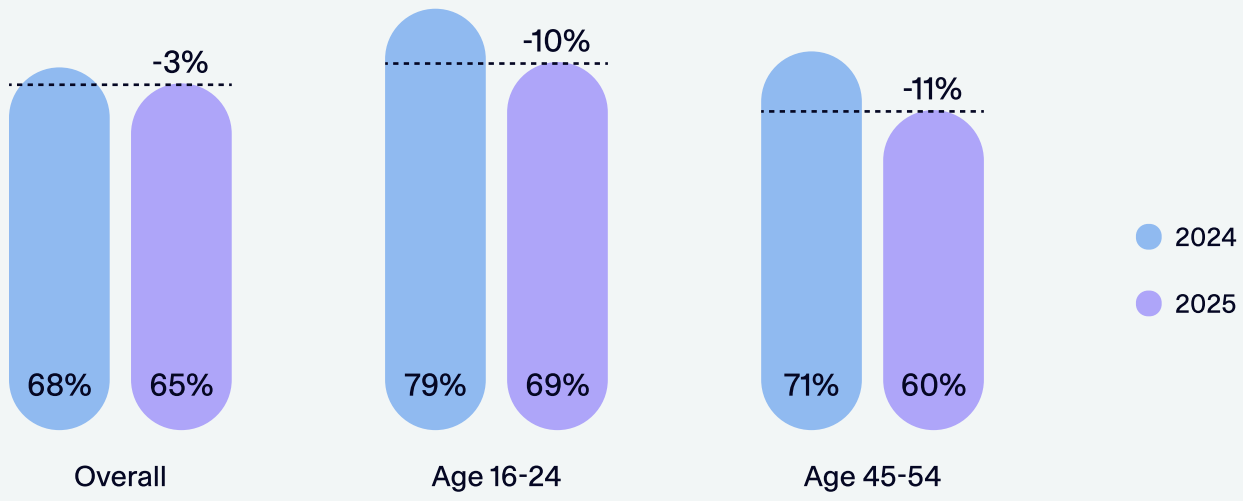
Connected TV was the top channel for ad attention, yet it was also perceived as the least secure for data privacy. Mobile in-app offers a compelling solution to this attention-trust gap.

Success requires geographic and demographic nuances

In advertising, we love a neat and tidy tagline — but the fine print matters, too. Geographic and demographic factors strongly shape consumer behavior. One telling example: In 2024, consumer confidence in privacy controls boosted trust and willingness to share data. This year, the top line looks stable: 65% of those who shared an opinion agreed that they felt more in control of their privacy settings, down slightly from 68% in 2024.

But that small dip masks significant shifts. The youngest age group (16-24) and peak income earners (45-54)[4] each saw drops of at least 10 percentage points. Publishers aiming to earn user trust (and data) may need distinct strategies for each of these age groups.

I feel like I have more control over my privacy settings than I had two years ago, and so I trust sharing my data more.

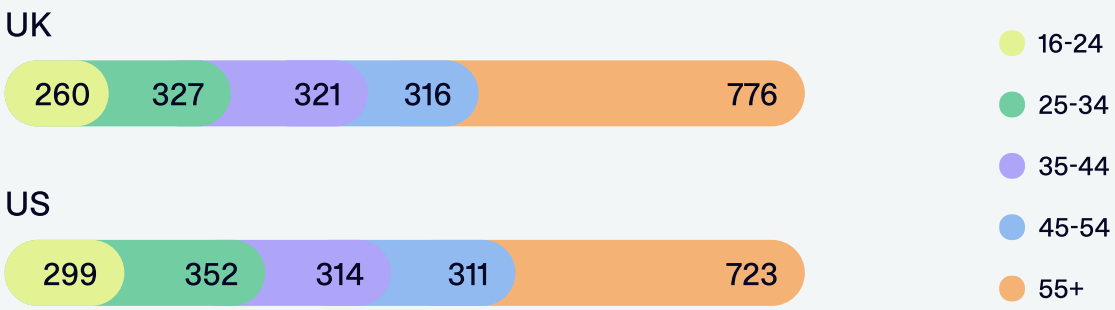


[4] US Bureau of Labor Statistics, 2025

Methodology

The research survey was conducted by Censuswide on behalf of Verve between August 13 and August 19, 2025.[5] Quantitative data was gathered via an online survey from a total of 4,000 respondents aged over 16 across the UK and US. The nationally representative respondent base featured an even split of 2,000 consumers in the UK and 2,000 in the US, in addition to covering a mix of genders and five core age groups: 16-24, 25-34, 35-44, 45-54, and 55 plus.

Year-over-year comparisons reference Verve's 2024 In-App User Privacy Report, for which CensusWide collected data from 4,001 consumers evenly split between the UK and US; this survey was conducted during August 2024.



[5] Censuswide abides by and employs members of the Market Research Society which is based on the ESOMAR principles. Censuswide is also a member of the British Polling Council.

Introduction

Screentime is at an all-time high. Globally, consumers now spend 3:48 hours each day on mobile devices[6]. If you're getting eight hours of sleep per night, that's a quarter of your waking hours on your phone.

All these hours generate a wealth of data that can transform how publishers monetize apps and how advertisers reach their audiences. But with stricter privacy regulations and new technological controls like Apple's ATT framework, consumers now have more agency over who can access their data.

It's been nearly a decade since GDPR passed, and privacy regulations have continued to expand in scope and influence. At the same time, tech platforms are phasing out personal identifiers, pushing the industry toward privacy-first alternatives. Together, these forces have redefined how advertisers, publishers, and tech partners use data to engage users.

But the real question is:
What do the users themselves think?

We initially published this survey in 2024 with a focus on in-app advertising. Recognizing that mobile exists within a rich tapestry of cross-channel media experiences, we expanded the survey in 2025 to touch upon connected TV and web while preserving the ability to glean year-over-year changes where possible.

[6] EMARKETER, Global Media Intelligence Report, 2024

Shifts in willingness to share data

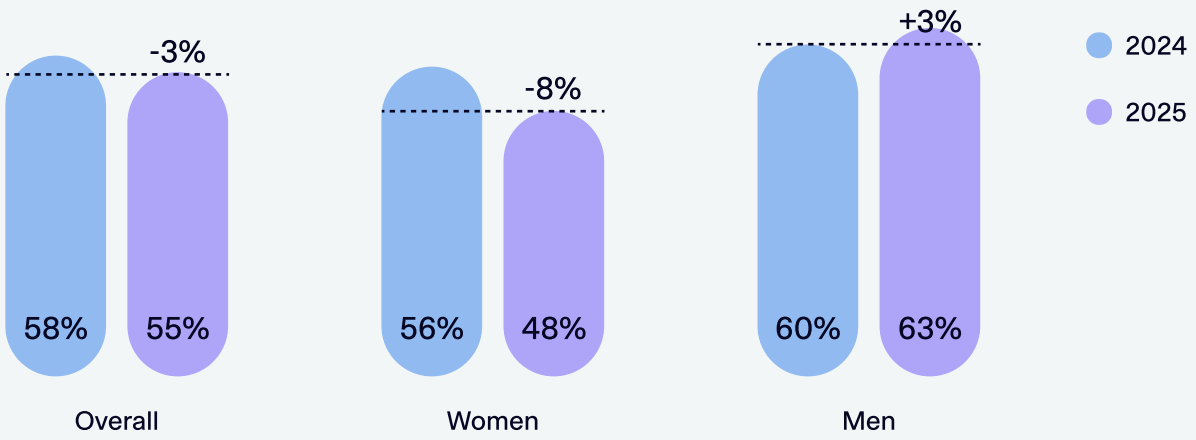
Factors shaping willingness to share data

Consumers are most willing to share data when they understand how it's used and feel in control of it. Transparency and user choice directly determine how much and what kind of data people are willing to provide.

Understanding of data

Knowledge is power, and consumers who feel confident in their understanding of their data feel more empowered to share it. In both the US and UK, the survey found that about 55% of respondents who shared an opinion felt more likely to share their data due to understanding it better than two years ago. However, the data revealed significant demographic differences among respondents.

Agree (net): “I am more willing to share my data on apps than I was two years ago, because I understand it more”



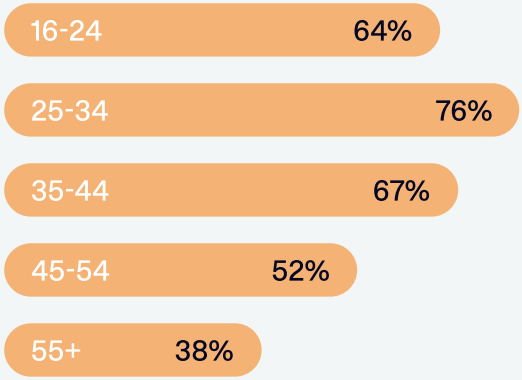
While men reported that a stronger understanding of their data made them more likely to share it, women reported the opposite.

Year over year, men gained 3 percentage points in likeliness, while women lost nearly triple that amount.

This sense of caution is echoed in women’s responses regarding which types of data they’re willing to share with various apps and platforms. For example, 26% were willing to share their mobile number with finance apps, but only 9% were willing to do the same for news apps.

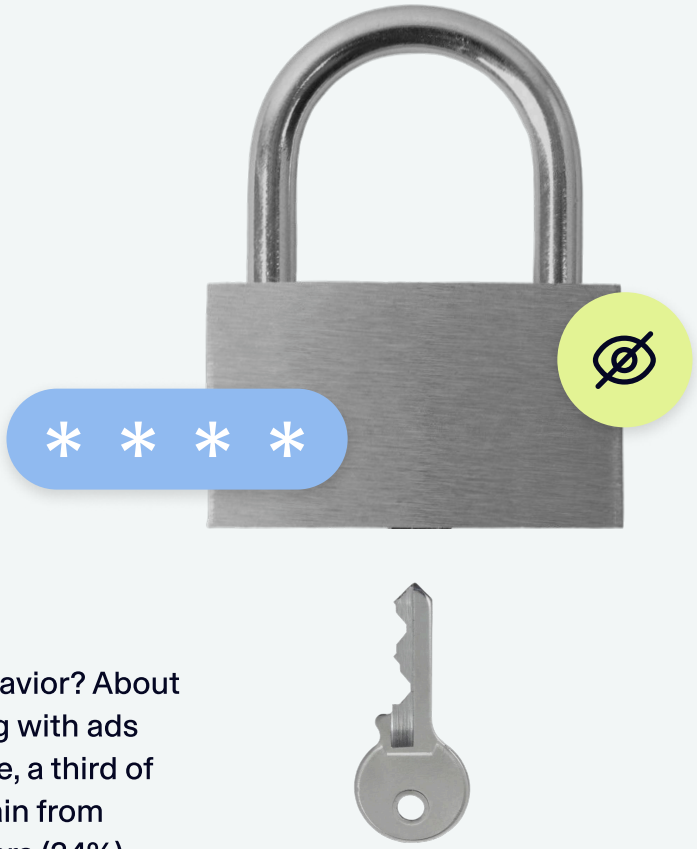
We also see major generational gaps, including a nearly 40-point disparity between the most confident (76.2% of 25-34 age group) and the least confident (37.5% of the 55+ group).

More likely to share data due to understanding it better



Control over privacy settings

Privacy controls are an important step forward, but they haven't eliminated user hesitation. While 65% of respondents said better controls make them more likely to share data, the trend is slipping (down from 68% last year). Younger users (16-24) saw the sharpest drop in confidence, falling 10 percentage points, with respondents aged 45-54 reporting a similar decline.



How do these privacy concerns affect behavior? About half of consumers regularly avoid engaging with ads across mobile, CTV, and web. On CTV alone, a third of those who do feel more in control still refrain from interacting with ads because of privacy fears (34%).

Jobie Tan VP, Business Development - Supply

"When ads are delivered in the right context, they capture attention and invite action. Poor contextual alignment can erode consumer trust and damage brand equity. Success lies in pairing relevance with responsibility."

What types of data are consumers willing to share — and who gets access?

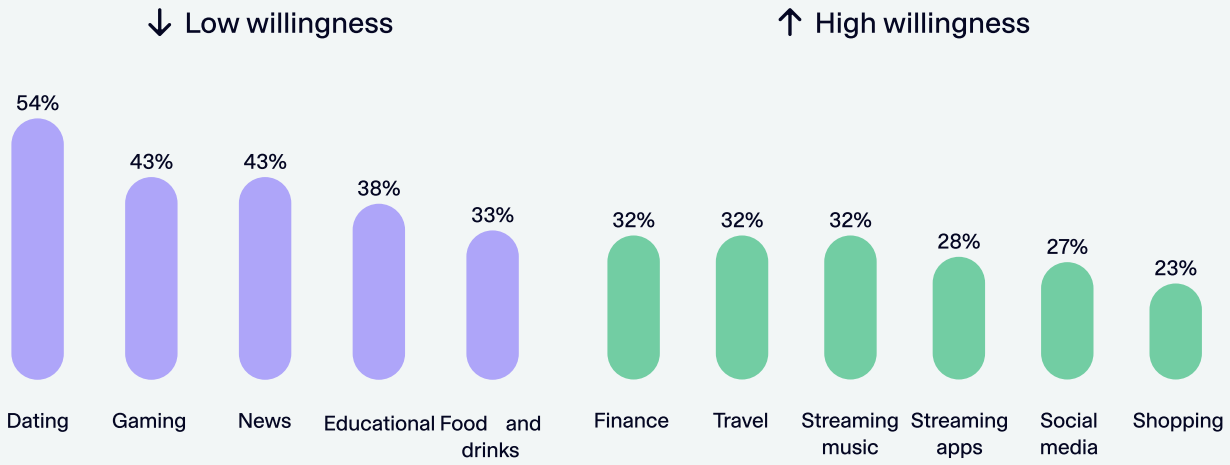
Depending on the environment, consumers have different willingness to share their data. Surprisingly, CTV was the environment where users were most willing to provide their email address. This could be a sign of reduced login friction, with improved user experience that eliminates typing with a remote control via QR codes and other cross-device solutions.

For mobile apps, consumers were more likely to share more personal details like name, gender, region, and age/DOB. Understandably, the mobile app environment was also where users were most likely to share their mobile number. Mobile web fared poorly across most types of data requests, perhaps due to UX challenges.

	CTV platforms	Mobile web	Mobile apps[7]
My email adress	37.8%	32.5%	35.3%
My name	32.8%	28.7%	33.0%
My gender	30.5%	30.4%	32.8%
My region	24.7%	23.7%	24.6%
My DOB/age	22.9%	21.5%	24.7%
My ethnicity	20.5%	22.0%	21.5%
My mobile number	18.5%	16.4%	19.4%
My health data	7.5%	8.6%	8.5%

[7] Average willingness across all 11 categories of mobile apps evaluated.

Share of respondents not willing to share any personal data with this type of app/platform



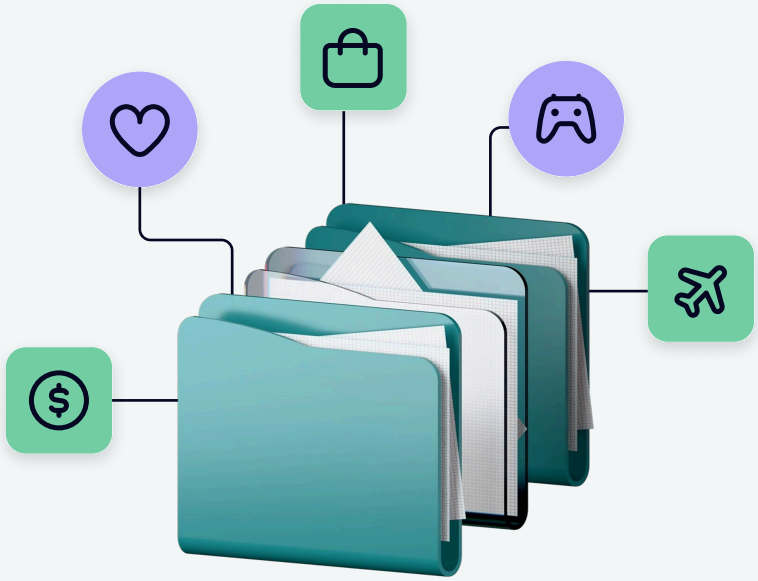
Mobile app categories

Drilling into mobile apps only, the survey respondents were least willing to share any data with dating, gaming, and news apps. On the other hand, they were most willing to share some data with shopping, social media, and streaming apps.

This makes sense from the user perspective: why would a game need to know someone's gender to accomplish its primary function of entertainment?

Meanwhile, contact information (especially email) is required to log into social media and streaming accounts.

For shopping, sharing data with the publisher is a matter of practicality: payment and shipping details are required to get the physical product being sold on the app.



What personal data, if any, are you willing to share with the following apps? (Select all that apply)

	Average	Email	Gender	Name	Age/DOB	Region	Ethnicity	Mobile number	Health data
Shopping	30.1%	47.3%	38.2%	41.1%	26.8%	29.6%	22.8%	26.8%	8.3%
Finance	29.3%	41.0%	36.0%	38.3%	32.4%	26.6%	24.7%	26.6%	9.2%
Social media	28.8%	37.2%	42.3%	42.1%	30.1%	26.1%	25.3%	18.6%	8.8%
Streaming apps	27.8%	43.9%	39.0%	38.6%	27.2%	26.7%	22.3%	21.3%	8.0%
Travel	27.8%	39.0%	34.6%	35.3%	26.8%	30.1%	23.3%	23.4%	10.0%
Food & drink	24.7%	34.6%	37.4%	32.6%	21.6%	25.6%	20.5%	21.0%	11.2%
Streaming music	24.4%	37.4%	33.7%	31.9%	24.2%	23.3%	20.5%	18.6%	7.7%
Educational	24.3%	33.7%	28.0%	31.3%	24.8%	23.1%	22.4%	17.9%	9.2%
Gaming	19.6%	28.0%	37.5%	25.7%	20.0%	18.0%	16.8%	13.8%	6.9%
News	19.4%	26.9%	26.1%	23.2%	17.4%	22.9%	18.4%	12.9%	7.5%
Dating	18.7%	19.8%	19.8%	23.3%	20.5%	18.7%	20.0%	12.9%	7.1%

Year-over-year findings across all app categories

The data reveals a sophisticated privacy mindset emerging in 2025, where users are:

More protective

of highly identifying information (names, contact details).

More open

to sharing demographic and contextual data (health, location, personal characteristics).

More selective

rather than completely sharing-averse across most app categories.

↘

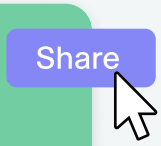
Decreased willingness to share

- Name
- Email address
- Mobile number

↗

Increased willingness to share

- Health data
- Gender
- Age/DOB
- Regional information



App category highlights

Dating apps

Remain the most privacy-sensitive category (54% unwilling to share any data)

Shopping apps

Highest willingness for email sharing (47%) but significant name-sharing decline

Social media apps

Greatest reduction in privacy refusal (-11%), suggesting growing acceptance

What personal data, if any, are you willing to share (Select all that apply.)

	2024	2025	Change	Change %
My name	38.3%	33.0%	-5.3 pp	-14%
My email adress	37.0%	35.3%	-1.7 pp	-5%
My gender	31.5%	32.8%	1.3 pp	4%
My mobile number	21.8%	19.4%	-2.4 pp	-11%
My DOB/age	23.4%	24.7%	1.3 pp	6%
My region	20.5%	24.6%	4.1 pp	20%
My ethnicity	20.9%	21.5%	0.4 pp	3%
My health data	6.6%	8.5%	1.9 pp	29%
Not willing to share any data	36.2%	35.1%	-1.1 pp	-3%

2025 data includes all seven categories from 2024, with the addition of streaming apps, streaming music, and news categories. On average, the differences between data type willingness to share with seven vs. ten app categories came to 0.1%. In the interest of offering the most complete data possible, the 2025 data in this table reflects all ten app categories.

You can find the granular data for all app categories in the appendix.

Takeaways

Implications for publishers

Even if more data means better targeting that boosts ad inventory value, overstepping can turn off users and lead to churn. Align your data requests with your users' expectations of the app — and communicate the value of data-sharing. For example, providing regional information makes sense in a news app context: the user understands that they will see locally-relevant content. A gaming publisher can also provide value with data about a user's location, perhaps offering seasonally-themed content.

Implications for advertisers

Lean into contextual and cohort-based targeting that can deliver strong campaign performance without requiring personally identifiable information. If you already have first-party data from your existing customers, work with your adtech partners to ensure messaging appears in an ideal in-app context.

The value exchange model

User monetization preferences

Consumer sentiment around ad-supported experiences is shifting. This year, 75% of respondents said they're willing to accept ads in exchange for free content, up from 67% in 2024. This jump reflects the growing recognition of the value exchange that advertising enables.

But stated preferences only tell part of the story. While around a quarter of consumers claim to dislike ad-supported models, far fewer actually pay for content. In dating apps, only 7% of users pay for premium features, and less than 2% of mobile gamers make in-app purchases. [9, 10]

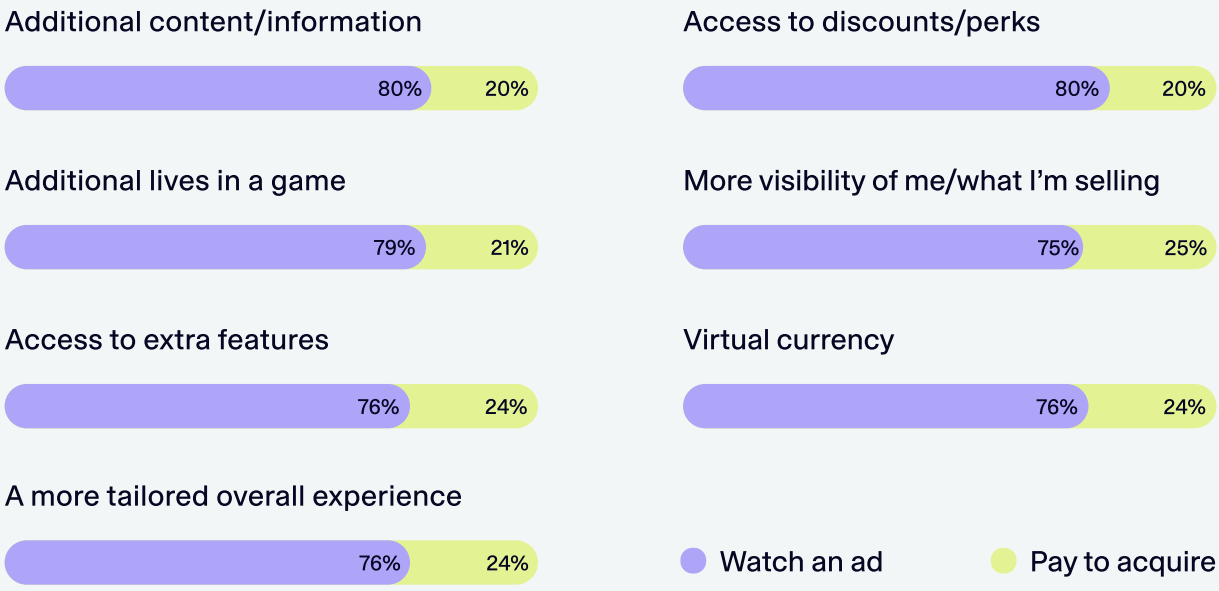
Agree (net)[2]: "I am more willing to watch/receive advertisements in exchange for free content than I was two years ago."

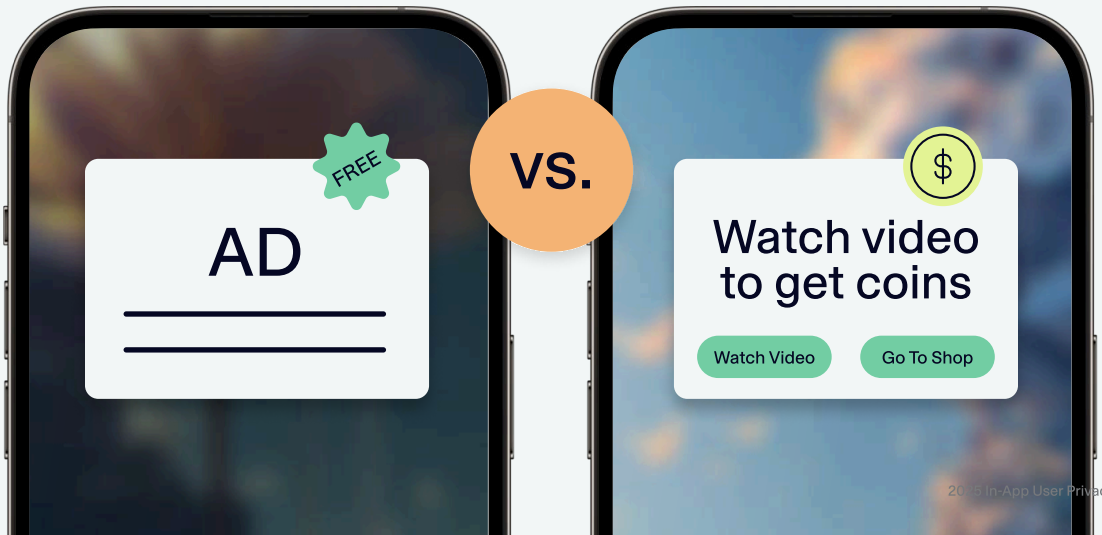
[8] Agree (net) combines "Strongly agree" and "Somewhat agree" responses.
[9] Business of Apps, Dating App Revenue and Usage Statistics (2025)
[10] PocketGamer, Mobile Growth and Monetization Report (2024)

Free vs. paid content

Digging deeper, we asked users which app benefits they would prefer to watch an ad to acquire. Regardless of the benefit, the majority of users would always prefer to watch an ad rather than pay. This reinforces the strong role of rewarded and value-exchange formats in app monetization.

Of the list of additional app benefits, would you prefer to pay or watch an advert to acquire them?



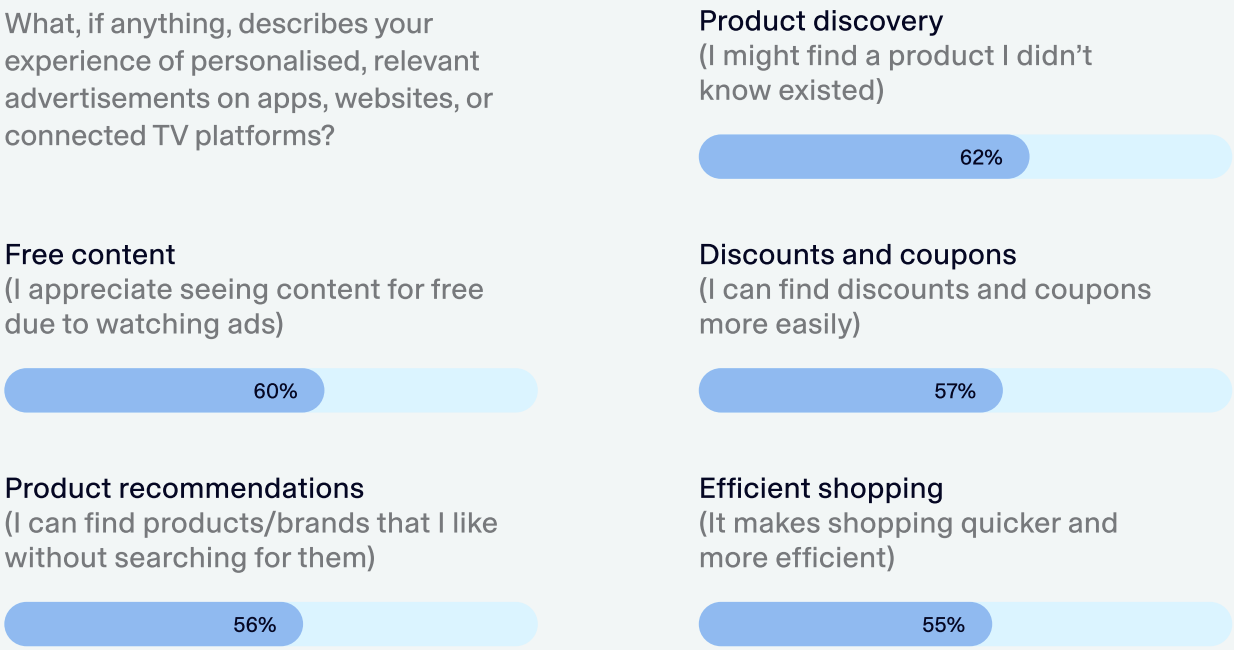


Effects of relevant advertising

A crucial factor in how consumers feel about advertising is the content of the ad itself. Almost three-quarters (72%) said they would be less likely to pay to remove ads if those ads are targeted and interesting. Relevance can transform ads into an engaging and valued part of the in-app experience.

User experience

Despite ongoing privacy concerns, consumers clearly recognize the benefits of relevant advertising. Product discovery, free content, and discounts topped the list of positive outcomes users associated with personalized ads. Contextual relevance and precision targeting are now critical to improving brand perception, accelerating shopping intent, and driving returns across the funnel.



Brand perception

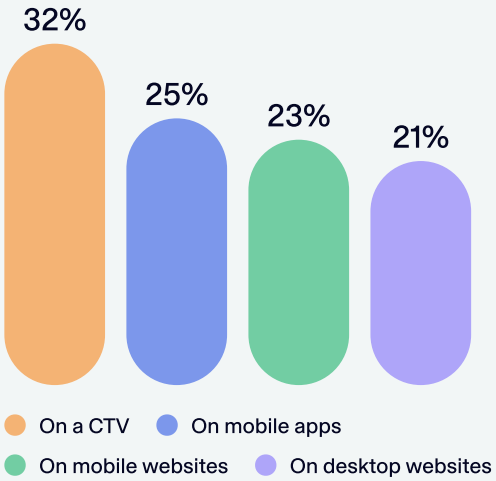
Context matters. Nearly half of respondents said that relevant ads (e.g., sports ad in a sports app or beauty ad in a beauty app) are the most appealing to them. Almost the same number (48%) noted they are most likely to engage with such ads.

The opposite also holds true: 49% of respondents said that seeing a contradictory ad placement (e.g., sports ad in a beauty app or beauty ad in a sports app) would discourage them from engaging. Even more concerning for brands: 43% reported that such a mismatch would negatively affect their perception of the brand itself.

Jobie Tan VP, Business Development - Supply

"When ads are delivered in the right context, they capture attention and invite action. Poor contextual alignment can erode consumer trust and damage brand equity. Success lies in pairing relevance with responsibility."

Where are you most likely to pay attention to an advertisement, if it is relevant to you? (Select up to 2.)



Advertising channel

Among channels, CTV emerged as the most powerful environment for relevant advertising, with 36% of respondents saying they are most likely to engage with relevant ads while streaming. Mobile apps (28%) and mobile web (26%) follow closely, but the immersive nature of CTV makes it a uniquely valuable environment for advertisers.

PARTNER PERSPECTIVE

John Koetsier
VP Insights, Singular

Future outlook and emerging trends: Privacy in mobile marketing

When given a direct choice, people choose privacy. At Singular we see that in global opt-in rates to Apple's App Tracking Transparency. As we shared in our Q3 2025 Quarterly Trends Report, globally only 6.26% of people globally opted into tracking. But there's context to consider. Because in the Utilities genre, 34.2% opt in. And in Gaming, 21.68% of people opt in. In both cases, opting in often promises additional value to users.

So the bigger story here is that without context and without incentive, people choose privacy almost without fail. However, with a direct ask that includes insight into why a brand wants a particular piece of data, and possibly a benefit or reward for providing it, many more people will share at least some of their data.

The takeaway is that companies that fail to deliver meaningful value in exchange for data don't get that data. Apps must be clear about the benefits of sharing personal data, whether that's through personalized offers, premium features, or ad-free experiences.

Technology and regulatory landscape

Despite expanded privacy regulations, in some ways marketers are getting more data than ever before. Meta's Advanced Mobile Measurement is back, Google's releasing Integrated Conversion Measurement, and all the big platforms have programs like Advanced SAN or Aggregated Event Measurement that provide significant insight into customers, users, and players' journeys with mobile apps.

There are some caveats, of course. Most of these are provided only via mobile measurement partners (MMPs), who need

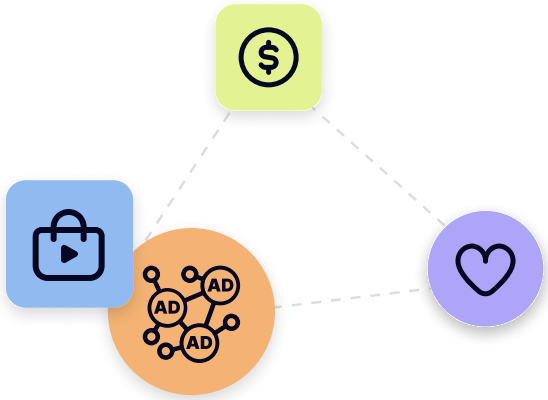
contractual agreements with the platforms and are bound to privacy terms. Others, like Meta's AMM, require app publisher opt-in with specific commitments around privacy.

And while these don't replace device identifiers like the IDFA, they provide a wealth of data that in aggregate, with SKAdNetwork and first-party data, can provide unified measurement that rivals what we had before.

Why? Because now we have a broader, more contextual understanding. We're not just basing everything off a single last-click touchpoint anymore. Laws will continue to evolve, and platforms will continue to change. But in some ways, we're seeing 2025 and on as an emerging golden age of marketing measurement.

Innovation opportunities

The key innovation right now is what Singular calls Unified Measurement. That's taking all the available data points from platforms, ad networks, app stores, and first-party data like app activity, engagement, and purchases, and combining it to arrive at deep, contextualized, and rich attribution. This is what Aperture's Hannah Parvaz calls "triangulation." It's truthy, not necessarily 100% truthful. But it's close enough for successful campaign optimization and bids and budgets allocation. And let's be honest: last-click device identifier-based attribution was never the full story.



Privacy matters. Doing the right thing matters. That's just good business, and it's also good optics. The good news for marketers is that within that context, we've seen a significant evolution since ATT and Privacy Sandbox launched. Now, arguably, with more data points, more context, and more insight from different angles, we have an opportunity to create better attribution and marketing measurement than we had before privacy became as important as it now is. The future is bright!

Takeaways

Implications for publishers

Ad-supported models remain the most sustainable path to monetization, and the data proves it. Crucially, relevance determines success: users are more tolerant of ads when creatives are targeted, engaging, and aligned with the app experience. This means prioritizing rewarded formats, and partnering with platforms that can ensure ad quality and contextual fit, are key to maximizing revenue while keeping users satisfied.

Implications for advertisers

The data underscores a clear opportunity: consumers reward relevance. Ads that align with context and consumer needs drive engagement and strengthen brand perception. Conversely, misaligned placements risk wasting spend and damaging trust. To maximize outcomes, prioritize contextual strategies and privacy-first targeting. And pay special attention to high-impact environments like CTV where relevance is most likely to capture attention and drive measurable results.

The personalization-privacy paradox

Consumers are conflicted about personalized advertising. Although our data shows that they recognize the value of personalized ads, the emotional response isn't always positive.

We asked: "How do you feel when an advertisement seems personally relevant to you, based on your behavior or preferences, if you feel anyway at all?" Respondents could select as many responses as they liked (as long as they didn't also select N/A).[11]

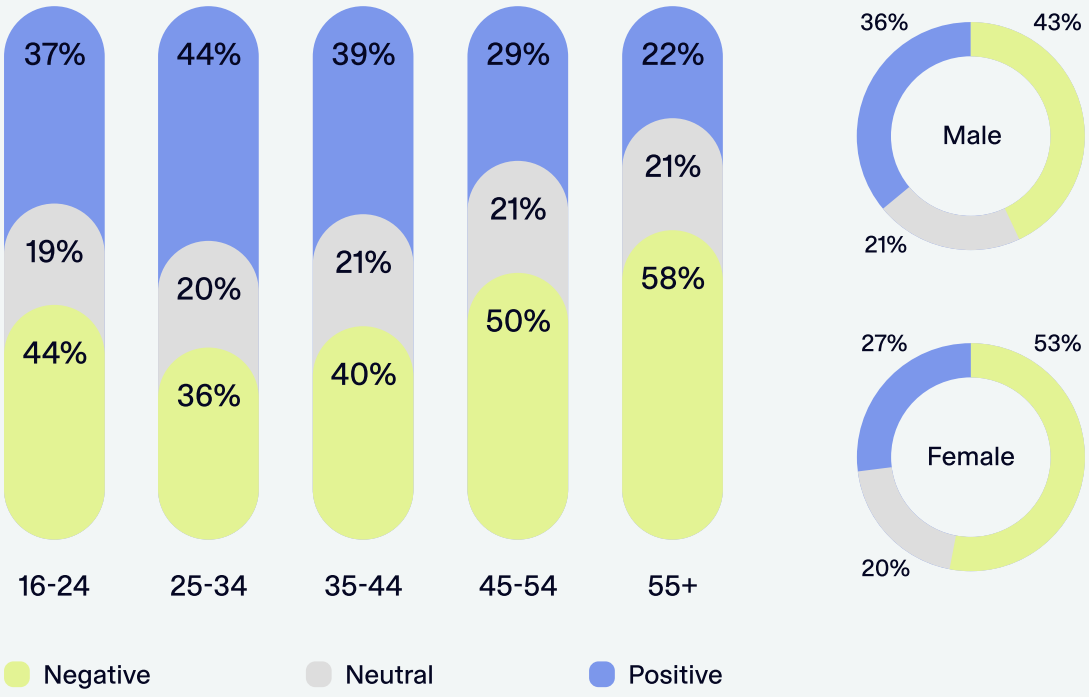
Positive	I feel that my data is being used in the correct way I feel appreciated and understood I feel that the advertisements enhance my user experience The advertisements are nice but don't impact my app experience
Neutral	I feel that the advertisements have been tailored for me N/A - It doesn't make me feel any particular way
Negative	I feel that my data is being used incorrectly It makes me feel like I'm being watched I feel uneasy about how my data is being used I feel my privacy has been breached

[11] A note on methodology: in one of our 2024 survey questions gauging consumer perceptions of personalized ads, respondents could also select as many options as they liked. The 2024 options tended to be more favorable to advertisers and publishers. We revised the options in 2025 to offer a more balanced perspective, but this nullifies year-over-year comparisons.

Our survey highlights clear demographic divides in how consumers perceive personalized advertising. Younger audiences (16–44) are the most receptive, reporting more positive associations with personally relevant ads. By contrast, consumers 55 and older are much more skeptical (58% selected negative responses), making them the most resistant audience.

Gender differences were also notable: women were more likely to report negative feelings (53%), while men expressed a higher share of positive sentiment (36% compared to 27% for women).

Sentiment toward personalization

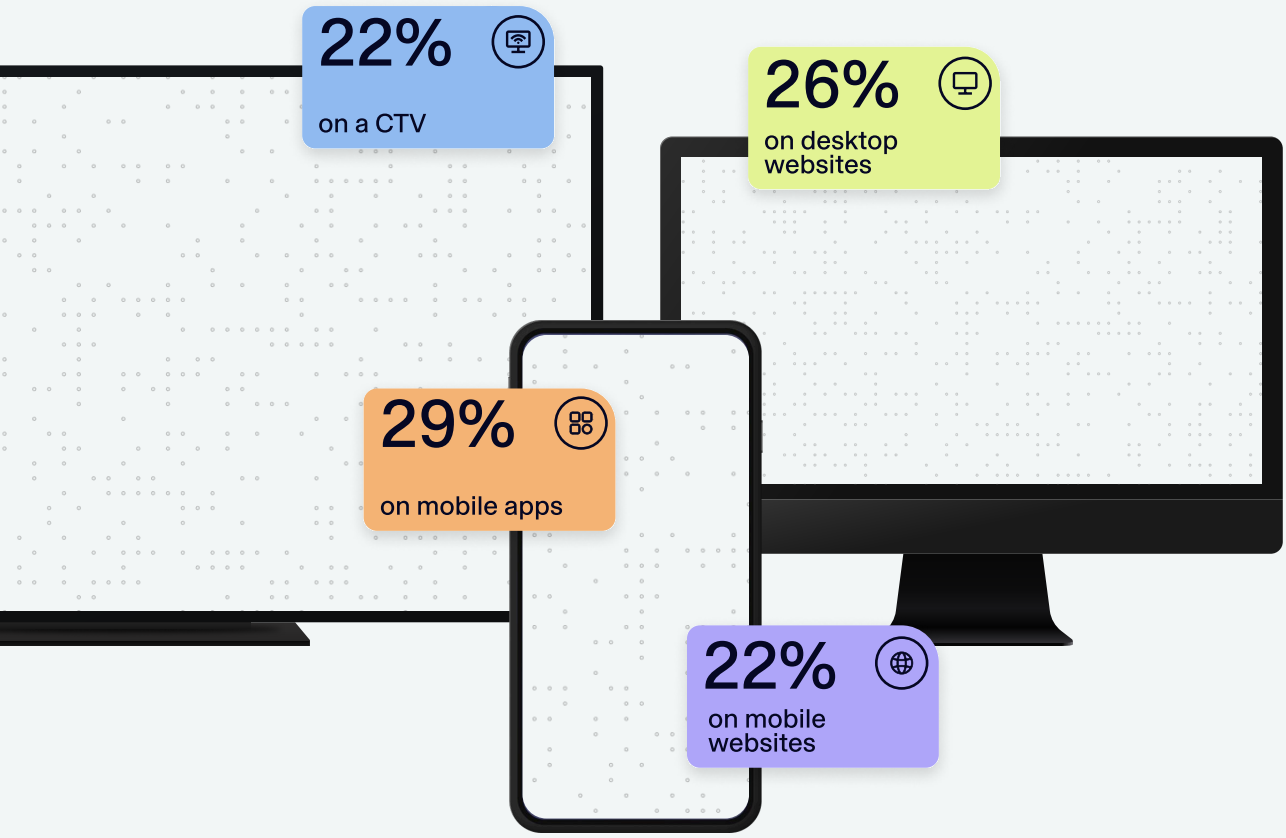


For advertisers, these findings underline the importance of tailoring personalization strategies by audience. To reach more cautious audiences, a value-driven approach that emphasizes relevance without overstepping privacy boundaries is key.

Device/platform differences

The personalization-privacy paradox also plays out differently across devices and platforms. While privacy concerns remain a barrier everywhere, our survey shows that trust shifts depending on the context.

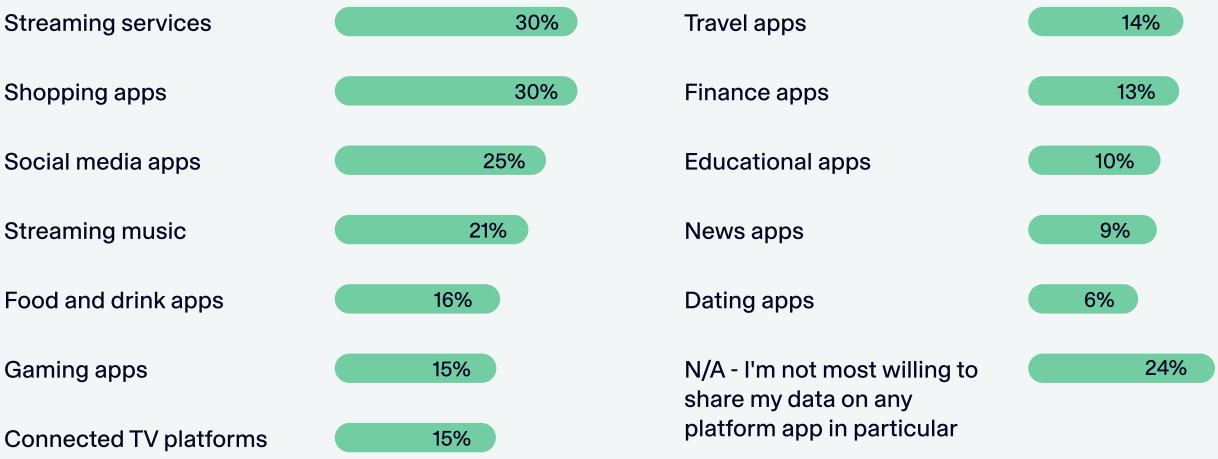
On which platforms, if any, do you feel your personal data is most protected? (Select up to 2.)



Mobile apps may be the most-trusted environment overall (and CTV the least-trusted), but the picture changes when you zoom in on individual categories.

Streaming services and social media apps actually top the list, suggesting that consumers are most open to sharing data in contexts where they see clear value in exchange for personalized recommendations or tailored content.

What type of app or platform, if any, are you most willing to share your data on? (Select up to 4)



Steve Gordon Senior Director, Partnerships - EMEA

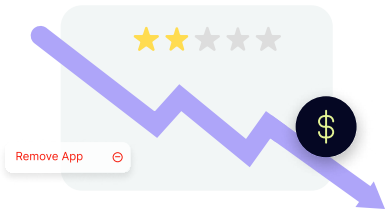
"Strategies around data collection need to be tailored to device contexts. For personalized advertising to work effectively across all groups, publishers and advertisers must be transparent about which data is collected and how it's used. Clear communication and user-friendly privacy controls can help build trust, reduce resistance, and make personalization feel like a value exchange rather than a privacy trade-off."

PARTNER PERSPECTIVE

Amnon Siev
CEO, GeoEdge

How publishers can improve trust through high-quality ad experiences

In-app user trust is fragile, won slowly and lost in an instant. It can be undone by a single auto-redirect, a fake close button, or an ad disguised as a trusted brand. Users do not think in terms of “ad quality”; they think in moments. One intrusive ad is not just a bad impression, it often rewrites their entire perception of the app.



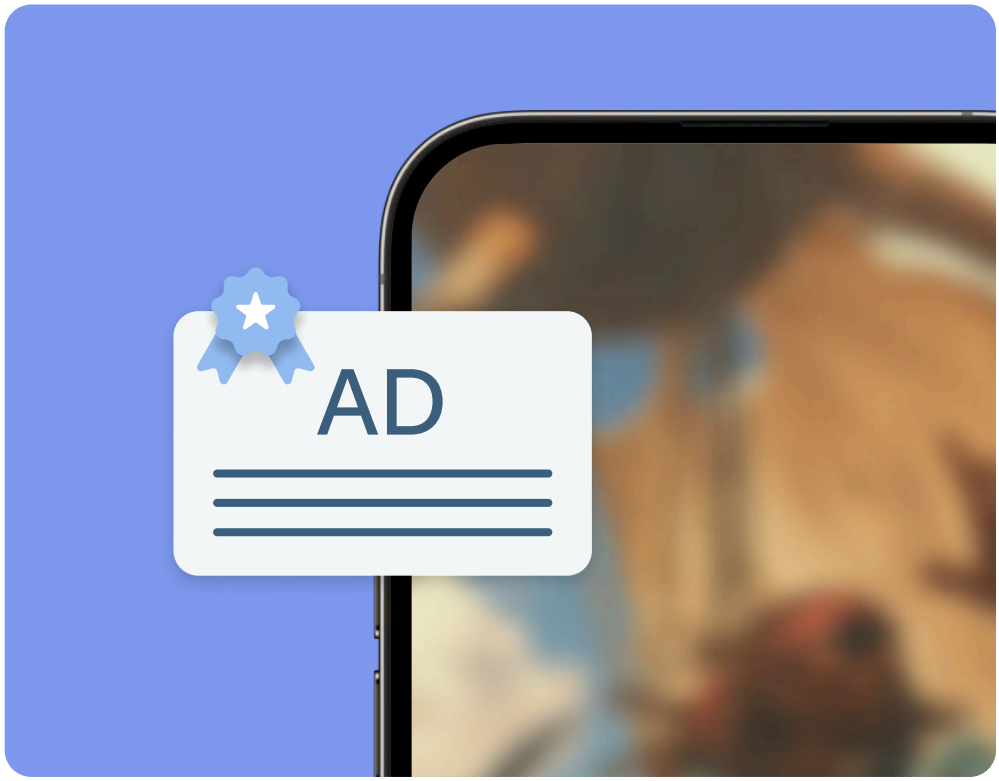
Once trust is broken, the damage ripples through every metric that matters: session depth declines, retention drops, ratings suffer, and ultimately, revenue takes a hit.

Across the mobile ecosystem, bad ads have become a common and costly part of the user experience. While bad ads can take many forms, their impact is consistent. Low-quality in-app ads appear across three layers: malvertising, poor quality or disruptive behavior, and problematic creative content. Each disrupts the user journey, replacing moments of seamless engagement with friction, adding frustration where there should be flow, and putting long-term monetization at risk. When bad ads break immersion, users are more likely to abandon sessions early, churn entirely, or leave negative reviews that deter new downloads.

When advertising is designed to complement, not compete with, an app’s context, audience, and content, it transforms the value exchange between publisher and user. Publishers can get there by applying ad quality standards to every

session, across all formats and geos, to block deceptive, dangerous, or disruptive creatives and deliver an immersive, trustworthy experience.

In the mobile economy, ad quality is no longer a maintenance task. It's a growth strategy. As recognizable as their design or gameplay. Trust built through positive ad experiences fuels deeper engagement, higher ARPU, and stronger loyalty. With competition for attention tighter than ever, the apps that pull ahead will be those that make ad quality a signature of their product, a clear commitment to respect, relevance, and reliability. These apps will not just capture attention; they will cultivate lasting loyalty, turning audiences into advocates and revenue into resilience.



Takeaways

Implications for publishers

Consumers are more open to sharing data in contexts where the value exchange is clear. Publishers should focus on making data practices explicit and giving users simple, intuitive privacy controls. This can help reduce resistance, while reinforcing the perception that personalization enhances rather than compromises the user experience.

Implications for advertisers

Personalization strategies must be audience-specific. Emphasize relevance and value without crossing perceived privacy boundaries, especially when targeting cautious groups. Channel context also matters. By tailoring personalization efforts and maintaining transparent communication, advertisers can balance effectiveness with user comfort, building longer-term engagement.

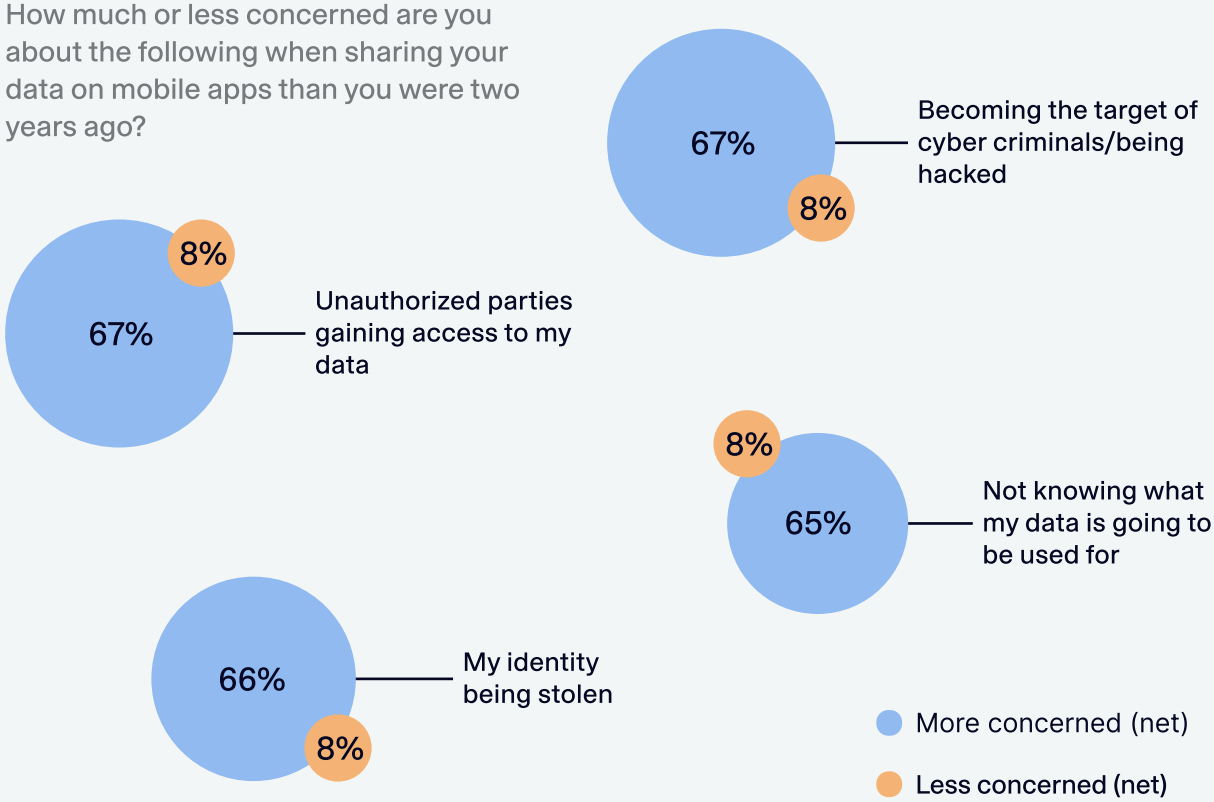
Privacy concerns and barriers to trust

Consumers' expectations around privacy have never been higher, and their concerns are only intensifying. To build trust, the adtech industry needs to address consumers' specific fears around data privacy.

Current concerns

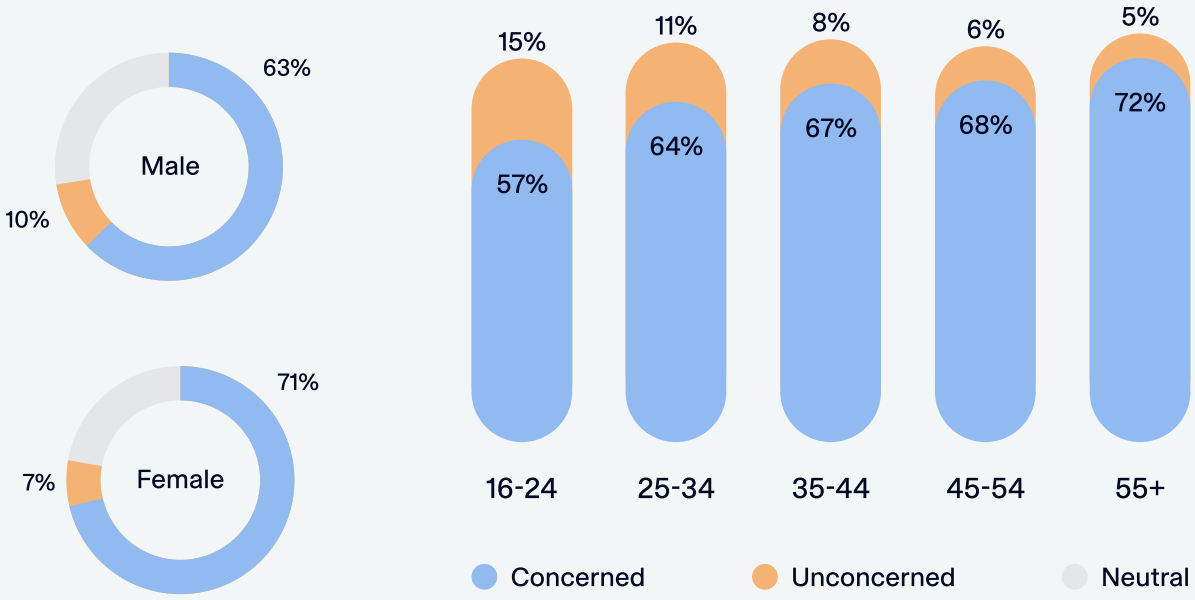
Consumer anxiety around data sharing has intensified dramatically over the past two years. Our survey shows that two-thirds of respondents are now more concerned about key risks such as unauthorized access (67%), cybercrime and hacking (67%), and identity theft (66%). Equally troubling is the lack of clarity around how data is used: 65% of consumers are increasingly worried about what their information is being used for.

How much or less concerned are you about the following when sharing your data on mobile apps than you were two years ago?



The rise in concern is not evenly distributed. Concern increased with age, and women registered the steepest increase. This points to demographic segments that publishers and advertisers will need to approach with particular care. Taken together, these findings signal that transparency, clarity, and robust security measures are essential for earning and sustaining consumer trust.

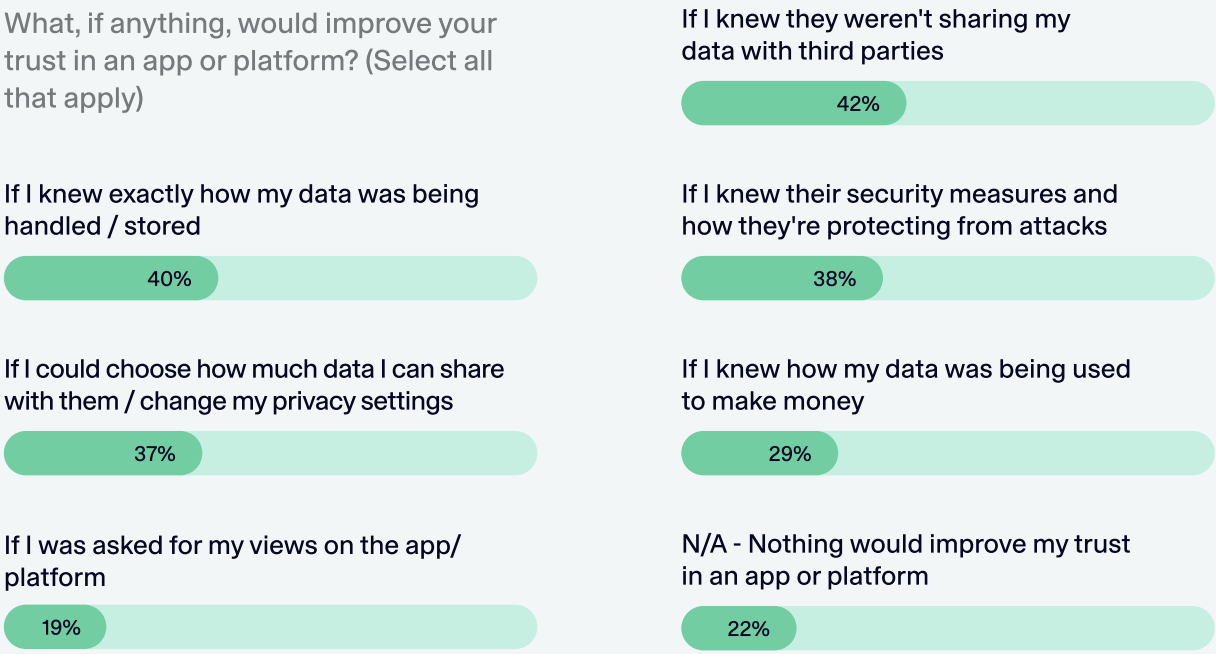
Who is most concerned about unauthorized parties gaining access to their data?



Improving trust

Trust hinges not only on compliance, but on proactive communication and user empowerment. Consumers want to see, and influence, how their data is being used. Nearly half of respondents said their trust would improve if they knew their data wasn't being shared with third parties, while 40% want more transparency around how their data is being stored and handled.

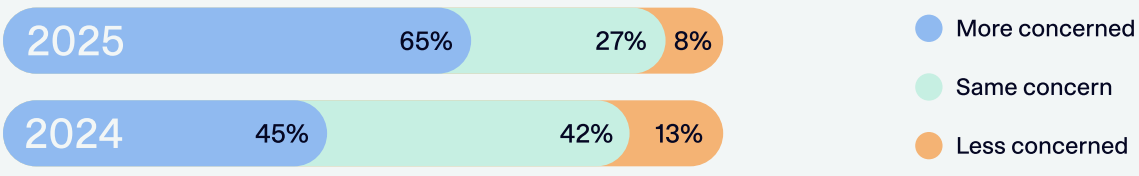
What, if anything, would improve your trust in an app or platform? (Select all that apply)



For publishers and platforms, addressing these concerns directly is no longer optional; it's essential to maintaining engagement and loyalty in an increasingly skeptical market.

The AI data training factor

A striking shift from 2024 to 2025 was the rise in consumer concern over how their data is being used in relation to AI. Nearly two-thirds (65%) of respondents said they are more concerned than they were two years ago, with a sharp 40% increase in the past 12 months alone.[12]



[12] 2024 "Same concern" data combines responses for "Same concern" (32.78%) and "Was never and am still not concerned about this" (9.26%). Excluded "Not sure" responses for year-over-year consistency.

This growing anxiety places additional pressure on publishers and platforms to strengthen trust. Communication around AI and data usage can no longer be vague or reactive; it must be transparent, proactive, and aligned with consumer expectations.

The data makes this crystal clear: an overwhelming 97% of respondents agreed that app publishers and platforms need to do more to be transparent about how consumer data is collected, handled, and applied.

Beyond communication about AI and data usage, publishers and platforms still need to do more to meet consumers' expectations. A striking 97% of respondents agreed with the statement that "app publishers and platforms need to do more to be transparent with how consumer data is used and handled."

Matina Thomaidou VP Data Science

"Consumer concerns around AI are at an all-time high, but it's important to remember that AI and machine learning have been foundational in advertising for years. The challenge now goes beyond advancing the technology. It's about bringing consumers along by showing them the usefulness, safety, and value of these tools in creating better, more relevant experiences."

PARTNER PERSPECTIVE

Davide Rosamilia
VP of Product, ID5.io

Beyond ATT: Why true in-app privacy requires more than just following Apple's rules

Apple's AppTrackingTransparency (ATT) framework has been marketed as a major win for user privacy — but in reality, it's a narrow, Apple-controlled policy that offers neither full compliance with global privacy laws nor a level playing field for publishers. Treating ATT as the definitive privacy standard is a mistake that can expose publishers to serious legal and commercial risks.

In the US, iOS leads as the mobile operating system, with about a 59% share compared to Android's 41%. In the UK, the market is split almost evenly: around 52% Android and 47% iOS. This means a privacy approach built around Apple's rules will miss nearly half the market in some regions. Even for iOS users, ATT is not a substitute for actual legal compliance.

Recent regulatory scrutiny in Europe has made this crystal clear. Competition authorities have found that ATT imposes onerous, multi-step consent prompts on third-party apps, while Apple's own apps avoid similar hurdles. This creates a structural disadvantage for independent publishers. In some jurisdictions, regulators are now investigating whether this amounts to an abuse of dominance, with significant fines already issued.

Even more importantly, following ATT does not guarantee publishers have met the legal requirements for valid consent, transparency, or lawful data processing. ATT is a set of platform rules designed to govern access to Apple's ecosystem, not to ensure compliance with privacy laws like GDPR or CCPA. In many jurisdictions, showing an ATT prompt without collecting proper, specific, and informed consent for all processing activities could still leave you in breach of the law.

Privacy regulations demand more:

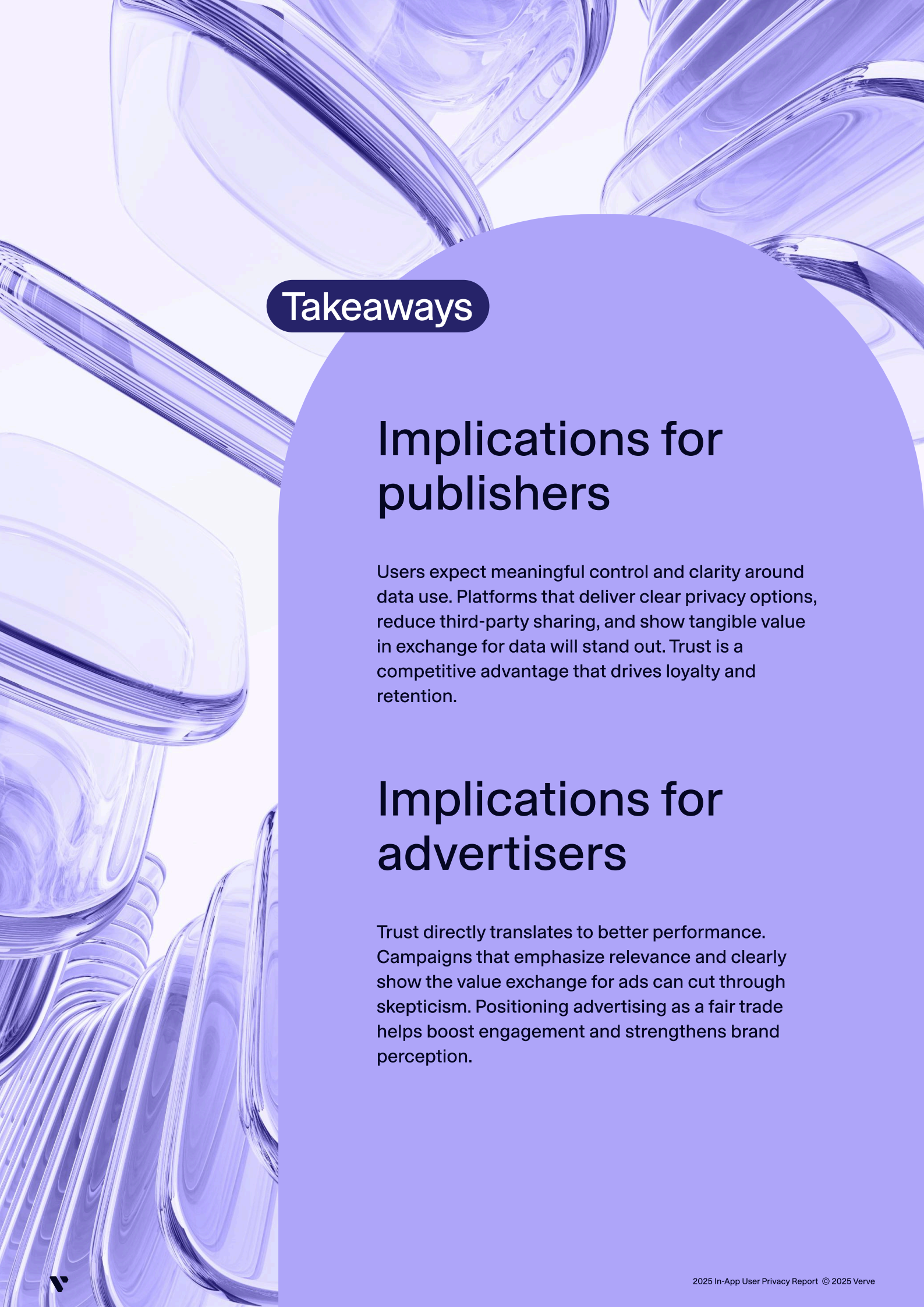
- Valid, explicit consent before tracking or using personal data.
- Transparency about the nature, purpose, and scope of data use.
- Equal treatment of all services, without bias toward platform owners.

In short, ATT does not ensure valid consent, prevent all tracking, or audit how data is handled once collected.

To truly protect users and remain compliant, publishers must go beyond ATT by:

1. Minimizing data collection
   Only collect the information you genuinely need, reduce retention periods, and design features that work for users who decline tracking.
2. Auditing SDKs and third-party integrations
   Maintain a complete inventory of all SDKs, understand what data they collect and where it goes, and contractually bind vendors to follow your consent framework.
3. Implementing robust identity solutions
   While these can also be deployed alongside ATT, consider identity solutions that enable privacy-safe audience targeting tied to explicit user consent, not device identifiers restricted by ATT.
4. Deploying a CMP
   Collect, record, and enforce consent in real time, ensuring it meets the strictest legal standards in the markets where you operate.

Relying on ATT alone is a compliance shortcut, and a risky one. Apple can control access to its ecosystem, but it is not the regulator. Only publishers can take responsibility for their legal obligations and in an era of increasing regulatory enforcement, doing the minimum is no longer enough.



Takeaways

Implications for publishers

Users expect meaningful control and clarity around data use. Platforms that deliver clear privacy options, reduce third-party sharing, and show tangible value in exchange for data will stand out. Trust is a competitive advantage that drives loyalty and retention.

Implications for advertisers

Trust directly translates to better performance. Campaigns that emphasize relevance and clearly show the value exchange for ads can cut through skepticism. Positioning advertising as a fair trade helps boost engagement and strengthens brand perception.

Conclusion

The survey findings point to a simple formula:

Trust = (Transparency × Value × Control) ÷ Data Requests

Consumers are clear about what they want: honesty, control, and tangible benefits in exchange for their data. For publishers, that means building stewardship into platforms. For advertisers, it means turning transparency into a performance advantage.

Critical success factors:

- Make privacy part of the product, not an afterthought.
- Communicate value clearly and consistently.
- Minimize friction and unnecessary data collection.
- Collaborate across the ecosystem to align standards and expectations.

Trust is the industry's most valuable currency. Publishers, advertisers, and tech partners that treat trust as the foundation of user engagement will not only meet rising consumer expectations but unlock the next era of sustainable growth.

About Verve

Verve has created a more efficient and privacy-focused way to buy and monetize advertising. Verve is an ecosystem of demand and supply technologies fusing data, media, and technology together to deliver results and growth to both advertisers and publishers — no matter the screen or location, no matter who, what, or where a customer is. With an eye on servicing forward-thinking advertising customers, Verve's solutions are trusted by more than 90 of the United States' top 100 advertisers, 4,000 publishers globally, and the world's top demand-side platforms.

Get in touch with us:
verve.com/contact

