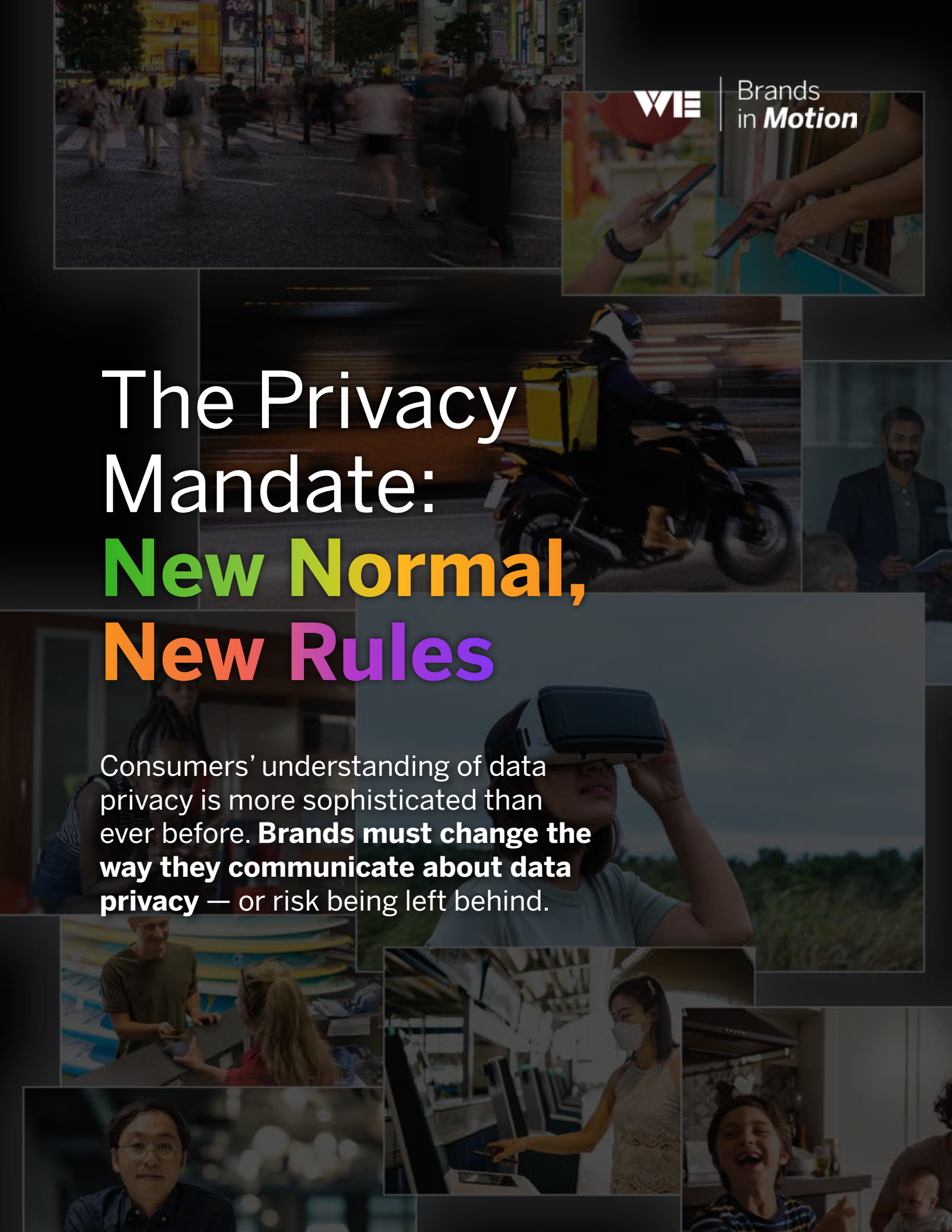


WE | Brands in *Motion*

The Privacy Mandate: New Normal, New Rules

Consumers' understanding of data privacy is more sophisticated than ever before. **Brands must change the way they communicate about data privacy** — or risk being left behind.

Table of Contents

Change is coming.

For years, most consumers reacted to brands' data privacy stories with disinterest or distrust. Hard-to-decipher end-user license agreements (EULAs), high-profile data breaches and ethical abuses dominated the data privacy conversation, and many consumers tuned out. But the rise of broad data regulation and the pandemic's reconfiguration of work and life have made the average consumer much more sophisticated in their understanding of how their data is collected and used.

For brands, the old check-the-box approach of burying data usage policies in a EULA won't cut it anymore. It's time to rethink what privacy means to consumers and how to communicate the value that brands' usage of first-party data can provide to both their customers and the world at large. Brand communicators must take the lead in privacy conversations and make data privacy a compelling, relevant part of a brand's relationship with its customers. **Brand communicators must take the lead in privacy conversations and make data privacy a compelling, relevant part of a brand's relationship with its customers.**

Three new normals changing the data privacy landscape

1. More sophisticated consumers

The average internet user is more global, more sophisticated and more ready to spend money on products online. Between 2019 and 2021, more than 780 million people[1] accessed the internet for the first time, with much of that growth driven by consumers in APAC[2]. Many of these new users turned to online shopping when lockdowns and movement restrictions made it more challenging to visit physical stores. Since the beginning of the pandemic, Southeast Asia alone has added 70 million internet shoppers.

2. International regulation

The last few years have seen governments enacting broad, headline-catching regulations, including the EU's General Data Protection Regulation (GDPR), China's Personal Information Protection Law (PIPL) and Singapore's recent bolstering of its Personal Data Protection Act (PDPA). Brands must navigate overlapping regulatory environments, too — in the U.S., certain states have privacy legislation that brands must follow along with the federal government's guidelines, and the U.K. is looking to write its own GDPR-overlapping data protection laws following its exit from the EU.

3. The pandemic

During the COVID-19 pandemic, consumers in most developed markets have had to surrender a certain amount of privacy to participate in society. Contact tracing solutions that track citizens' movements, such as TraceTogether in Singapore, color-coded QR codes in China and Test & Trace in the U.K., are commonplace. Even in the U.S., where consumers often hesitate to share personal information with government agencies, mobile contact tracing apps have become part of daily life.

[1] https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

[2] https://techwireasia.com/2020/05/3-trends-underpinning-asias-booming-internet-economy/

Modern customers understand how brands use their data:

97% say data privacy is important.

73% think their data is used to target or re-target ads that serve them better.

69% think that brands use collected data to develop or refine their marketing strategy to better suit their customers' needs.

69% believe that brands use their data to create personalized content and advertisements.

The white space for communicators

In 2021, WE Communications' Brands in Motion report "The Bravery Mandate" showed that over 73% of consumers globally[3] would stop using a brand's product or service if they felt their data was being used unethically. But as the data privacy landscape shifts, where's the line between uncomfortable and unethical? And what do consumers want out of data privacy communications?

Communicators have a unique role to play in helping win the hearts and minds of online consumers. Across an enterprise, many departments contribute to collecting, maintaining and using consumer data. Technology teams are assigned to make sure that the data is safe, and compliance teams decide how to manage data to comply with regulations. The role of communicators has generally been limited to managing the response and stakeholder impact of data breaches or failures to meet regulatory requirements.

For modern consumers, data privacy is not just about cybersecurity or keeping confidential material such as identifiable data, financial information and electronic health records secure, nor is it the legal and regulatory work that goes into making sure brands are acting within the law.

For modern consumers, "data privacy" refers to the consumer's understanding of how an organization is gathering their data and what it's using their data for. The key word here is "understanding." **This is where communications teams must operate in the new normal — educating, telling data privacy stories and engaging with consumers as part of their experience with the brand.**

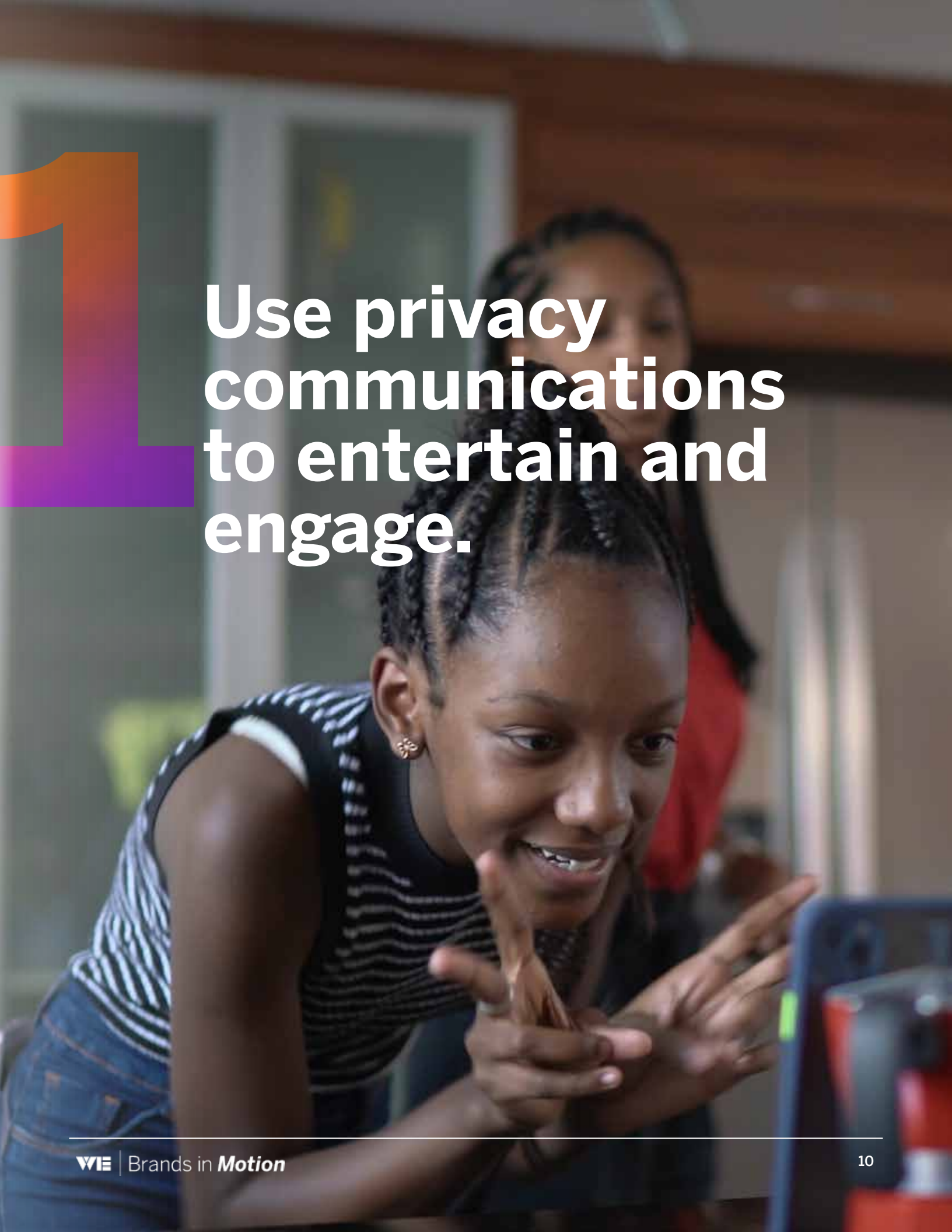
[3] "The Bravery Mandate" dataset includes Germany and South Africa, which were not surveyed for "The Privacy Mandate."

Three ways communicators can own the data privacy conversation

1 Use privacy communications to entertain and engage.

2 Establish a relationship built on safety.

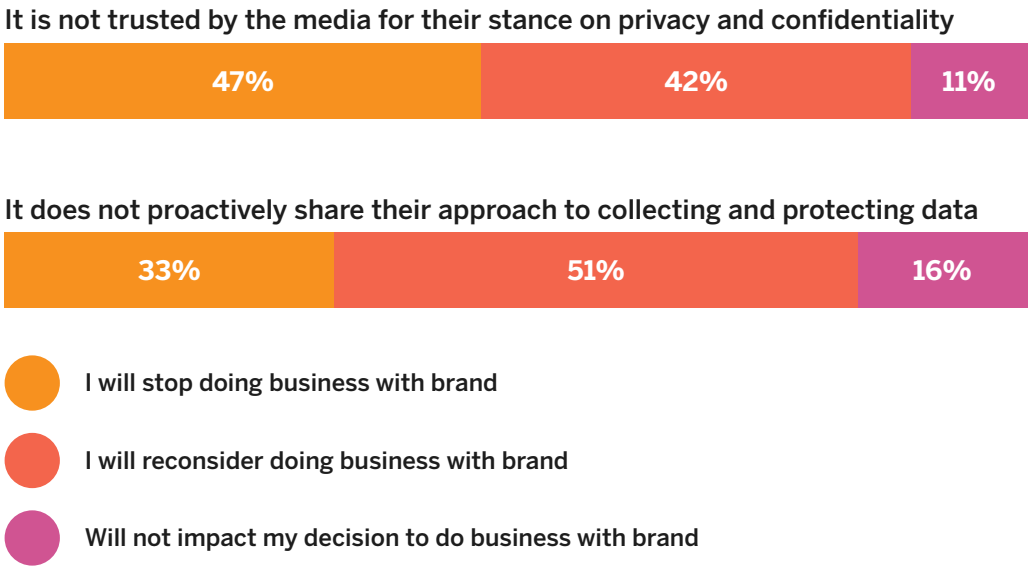
3 Prove you've kept your promises.



1 Use privacy communications to entertain and engage.

Too often, the communications function only works on data privacy when something goes wrong — think crisis communications teams activating to clean up the damage after a data breach — but brands that only engage comms teams in a crisis are missing out on an engagement opportunity. Global consumers want brands to **proactively share their approach to collecting and protecting data** and to **build trust with the media for their stance on privacy and confidentiality**. If a brand chooses not to do this, most consumers will reconsider doing business with it — or stop entirely.

Impact on willingness to do business with brands



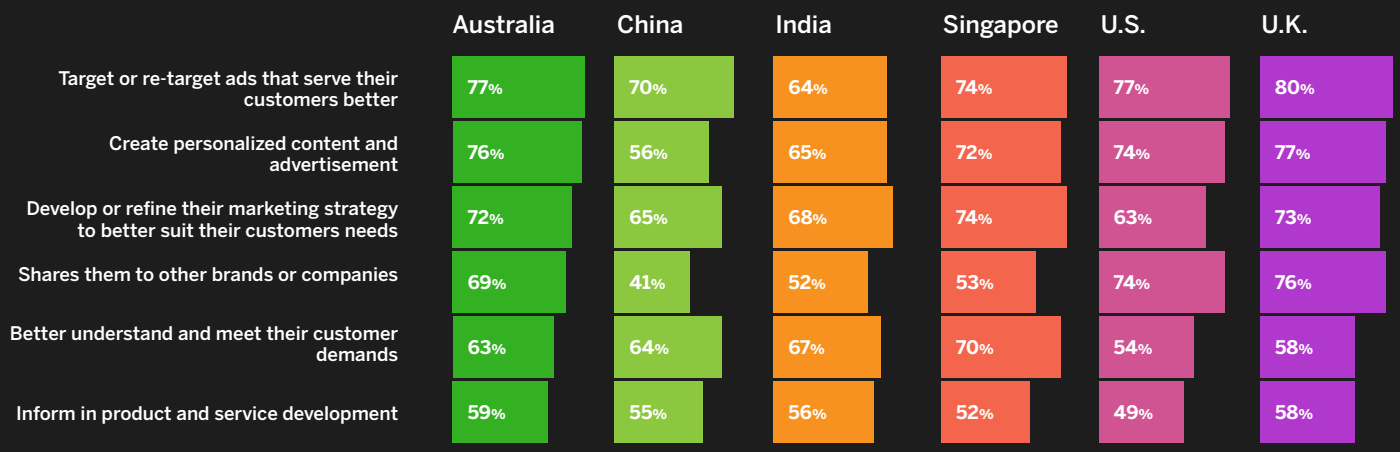
Building trust with the media and proactively engaging consumers is where communicators can shine. **Communications can and must be part of the customer's data privacy experience from end to end** — not just when disaster strikes — creating outstanding experiences and relevant stories through the transparent use of first-party data.

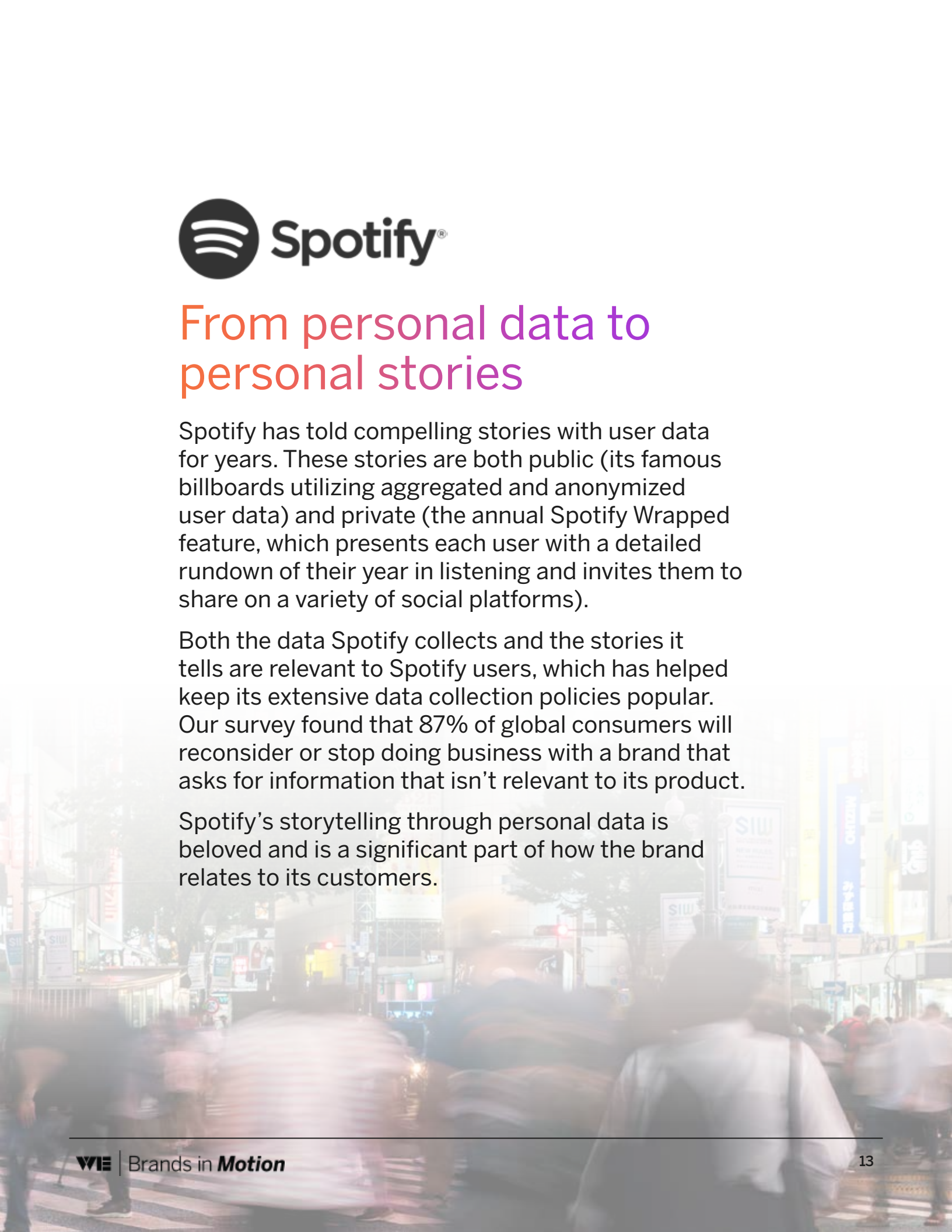
In 2018, Li Yanhong, chairman and CEO of Baidu, summed up the complicated relationship between Chinese consumers and the tech companies that collect and use their data. "I think that the Chinese people are more open, or not so sensitive, about the privacy issue," he said at the China Development Forum in Beijing. "If they are able to exchange privacy for convenience or efficiency, they are willing to do so in many cases." His comments drew sharp criticism, but in 2022, that bargain — privacy for convenience — is foundational for brands collecting and using personal data.

Consumers understand this, and brands that win in this privacy-first age do so by delivering benefits directly to the customer. **Data privacy is an exchange.** Customers give up some of their personal data to get something beneficial to them — more relevant marketing, a personalized experience or a more refined version of the product or service in the future. Customers know and understand the nature and value of this exchange.

A data transaction is an opportunity to move beyond check-the-box disclosures and notifications. Innovative brands use these moments to engage customers, tell stories and create a truly memorable user experience.

How consumers think brands use their data





From personal data to personal stories

Spotify has told compelling stories with user data for years. These stories are both public (its famous billboards utilizing aggregated and anonymized user data) and private (the annual Spotify Wrapped feature, which presents each user with a detailed rundown of their year in listening and invites them to share on a variety of social platforms).

Both the data Spotify collects and the stories it tells are relevant to Spotify users, which has helped keep its extensive data collection policies popular. Our survey found that 87% of global consumers will reconsider or stop doing business with a brand that asks for information that isn't relevant to its product.

Spotify's storytelling through personal data is beloved and is a significant part of how the brand relates to its customers.

2 Establish a relationship built on safety.

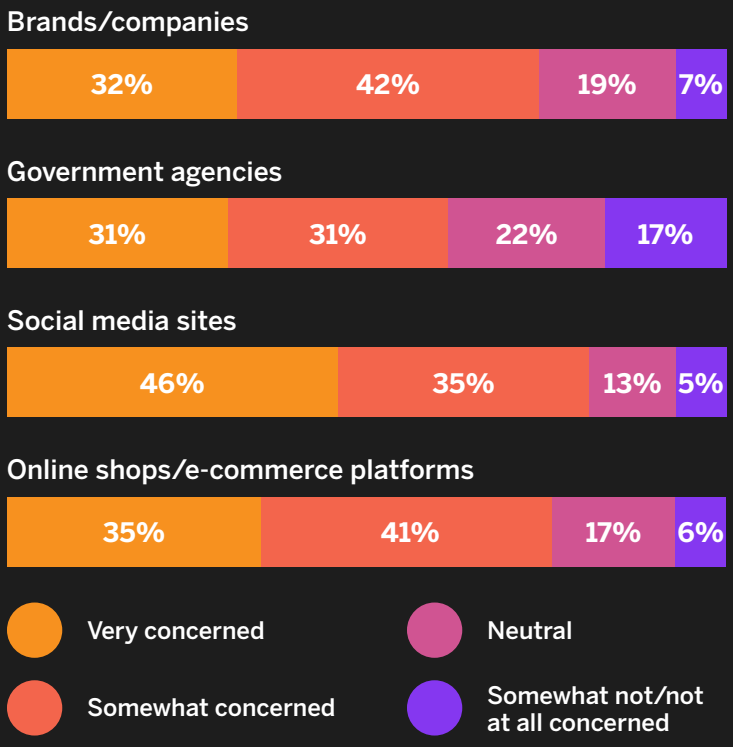
If data privacy is a transaction, consumers need to know that it's a safe transaction. **The underlying message for any brand that collects and uses personal data must be "You can trust us."** One important way to build that trust is to let consumers decide what and when to share.

Another is transparency. Overcommunicating with customers about how their data is being collected and used is critical: 65% of global consumers say it is important for them to know how brands handle their personal information, and the vast majority are at least somewhat concerned about how their data is collected and used — particularly by social media sites and online shops or e-commerce brands.

	I am happy for brands to collect my data if I get better service	I want to choose when and how I give access to my data
Australia	45%	90%
China	30%	68%
India	54%	83%
Singapore	35%	84%
U.S.	31%	86%
U.K.	29%	89%

* Percentage of respondents who "somewhat" or "strongly" agree

Q: How concerned are you about how the following types of institutions collect and use your data?



CEOs take the lead

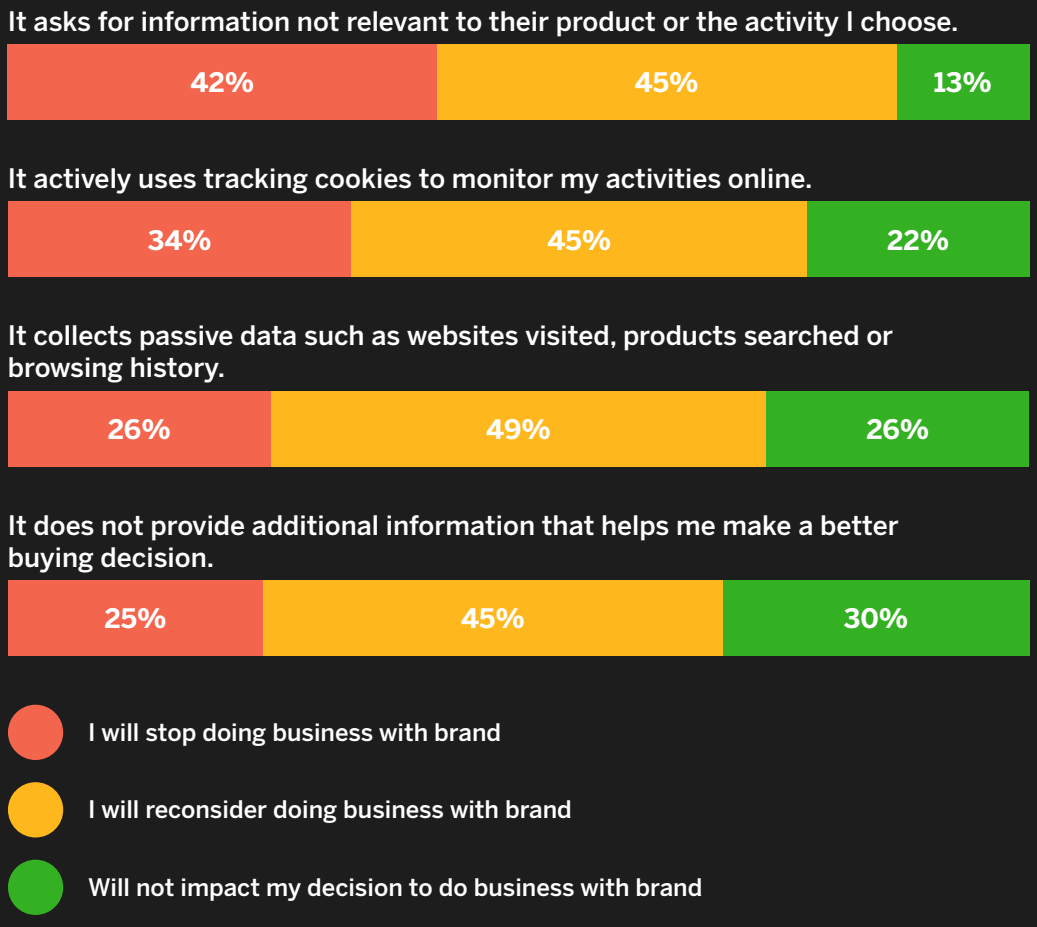
2021's Brands in Motion global report, "The Bravery Mandate," found that an engaged CEO willing to communicate frequently and authentically will stand out as a leader. Seventy percent of respondents said executives should convey their personal positions to at least one of five different audiences (employees, social media, customers, shareholders or the media) with very high frequency — from "almost constantly" to at least every six months.

Making data privacy a key part of a brand's relationship with consumers will require the CEO's buy-in and engagement. **Foo Fang Yong**, CEO of Huawei International — Huawei's subsidiary in Singapore — is a good example. After Huawei received the Singaporean government's prestigious DPTM (data protection trustmark) certification, he announced, "Personal data protection is not simply a legal requirement; it is a social responsibility. This certification underscores our commitment to privacy protection.... We have incorporated privacy protection requirements into all our day-to-day business processes."

3 Prove you've kept your promises.

Once a user has chosen how to share their personal data with a brand, that choice must be honored. Consumers aren't afraid to stop supporting a brand if they're suspicious.

What a brand does with data that drives consumer distrust



But while consumers will punish brands for using data poorly, the opposite is also true — **they'll reward brands that follow through on their promises of transparency and benefits**. This is an opportunity to communicate how the data your brand has collected and used is changing consumers' lives for the better.

What happens when that promise gets broken? It depends on where the brand is doing business. We gave respondents a scenario about a brand working with healthcare providers and a government health department that was affected by a data breach. The personal information of 120 million customers, including patient information, bank details, user website actions, direct messages, financial records and social media accounts, was leaked on search engines and a few ecommerce platforms.

We asked respondents who would be responsible for acting on the impact of the breach.

Consumers in APAC markets were more likely to see the government agency and healthcare provider-partners as responsible for taking action. In the U.S. and U.K., however, consumers put a much greater emphasis on the brand being responsible. In both markets, consumers often have higher expectations of the business community than they do of politicians and look to brands to take the lead on finding solutions to societal issues. That brand-first mentality carries through to which parties are responsible for dealing with data breaches as well.

Imagine going into a brand's store in the real world. In a sense, that brand is promising that you'll be safe, secure and allowed your privacy while you're shopping there. If the roof collapses, if someone steals your credit card just as you're about to pay or if someone follows you home to make sure you put your couch in the right spot, who could blame you for having a negative view of that brand? The promise has been broken.

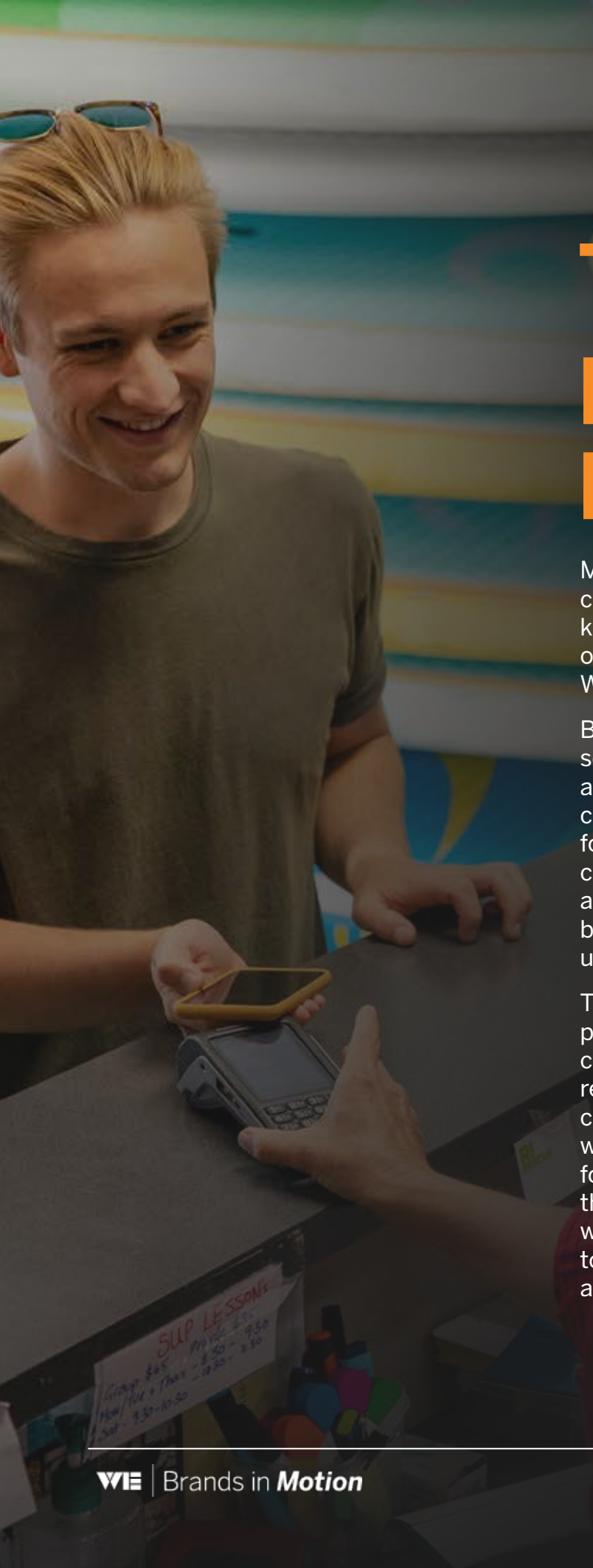
Interacting with a brand online shouldn't be any different. A brand still has the same responsibilities to the customer. Any interaction — in a physical space or a virtual one — must be safe, secure and private.

	Australia	China	India	Singapore	U.S.	U.K.
1	Government agencies (71%)	Healthcare providers working with brand (70%)	Healthcare providers working with brand (59%)	Healthcare providers working with brand (67%)	Brand affected by breach (64%)	Brand affected by breach (78%)
2	Brand affected by breach (69%)	The hackers who target healthcare data (65%)	Government agencies (54%)	Government agencies (64%)	Healthcare providers working with brand (59%)	Government agencies (64%)
3	Healthcare providers working with brand (68%)	Government agencies (56%)	Brand affected by breach (49%)	Brand affected by breach (64%)	Government agencies (51%)	Healthcare providers working with brand (62%)

Using data to solve traffic congestion

Super app Grab began as a ride-hailing app in Southeast Asia. Since 2016, Grab has partnered with governments, nongovernmental agencies (NGOs) and the World Bank to provide access to its extensive ride data to the OpenTraffic project, a global data platform that processes the locations of vehicles and smartphones to provide both real-time and historical traffic statistics.

Traffic jams cost Asian economies an estimated 2%-5% of GDP every year. Grab's data on the routes of its 500,000 drivers helped reduce urban pollution and traffic congestion in countries such as Thailand, Cambodia and the Philippines. Grab was able to prove the value of its data collection policies and create benefits for its customers and anyone who drives in Southeast Asian cities.



The future: privacy as partnership

Many brands are apprehensive about communicating about data privacy. A newly knowledgeable audience means more opportunities to be publicly second-guessed. Why risk it?

But sophisticated audiences expect sophisticated stories. Silence, obfuscation and burying any and all data privacy communications in EULAs won't work. And for brands willing to change the way they communicate about data privacy, the rewards are great. Data privacy is an exciting partnership between brand and customer and a relatively untapped space for storytelling in tech.

The work won't always be easy. Making data privacy an exciting and relevant part of a customer's relationship with a brand will require bold leadership and cross-functional cooperation. It will require building deep trust with customers, and it will require the courage for a brand to use first-party data to do more than simply market itself more effectively — it will require the courage to leverage private data to create a better world for brands, consumers and all of us.

Methodology

Qualified respondents made a purchase within the last six months in one of the following categories:

- Computing devices
- Consumer technology
- Finance/banking products
- Health and wellness
- Health technology
- Prescription health

In addition, qualified respondents had a minimum household income of:

Australia	≥ AUD 60,000 gross household income per year
China	≥ ¥72,000 net household income per year
India	≥ Rs 36,000 gross household income per year
Singapore	≥ SGD 48,000 net household income per year
U.K.	≥ £30,000 gross personal income (individual)
U.S.	≥ $50,000 annual family income

Survey was fielded in January and February of 2022.

Respondents:

Australia	1,000
China	1,008
India	1,014
Singapore	1,009
U.S.	510
U.K.	505

Your Brand in Motion

Our world is constantly changing. Brands in Motion reports provide data-driven tools that will help you develop the agility to respond to disruptions and the stability to build an enduring legacy.

To learn more about Brands in Motion or find out about Brands in Motion events in your area, contact WE:

Sara Pereira
APAC
spereira@we-worldwide.com
+65 9794 8380

Laura Gillen
EMEA
lgillen@we-worldwide.com
+44 7917157002

Mark Martin
U.S.
markm@we-worldwide.com
+1 (503) 799-2997

The world, your brand and your stories are in motion.
WE helps you go the distance.

we-worldwide.com | @WEcomms

Publication Date: 06.14.22