Meet the Analyst Webinar
July 8, 2021 | Begins at 2:00 PM ET

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

Kelly Kimura
Senior Director of Product Management
Vericast

Debra Aho Williamson
eMarketer Principal Analyst
Insider Intelligence

*Made possible by Valassis*
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

- **89%**
  - I care
    - I care about data privacy
    - I care about protecting others
    - I want more control

- **70%**
  - 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

- **29%**
  - 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
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.
Trust in the tech industry is declining, including trust in emerging technologies.
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

<table>
<thead>
<tr>
<th>Reasons why not</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Too hard to figure out what companies are actually doing</td>
<td>79</td>
</tr>
<tr>
<td>with my data</td>
<td></td>
</tr>
<tr>
<td>If I want the service, I have to accept how my data</td>
<td>51</td>
</tr>
<tr>
<td>is used</td>
<td></td>
</tr>
<tr>
<td>Feel my personal data is already available</td>
<td>45</td>
</tr>
<tr>
<td>Don’t understand what service choices are</td>
<td>44</td>
</tr>
<tr>
<td>Don’t trust companies to follow stated policies</td>
<td>40</td>
</tr>
</tbody>
</table>

Note: n=2,602 ages 18+
Source: Cisco, “Consumer Privacy Survey,” Oct 21, 2020

Able to effectively protect personal data

No 48%
Yes 52%
Innovation-leading companies prioritize and invest in data privacy.

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

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
Smart speakers have been rapidly adopted, but growth may be tapering off.
Smart speakers still face trust issues.

<table>
<thead>
<tr>
<th>Reason</th>
<th>% of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>It bothers you that smart speakers are always listening</td>
<td>66%</td>
</tr>
<tr>
<td>You worry that hackers could use smart speakers to get access to your home or personal information</td>
<td>65%</td>
</tr>
<tr>
<td>You don’t trust the companies that make the smart speakers to keep your information secure</td>
<td>58%</td>
</tr>
<tr>
<td>You worry that smart speakers could allow the government to listen to your private conversations</td>
<td>46%</td>
</tr>
</tbody>
</table>

Note: ages 18+
Source: National Public Radio (NPR) and Edison Research, "The Smart Audio Report," April 30, 2020
Amazon increasingly faces competition.
“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.
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
Privacy is a fundamental human right...

and a core brand value for Apple.
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 |
|---------------------------------|------------------|
| Leading tech companies (e.g., Apple, Google, etc.) | 53% |
| Content publishers and app developers | 32% |
| Brands/marketers | 31% |
| Government organizations | 27% |
| Industry consortiums | 17% |
| Trade associations | 14% |
| Other | 4% |
| Not sure | 24% |

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

<table>
<thead>
<tr>
<th>Preference</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Would allow tracking to all the apps that I use to avoid paying subscription</td>
<td>31%</td>
</tr>
<tr>
<td>Would not allow tracking to any apps, but I would prefer to pay a subscription for certain apps only</td>
<td>30%</td>
</tr>
<tr>
<td>Would do something in the middle (e.g., allow some apps to track me and pay for some others)</td>
<td>30%</td>
</tr>
<tr>
<td>Other</td>
<td>9%</td>
</tr>
</tbody>
</table>

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.
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.

<table>
<thead>
<tr>
<th>Country</th>
<th>Penetration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Argentina</td>
<td>96.8%</td>
</tr>
<tr>
<td>Austria</td>
<td>94.4%</td>
</tr>
<tr>
<td>Brazil</td>
<td>98.8%</td>
</tr>
<tr>
<td>Finland</td>
<td>95.6%</td>
</tr>
<tr>
<td>Germany</td>
<td>95.4%</td>
</tr>
<tr>
<td>India</td>
<td>97.0%</td>
</tr>
<tr>
<td>Indonesia</td>
<td>85.3%</td>
</tr>
<tr>
<td>Italy</td>
<td>96.8%</td>
</tr>
<tr>
<td>Mexico</td>
<td>87.7%</td>
</tr>
<tr>
<td>Netherlands</td>
<td>92.8%</td>
</tr>
<tr>
<td>Russia</td>
<td>84.6%</td>
</tr>
<tr>
<td>Spain</td>
<td>92.1%</td>
</tr>
<tr>
<td>Switzerland</td>
<td>96.4%</td>
</tr>
<tr>
<td>US</td>
<td>52.6%</td>
</tr>
</tbody>
</table>

*Source: eMarketer, June 2021*
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.
Users misinterpreted the policy changes to mean that Facebook could now read encrypted messages.

<table>
<thead>
<tr>
<th>% of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Believe it will not affect the information they collect about my profile</td>
</tr>
<tr>
<td>It's an invasion/disrespect of privacy</td>
</tr>
<tr>
<td>It is wrong to change the rules of use of the application later when I already use it</td>
</tr>
<tr>
<td>I find it efficient to receive ads, friend suggestions, content more personalized to my profile, etc.</td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td>Other</td>
</tr>
</tbody>
</table>

*Note: n=823 ages 18+  
Source: Toluna, “Redes sociais,” Feb 23, 2021*
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.
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

- 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