

# Privacy as a Competitive Advantage: How Tech is Building Consumer Trust

The discussion will begin at 2:00 PM ET. You can listen using computer speakers or headphones. Please submit any questions you have and we'll do our best to address them during the Q&A session.

**PRESENTER**



**Sara M. Watson**  
Senior Analyst,  
Connectivity and Tech  
Insider Intelligence

**PRESENTER**



**Kelly Kimura**  
Senior Director of  
Product Management  
Vericast

**MODERATOR**



**Debra Aho Williamson**  
eMarketer Principal  
Analyst  
Insider Intelligence

Made possible by



July 2021

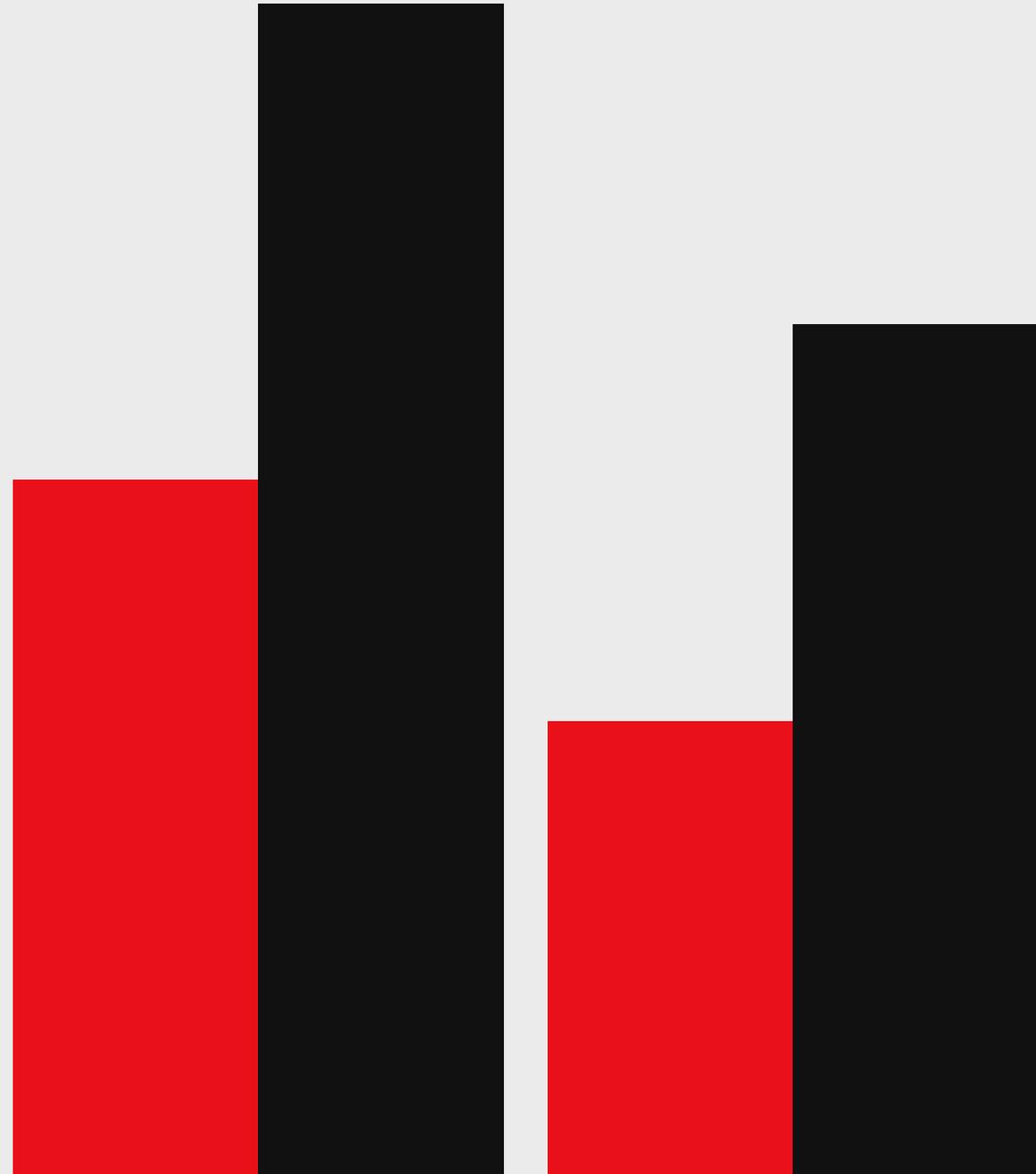
# Privacy as a Competitive Advantage: How Tech Is Building Consumer Trust

---



**Sara M. Watson**

Senior Analyst



# The market for privacy is here.

Seven out of 10 consumers worldwide are willing to spend time and money to protect their data.

## Priorities and Actions in Protecting Their Privacy According to Consumers Worldwide, June 2020

% of respondents



### I care

- I care about data privacy
- I care about protecting others
- I want more control



### I'm willing to act

- I am willing to spend time and money to protect data
- This is a buying factor for me
- I expect to pay more



### I've acted

- I have switched companies or providers over their data policies or data sharing practices

Note: n=2,602

Source: Cisco, "2020 Consumer Privacy Survey"; Insider Intelligence calculations; Oct 21, 2020

265586

[InsiderIntelligence.com](https://www.insiderintelligence.com)

# Privacy is at an inflection point.

## MARKETS

### Consumers are voting with their feet

45% of US consumers are willing to pay for products in lieu of having companies collect, share, or sell their personal data (Consumer Reports, 2020).

## NORMS

### Trust in tech is declining

The tech industry lost more trust over the last year than any other industry, according to Edelman's 2021 Trust Barometer.

## LAW

### GDPR and CCPA lead the way

Global data privacy regulations are setting new standards for compliance. They put emphasis on first-party relationships, shift to opt-in, rather than opt-out, consent models, and give users power to demand their data.

## CODE

### Product, business models shift

Tech giants are starting to question long-held assumptions that more user data is always better. Product teams and org structures are considering privacy from the start, rather than checking a legal box before shipping.

**Privacy is more than a compliance concern;  
it's a competitive advantage.**

**Misuse or abuse of personal data is the top reason consumers lose trust in a company.**

---

## What Would Make US Adults Lose Trust in a Company?

*% of respondents, April 2020*

---

Misusing or abusing their personal data

41%

Failing to deliver a product or service as promised

21%

Poor customer service when resolving issues

20%

A lack of empathy in helping address their needs

10%

Overwhelming them with advertisements and notifications

8%

---

*Note: ages 18+*

*Source: Genesys, "Personalization & Empathy in Customer Experience" conducted by Wakefield Research, May 20, 2020*

---

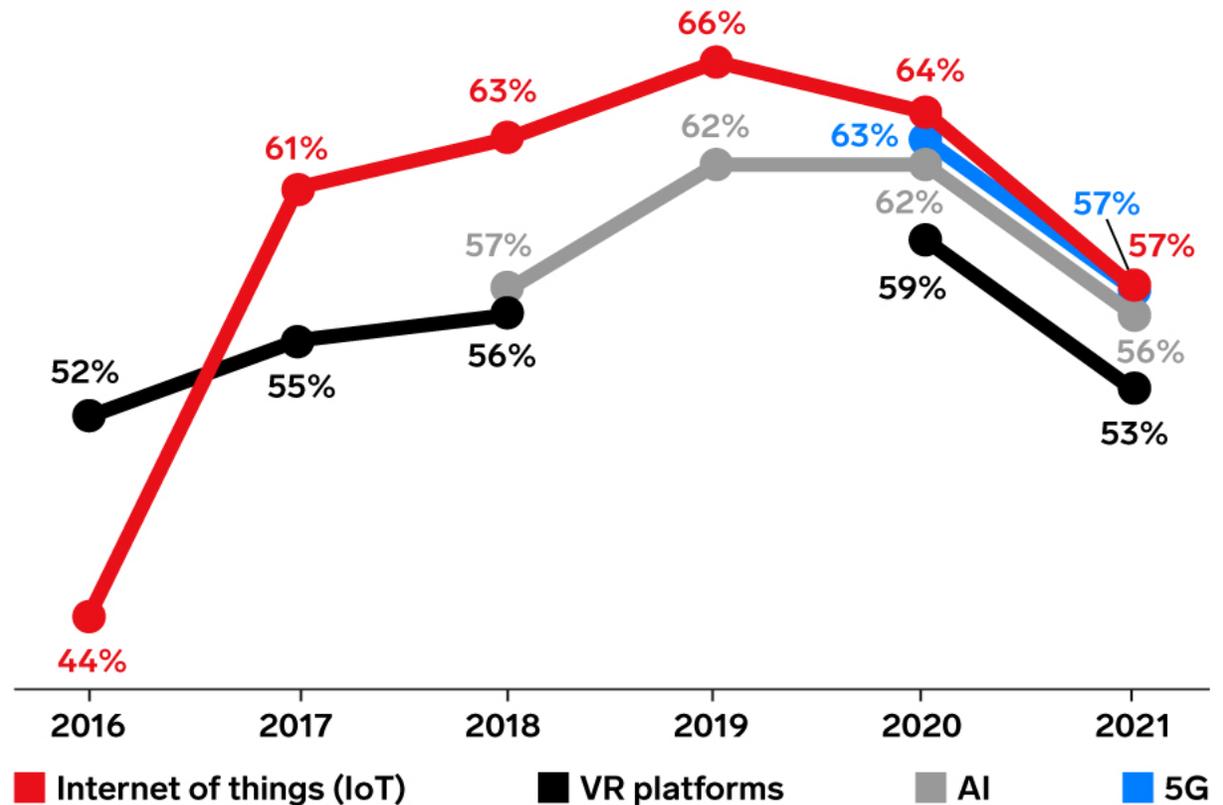
259555

eMarketer | [InsiderIntelligence.com](https://www.insiderintelligence.com)

Trust in the tech industry is declining, including trust in emerging technologies.

### Trust in Select Technology Sectors Among Internet Users Worldwide, 2016-2021

% of respondents



Note: ages 18+; respondents were asked to rate their trust in businesses to do what is right on a 9-point scale; percentages reflect responses in top 4 boxes

Source: Edelman, "2021 Edelman Trust Barometer: Trust in Technology," March 31, 2021

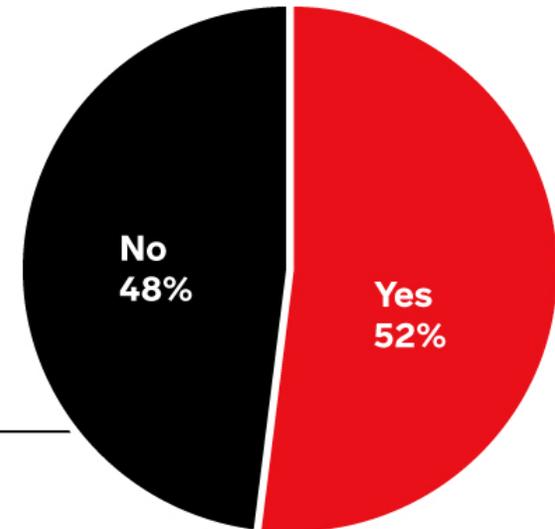
**Half of consumers (48%) feel like they don't have control over their data.**

## Reasons Consumers Worldwide Are Not Able to Effectively Protect Their Personal Data Today, June 2020

*% of respondents*

### Reasons why not

Too hard to figure out what companies are actually doing with my data	79%
If I want the service, I have to accept how my data is used	51%
Feel my personal data is already available	45%
Don't understand what service choices are	44%
Don't trust companies to follow stated policies	40%



**Able to effectively protect personal data**

Note: n=2,602 ages 18+

Source: Cisco, "Consumer Privacy Survey," Oct 21, 2020

**Innovation-leading companies prioritize and invest in data privacy.**

## Attitude of Business Executives Worldwide Toward Data Privacy and Security Affecting the Customer Experience, by Maturity Level, Oct 2020

% of respondents

	Executives at all organizations	Innovation leaders	Innovation laggards
Organization considers ensuring data privacy and security important to the customer experience	38%	41%	33%
Organization has/plans to invest in data privacy and cybersecurity management to improve the customer experience	37%	46%	28%
Organization is prioritizing data privacy and security to enhance the customer experience	26%	36%	19%
Organization made recent investments in data privacy and cybersecurity specifically in response to the coronavirus pandemic	15%	23%	9%

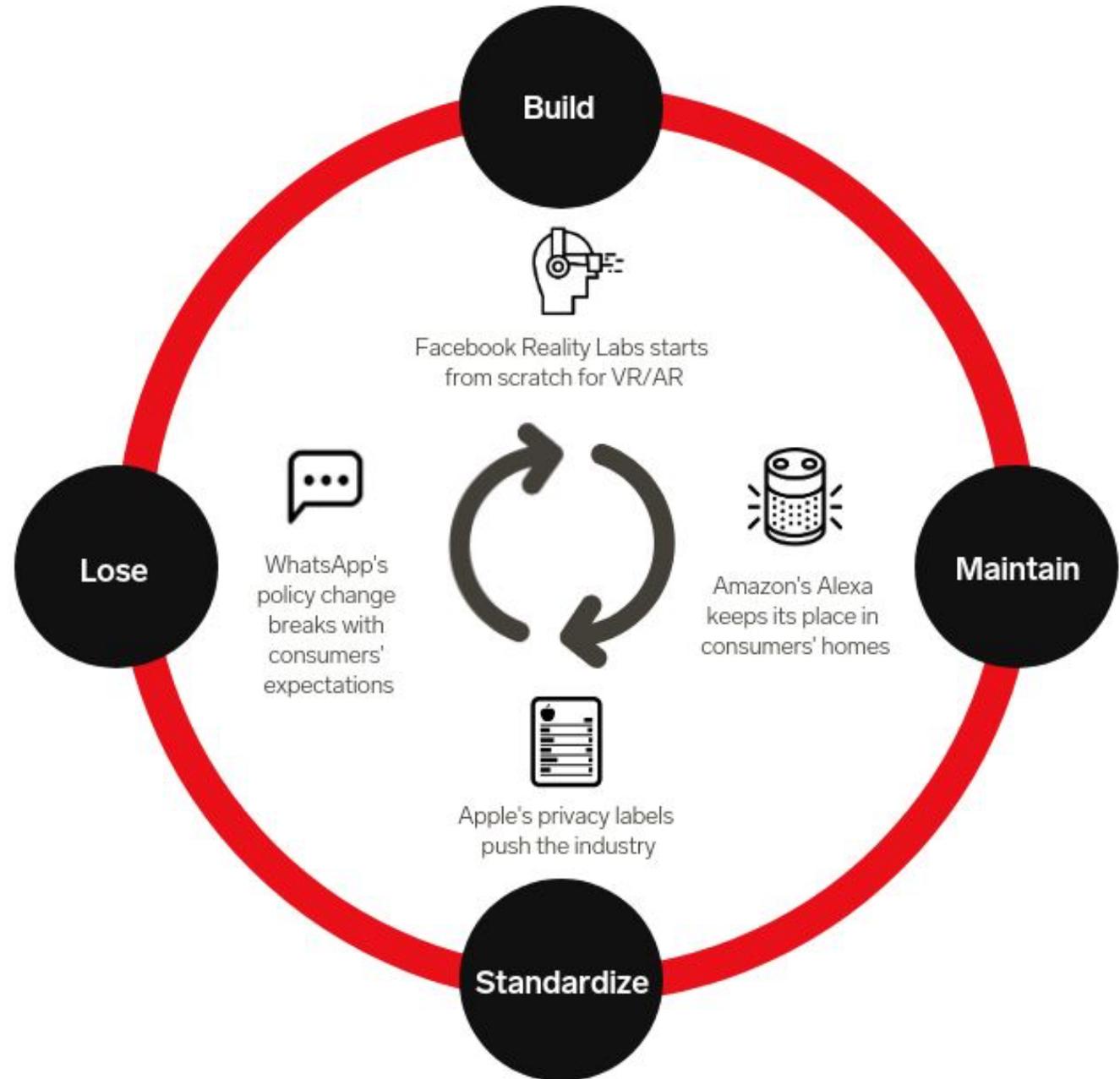
Source: Harvard Business Review (HBR), "The Value of Experience: Customer Needs Top the Innovation Agenda" commissioned by Mastercard, March 30, 2021

**Tech companies face many challenges in rebuilding consumer trust around data.**

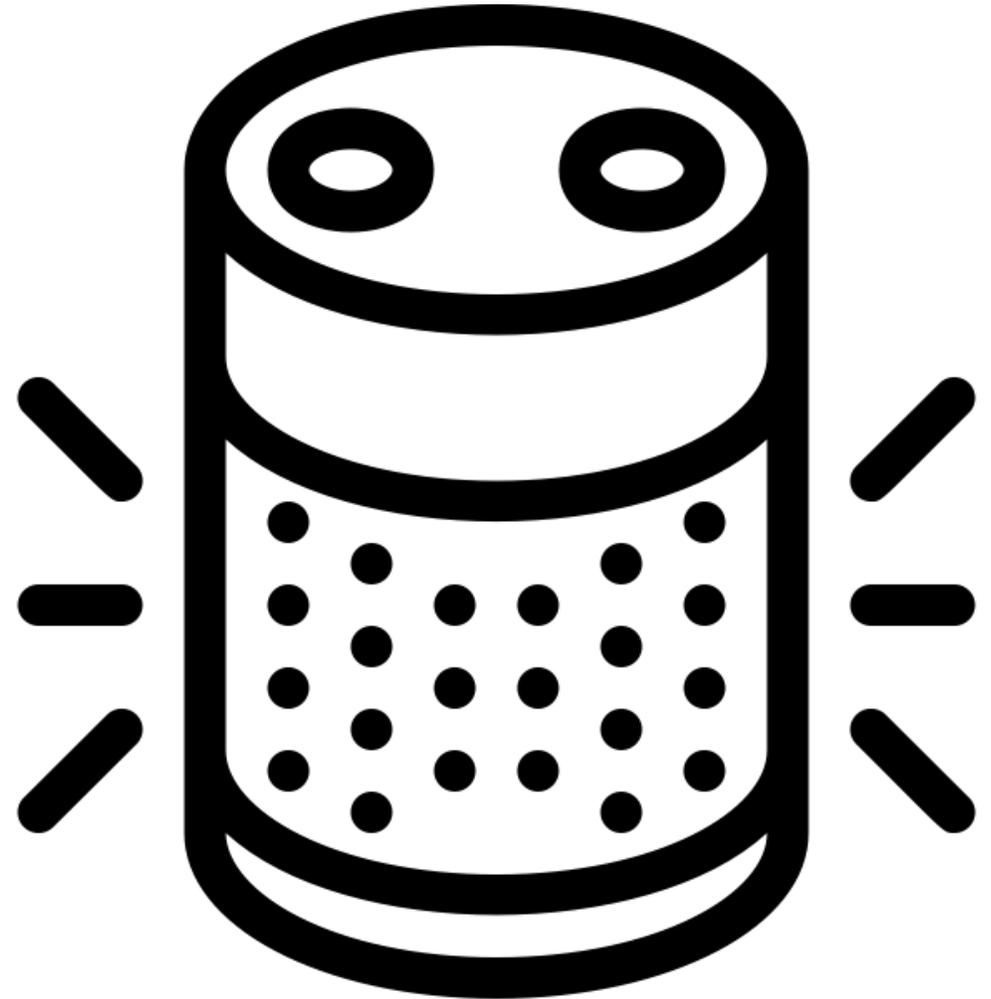
**Many are now developing data privacy strategies to address these trust issues.**

# Emerging technologies need strategies to address consumers' privacy and trust concerns.

The following case studies illustrate how technology companies are building, maintaining, standardizing—and sometimes losing—trust by being clear about their data practices and policies.



# Maintaining Trust in an Intimate Assistant: Alexa Trust

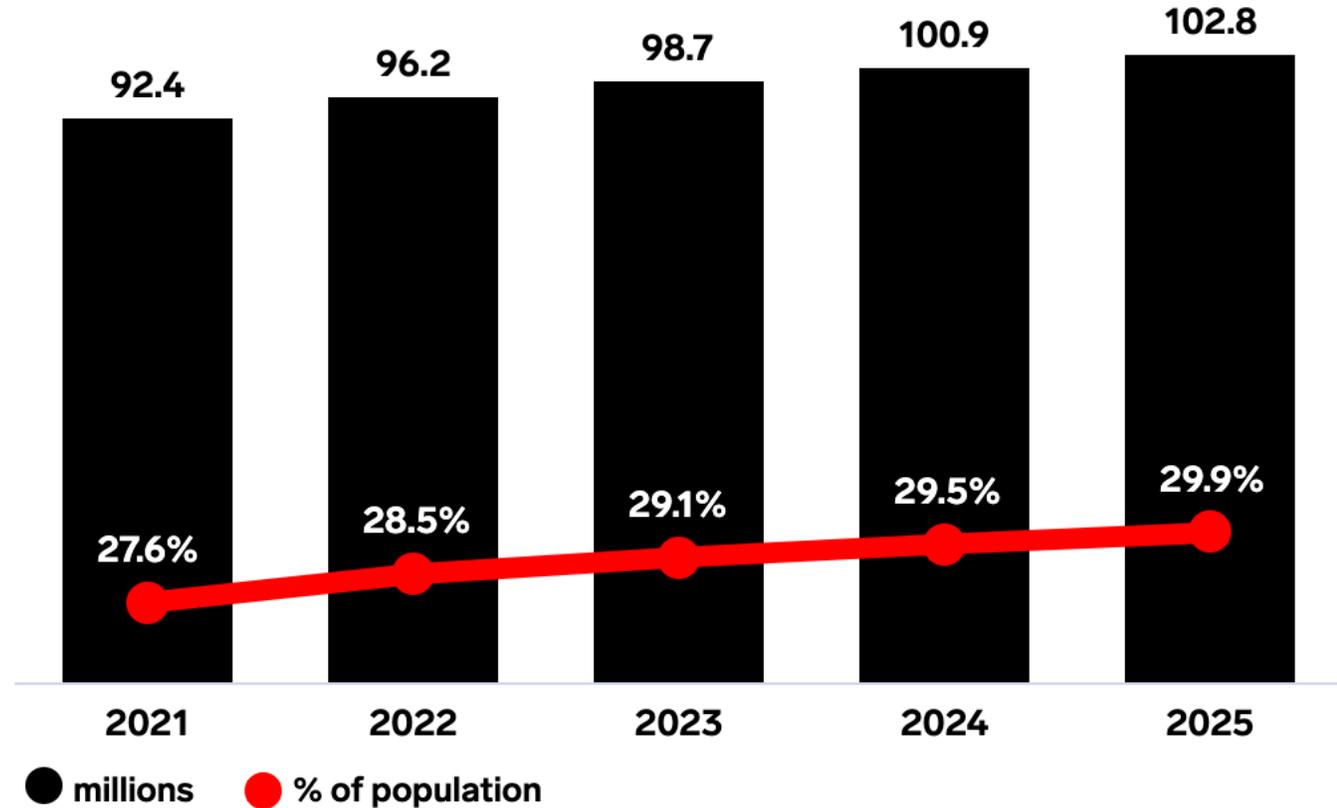


THE CHALLENGE

Smart speakers have been rapidly adopted, but growth may be tapering off.

## Smart Speaker Users

US, 2021-2025



Source: eMarketer, June 2021

eMarketer | InsiderIntelligence.com

# Smart speakers still face trust issues.

## Reasons that US Internet Users Do Not Own a Smart Speaker, April 2020

*% of respondents*

**It bothers you that smart speakers are always listening**

**66%**

**You worry that hackers could use smart speakers to get access to your home or personal information**

**65%**

**You don't trust the companies that make the smart speakers to keep your information secure**

**58%**

**You worry that smart speakers could allow the government to listen to your private conversations**

**46%**

*Note: ages 18+*

*Source: National Public Radio (NPR) and Edison Research, "The Smart Audio Report," April 30, 2020*

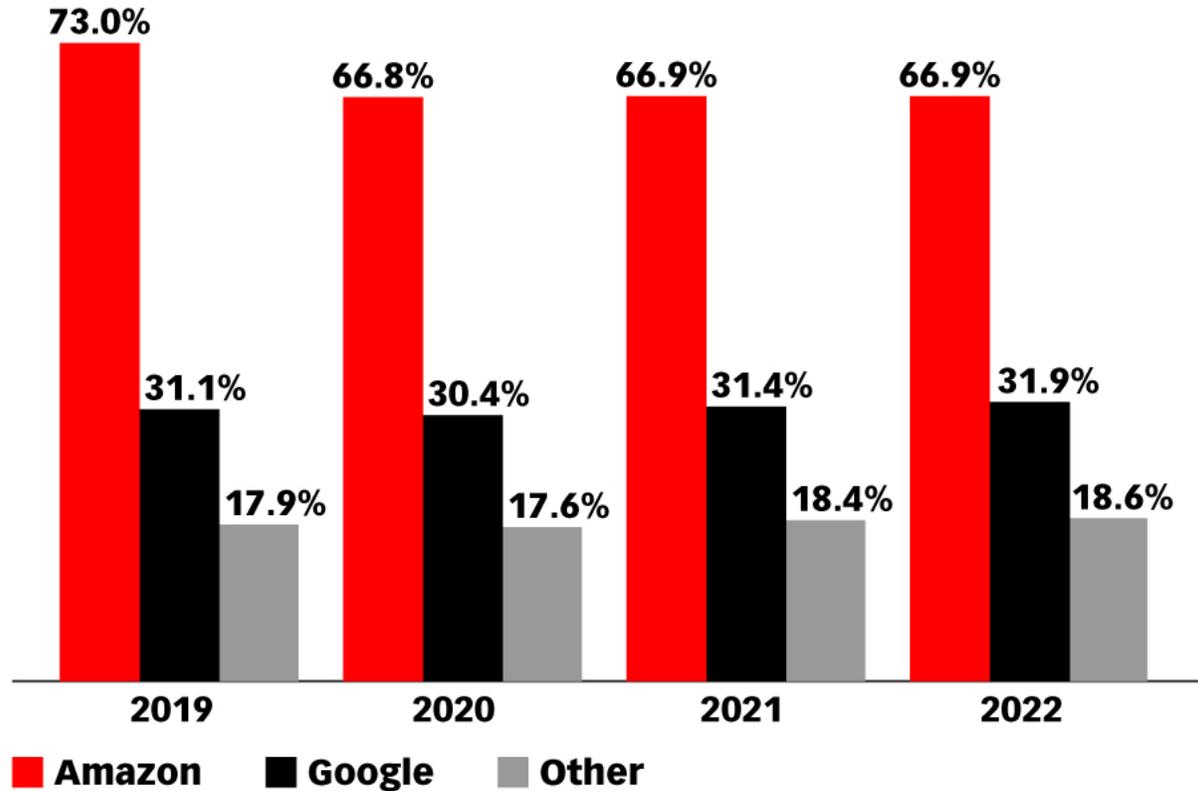
255316

[www.eMarketer.com](http://www.eMarketer.com)

Amazon increasingly faces competition.

### US Smart Speaker Users, by Brand, 2019-2022

% of smart speaker users



Note: individuals of any age who use smart speakers at least once a month on any device

Source: eMarketer, July 2020

258929

www.eMarketer.com

**“The future we envision for Alexa is not possible unless we earn and continually re-earn our customers’ trust in us.”**



Anne Toth

Director of Alexa Trust, Amazon

# Amazon's strategy to continually re-earn trust

## Design for transparent interactions.

Amazon has put a lot of emphasis on the **wake word**—saying “Alexa” to trigger user interactions. Such design features create “conscious friction” that help train and educate users about what to expect in an interaction with a relatively new user interface and experience.

## Explainability is key to maintaining trust.

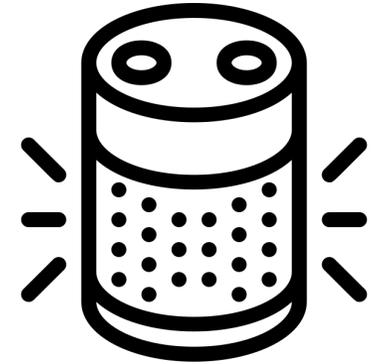
Alexa has introduced numerous commands that help explain its actions and behaviors. Like, “**Alexa, why did you do that?**” or “**Alexa, how do I review my privacy settings?**”

## Give users control.

Users can ask to “**delete everything I've ever said,**” and can change how long the platform holds on to interaction history and review which skills are connected to Alexa, including third-party interfaces with other smart home devices and applications.

## Dedicate organizational resources.

Amazon has an entire team dedicated to consumer perceptions of its smart assistant: **Alexa Trust**. Led by Toth, the team looks across the range of policy decisions that inform features on the platform.



# Maintaining Trust in an Intimate Assistant: Alexa Trust

## THE CHALLENGE

### Always-on listener

Barriers to adoption for new users are high. For US internet users who don't own a smart speaker, most said it bothers them that devices are always listening, and they don't trust companies to keep information secure, according to a 2020 NPR and Edison survey.

## THE STRATEGY

### Privacy by design

“Earn and continually re-earn our customers’ trust in us.” — Anne Toth, Alexa Trust

- **Design for transparent interactions**
- **Explainability is key to maintaining trust**
- **Give users control**
- **Dedicate organizational resources**

## COMPETITIVE IMPACT

### Maintain market share

27.2% of the US population will have smart speakers in their homes this year, and nearly two-thirds (66.9%) of smart speakers will be Amazon devices.

But Amazon's market dominance has taken a hit over time as competitive products from Google and Apple gain traction.

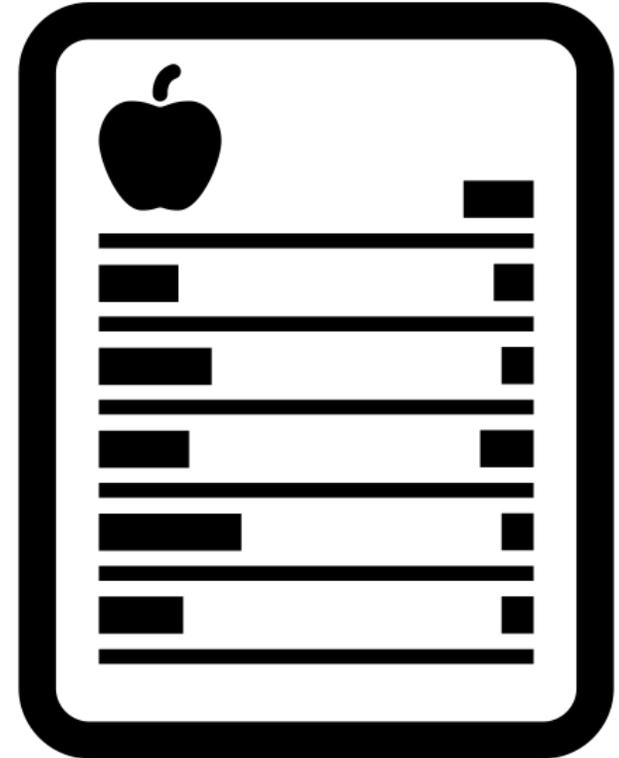
# The Washington Post

Consumer Tech • Perspective

## Amazon is about to share your Internet connection with neighbors. Here's how to turn it off.

You have no control over what sort of data flows over Amazon's new Sidewalk wireless network, which has been lying dormant in Echo smart speakers and Ring cameras ... until now

# Standardizing Trust in Platform Values: Apple's Privacy Strategy



THE STRATEGY

**Privacy is a  
fundamental  
human right...**

**and a core brand  
value for Apple.**

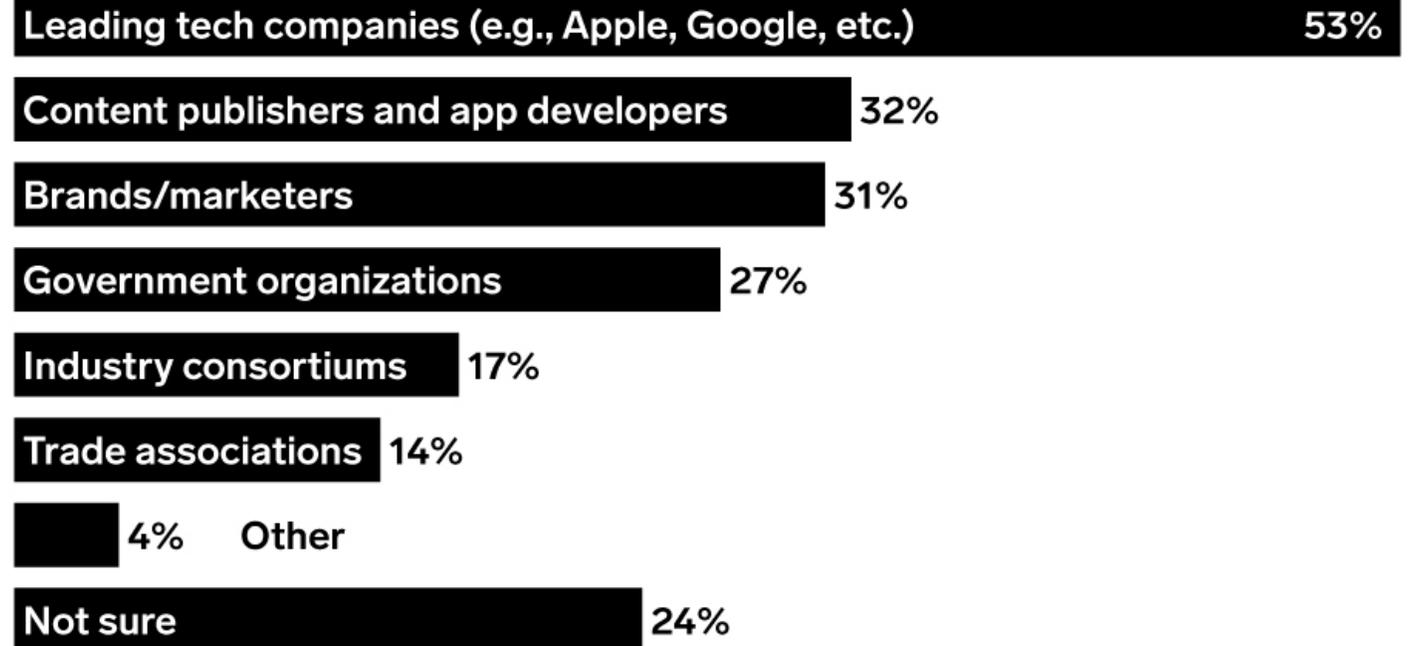


THE CHALLENGE

Consumers think tech firms are most responsible for educating consumers about the use of their personal data.

## Who Do US Smartphone Owners See as Responsible for Educating Consumers About the Usage of Personal Data?

% of respondents, Feb 2021



Source: AppsFlyer and MMA Global, "Personal Data, Privacy, & Smartphones: The Cautious Consumer," March 17, 2021

264613

eMarketer | [InsiderIntelligence.com](https://www.insiderintelligence.com)

# Apple doubles down on privacy features

## App Tracking Transparency

App Tracking Transparency requires apps to ask users for permission to track user activities across other apps and websites. The alerts are the platform's attempt to introduce meaningful, opt-in consent for advertisers using Apple's unique device identifier, **IDFA**.

## App Store Privacy Nutrition Labels and App Privacy Report

Privacy nutrition labels aim to put policies in plain terms for users, requiring app publishers to describe what types of data are being collected and for what purpose. App Privacy Report details what apps have used location, camera, and microphone access.

## Private Relay and Hide My Email

These iCloud features will encrypt internet traffic in Safari and allow users to share unique, random email addresses when they want to keep their email hidden.

## On-device processing for Siri

Rather than send voice assistant requests to the cloud, Apple devices are now capable of processing Siri requests on the device. This privacy feature also results in speed improvements and offline capabilities for voice commands.

**Users are increasingly willing to pay for subscriptions to avoid tracking.**

---

## Would US Smartphone Owners Prefer to Allow Data Tracking or to Pay a Subscription to Access an App?

*% of respondents, Feb 2021*

---

Would allow tracking to all the apps that I use to avoid paying subscription **31%**

Would not allow tracking to any apps, but I would prefer to pay a subscription for certain apps only **30%**

Would do something in the middle (e.g., allow some apps to track me and pay for some others) **30%**

Other **9%**

---

*Source: AppsFlyer and MMA Global, "Personal Data, Privacy, & Smartphones: The Cautious Consumer," March 17, 2021*

---

**Privacy is good for Apple's bottom line...**

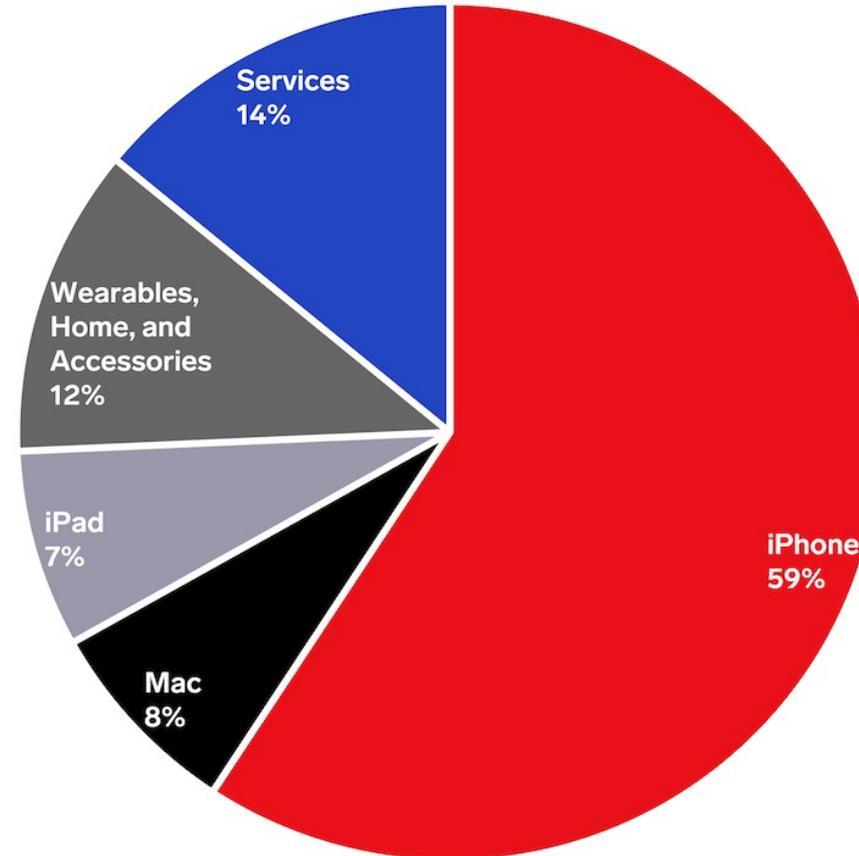
**and growth in services as the app ecosystem shifts away from ads to subscriptions.**

---

## How Apple Makes Money

Percentage of revenues by product, Q4 2020

---



---

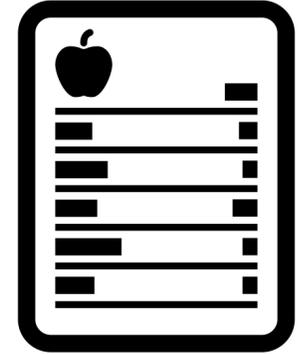
Note: Apple's Q4 ended December 26, 2020.

Source: Apple, 2020 Q4 Quarterly Earnings Report

1033314177183

InsiderIntelligence.com

# Standardizing Trust in Platform Values: Apple's Privacy Strategy



## THE CHALLENGE

### Platforms have values

Apple has already established itself as a privacy-friendly company among consumers. Now, it's leading the charge to hold the rest of the tech industry to its claims of high standards in the name of consumer protection.

## THE STRATEGY

### Set the standard

**Privacy nutrition labels** aim to put policies in plain terms for users, requiring app publishers to describe to users what types of data are being collected and for what purpose.

**App Tracking Transparency** requires app publishers to ask users to opt in to tracking their activities across other apps and websites.

## COMPETITIVE IMPACT

### Privacy versus antitrust?

Google announced it will require developers to disclose data practices for apps in a security section of its Google Play marketplace.

A shift toward subscriptions and away from ad-based app models is good for Apple's bottom line and its 30% cut.

# Losing Trust: WhatsApp's Policy Messaging



WhatsApp dominates messaging category penetration in key global markets.

**WhatsApp User Penetration, by Country**  
*2021, % of mobile phone messaging app users*

Argentina	96.8%
Austria	94.4%
Brazil	98.8%
Finland	95.6%
Germany	95.4%
India	97.0%
Indonesia	85.3%
Italy	96.8%
Mexico	87.7%
Netherlands	92.8%
Russia	84.6%
Spain	92.1%
Switzerland	96.4%
US	52.6%

Source: eMarketer, June 2021

eMarketer | [InsiderIntelligence.com](https://www.insiderintelligence.com)

# New monetization strategy demands policy updates.



## We're Updating Our Terms and Privacy Policy

Before you review, here are some things to know.



**We can't read or listen to your personal conversations, as they are end-to-end encrypted.**  
This will never change.



**We're making it easier to chat with businesses to ask questions and get quick answers.** Chatting with businesses is optional.

THE CHALLENGE

**Users misinterpreted the policy changes to mean that Facebook could now read encrypted messages.**

**Attitude Toward the Change in WhatsApp's New Privacy and Data Sharing Policy with Facebook According to Internet Users in Brazil, Feb 2021**

*% of respondents*

Believe it will not affect the information they collect about my profile

40.2%

It's an invasion/disrespect of privacy

25.8%

It is wrong to change the rules of use of the application later when I already use it

22.8%

I find it efficient to receive ads, friend suggestions, content more personalized to my profile, etc.

19.1%

None

13.7%

Other

0.6%

Note: n=823 ages 18+

Source: Toluna, "Redes sociais," Feb 23, 2021

264516

eMarketer | [InsiderIntelligence.com](https://www.insiderintelligence.com)

# Signal and Telegram Downloads Soared

**7.5M**

downloads of Signal worldwide from January  
6–10, 2021

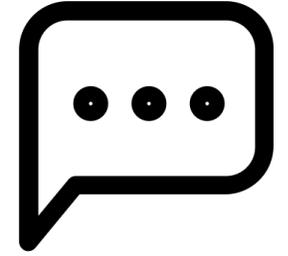
40x higher than the preceding week

(Sensor Tower, 2021)

**5.6M**

downloads of Telegram during the same  
period

(Apptopia, 2021)



# Losing Trust: WhatsApp's Policy Messaging

## THE CHALLENGE

### Monetization moment

WhatsApp maintains that “Privacy and Security is in our DNA,” and the app encrypts messages by default.

But the messaging platform needs to change its data handling policies to enable businesses to reach consumers for ecommerce and payments transactions, as well as to monetize the platform.

## THE STRATEGY

### Bungled messaging

Users interpreted the new terms to mean that Facebook would be able to access the content of their private, encrypted messages because the messaging wasn't clear.

And the ultimatum was aggressive—accept or stop using WhatsApp altogether by the deadline.

## COMPETITIVE IMPACT

### Competitors surge

Consumers voted with their feet by downloading encrypted messaging apps from Signal and Telegram.

The policy rollout is still uncertain across the globe as regulators push back.

**Digital transformation elevates  
the importance of every company's  
relationship to consumers  
through their data.**

# Best Practices for Differentiating on Privacy

## Give users agency and control.

Concerns over consumer privacy have evolved away from exposure and data collection and toward **autonomy, choice, and control**. Consumers need mechanisms for stating their preferences and intent.

## Take first-party responsibility seriously.

Evaluate where consumer trust lies and focus on providing benefits to consumers there. The paradigm shift to first-party relationships **should not be an opportunity for exploitation**.

# More Best Practices for Differentiating on Privacy

## Build in privacy by design.

Ask yourself, what's the minimum amount of data needed to serve a customer's needs?

## Ask for meaningful consent.

Allow users to opt in, rather than opt out.

## Reveal default settings.

Make defaults privacy-protecting from the start. Make them clear to users and provide opportunities to change settings from the outset.

## Write simple, clear policies.

Spell out what the firm will and won't do with users' data. Don't make them wade through 75+ hours' worth of legalese.

## Be honest about the business model.

Consumers increasingly understand the value exchange for their data. Companies that are honest and upfront about their business models will earn more trust and respect from consumers.

## Prioritize user testing and feedback.

Solicit user feedback at every step of the development cycle, seek out your blind spots, watch for unanticipated use cases, and evaluate how nonusers are affected by the technology in their environments.

## Value changes require culture shifts.

Dedicate cross-functional teams to oversee privacy-centric thinking across the organization. Establish processes and performance metrics that prioritize and value consumer privacy.

**What are you going to do to  
earn consumers' trust based on  
your data and privacy practices?**

# Thanks for joining today's Meet the Analyst Webinar!

You can register for upcoming Meet the Analyst and Tech-Talk Webinars at [emarketer.com/webinars](https://emarketer.com/webinars)

July 14 | How to Get Started with Customer Journey Analytics

July 15 | Ad Targeting in the Extended Identity Crisis

July 19 | Trendspotting: Keep Your Finger on the Pulse of Your Industry

July 20 | The State of Email Analytics: How Privacy Updates Will Affect Your Reporting

Be sure to also check out eMarketer's "Behind the Numbers" podcast for daily, freewheeling conversations about the ways digital is transforming media, marketing, business and even life.

Tune in: [emarketer.com/articles/topics/emarketer-podcast](https://emarketer.com/articles/topics/emarketer-podcast)

Made possible by

