# People feel watched, weary and lacking control in the digital age

Consumers are often pragmatic about sharing data, but willingness falls as it becomes more personal

Summarise Share ··· Add BT as a preferred source

阅读简体中文版 (beta)

At the heart of privacy anxiety is a basic human need: the desire for control in a world that feels increasingly opaque. PHOTO: PIXABAY

Ramanathan Vythilingam

Published Sat, Mar 28, 2026 · 07:15 AM

WE LIVE in a world shaped by the idea that data is the new oil.

It rests on an unspoken bargain: people give organisations access to their personal data in exchange for convenience, speed and more tailored experiences in how they shop, travel, bank, consume content and even manage their healthcare.

But as data collection accelerates, that bargain is becoming harder to understand and trust.

Every headline about a data breach now feels personal. The systems under attack are the very ones people rely on daily, and in many incidents the data at risk is their own.

For instance, the recent disclosure by the Singapore government that cyber-espionage group UNC3886 had targeted critical information infrastructure, including major telcos, was a reminder that data risk is no longer a niche technology issue. It is now a mainstream business issue with implications for trust, continuity and national resilience.

New research conducted by the Nanyang Centre for Marketing and Technology at Nanyang Business School across 10 markets – Singapore, Malaysia, Indonesia, Thailand, the Philippines, South Korea, Japan, China, the US and UK – showed that privacy is no longer viewed simply as a technical matter. It is a lived emotional experience.



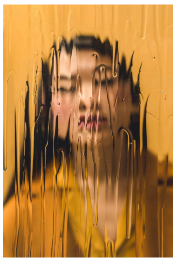
## People know their data is valuable

One of the clearest signs of discomfort is how people react to being targeted online by brand messages.

Consumers may not understand the technical details of cookies, personal identifiers or cross-device tracking, but they can tell when their digital activity is being watched.

The survey captures this unease. In the UK and US, 73 per cent and 67 per cent of consumers, respectively, said such targeting leaves them feeling "creeped out" or "annoyed".

SEE ALSO



**The terrible cost of the infinite scroll**

**Beyond the breach: Legal risks following cyber incidents**


**Budget 2026: Singapore mandates stricter security for home routers, raises bar for critical infrastructure**

More

That contrasts sharply with South-east Asian markets such as Singapore, Malaysia and the Philippines, where fewer than 35 per cent express the same sentiment.

Despite their concerns, consumers are often pragmatic about sharing data. Globally, 71 per cent are willing to share basic demographic information such as age, gender and date of birth.

But willingness falls sharply as the data becomes more personal, such as contact details, online behaviour or location data.

Across countries and age groups, one point is clear: people know their data has value. In return for sharing it, they expect something meaningful. Exclusive discounts, loyalty rewards, faster service and personalisation all form part of that value exchange.

When handled well, data can create a genuine win-win. Companies gain loyalty and relevance, while customers receive experiences that feel more useful and less wasteful.

But that exchange depends on one thing above all: trust.

---

"Consumers are not demanding perfection. They are asking for honesty, transparency and the ability to say no, or to withdraw an earlier yes, without being penalised."

---

When people have greater trust in regulators to hold companies accountable for protecting personal data, willingness to share rises.

In our survey, that increase is particularly pronounced in China, where higher trust corresponds with a 42-percentage-point increase in willingness to share data. This comes as China's Cyberspace Administration issued fresh guidance in January clarifying expectations around personal information protection.

We also see this trend in other markets such as the Philippines (+29 percentage points) and Indonesia (+24 percentage points).

The business implications are significant. Once trust breaks down, the fallout can quickly extend beyond compliance into reputation and leadership accountability.

South Korean e-commerce giant Coupang has faced intense scrutiny and legal action following a major customer data leak in 2025, showing how quickly a privacy incident can escalate into a leadership issue.

Consumers are not demanding perfection. They are asking for honesty, transparency and the ability to say no, or to withdraw an earlier yes, without being penalised.

## Trust must be earned, not assumed

At the heart of privacy anxiety is a basic human need: the desire for control in a world that feels increasingly opaque.

Companies can no longer rely on the legal cover of dense terms and conditions. While such language may help in a court of law, it does little in the court of public opinion. Singapore's Personal Data Protection Commission told private organisations to stop using NRIC numbers for authentication by Dec 31, 2026, with enforcement to start from Jan 1, 2027.

When asked what would increase their trust in companies requesting data, consumers across markets consistently point first to transparency in how their information is used.

They also value certifications of data security, easy ways to opt out or delete their data, and clear explanations of why specific information is needed. These are not merely technical features. They are signals of respect and control.

The lesson for business is clear. As technology becomes more sophisticated in collecting, inferring and deploying personal data, companies must ensure these capabilities do not come at the expense of trust.

The privacy challenge goes beyond how much data is collected. It is about whether consumers believe the exchange is fair – whether they receive real value, understand how their data is being used and retain some control over it.

Across markets, the survey points to the same conclusion: people are willing to share data, but only when they trust the institution on the other side.

Artificial intelligence will only raise these expectations. Companies that embed privacy into products, governance and customer experience will be better placed to earn trust and keep it. Those that continue to treat privacy as a compliance function risk losing far more than data, which is customer confidence.

**The writer, an associate professor at Nanyang Business School, Nanyang Technological University, has over 20 years of industry experience in consumer and market insights**