tinuiti

A Marketer's Guide to **Consumer Sentiment Towards Online Privacy** in 2022

Introduction

In the past year, online privacy has taken center stage like never before. Tech companies instituted sweeping changes that have upended the online advertising landscape. Digital privacy laws went into effect from California to Maine, and another 23 states introduced legislation.

As a result, privacy is top of mind for consumers – but how does that awareness impact online behaviors? What information are consumers comfortable sharing on the web, and do they love or loathe targeting technologies that power today's digital advertising ecosystem? Ultimately, do they believe they have control over their own online privacy, or do they believe the government or businesses must offer more protections?

Tinuiti's second annual privacy study aims to explore the answers to these questions and more. Based on the responses of 1,000 U.S. consumers, this report reveals the attitudes that shape online behavior and preferences surrounding online privacy. With the survey findings as a guide, companies can chart a course toward marketing campaigns that resonate as cool – not creepy.

Key Findings

➔ **Consumers feel insecure about their digital privacy.** More than half say there's no such thing as online privacy, and just 1 in 5 believe they have control of their data. To protect themselves, nine in 10 consumers have taken some kind of proactive measure, with more than half having cleared browser cookies and turned off location tracking on mobile devices.

➔ **Consumers believe tech companies are ultimately responsible for protecting privacy.** More than half of consumers believe tech companies should do more to protect privacy, versus 43% of those who seek more government intervention; when asked which single entity or group is responsible for protecting online privacy, 44% named tech companies, 32% said consumers themselves are responsible, and 24% said government should take the lead.

➔ **Consumers most fear that their data will be misused for identity theft by criminals, with few concerned about commercial misuse.** At the same time, 27% believe the government should require tech companies to make opting out of online tracking easier, and another 24% say tracking should be completely illegal unless consumers explicitly opt in. A minority, 29%, believe government should focus on prosecuting criminal activity like identity theft and leave the rest to the private sector.

➔ **Among major tech companies, Amazon enjoys a strong reputation for privacy protection, and Google is the privacy leader for search.** But when it comes to social media, the majority of consumers either believe there's no difference among sites when it comes to privacy or don't know which offers the best protections.

➔ **On mobile devices, Apple is the perceived privacy leader over Android.** Privacy is an important purchase consideration for more than half of consumers, and most believe that mobile operating systems have improved safeguards in the past year.

➔ **The vast majority of consumers, nearly nine in 10, would rather view ads than pay for digital content or services, but 70% prefer to opt out of ad tracking.** Consumers are reluctant to share information beyond an email address in order to access a promotional offer.

9 in 10 consumers have taken some kind of proactive measure to protect their personal information.

Consumers Look to Tech Companies for Privacy Protection

Online privacy is on center stage like never before, and awareness is high of companies' privacy stances and mishaps. More than half of consumers now believe there's no privacy online and 9 in 10 have taken some kind of action to protect their personal information.

When it comes to societal solutions for privacy protection, consumers expect tech companies to lead. Commercial misuse of data isn't a top concern compared with criminal activity such as identity theft – but at the same time, consumers believe the government should go beyond crime prevention to regulate digital advertising.

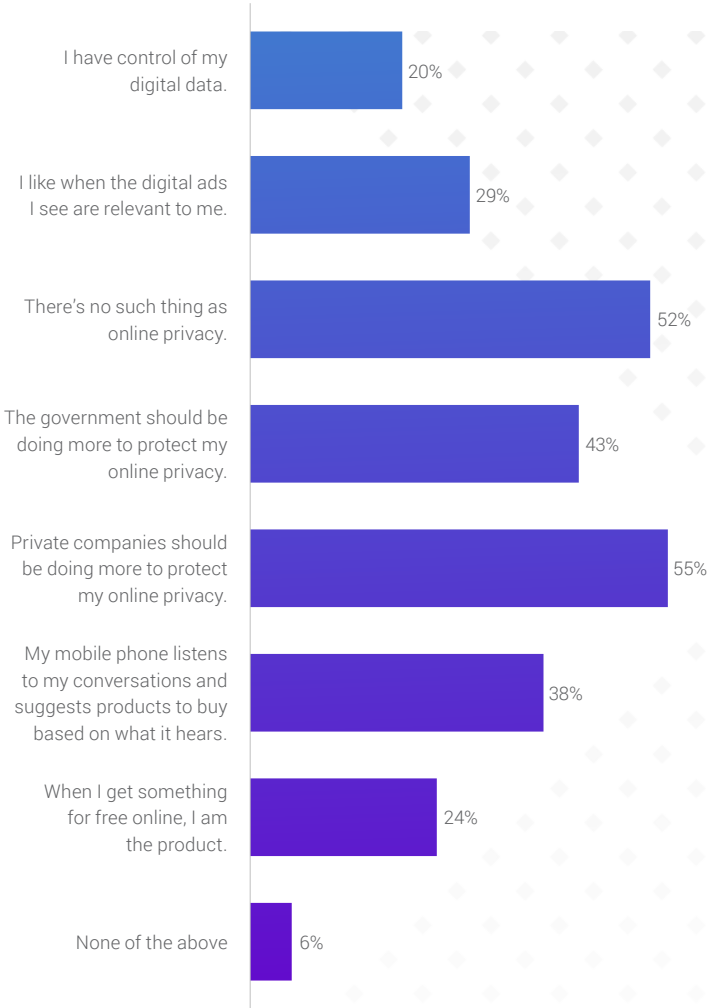
Online privacy is elusive, and consumers are wary

More than half of consumers, 52%, agree with the sentiment that "there's no such thing as online privacy." Just 1 in 5 believe they have control of their digital data.

These baseline beliefs fuel suspicion of constant surveillance: 38% of respondents believe that their mobile phones listen to their conversations and suggest related products. That percentage jumps to fully 50% among young adults ages 18 to 25; these members of Gen Z have unique concerns and beliefs spotlighted throughout this report, starting on page 9.

Personal targeting is unwelcome to most, with just 29% of respondents saying they like digital ads to be tailored to their tastes. Fewer still, 24%, agree with the trade-off implicit in targeted advertising – that is, when they get something for free online, they themselves (and their data) are the product.

Survey Question: Select all of the following sentiments that you agree with:



Consumers most fear criminal behavior

Online privacy concerns are primarily focused on criminal activity such as identity theft. Among entities or groups that might misuse their data, consumers are most concerned about criminals, at 44%. Women are more worried than men about criminal behavior, with 46% saying it's the top concern, compared with 40% of men.

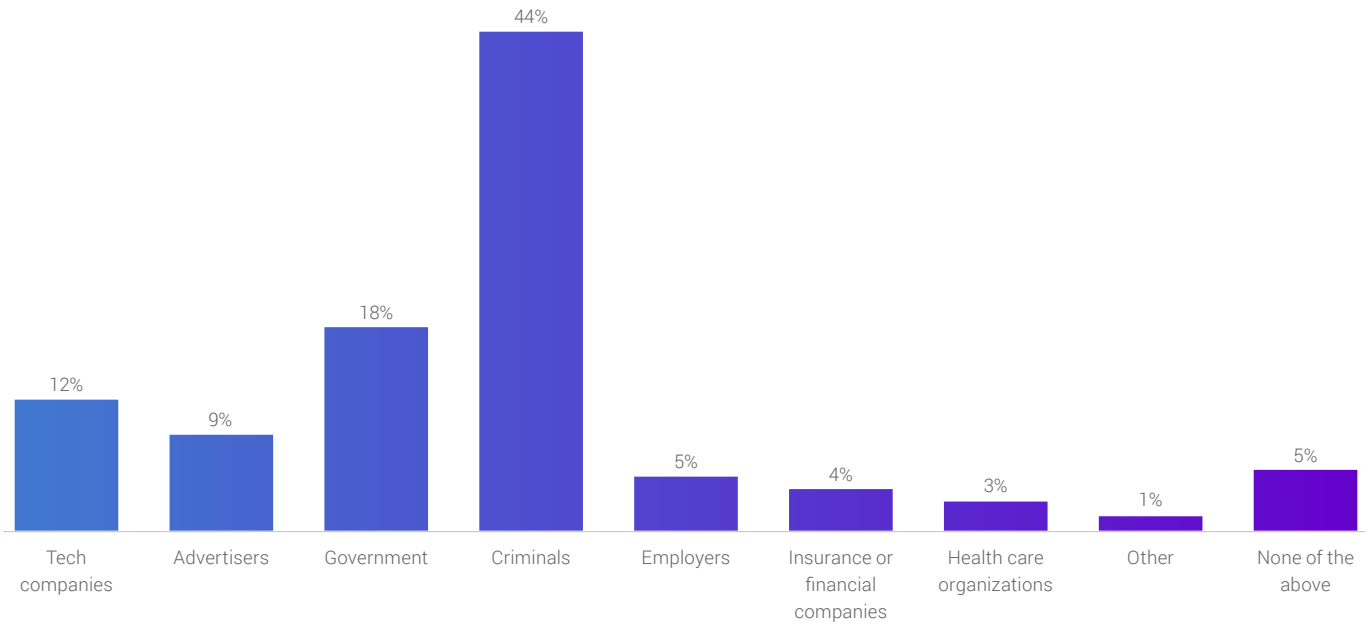
Similarly, when asked what types of data are most worrisome to have shared or tracked, information that could be used in identity theft is of highest concern, at 46%, while another 26% of respondents say they're most worried about safeguarding information about their financial situation, such as income, debt, or savings.

Relatively few consumers are fearful about misuse of data for commercial purposes: 12% say they worry most about tech companies, and 9% are most concerned about advertisers, while only 8% say they're most worried about products or websites they've viewed online being tracked.

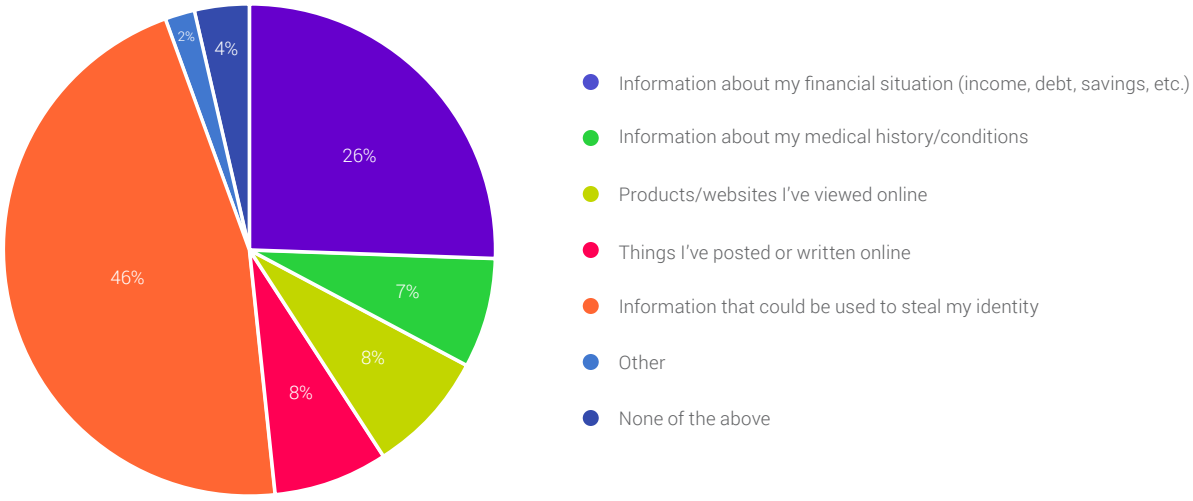
By contrast, 18% of consumers fear government misuse of their data the most. Negative perceptions of government in general may be fueling this suspicion: just 43% of Americans trust the government, down 10 percentage points since 2017, according to Edelman.

At the lowest level of concern is privacy surrounding health data. Despite two years of debate about pandemic-related health tracking and vaccine mandates, just 3% of respondents say they worry most about misuse of information by health care organizations, and 7% are most concerned about the sharing or tracking of their medical information.

Survey Question: Which of the following are you most concerned will misuse data?



Survey Question: Which one of the following types of data are you most concerned about being shared/tracked online?



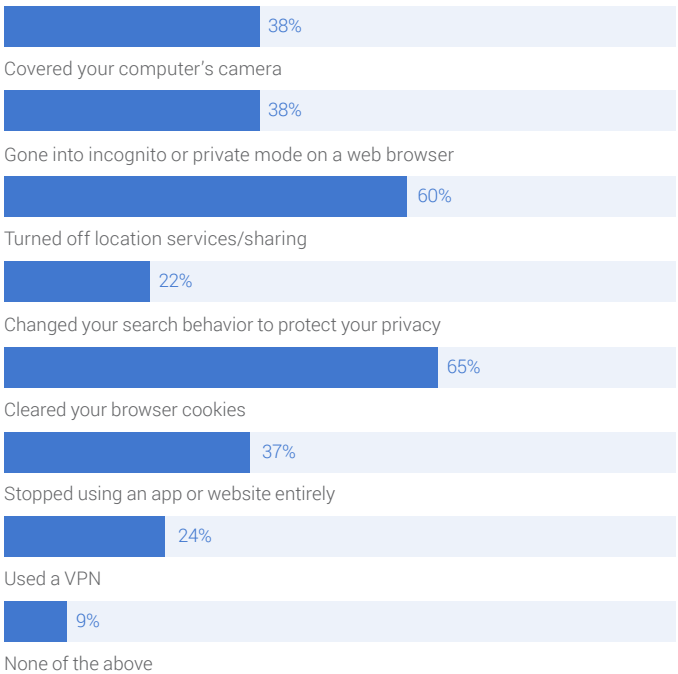
Erasing tracks online is commonplace

To safeguard their data, 91% of consumers have taken at least one common measure to protect their information online. Clearing browser cookies is the most commonplace action, with 65% of respondents saying they've done so. That's more than 25 points higher than the percentage who've used their browser's incognito or private mode in an attempt to avoid cookie tracking in the first place.

Consumers also attempt to block transmission of background data. Turning off location services on mobile devices is the second most popular privacy measure, at 60%, while 38% cover their computer camera to prevent surreptitious image/video capture. And 24% use a VPN to avoid interception of information transmitted via their Internet connection.

Taken together, these measures are more popular than changing behavior to avoid exposure of personal information. While 37% report they've stopped using a website or app entirely, just 22% have changed their search behavior to avoid risk.

Survey Question: Have you ever done any of the following for privacy reasons? Select all that apply.



Consumers want tech companies to step up

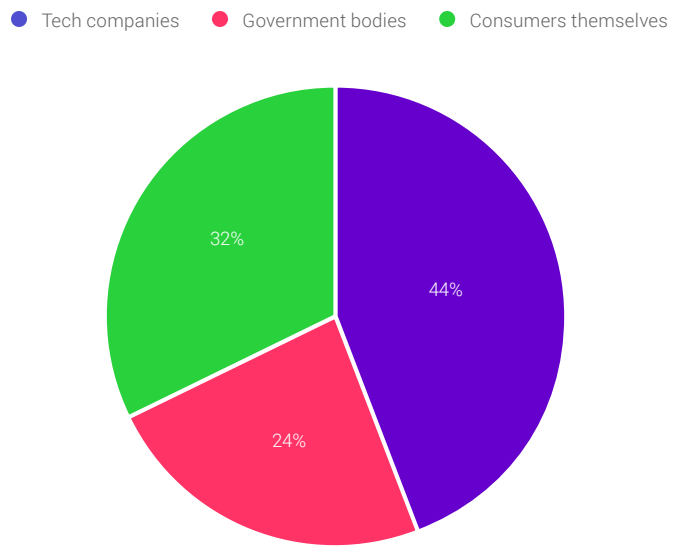
Even as consumers take steps to protect their individual information, they also want broader-based intervention – and they expect tech companies to take the lead. More than half, 55%, believe private businesses should step up privacy protection efforts, while 43% say the government should do more.

Furthermore, when asked to choose which single group is most responsible for protecting online privacy, respondents chose "tech companies" by a wide margin, 44%, 20 points higher than those selecting "government bodies." In fact, consumers were more likely to believe they themselves were responsible for protecting privacy, 32%, than they were to hold the government accountable.

These views reflect prominent privacy actions and competition on the part of leading tech companies over the past year. In April of 2021, Apple instituted its App Tracking Transparency (ATT) feature, which requires apps to ask for permission up-front to track users' data across the Web and apps; since then, Apple has added further privacy features, such as email masking. In February of 2022, Google followed suit, saying it plans to phase out tracking on devices using its Android mobile operating system. Already, October's Android 12 release granted users enhanced privacy control. The search giant has also announced its intention to phase out third-party cookie tracking in its Chrome browser.

By contrast, not only do more consumers distrust government than business when it comes to online privacy, but regulatory protections so far have been far from sweeping. Amidst inaction at the federal level, a majority of U.S. states are now actively debating privacy legislation, raising the possibility of a patchwork system of laws.

Survey Question: Which of the following groups do you believe is most responsible for protecting online consumer privacy?



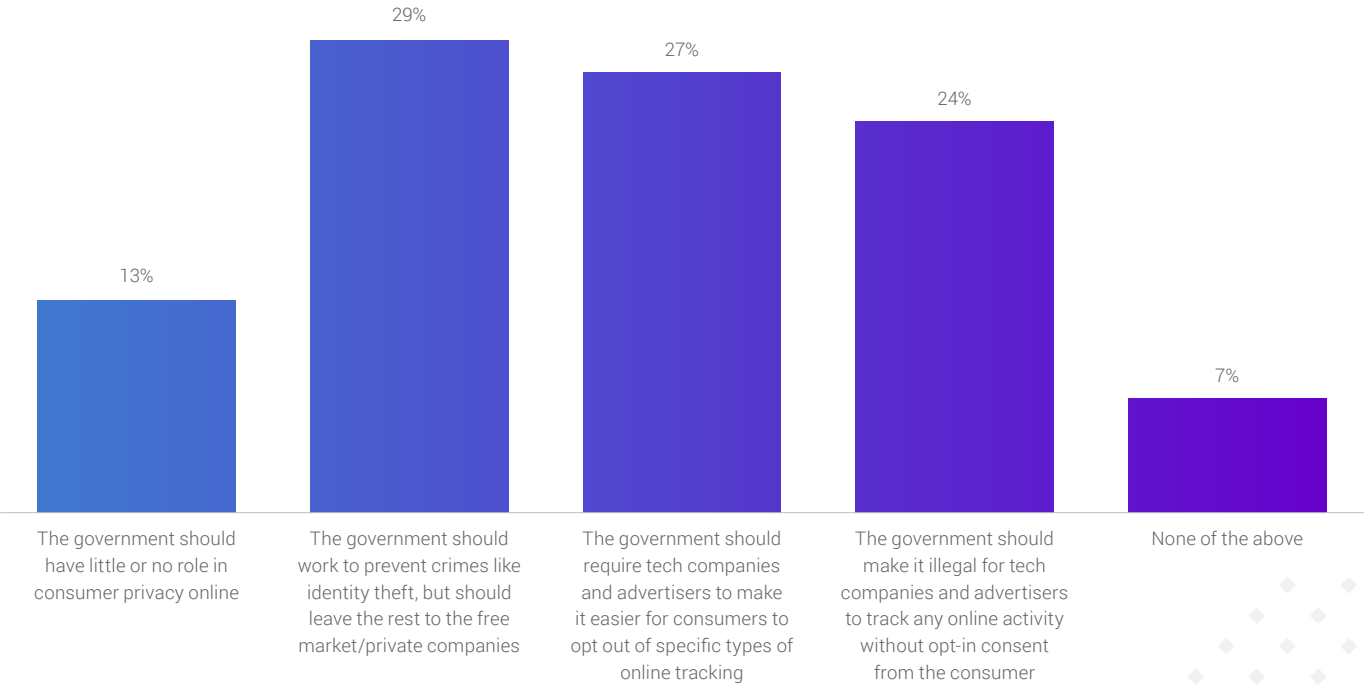
Consumers favor oversight of ad tracking

While consumers believe tech companies are primarily responsible for privacy protection, most do believe the government has a role to play – and a significant percentage want oversight of digital ad tracking.

The majority of respondents, 52%, say tech companies and advertisers should be regulated. Within this cohort, 27% believe government should require tech companies to make online tracking easier to opt out of, while 24% believe tracking should be outright illegal unless consumers grant consent.

This response contrasts with the finding that fewer than 1 in 10 respondents say they worry the most about advertisers misusing their data, and just 8% say they are most concerned about the websites and products they view being tracked. Taken together, those who want oversight of ad tracking outnumber those who believe government's role should be limited to crime prevention, who make up 29% of respondents.

Survey Question: Which of the following best describes what you feel the role of government should be with respect to online consumer privacy?



"While consumers believe tech companies are primarily responsible for privacy protection, most do believe the government has a role to play."

THE VIEW FROM GEN Z

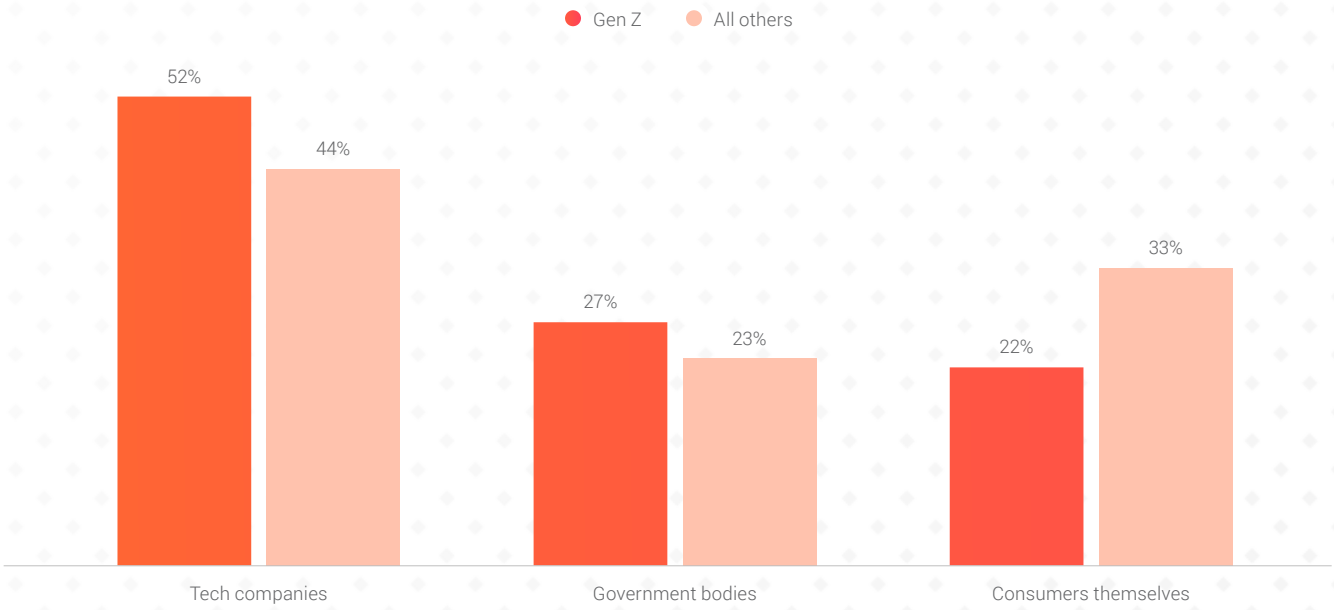
In Control of Their Privacy and Holding Big Tech Accountable

When it comes to attitudes and behaviors surrounding privacy online, young adults ages 18 to 26 stand out among all other age cohorts. As digital natives, these members of Gen Z have different attitudes to privacy than any other demographic. Throughout the report, we'll take a deep dive into their views.

In general, members of Gen Z are more apt to believe in online privacy. Just under half (49.5%) agree that there's no such thing as privacy online – the lowest percentage of all age groups – and 26% believe they have control of their data. Fully 93% have taken some kind of action to protect their privacy online.

More than half of Gen Z respondents, 52%, place primary responsibility for privacy with tech companies – by 25 percentage points, the widest margin of any age group – but government is the second most popular choice, whereas older respondents are more evenly divided, with a higher percentage saying consumers themselves are responsible for protecting their own information.

Survey Question: Which of the following groups do you believe is most responsible for protecting online consumer privacy?



While they're more likely than other age groups to say the government should be responsible for privacy, a minority of Gen Z believe regulation of ad tracking is a priority, at 43%. Instead, 34% say the government should stick to preventing crime and 18% say the government's role is limited or nonexistent – in both cases, 6 percentage points higher than all other respondents.

Apple and Amazon Perceived as Privacy Protectors, While No Social Network Receives High Marks

Awareness of privacy lapses, preoccupation with ad tracking, and belief that tech companies are responsible for protecting their information have created clear winners and losers in consumers' minds among the web's most popular sites and apps.

These perceptions may be shaped more by headlines than by privacy reality. For example, social networks, which have caught media flak for using personal data to make ads more profitable and whose algorithms are closely scrutinized, are more negatively perceived than shopping giant Amazon, which receives high marks despite selling its own version of the targeted advertising search engines and social networks offer.

In a 3-way matchup of titans, Amazon is the privacy winner

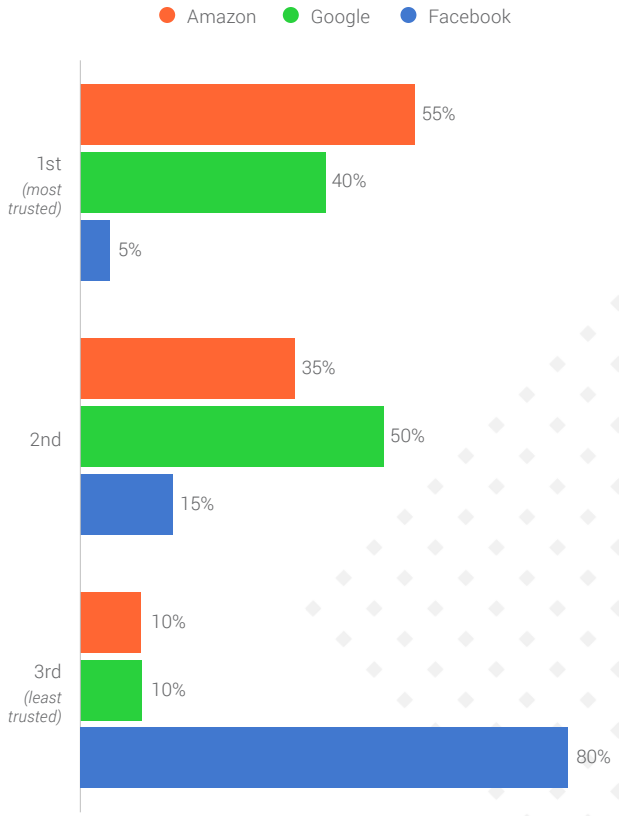
When asked to rank three of the Internet's biggest shopping, social, and search sites based on their trustworthiness, Amazon was the winner, with Google in second place and Facebook placing distant third.

Overall, Amazon received 55% of the first-place votes, while Google received 40%. Facebook received just 5%.

By contrast, Facebook received 80% of the third-place votes, with Google and Amazon receiving 10% of third-place votes apiece.

This ranking is consistent across age groups and genders, although Amazon ranks slightly higher with women (56% of first-place votes) than with men (52%). Among men, 42% rank Google in first place, compared with 39% of women.

Survey Question: Rank the following websites/apps from most trusted to least trusted based on how much you trust them to protect online consumer privacy.



Consumers believe social networks' privacy protections are all the same

Facebook's poor showing is understandable, given the broad perception that social media networks are undifferentiated in their approaches to privacy.

When asked which social network best protects online privacy, fully 43% of respondents say "there's no difference," while another 23% say they don't know – making for a combined two-thirds of the total.

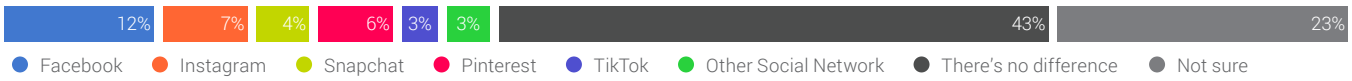
Among the individual sites, only Facebook earned more than 1 in 10 votes, at 12%, with its fellow Meta destination Instagram coming in second at 7%, giving the company a combined total of just 19% – four points lower than those who don't know which site is better. The low trust numbers are especially stark given that Facebook enjoys 69% penetration among U.S. adults and 40% use Instagram, far outpacing other social media destinations.

All the other options earned fewer votes still, with the relative newcomer TikTok earning the lowest percentage at 3%, despite soaring popularity since the beginning of the pandemic. Mainstream media coverage describing its Chinese origins and its addiction-inspiring algorithm may be driving this distrust.

The uncertain or undifferentiated perception of social media networks is predominant across genders and age groups, with the exception of Gen Z, the only cohort for which the "no difference" and "not sure" respondents are in the minority. (Gen Z has a different social media viewpoint in general; see this section's "View from Gen Z" on page 9 for details.) The "no difference"/"not sure" combination reigns even among the 30% of respondents who say they choose which social media platforms to use based on their privacy protections.

Survey Question: Which social network do you think best protects online consumer privacy?

› *Overall Responses*



› *Segmented*

	Survey Avg.	Gen Z	Millennial	Gen X	Boomer+	Men	Women	Choose Social for Privacy
There's no difference	43%	33%	42%	44%	46%	42%	44%	39%
Not sure	23%	12%	15%	25%	34%	22%	23%	16%
Meta (Facebook + Instagram)	19%	24%	23%	17%	12%	21%	17%	23%

DuckDuckGo's privacy-first marketing pays off

In contrast with their beliefs about social media, consumers consider search engines to be distinct when it comes to privacy.

Just 20% believe there's no difference among leading search destinations, compared with 43% and 25% who believe there's no difference between social media sites and online marketplaces, respectively. Another 16% say they're unsure about which search engine is the best, bringing the "no difference"/"not sure" total to just over a third of respondents (35%).

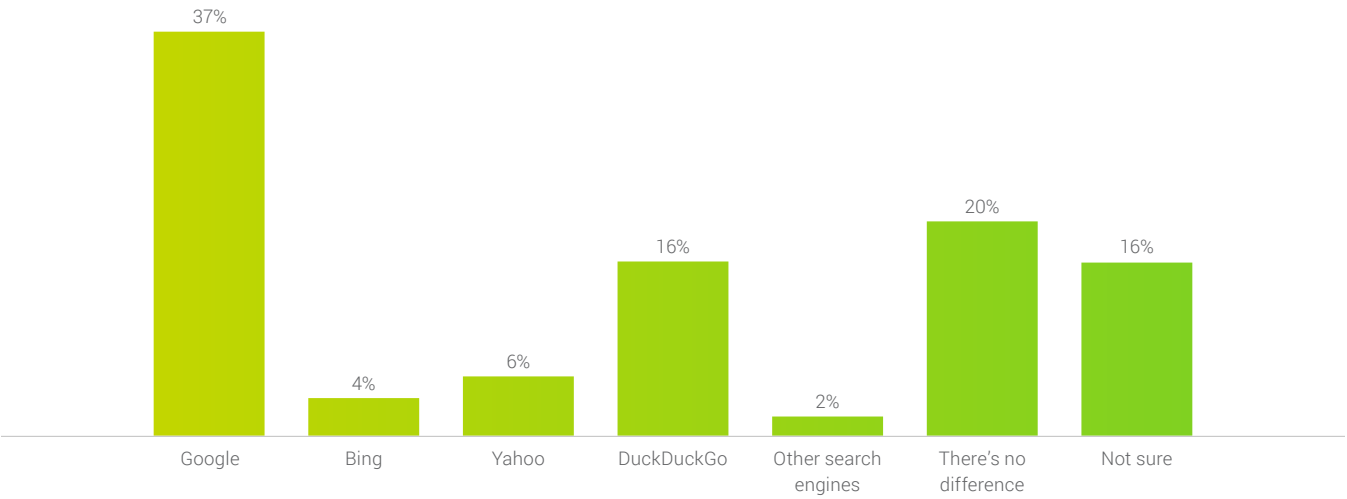
Google is the clear leader among search engines, with 37% of consumers saying it does the best job of protecting privacy. Google's leading position may be due to familiarity, since it currently enjoys a dominant share of 88% of the U.S. search market.

DuckDuckGo is in distant second place, at 16%. That percentage is significantly higher than its market share, which hovers around 2.5%, suggesting that the brand's persistent privacy messaging is having an impact on consumer perceptions. More men than women favor DuckDuckGo, with 22% of men and 13% of women saying it offers the best privacy protections.

DuckDuckGo also receives higher marks from the 36% of survey respondents who say they consider privacy when choosing which search engine to use – although Google does, too. Among this cohort, 42% say they trust Google to offer the best privacy, and 21% choose DuckDuckGo. The percentage of respondents in this cohort choosing either "no difference" or "not sure" is much lower than the survey average, at 23%.

Meanwhile, properties powered by Microsoft search are most trusted by 10% of respondents, with Bing's search engine (4%) trailing Yahoo's, at 6%.

Survey Question: Which search engine do you believe best protects online consumer privacy?



Amazon enjoys a strong privacy reputation

When it comes to consumers' perceptions of the privacy protections offered by shopping brands, Amazon is dominant. Fully 40% of respondents say it's the shopping marketplace that offers the best privacy, more than 30 percentage points higher than any of the other shopping sites, which each score under 10%. A quarter of respondents say there's no difference, and 15% say they're not sure which destination is best.

The gap between Amazon and its rivals only widens among those who consider privacy when choosing where to shop, who make up 36% of all respondents. Amazon is the top pick for 46% of these shoppers, a 38-point lead over Walmart, at 8%.

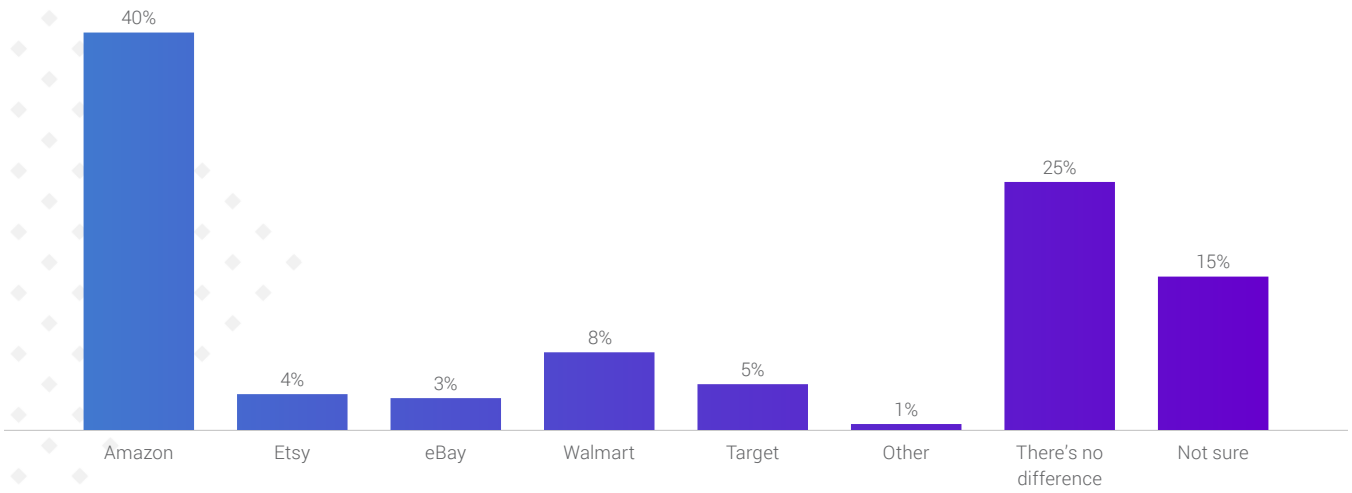
This strong reputation may be partly attributable to Amazon's overall market dominance, claiming 40% of eCommerce sales according to estimates. Consumers may assume Amazon's prized efficiency and customer service carries over to privacy protection, too.

In addition, Amazon's targeted advertising may be considered more appropriate than on other sites and apps. By some counts, Amazon has overtaken Google as the top destination for shopping search; consumers visit Amazon expressly to find out about products and therefore may be more receptive to relevant recommendations.

But another reason may be that consumers simply don't realize Amazon sells ads in the first place. Half of consumers participating in a 2019 survey were unable to distinguish Amazon ads from organic content, and the ads are so well integrated into product listings that late in 2021, a consumer group filed an FTC complaint alleging deceptive practices.

Consumers' trust in Amazon is also disconnected from their concerns about surveillance, given that

Survey Question: Which online marketplace do you believe best protects online consumer privacy?



38% believe their mobile devices "listen" to their conversations. Amazon's Alexa intelligent agent has been accused of such eavesdropping in a class-action lawsuit, and media reports routinely advise consumers to activate Alexa privacy settings. Among those survey respondents who worry about digital eavesdropping, Amazon receives slightly lower marks for privacy, 36%, but remains the top choice.

Apple's privacy stance pays off

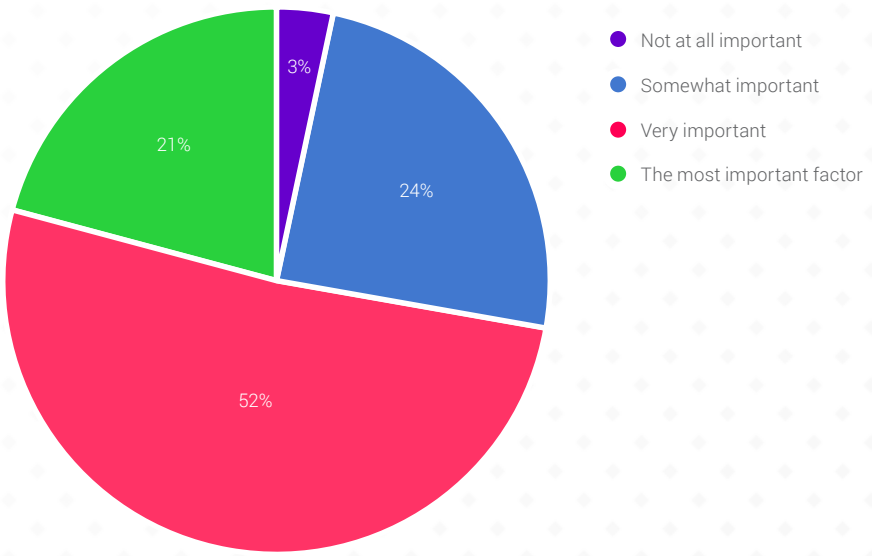
Mobile devices are a trove of personal information, from photos and text messages to location and app usage logs. It's no surprise, then, that consumers are sensitive to privacy protection on their phones. Fully 72% say privacy considerations are at least very important, and 21% believe it's the single most important factor when deciding which type of phone to buy. More women than men prize privacy above all other considerations: 22% of women say it's the most important decision factor, compared with 17% of men.

Consumers are also attuned to the privacy messaging technology companies are sharing; 64% believe mobile operating systems have made strides toward better privacy protection in the past year.

When asked which platform specifically supports privacy better, consumers choose Apple as the clear winner. Apple has long positioned itself as a privacy leader, and more than half of consumers, 53%, believe Apple's iOS is better at protecting privacy than Android, while only 35% choose Android over iOS. Even 12% of respondents who use Android devices believe Apple does a better job with privacy, whereas just 2% of Apple device users say Android is superior.

72%
say privacy considerations are at least very important when deciding which type of phone to buy.

Survey Question: How important are online privacy considerations to your choice of a mobile phone?



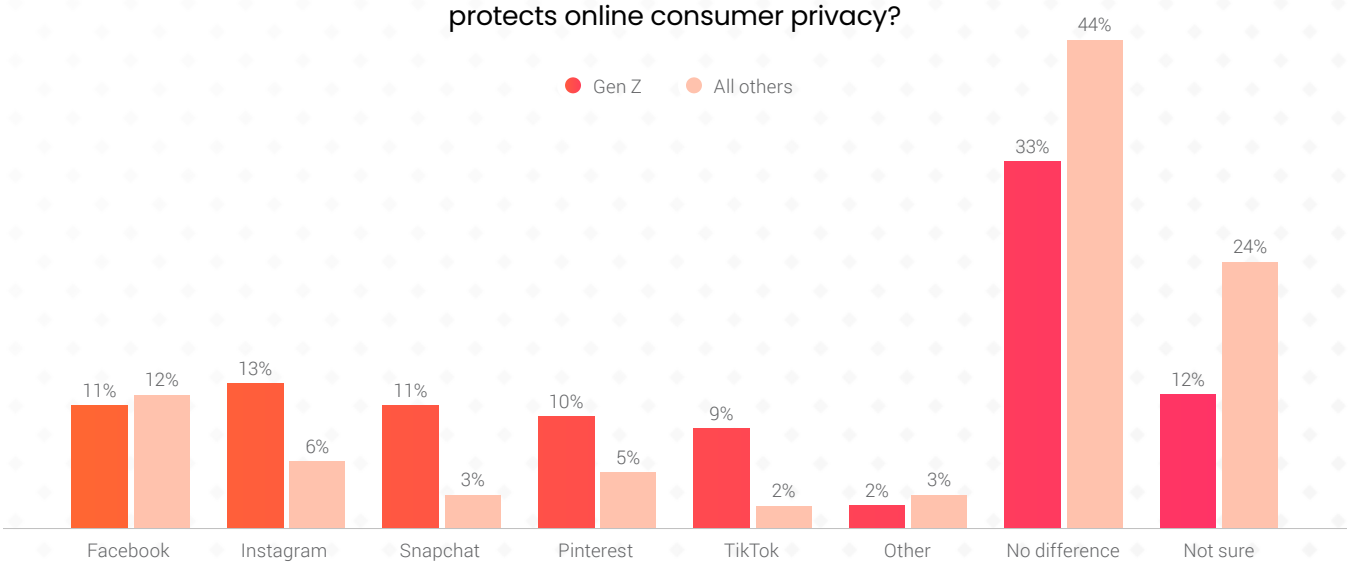
THE VIEW FROM GEN Z

A Different Take on Social Media Privacy

Unlike other age groups, the majority of Gen Z respondents believe social networks are distinct when it comes to their privacy protections – although there is no single standout. "No difference"/"Not sure" responses from Gen Z total just 45%, compared with 68% for all other age cohorts.

Nearly 1 in 4 Gen Z members, 24%, say Meta properties offer the best privacy protections, with 13% selecting Instagram and 11% Facebook. The percentage of Gen Z respondents saying Snapchat offers the best privacy protection (11%) is more than triple the percentage of older consumers (3%), while 9% of Gen Z believe TikTok safeguards privacy best – more than 4x the percentage among older respondents.

Survey Question: Which social network do you think best protects online consumer privacy?



Beyond social media, Gen Z aligns with the rest of survey respondents when it comes to privacy leaders – even giving some of them wider margins of support. For search, 41% of Gen Z say Google offers the best privacy protection, four percentage points higher than older respondents, and when it comes to mobile operating systems, a stunning 72% say Apple's iOS is superior – 21 percentage points higher than older age groups.

With regards to online shopping marketplaces, however, Gen Z is a little more circumspect. Amazon is still far and away the most trusted site from a privacy perspective, at 35%, but Etsy is number two at 12% – 4x higher than among older shoppers. Equal numbers of Gen Z respondents give Target and Walmart the best privacy score, at 10% apiece. By contrast, among older shoppers, Walmart was a distant second behind Amazon at 8%, with all other sites ranking lower still.

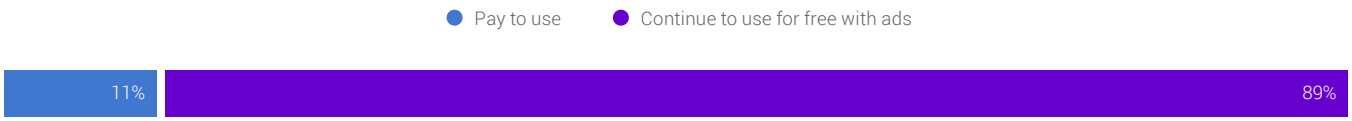
Ads Are Better Than Paying for Content, But Support for Tracking Is Low

The Internet wants to be free, consumers believe – but their tolerance for viewing ads in exchange for cost-free online experiences only goes so far. Ad tracking is viewed with suspicion, and the majority of consumers are unwilling to surrender more than an email address in order to access discounts or deals.

Ads are preferable to paid services, but few accept tracking

In principle, consumers accept that advertising is necessary as a funding source for providers of online services or content. When asked whether they would rather pay for access to social platforms, search, or media, or view ads to keep those experiences free, 89% say they'd rather view ads.

Survey Question: Would you rather pay for online platforms like Google, Facebook, Instagram, Pinterest and other news and media outlets, or continue using them for free with ads?



Men are more willing to pay for access than women, with 16% of men saying they'd buy an ad-free experience, compared with 11% of women.

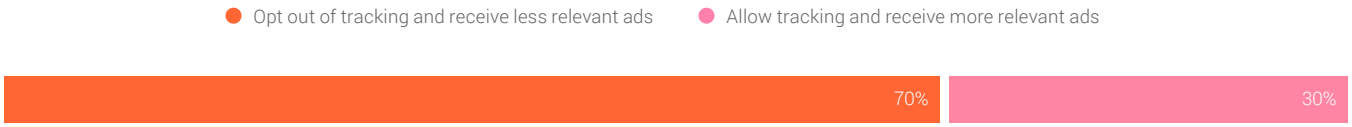
At the same time, the majority of consumers would rather opt out of tracking technologies that enable targeted ad messaging. Just 24% of respondents agree with the sentiment that "when I get something for free online, I am the product" – and they'll take action to avoid becoming that product.

Rather than having their online behavior tracked in order to target advertising, 70% of consumers say they would rather opt out and receive less relevant messages. These responses align with industry data showing that just 25% of consumers using the iOS ATT feature choose to enable tracking.

The impact of this move has already manifested itself in advertising results on social media. For example, in the fourth quarter of 2021, purchases declined 30% year over year in Meta's in-platform reporting across Tinuiti advertisers, as Meta's ability to track and report on these metrics has been limited by opt-outs due to the Apple ATT feature. For more details about the implications of privacy features for Meta advertising, download Tinuiti's Facebook Ads Benchmarks Report for Q4 2021.

Interestingly, those who would choose to pay for online services and content are also slightly more willing to enable ad tracking, at 33%, versus 67% who would opt out. These respondents skew younger: 59% are Gen Z members or Millennials, which comprise 44% of the overall respondent pool. As younger consumers who live and work online, they may be more cognizant than older respondents of what it takes for digital brands to be economically viable. Fully 30% agree that "when I get something for free online, I am the product," 5 percentage points higher than average. This awareness may boost openness to both payment and tracking.

Survey Question: Would you rather opt out of tracking that advertisers use to target ads – and receive less relevant ads – or allow tracking and receive more relevant ads when using online news and media platforms?



Tracking perceived as necessary as well as a nuisance

When asked about their sentiments toward ad tracking, such as in retargeting campaigns that display previously-viewed products in ads across different websites, the majority of consumers say these techniques are invasive, while also recognizing their benefits.

More than half of respondents, 54%, say it's "creepy that the ads seem to be able to follow me." At the same time, however, a combined 43% of respondents say retargeting is "fine" if it keeps content free and/or "helpful" for reminding them of products. The overlap between these two groups is far from trivial: 20% who say retargeted ads are creepy also acknowledge they're helpful or at least acceptable if they help keep web platforms free.

Nearly a quarter of respondents, 24%, are less worried about tracking per se, and more worried that someone else spotting the ads could see they're interested in the featured products. This percentage rises to 31% among those who believe the ads are creepy.

Not surprisingly, those who would opt in to ad tracking are more likely to perceive its benefits, with 43% of those users saying targeted ads are helpful reminders and 46% agreeing they're fine if they keep content free. Similarly, 63% of those who opt out of tracking say targeted ads are creepy, 9 percentage points higher than average. While these findings are predictable, they at least offer the reassurance that users who opt in to tracking are genuinely receptive to tailored offers.

Appetite limited for sharing more than email

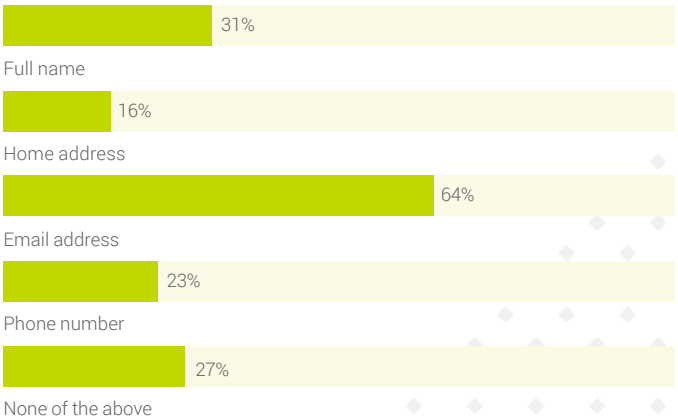
While most respondents are unwilling to have their behavior tracked in order to receive relevant advertising, the majority will explicitly share information in exchange for a deal. When asked what they might share online to receive a $20 discount coupon, more than 7 in 10 (73%) would voluntarily submit at least one piece of information, while 27% said they wouldn't share anything.

Nearly two-thirds of respondents, 64%, say they would be willing to share their email address – but that's the only type of information a majority of respondents say they'd surrender. Just 31% would divulge their full name, 23% would share a phone number, and fewer still, 16%, would submit their home address. Baby Boomers and seniors ages 57 and up are less likely to be willing to share information, with 33% opting for "none of the above."

Respondents who believe some online retailers offer better privacy protections than others – whether Amazon or another site – are more willing to share not only their email address (68%), but also their name (35%) and phone number (26%) in order to receive a discount, while just 1 in 5 say they wouldn't divulge anything. By contrast, those who select "no difference"/"not sure" when it comes to online retailers' privacy practices are less likely to share information, with 35% opting for "none of the above." These findings suggest that retailers who can convince shoppers of their privacy trustworthiness may be able to request and voluntarily receive more user data.

Survey Question: When products I've viewed online appear in ads across different websites, I find it (select all that apply):

Survey Question: What information would you be willing to provide to an app or website to get a $20 coupon or discount code? Select all that apply.

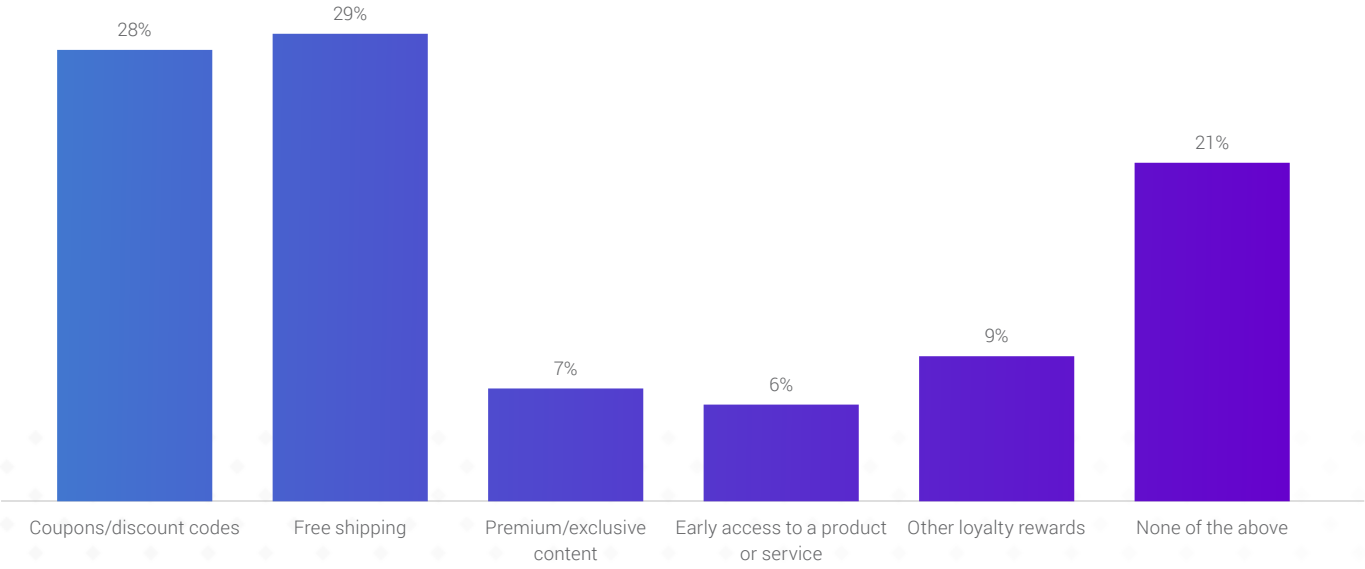


Coupons and free shipping are top incentives to share information

When asked what kind of promotional offer would prompt sharing their email address, consumers favor cost savings. Nearly 3 in 10 respondents chose both free shipping (29%) and a discount coupon (28%), while other rewards and perks each scored less than 10% as an incentive and 1 in 5 consumers (21%) wouldn't surrender an email address.

Cost-related incentives appeal more to women, 59% of whom would choose either free shipping or a discount. While those options are also the leading incentives for 53% of men, other perks are also appealing to them. One in 10 men say they'd share their email address in exchange for loyalty rewards, compared with 8% of women, and 9% say exclusive content is the most effective incentive, compared with 6% of women.

Survey Question: For which benefit or perk would you be most likely to provide an app or website with your name and email address?



"When asked what kind of promotional offer would prompt sharing their email address, consumers favor cost savings."

THE VIEW FROM GEN Z

More Acceptance of Tracking – and Free Shipping Offers

While Gen Z respondents don't exactly relish the tracking that makes targeted ads relevant, they're more apt to see its benefits than other age groups.

For starters, they're more aware of ad tracking than other cohorts: just 3% say they've never noticed targeted ads, less than half the percentage of older cohorts (7%).

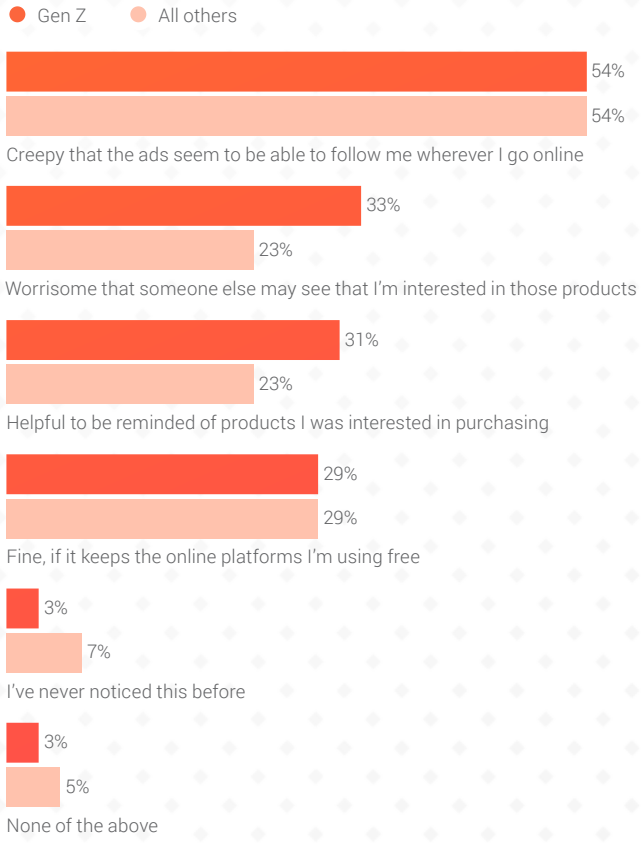
While they're only slightly more willing to pay for digital content and services than older consumers, Gen Z respondents are more likely by seven percentage points to allow tracking for targeted ads, at 36%.

In addition, while the same percentage of Gen Z respondents as older consumers find tracking ads creepy, 31% of Gen Z say they're helpful - 10 percentage points higher than other age groups. Interestingly, Gen Z is also more concerned about others seeing that they're interested in the products featured in targeted ads, at 33% compared with 23% for older consumers.

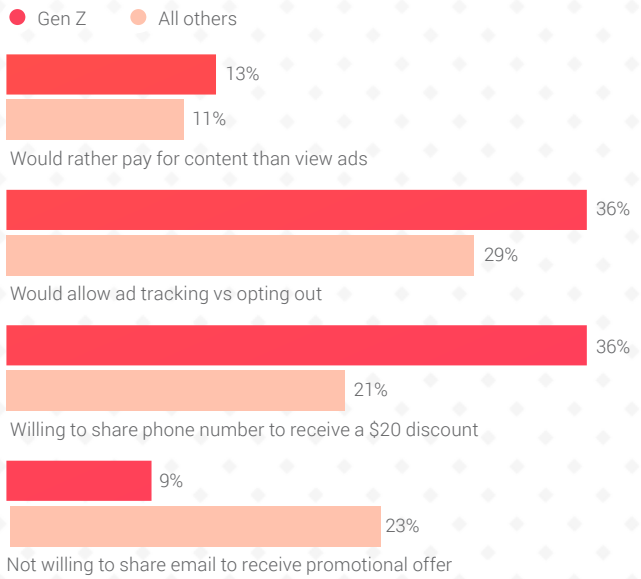
Gen Z are roughly as likely to surrender their email address and full name as other age groups, but they're more likely to share a phone number, with 36% willing to do so compared with 21% of older respondents.

And when it comes to which perks would incentivize them to share information, free shipping is far and away the top motivator over discounts and other rewards. Fully 40% of Gen Z say free shipping would entice them to share their email address, compared to just 24% who say they'd do so for a discount, whereas other age groups are evenly split between the two. And while 23% of other age groups say they'd be unwilling to surrender their email in exchange for a promotional offer, just 9% of Gen Z would resist.

Survey Question: When products I've viewed online appear in ads across different websites, I find it:



Gen Z Attitudes on Digital Ads and Marketing



Top Takeaways

If companies weren't already prioritizing privacy, 2021 was a wake-up call to engage meaningfully with changing consumer expectations and new regulations. To navigate through this changing landscape in 2022, brands should take the following steps:

➔ Reduce dependence on third-party data in favor of first-party relationships.

Whether or not third-party data stays legal is a technicality at this point; the momentum is clearly shifting away from the models advertisers have used in the past in favor of focusing on new techniques for targeting consumers with relevant offers and products. While the transition is taking longer than anticipated, brands shouldn't wait to begin building a foundation of zero-party and first-party data they collect directly themselves. Although survey data shows consumers are reluctant to share more than an email address, tools that deliver highly tailored experiences, such as style profile builders or interactive quizzes, can demonstrate the utility of data collection. Subtler sources of information such as live chat interactions or analytics data about SKU preferences can also help brands build data profiles. The sooner brands find ways to build, parse, and derive insights from their storehouses of wholly-owned data, the better-positioned they'll be to capitalize on the new (privacy) normal.

➔ Employ next-generation analytics to measure ad performance.

In response to the loss of cookies and third-party data, new techniques for measuring the success of ad campaigns are evolving quickly. Brands should move past relying on the reporting tools owned by individual ad platforms to explore new unified analytics practices that present a holistic picture of ad performance and rely on a combination of statistical modeling and real-world data to accurately attribute revenues. This new field of marketing science requires building a sophisticated data management toolset, so to ramp up capabilities, brands should consider hiring or at least learning from the experts as they go.

➔ Integrate privacy messaging into brand awareness campaigns.

Consumers have a positive perception of technology companies, such as Apple and DuckDuckGo, that have placed privacy front and center in their marketing and advertising, so sellers should consider how they can showcase their own privacy best practices in a way that feels organic for their existing brand identity. Given that consumers believe companies' treatment of their data reflects their treatment as customers, brands could integrate privacy as part of their fair practices policies for employees, customers, and communities. And of course, website and mobile web and app experiences should spotlight privacy with easy-to-understand text explaining why data is being collected, and clear-cut policies explaining how data will be used, stored, and shared.

→ Allocate ad dollars to Amazon and invest selectively on social networks.

Brands should capitalize on Amazon's reputation as a privacy-safe, trusted source for shopping information and invest in selling and advertising on the platform, which can drive both brand visibility and revenue. Consumers are more wary of social networks, so choose the platforms that work best for specific customer groups and align ad and organic strategy carefully with individual platform best practices to ensure messages reach the right audience, and stay on the right side of the creepy vs. cool divide. Brands may even want to allocate incremental budget to influencer marketing to supplement traditional paid placements, as a way of bringing a higher degree of personal authenticity to their social presence.

Consumers are watching - how will your privacy evolve?

After a year of radical change, online privacy in 2022 remains a fluid and shifting concept. With consumer awareness at an all-time high, brands' stances on privacy can make or break their reputations – so developing a thoughtful strategy across channels and devices is now a must. By transparently communicating privacy practices and delivering superior tailored experiences that encourage voluntary data sharing, brands can stake a leadership claim, win customer trust, and earn long-term loyalty.

Methodology

Tinuiti surveyed 1,000 online respondents ages 18 and older on February 9, 2022, via the Pure Spectrum Insights platform. All respondents were screened with the question, "How often do you go online?" and those who do not go online at least daily did not participate.

METHODOLOGY DETAILS

This survey was commissioned by Tinuiti and conducted by Pure Spectrum, which uses PureCore, proprietary technology for gathering quality responses. Consumers receive no monetary payment for their participation. More information on Pure Spectrum's methodology can be found at https://www.upwave.com/instant-insights/.

The Future of the Web is Here

Schedule Your Consultation
with a Privacy Expert

tinuiti.com/contact-us