

PUBLIC MORE OPEN TO TECH COMPANIES SHARING THEIR DATA—BUT THERE'S A LIMIT

An Ipsos Point of View

By Emmanuel Probst

GAME CHANGERS





KEY TAKEAWAYS

- People are increasingly comfortable sharing their data, especially Millennials and members of Gen Z.
- Despite this, users are increasingly concerned about how tech companies collect, analyze and monetize their data.
- 71% of consumers would stop doing business with a company if it gave away sensitive information without permission.

The COVID-19 pandemic prompted technology users to rely on devices not only to entertain ourselves, but to order groceries, find testing and vaccination sites, and keep in touch with loved ones. Indeed, we have been using technology across a wider range of tasks: in North America, the amount of data passing through our smartphones every month went from 5 gigabytes in 2017 to 11.1 gigabytes in 2020 and is projected to reach 48 gigabytes **by 2026**.

Further, more than 2 billion people use Facebook Messenger, Google Assistant, and Amazon Echo, allowing brands to communicate directly with them and serve them personalized content and offerings. Technically, the data each user provides to these devices can easily be combined with their search and browsing history, media consumption, email information, in-home security, geolocation data, and even facial recognition.

Most recently, TikTok updated its privacy policy to disclose that it “may collect biometric identifiers and biometric information” from user content. This includes things like [“faceprints and voiceprints.”](#)

Amid these trends, people are becoming increasingly comfortable sharing their data. Indeed, nearly half of users will happily give their information away in return for personalized services and products— a 7% rise **since 2013**.

Millennials and members of Gen Z are even more inclined than other age cohorts (over 50%) to share their data with tech brands, as they are more exposed to the benefits through curated Spotify playlists and TikTok’s algorithmically produced “For You” videos, along with similar offering on other platforms.

Where’s Your Data Going?

Despite this comfort, users have become increasingly concerned and mindful of the ways in which tech companies collect, analyze and monetize their data. A recent Ipsos Study reveals that 66% of people are more concerned about privacy and security, and 57% feel they need to learn more about ways to protect themselves.





Data usage is also increasingly regulated through legislation. In Europe, this is via the General Data Protection Regulation (GDPR); in the U.S., it's at the state level, with acts in California (the California Consumer Privacy Act), Virginia (the Consumer Data Protection Act), and Colorado (the Colorado Privacy Act). These laws bring some transparency into what data is being collected and stored and empowers users to control how their data is being used.

For example, Article 17 of the UK GDPR gives individuals the right to have their personal data erased. This is also known as the “right to be forgotten.” Indeed, users are anxious to protect themselves from having their information misused, and simply being “spied on.”

Brands must therefore reassure users on how their data is used, as 71% of consumers would stop doing business with a company if it gave away sensitive information **without permission**.

Consumers Ambivalent on Tech Brands

Ipsos research shows that brand trust is correlated with increased favorability, consideration and usage. For example, 77% of those who use Apple products trust Apple completely or a lot, versus only 20% of Apple users who trust the brand slightly or not at all. As for future usage, 84% of those who trust Apple a lot would use its product in the future compared to 31% for those who trust Apple slightly or not at all.

When it comes down to data privacy, users' trust in tech brands is ambivalent. That is, 62% of people surveyed say they trust Google completely or a lot, but only about a third believe Google does not force them to allow personalized ads (37%), does not sell their personal data (35%) or retain audio recordings from Google Assistant (30%).

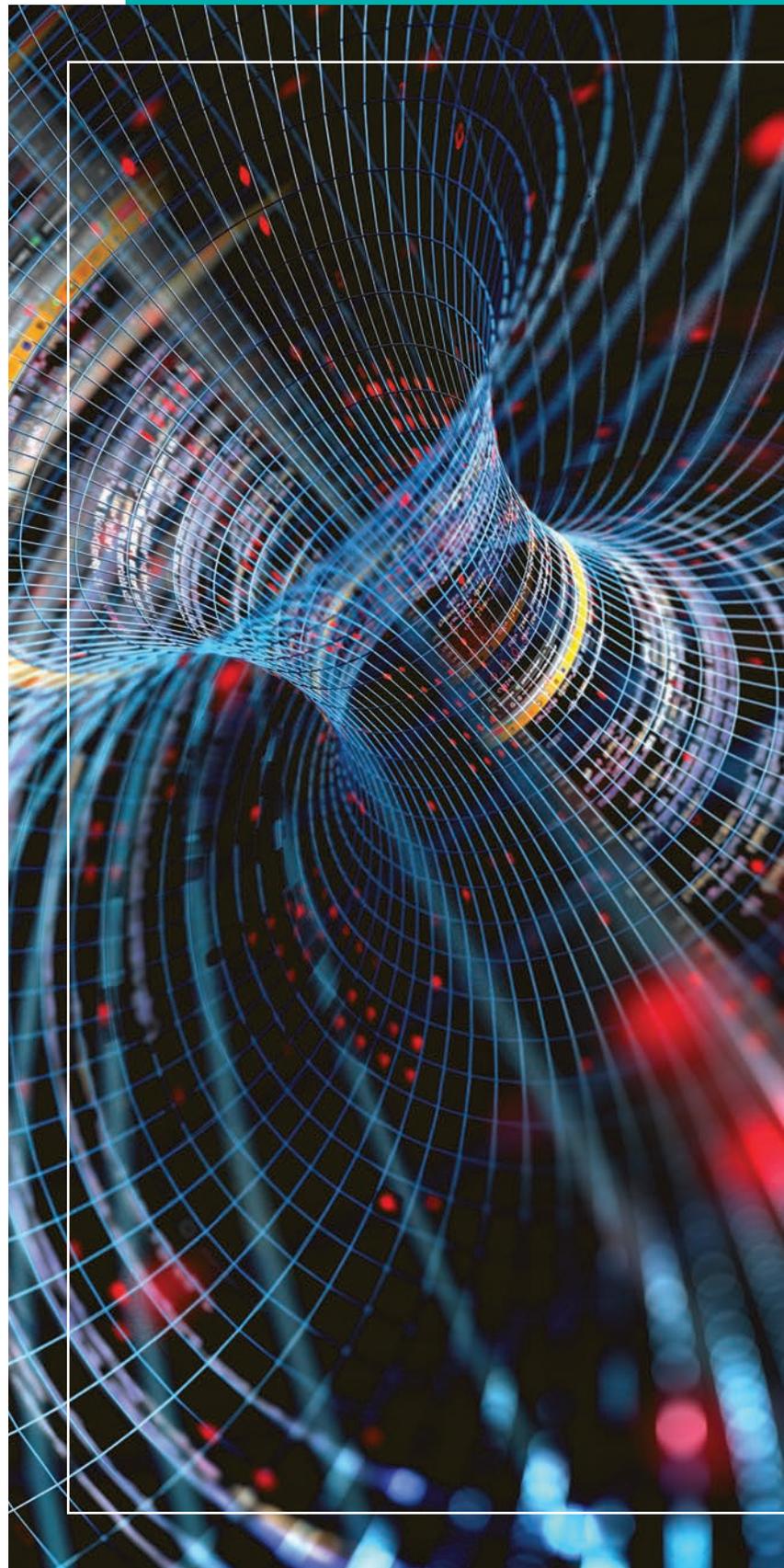
Interestingly, these same Ipsos studies reveal that consumer trust increases when tech brands educate them about privacy and security. Indeed, 78% of people believe that tech brands are responsible for educating them about privacy and security, ahead of schools (74%), government agencies and employers (70%), and their friends and family (59%).

Ipsos further investigated users' trust in tech brands, depending on whether the brand would provide users with: (1) no information about data privacy, (2) some information on the benefits of sharing their data, or (3) kept their data private. This survey shows that 40% of users trust Google with their purchase history no matter what, almost 50% trust Google when it articulates the benefits of keeping this purchase history, and 52% trust Google when the brand explains that it would not misuse said purchase history.

A Complicated Consumer-Tech Relationship

People will share an exponential amount of personal data with tech brands, across an increasingly wide and diverse range of devices and platforms. Tech brands can continue to further monetize data as long as they provide their users with tangible benefits and reassure them that their practices are transparent and ethical. Here are some guidelines to help tech brands collect and monetize for years to come.

- **Education:** as discussed above in this paper, tech brands must educate the public on how they collect, analyze, monetize, and store data, and how these actions benefit users
- **Data sovereignty:** tech-centric terminology such as “cloud computing” and “algorithm” sound elusive to most people and trigger anxiety for some. Tech brands can reassure the public by showing them where their data is stored, preferably in their users' country of residence.
- **Credibility:** with its “Azure Government Top-Secret” service, Microsoft demonstrates its ability to handle sensitive information on behalf of government agencies. In a similar vein, messaging services like Telegram and Signal promise to encode users' messages. This brings some credibility and even mystique to these brands, reminiscent of the spies depicted in popular culture.
- **Data preservation:** many data sets are important and precious for the future of humanity, like gene sequences, knowledge of geography and physics, and demographic data. Tech brands can help government agencies, scientists and academics store and organize this data, and help keep the world's knowledge safe and secure.



About the Author

Emmanuel Probst

Global Lead, Brand Thought-leadership, Ipsos
emmanuel.probst@ipsos.com

About Ipsos

At Ipsos we are passionately curious about people, markets, brands, and society. We deliver information and analysis that makes our complex world easier and faster to navigate and inspires our clients to make smarter decisions. With a strong presence in 90 countries, Ipsos employs more than 18,000 people and conducts research programs in more than 100 countries. Founded in France in 1975, Ipsos is controlled and managed by research professionals.