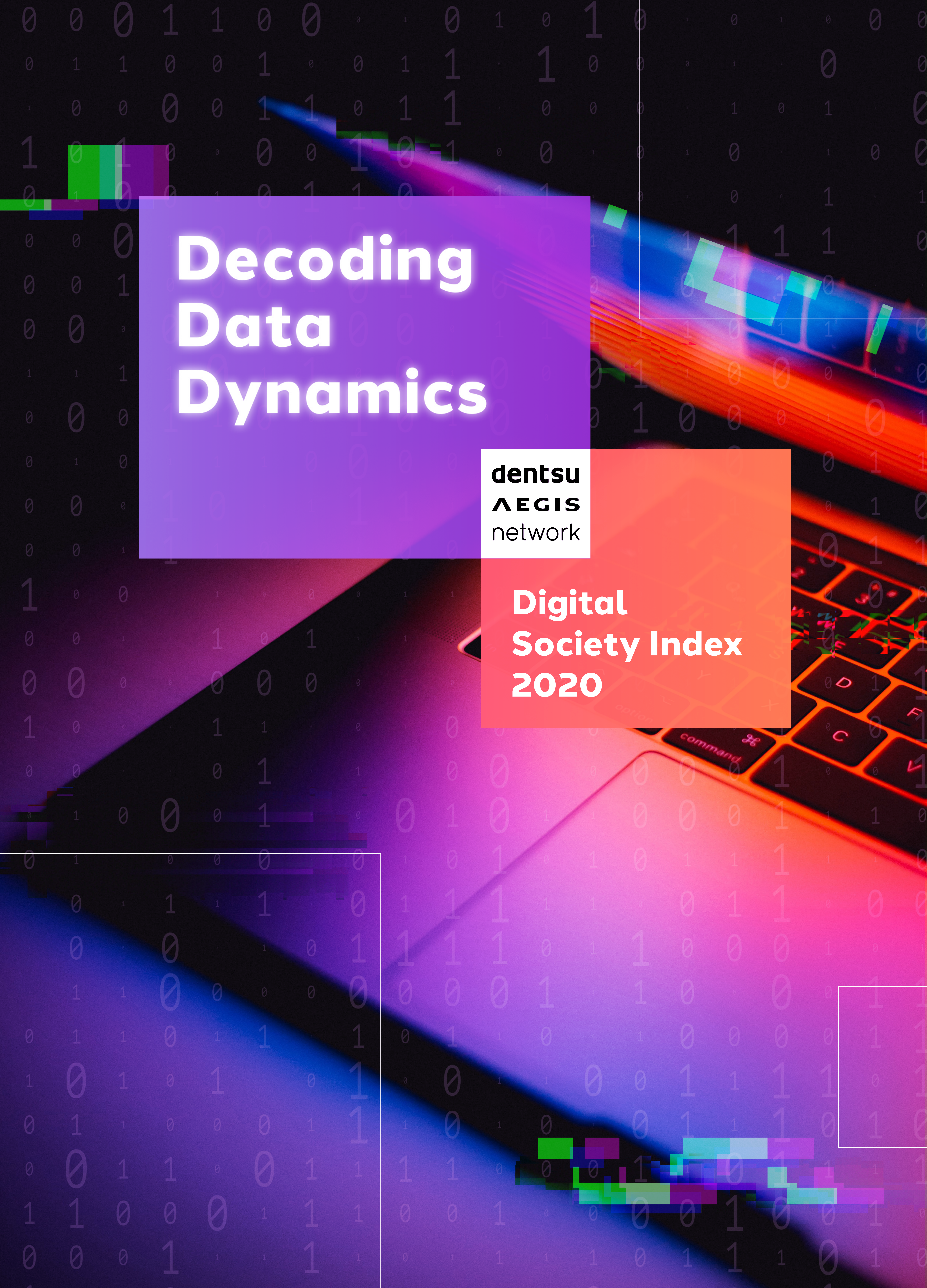
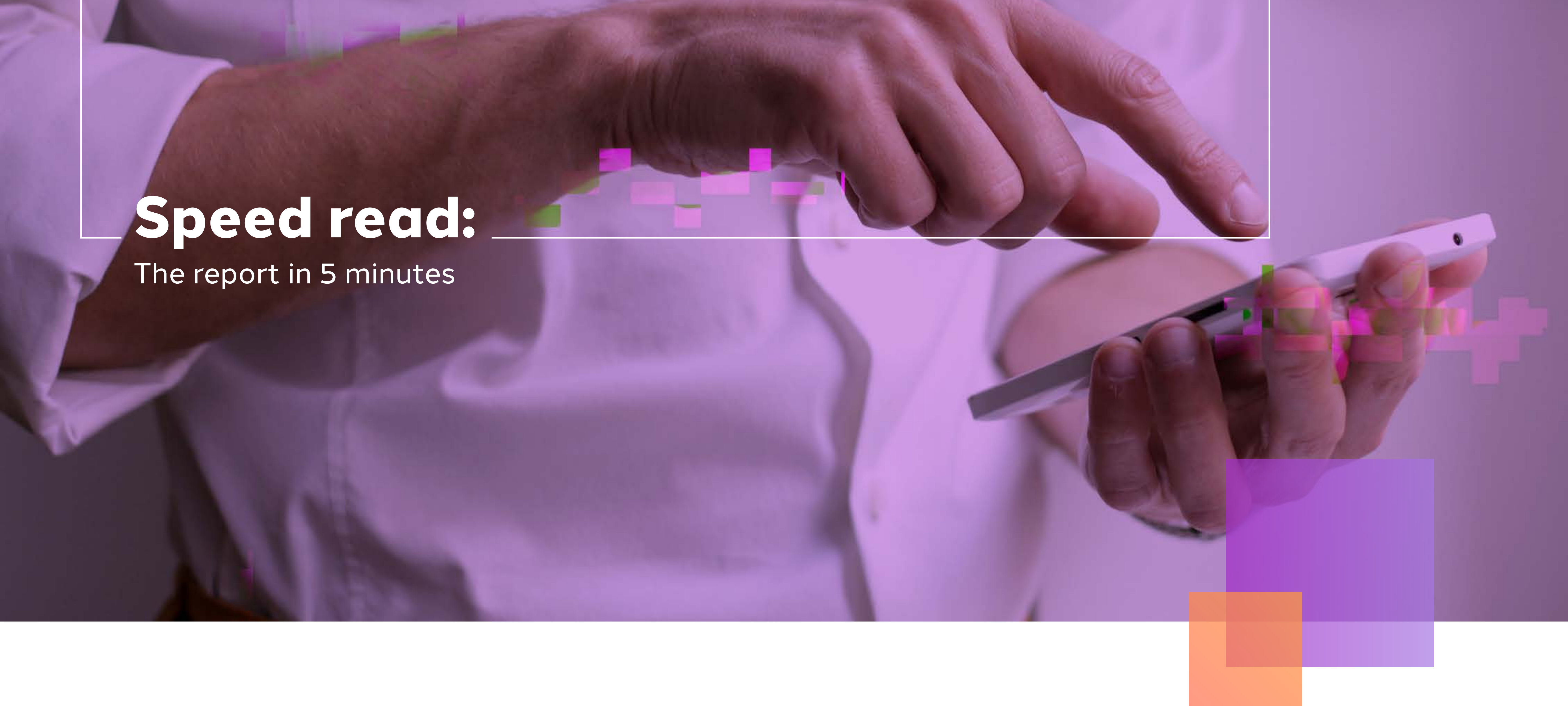


Decoding Data Dynamics

dentsu
AEGIS
network

Digital Society Index 2020

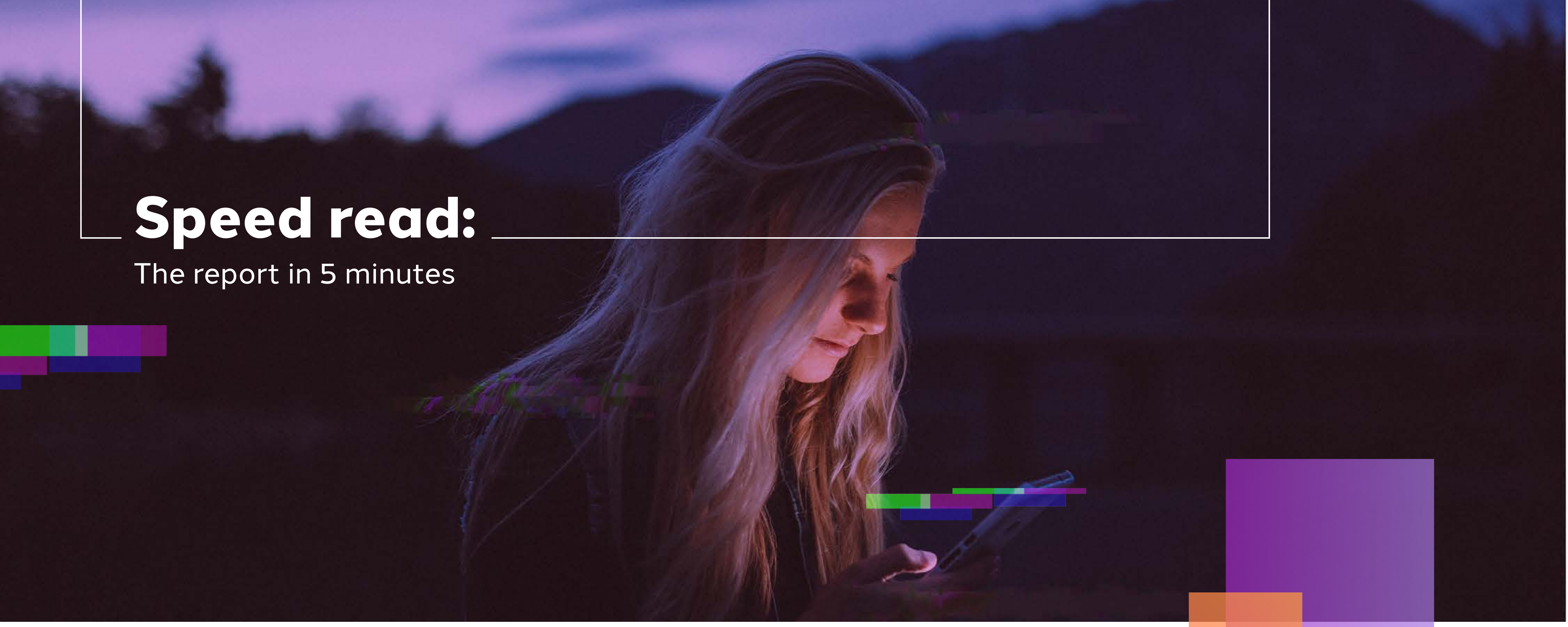


Speed read:

The report in 5 minutes

Consumer attitudes to personal data can be hard to decode. But understanding them is key to delivering more relevant, engaging consumer experiences. Our third annual survey of 32,000 people across 22 markets reveals a number of key dynamics, many of which are paradoxical. For example:

- **Big Tech isn't trusted with personal data—but consumers still sign up.** Misusing personal data remains the number one driver of distrust in the technology sector for the second year running. At the same time, adoption of digital platforms and social media continues to grow.
- **We don't want to share data, but we do.** Just a minority of people agree that it is acceptable for businesses to use many types of personal data to improve the services they deliver, from internet browsing habits (21%) to even the most basic forms of personal data, such as email addresses (45%) and name and age (43%). But at the same time, many people share this data without actually realising they are doing so.
- **We want personalisation—but not personalised ads.** While consumers demand personalisation to shape products, services and campaigns, it is not always welcome. A third (32%) of people globally have opted out of receiving personalised adverts.
- **We demand consent—but who reads Ts&Cs?** For many people, retaining control over their data is paramount. For example, two-thirds of people globally feel that it is important that organisations gain their explicit consent to use their personal data to support research and development that addresses societal challenges such as medical research. However, cookie notices and terms & conditions of data use are rarely read.



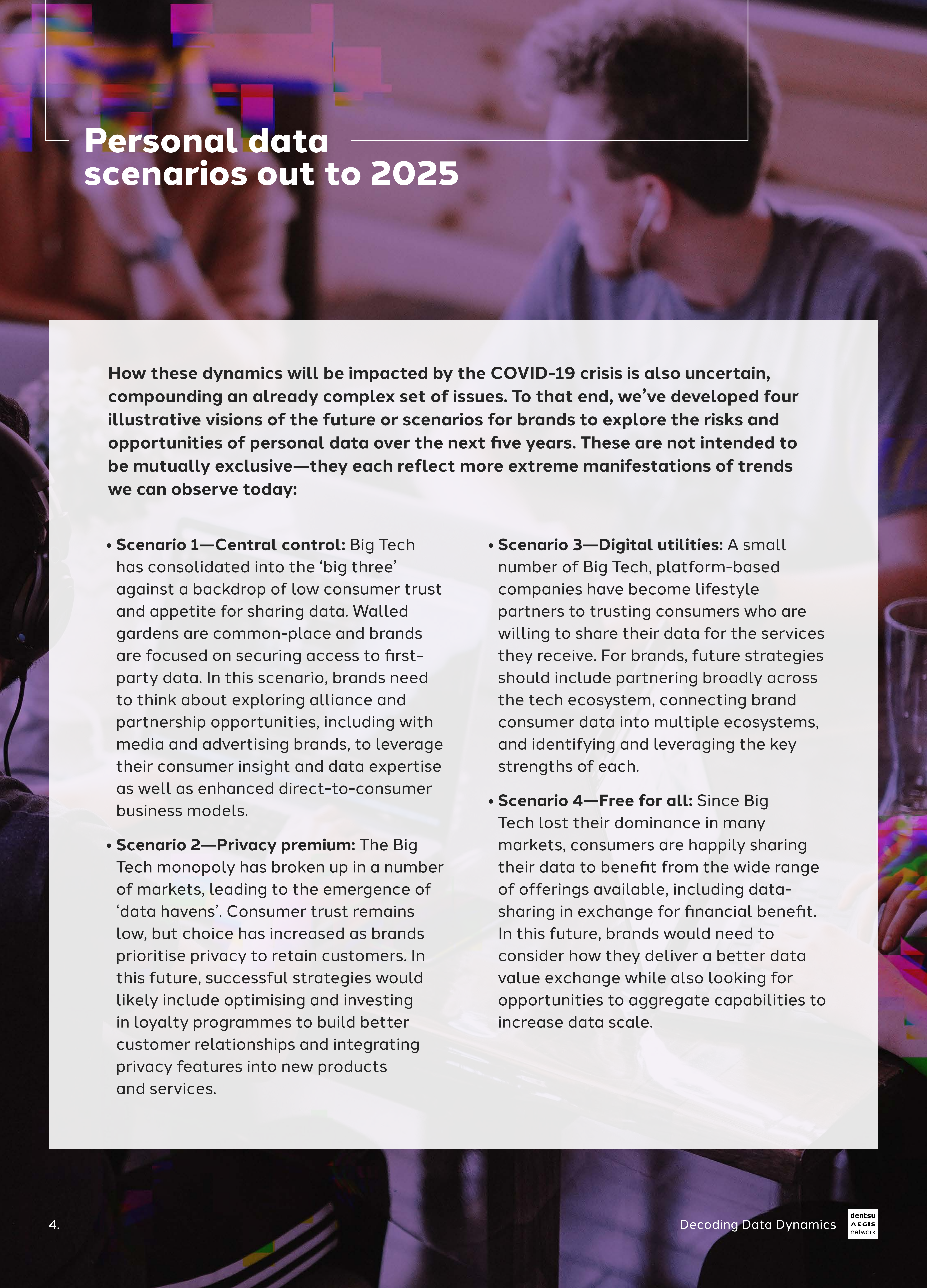
Speed read:

The report in 5 minutes

At the same time, consumers are giving a number of clear signals about the future shape of the personal data landscape. For example:

- **It's not just tech... lack of trust impacts all industries.** While Big Tech may take the headlines, it's clear that no industry is fully trusted with consumer data. Government agencies are the most trusted and media and entertainment companies the least. But all sectors need to step up to address the trust deficit.
- **Data security and privacy concerns are universal**. Eight out of ten people globally say they would stop doing business with an organisation that lost or misused their data. This pattern is consistent across all the markets we surveyed.
- **Consumers are taking back control of their data.** As in 2019, this year a quarter of people globally say that they have installed ad blockers in the preceding twelve months. Four out of ten have reduced the amount of data they shared online.
- **Clear value exchange is expected, although not yet a reality.** Nearly half of people surveyed expect to receive financial benefits in exchange for organisations using their data in the next 2-3 years, while 1 in 10 people today have sold their data online in the last 12 months.

In addition to these consumer dynamics, there is also uncertainty surrounding the evolution of data protection regulation and the ethical questions raised by new technologies—especially in potentially controversial areas such as facial recognition technology.



Personal data scenarios out to 2025

How these dynamics will be impacted by the COVID-19 crisis is also uncertain, compounding an already complex set of issues. To that end, we've developed four illustrative visions of the future or scenarios for brands to explore the risks and opportunities of personal data over the next five years. These are not intended to be mutually exclusive—they each reflect more extreme manifestations of trends we can observe today:

- **Scenario 1—Central control:** Big Tech has consolidated into the 'big three' against a backdrop of low consumer trust and appetite for sharing data. Walled gardens are common-place and brands are focused on securing access to first-party data. In this scenario, brands need to think about exploring alliance and partnership opportunities, including with media and advertising brands, to leverage their consumer insight and data expertise as well as enhanced direct-to-consumer business models.
- **Scenario 2—Privacy premium:** The Big Tech monopoly has broken up in a number of markets, leading to the emergence of 'data havens'. Consumer trust remains low, but choice has increased as brands prioritise privacy to retain customers. In this future, successful strategies would likely include optimising and investing in loyalty programmes to build better customer relationships and integrating privacy features into new products and services.
- **Scenario 3—Digital utilities:** A small number of Big Tech, platform-based companies have become lifestyle partners to trusting consumers who are willing to share their data for the services they receive. For brands, future strategies should include partnering broadly across the tech ecosystem, connecting brand consumer data into multiple ecosystems, and identifying and leveraging the key strengths of each.
- **Scenario 4—Free for all:** Since Big Tech lost their dominance in many markets, consumers are happily sharing their data to benefit from the wide range of offerings available, including data-sharing in exchange for financial benefit. In this future, brands would need to consider how they deliver a better data value exchange while also looking for opportunities to aggregate capabilities to increase data scale.

Conclusion

In reality, all of these scenarios will shape the future. The rise of walled gardens (scenario 1); privacy as a competitive differentiator (scenario 2); the rise of platform brands as lifestyle partners (scenario 3); changing expectations around value exchange (scenario 4). All of these trends will influence brands to different degrees, depending on sector and market.

Brands will therefore want to lean further into these trends and futures depending on their individual contexts. By doing so, they can start to master the complexities of today's consumer data dynamics and plan strategically for a future of continued uncertainty.

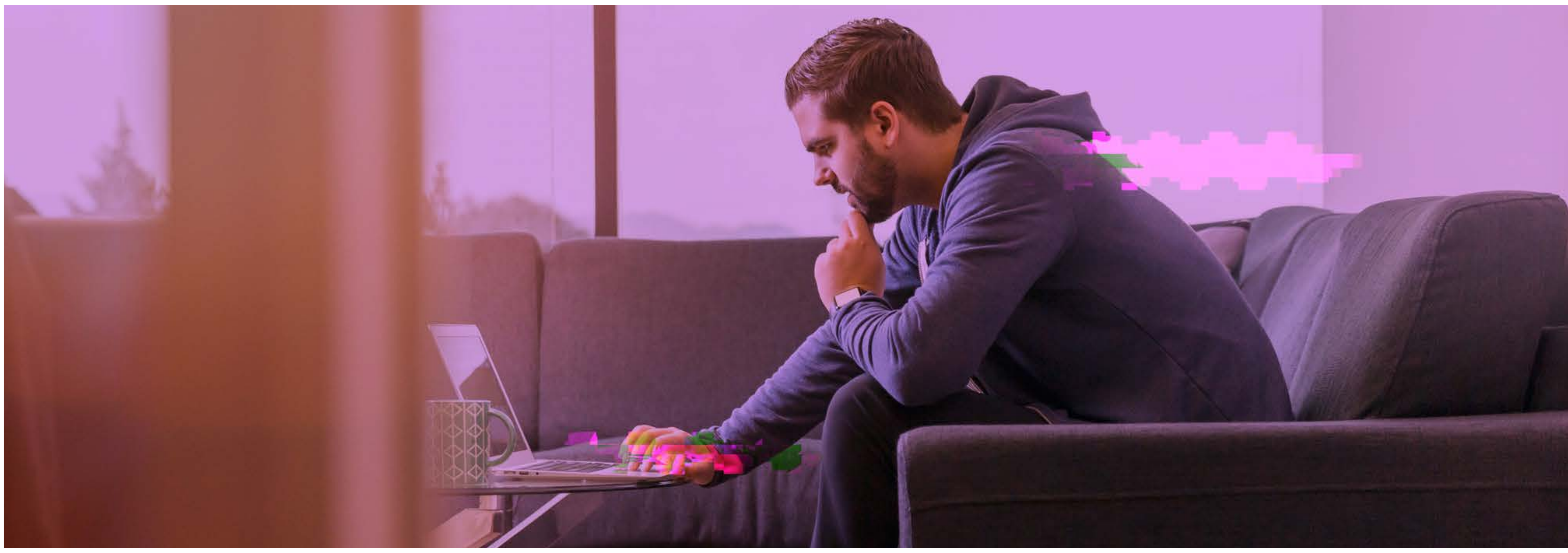
1. Introduction

Few issues have defined the digital era more appropriately than business use of personal data. The last decade has witnessed an almost constant process of triangulation between businesses, consumers and governments as we try to establish acceptable norms that fuel innovation while protecting individual rights. This pull and push between protecting and harnessing data has led many brands to have an unclear view on what actions they can and should take. And as the pace of tech innovation increases, the complexity and uncertainty surrounding many of these dynamics is growing.

The COVID-19 pandemic has put many of these issues into sharper focus. With the pandemic placing millions of people under lockdown, COVID-19 has accelerated the digital revolution—and the debate around fair and ethical use of personal data. Our survey of 32,000 people across 22 markets conducted in March-April 2020 confirms that people are increasing their use of digital technologies, as they turn to the online world for work, shopping, education, and entertainment, for example.

More online activity means people are sharing more data. Already, apps being developed to track the spread of the virus in Europe and Asia[i] are raising important questions around data privacy. Many activists are concerned that measures taken in the heat of the crisis could become the status quo, eroding hard-won rights and protections. And as more and more people use digital technologies to work and to stay healthy, using remote diagnostics for example, the volume of sensitive personal data we share is set to grow further.

How the crisis may impact the long-term trends transforming the personal data landscape is not yet known. From the role of Big Tech to consumer attitudes and behaviours to data regulations, events are constantly evolving to affect personal data in different ways. Helping brands decode these dynamics is the objective of this paper.



Trends

2. Consumer data dynamics

Consumer attitudes to personal data are notoriously hard to decode. Context plays a huge role and the inconsistencies of human nature can make it fiendishly hard to generalise. Based on our global survey of 32,000 people across 22 markets, there are a number of dynamics shaping how consumers perceive use of personal data. Many of these are paradoxical. Some reflect a gap between what people say in a survey versus what they do in practice. But all are critical for brands to understand if they are going to build more trusted relationships with their customers.

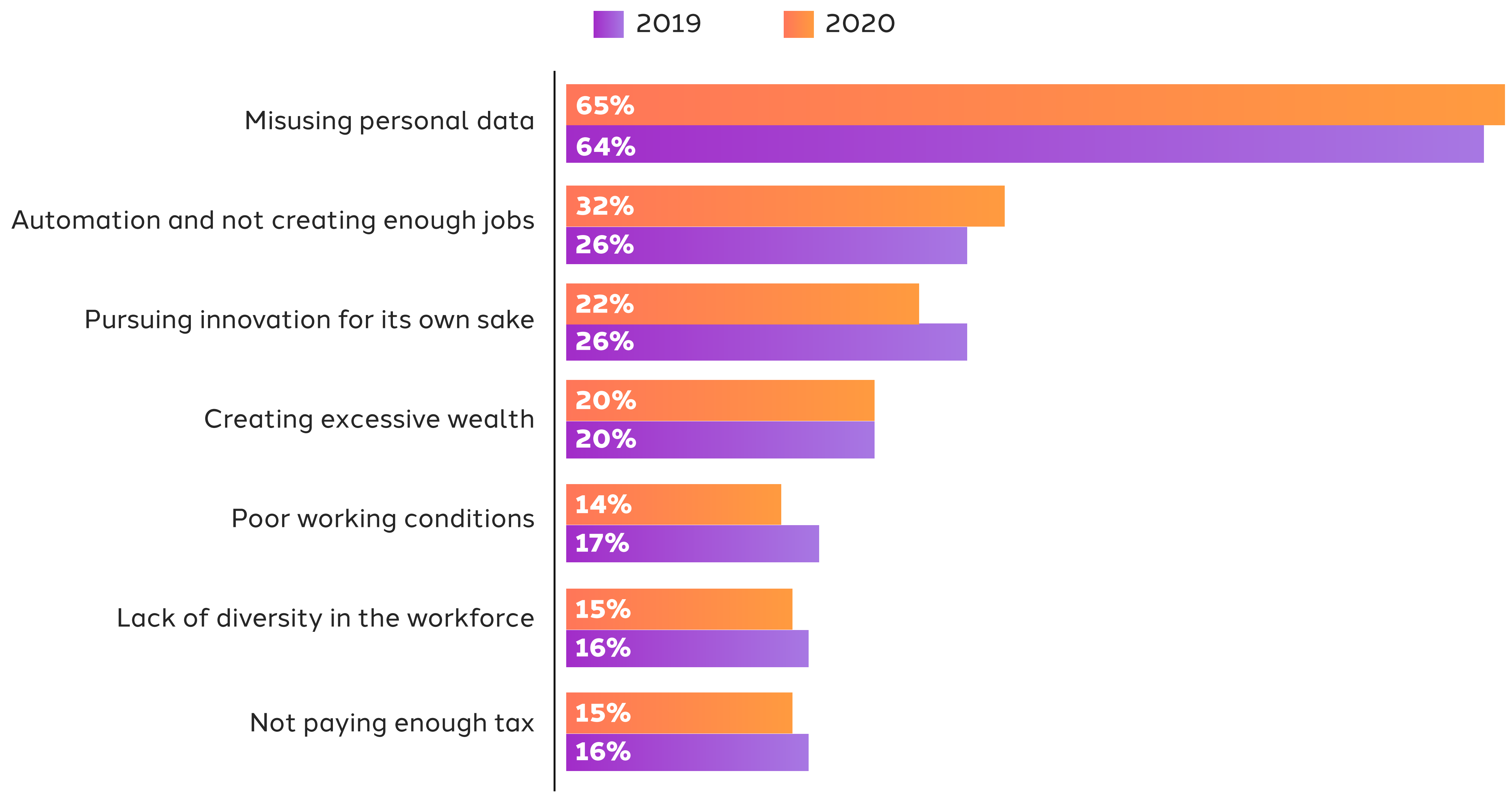
Big Tech isn't trusted with personal data—but consumers still sign up

Misusing personal data remains the number one driver of distrust in the technology sector (see Figure 1) for the second year running. And attitudes harden with age: while six out of ten of generation Z (18-24-year-olds) cite misusing data as a main cause of distrust in the tech industry, this rises to seven out of ten of 55-65-year-olds.

Despite our lack of trust, our appetite for the services provided by Big Tech remains strong. The adoption of tech platforms is still growing—exponentially so during the pandemic. Messaging across Facebook, Instagram and WhatsApp increased by 50% in countries most affected by the virus and in April, Twitter saw a 23% increase in daily users from the previous year[ii]. Clearly, our distrust in the tech industry is not strong enough to discourage us from using its products and services when we feel most in need.

Figure 1: Misusing personal data remains the number one driver of distrust in the tech sector

What do you believe are the main causes of distrust in the technology industry? (% agreeing)



Source: Dentsu Aegis Network Digital Society Index Survey 2019-2020

We don’t want to share data—but we do

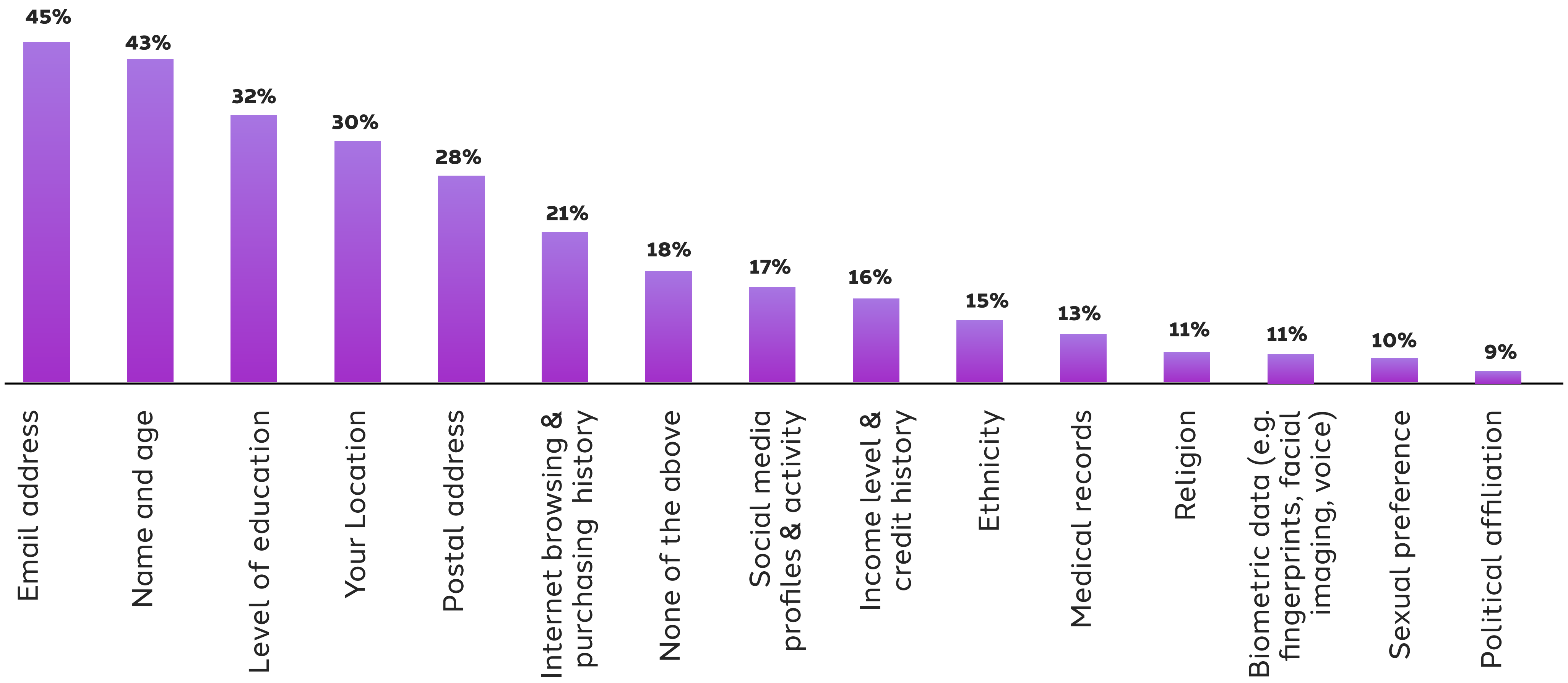
Our analysis shows people generally don’t believe it is acceptable for businesses to use any type of personal data to improve the services they deliver, from internet browsing (21%) to even the most basic forms of personal data, such as email addresses (45%) and name and age (43%) (see Figure 2). And in what might be a sign of the times, political affiliation is the least acceptable type of personal data for businesses to use—ranking even lower than medical records, religion, biometric data and sexual preference.

Yet, most people share a wide array of their personal data without knowing they are doing so and feeling they have little power to do anything about it. A US study found that eight in ten people felt they had little to no control over the data businesses were collecting and six out of ten had little to no understanding about what happens with the data that has been collected them.[iii]

The COVID-19 crisis has demonstrated that some of these concerns may be well-founded. New products and services that have grown rapidly in popularity during lockdown have already been pulled up for data misuse. For example, in March video conferencing software Zoom was forced to stop sending iPhone users’ data to Facebook, having failed to mention this data transfer in its privacy policy.[iv]

Figure 2: People only expect basic personal data to be used to improve services

What types of personal data do you think it is acceptable for businesses to use in order to improve the service they deliver to you?



Source: Dentsu Aegis Network Digital Society Index Survey 2020

We want personalisation—but not personalised ads

While the trend of personalisation continues to shape products, services and campaigns, it is not always welcome. A third (32%) of people globally have opted out of receiving personalised adverts (see Figure 3). In South Africa, half of consumers have chosen to do so. Again, it is younger respondents who are more inclined to have taken this action. Having grown up using technology, this may reflect that younger generations have the digital skills and knowledge required to effectively manage their own data. With its volume and complexity, less tech savvy consumers may find achieving this more difficult.

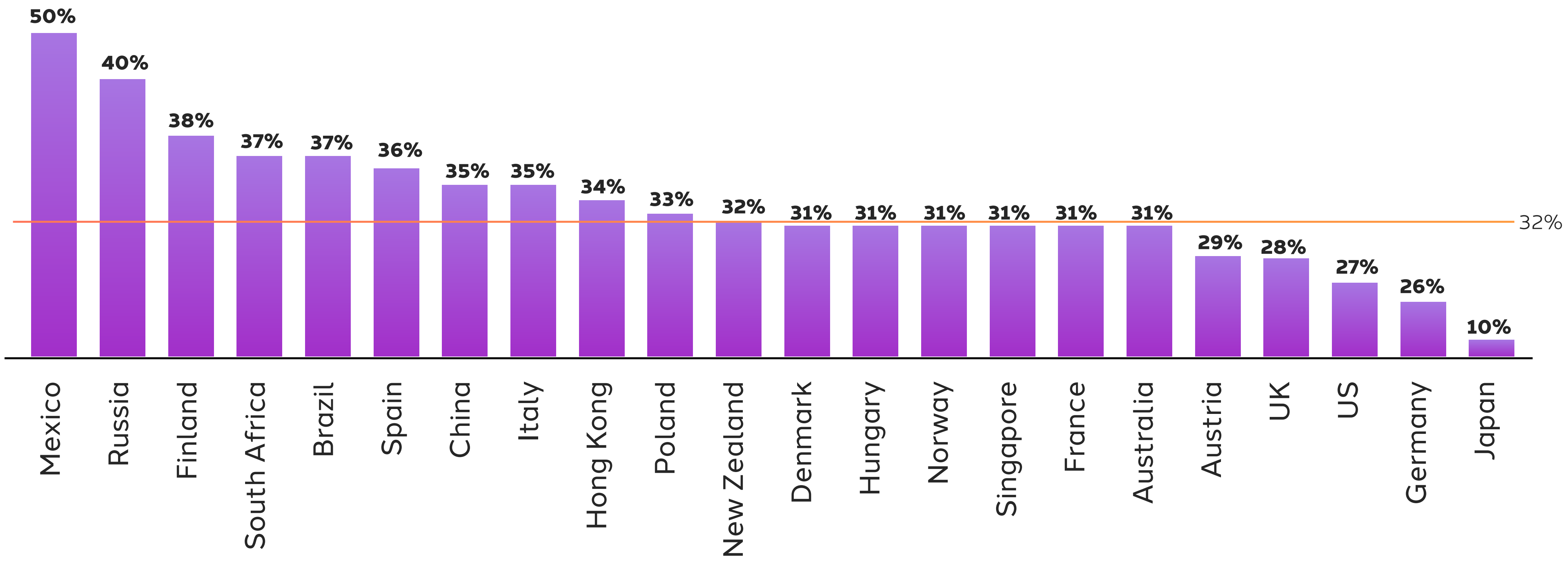
We demand consent—but who reads Ts&Cs?

For many people, retaining control over their personal data is paramount. Our analysis shows that the majority of people believe that it is important that organisations gain their clear consent to use their personal data for all the activities we surveyed. For example, even during the height of the COVID-19 pandemic, more than two-thirds of people feel it is important for organisations to gain their explicit consent to use their personal data to support research and development that addresses societal challenges such as medical research (see Figure 4 on the next page).

This is particularly acute in emerging markets, such as South Africa (79%), Brazil (76%), Poland and Mexico (75%) and among older generations. Six out of ten of gen Z respondents agree it is important to gain consent for research and development, rising to seven out of ten 55-65-year olds.

Figure 3: A third of people globally have opted out of receiving personalised ads in the last 12 months

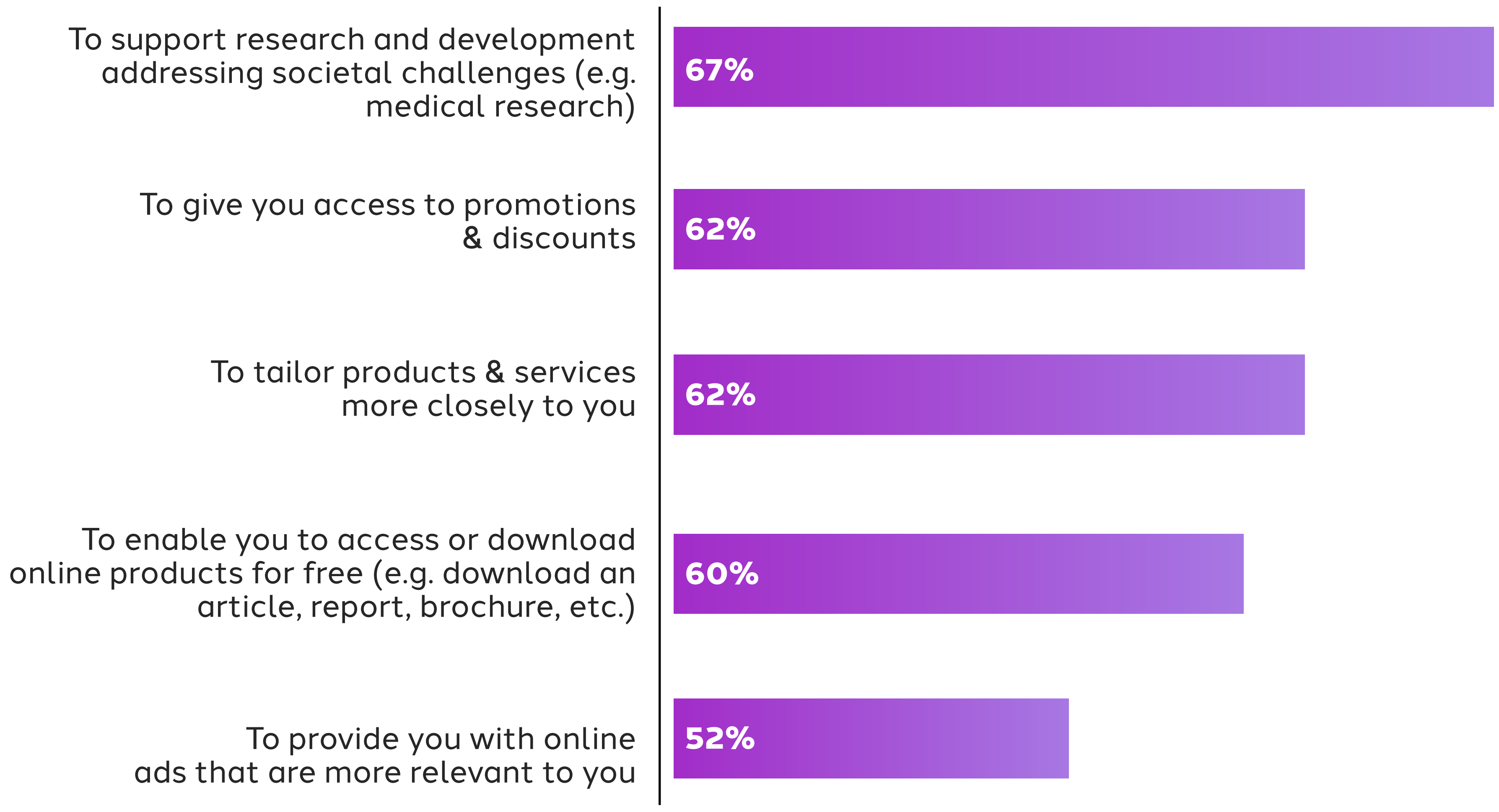
Have you taken any of the following actions over the last 12 months? - Opted out of receiving personalised adverts (e.g. by updating privacy settings on your internet browser)



Source: Dentsu Aegis Network Digital Society Index Survey 2020

Figure 4: People require consent before a range of benefits can be realised from use of their data

How important or unimportant is it that organisations gain your explicit consent to use your personal data to do the following? (% important)

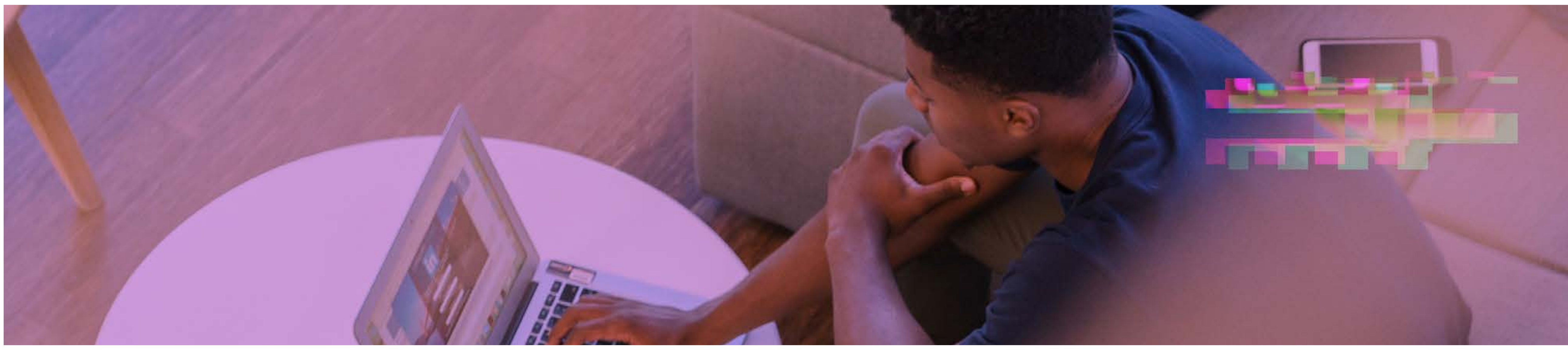


Source: Dentsu Aegis Network Digital Society Index Survey 2020

Consumers may consider this clear consent to be important, but how informed this consent is depends on the consumer. As customer experiences online have improved, customer expectations have risen. One fifth of consumers abandon their online shopping carts because the process is taking too long and a quarter of them do so because website navigation is too complicated.[v] This impatience crosses over to terms and conditions—most people do not read them. In fact, one recent social experiment found that only 1% of participants actually read the terms and conditions when purchasing an item or engaging a service—despite 70% of them claiming to have done so.[vi]

Clearer signals on personal data

Alongside these paradoxes and apparent contradictions, there are also a number of clear signals that consumers are giving to brands as far as use of personal data is concerned.



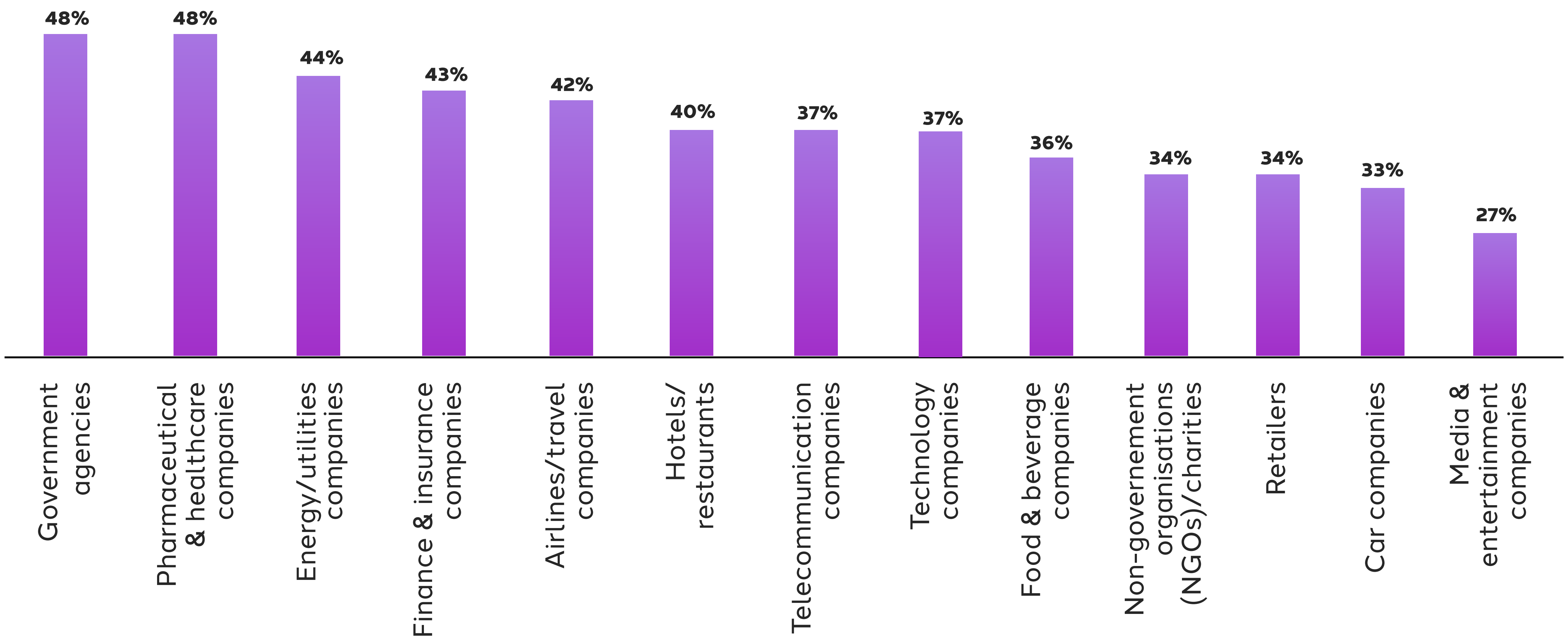
It’s not just tech… lack of trust impacts all industries

While Big Tech may take the headlines, it’s clear that no industry is fully trusted with consumer data. Government agencies and pharmaceutical & healthcare companies are the most trusted. At the other end of the spectrum, media and entertainment companies the least trusted at 27% (see Figure 5).

People in emerging markets, such as China, South Africa, Mexico and Brazil, tend to be more trusting. For example, over half of people in China trust retailers with their personal data, compared to three out of ten globally. More than half of people in Mexico and Brazil trust tech companies, compared to less than four out of ten globally. This may suggest in these fast-developing countries, people remain focused on the benefits that new technology and sharing data can bring rather than potential risks.

Figure 5: No industry is trusted by a majority of consumers with personal data

To what extent do you trust the following types of organisations with your personal data?



Source: Dentsu Aegis Network Digital Society Index Survey 2020

Data security and privacy concerns are universal

Data breaches have unfortunately become commonplace and the costs of a breach, both direct and indirect, can be huge. Consumers are generally of one mind on this issue too: lose our data and you lose our custom. Eight out of ten people globally say they would be likely to stop doing business with an organisation that lost or used some of their data irresponsibly (see Figure 6). While in reality this intent may not always translate into mass action, nevertheless all brands must be mindful of the ever-present risk of a breach.

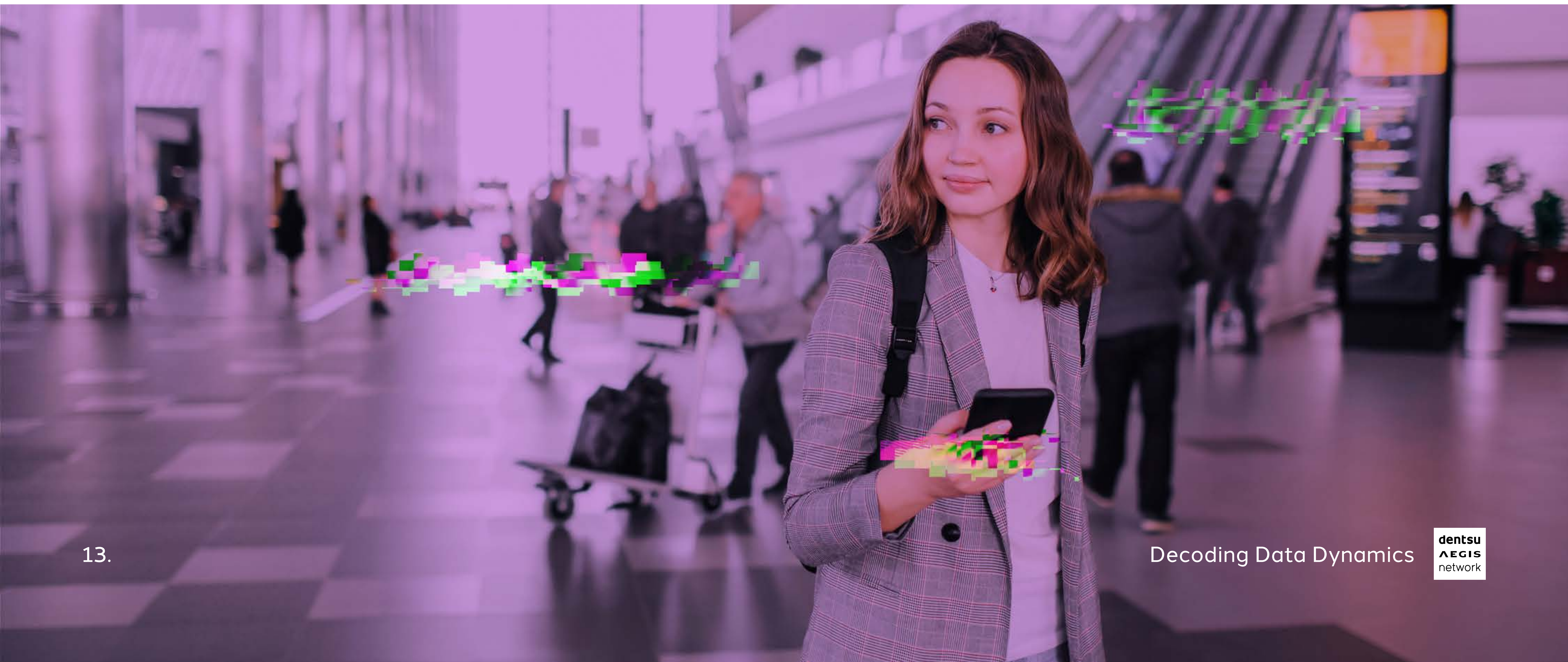
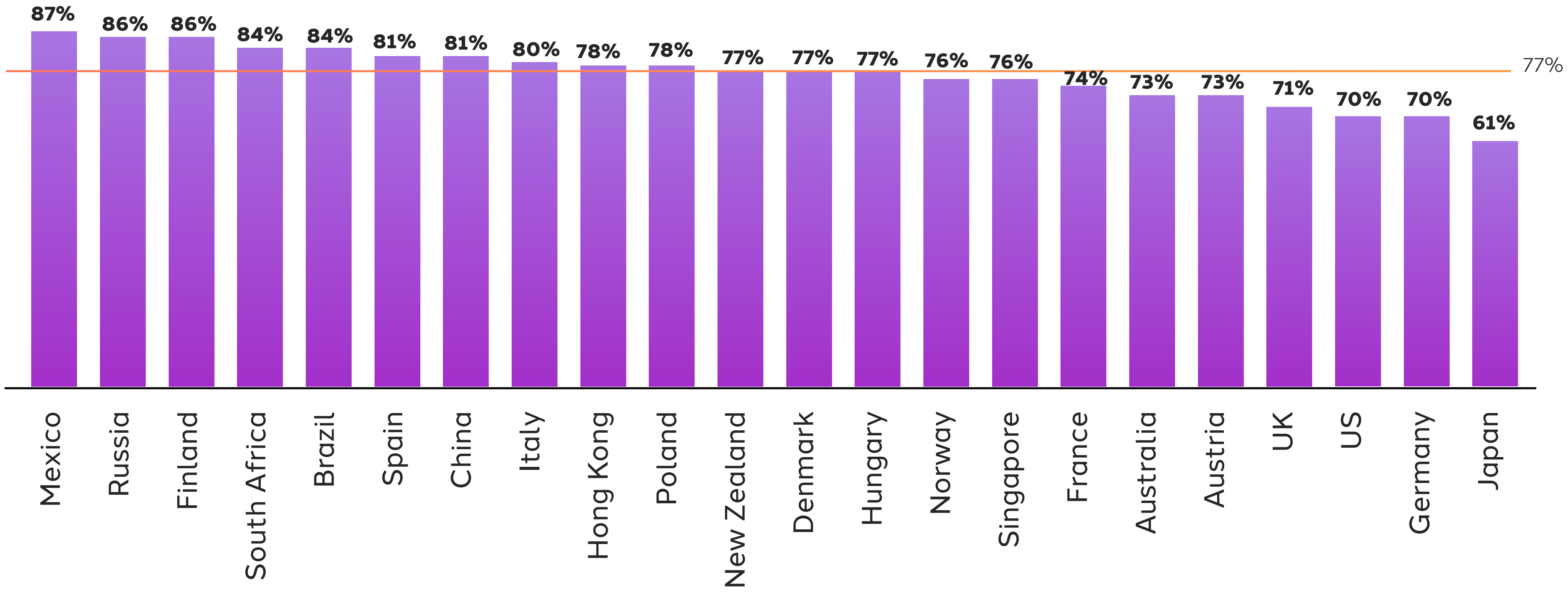


Figure 6: Eight out of ten people say a data breach would make them stop using a brand

Likelihood of stopping doing business with an organisation that lost some of your data or used it irresponsibly (% likely)



Source: Dentsu Aegis Network Digital Society Index Survey 2020

Consumers are taking back control of their data

As people have become more aware of how their data is used, they've taken steps to manage it on their own terms. A significant proportion of consumers is already taking actions to limit or modify their digital behaviour (see Figure 7).

Like last year's survey, a quarter of people globally say that they have installed ad blockers over the preceding twelve months, and over four out of ten have taken actions to reduce the amount of data they share online.

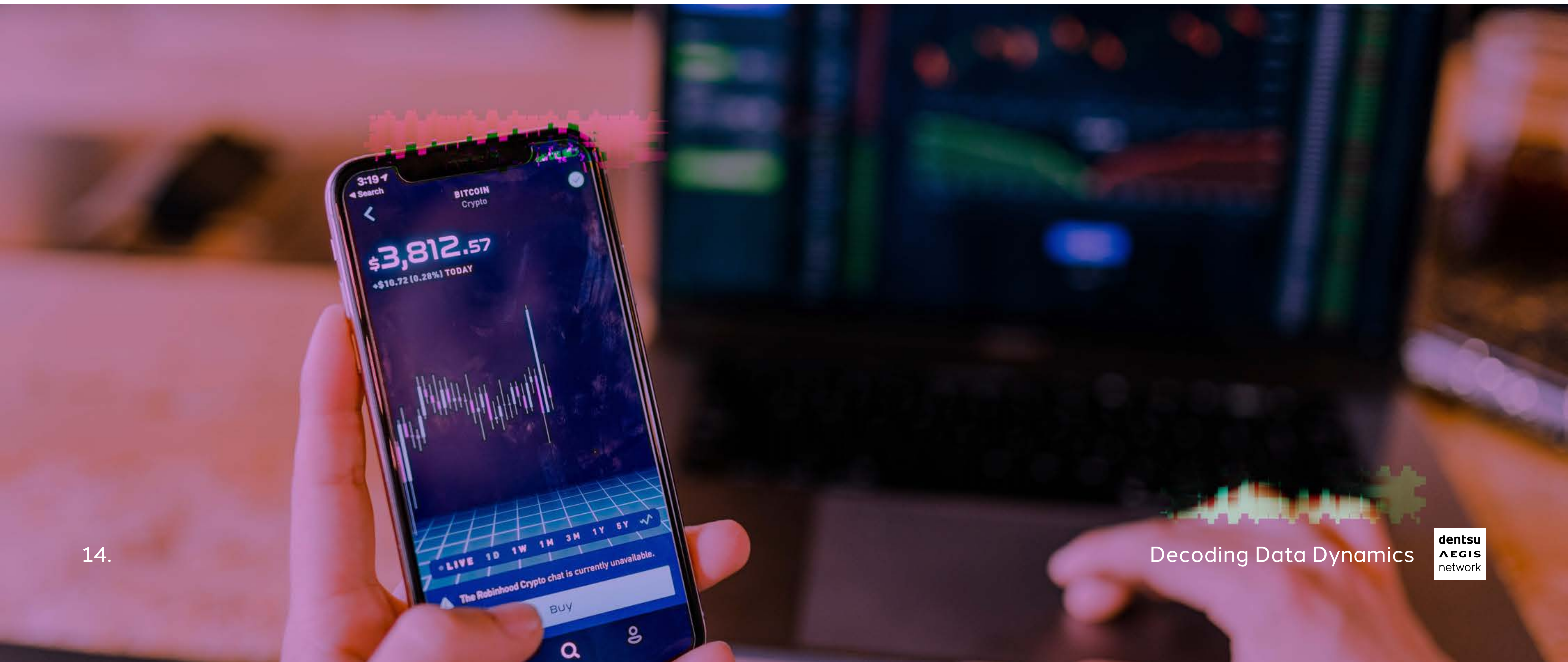
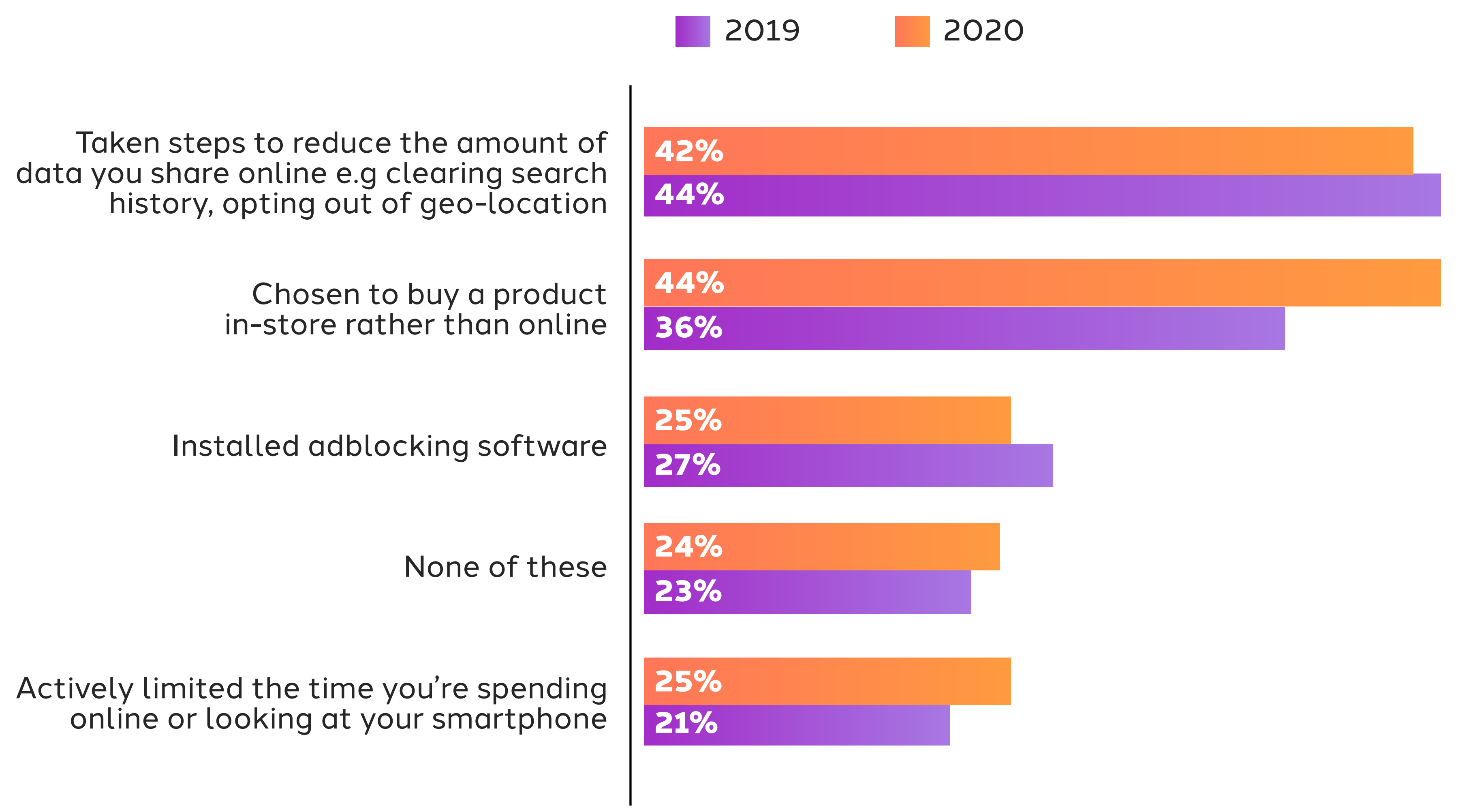


Figure 7: A significant proportion of consumers are limiting or modifying their online behaviour

Have you taken any of the following actions over the last 12 months?



Source: Dentsu Aegis Network Digital Society Index Survey 2019-2020

Younger people (18-24-year olds and 25-34-year olds) are more likely to take all the actions we surveyed. For example, one in five of Gen Z say that they have deactivated their social media accounts in the last year. That compares to less than one in ten people over the age of 45. This could be a sign of things to come—a growing movement of consumers as data activists, using their tech savvy to manage their online profiles on their own terms.

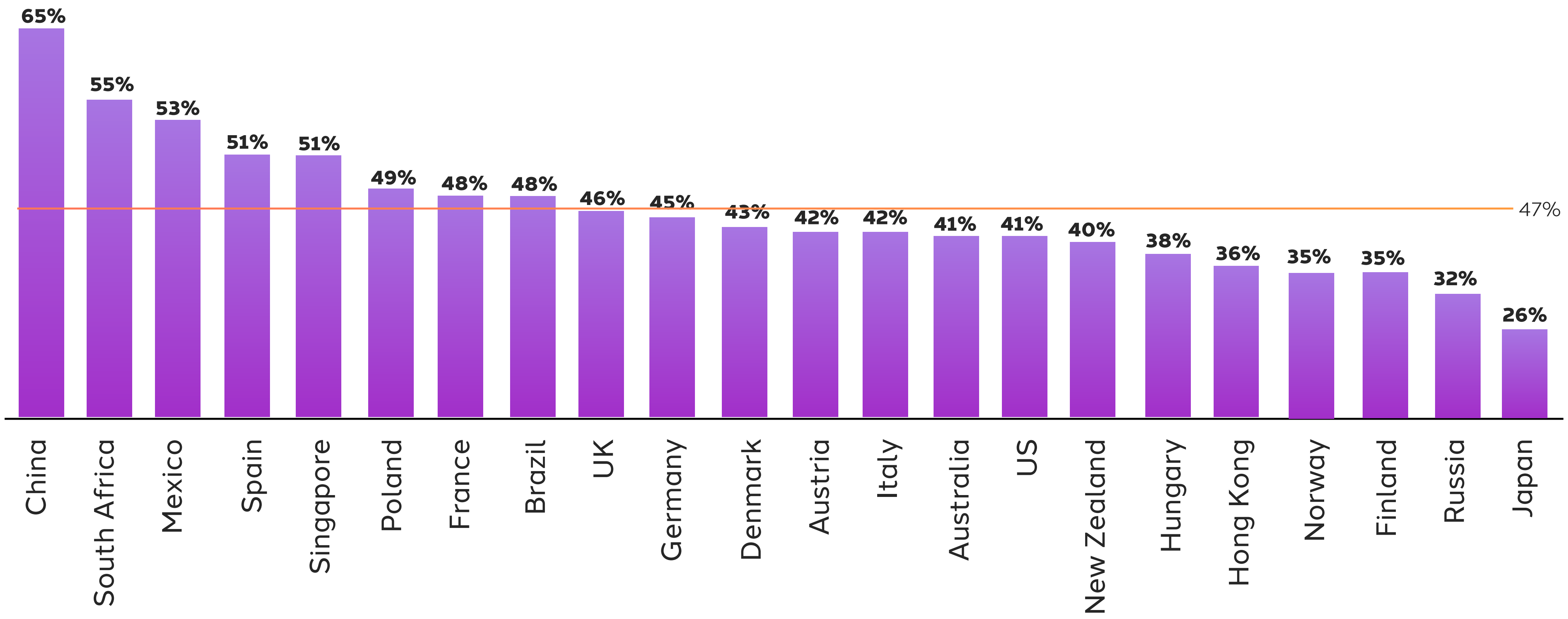
The challenge here is that with many services requiring data sharing to secure access, deciding to share less data can mean receiving an inferior service. However, half of consumers globally expect to be able to refuse to share their personal data, but still receive the same level of service.[vii] Increasingly this looks unlikely and we can expect to see more people going offline and becoming almost invisible to brands in terms of their online presence.

Financial value exchange is expected, although not yet a reality

Looking ahead, nearly half of the consumers we surveyed also expect to receive financial benefits in exchange for organisations using their data (see Figure 8) in the next 2-3 years. For example, Delphia is a start-up that invites consumers to invest their data, which it says could be worth $15,000 on the stock market within a decade.[viii] While this trend of data monetisation has been evolving for some years now, in markets such as China the expectation in the minds of consumers is clear. However, contrast that expectation with what is happening today: just one in ten people have sold their personal data over the last 12 months, although in Austria one quarter of people say they have done so.

Figure 8: Nearly half of people expect financial benefits from organisations using their data

In the future (i.e. next 2-3 years), I will receive financial benefits in exchange for organisations using my data (% agreeing)



Source: Dentsu Aegis Network Digital Society Index Survey 2020

Evolving regulation

As if these consumer dynamics were not hard enough to navigate, further uncertainties make it even more challenging for brands to plan. For example, to what extent will regulation evolve over the coming years—will it lead to more global co-ordination among policymakers, or more localised, fragmented approaches? Will the regulation of Big Tech be stronger in some parts of the world, such as the European Union and California, and more laissez-faire in others?

While consumers generally favour more collaborative approaches to governance (see Figure 9), a great deal of uncertainty remains around whether we'll see more regulatory convergence around common standards, or more divergence as governments go it alone. Some may even look to establish themselves as 'data havens', seeking to increase their attractiveness to business through more relaxed approaches to data protection regulation.

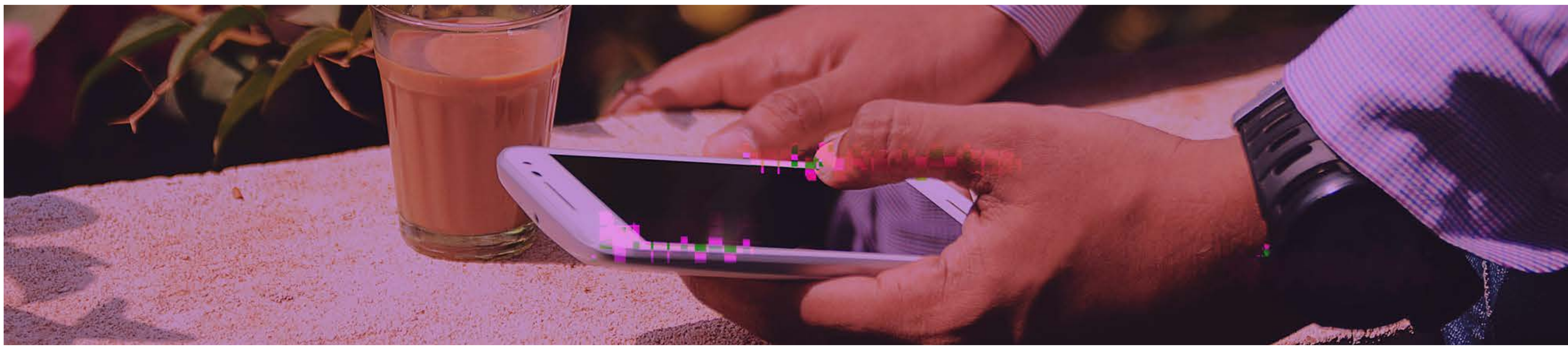
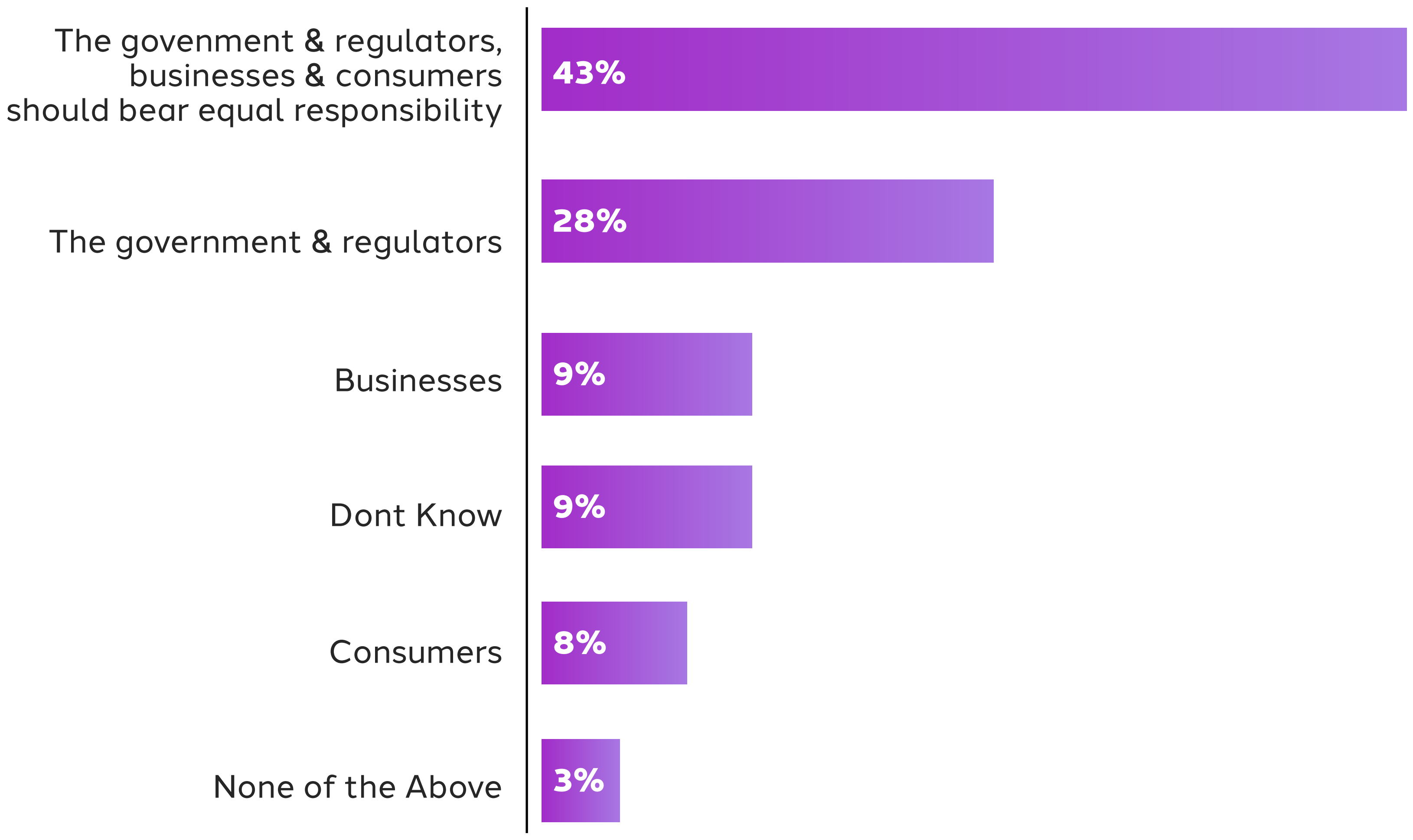


Figure 9: People favour collaborative forms of personal data governance

In the future (i.e. next 2-3 years), who do you think should be mainly responsible for ensuring personal data is protected and securely used?



Source: Dentsu Aegis Network Digital Society Index Survey 2020

What is clear is that consumers believe clear rules and standards will be required: more than two-thirds of people globally believe more regulation is needed to govern the development of new technologies such as artificial intelligence.[ix]

New tech, new ethical questions

Reflecting this anxiety about the future pace and scale of technological change, there are a number of privacy concerns about the deployment of facial recognition technology.[x] At the same time, many consumers expect these technologies to become commonplace in terms of applications such as payments (see Figure 10), particularly in emerging markets such as China, Mexico and Brazil. Technologies such as this (as well as voice assistants, for example) will raise new questions about how such data can be shared securely and with privacy concerns fully addressed.

But again, consumers are clear in their expectations: six out of ten believe that organisations will need to demonstrate higher standards of ethical behaviour over the next 2-3 years as far as personal data is concerned.[xi]

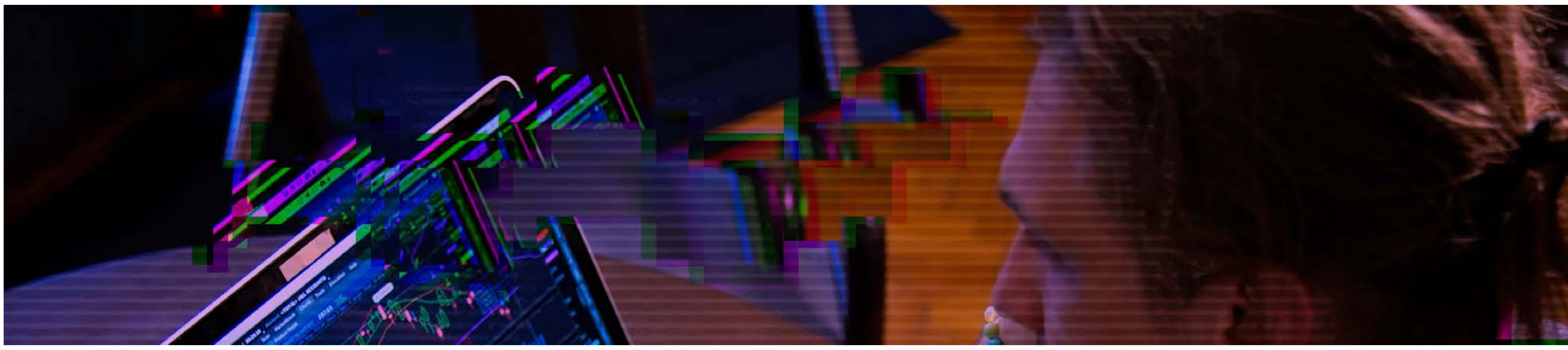
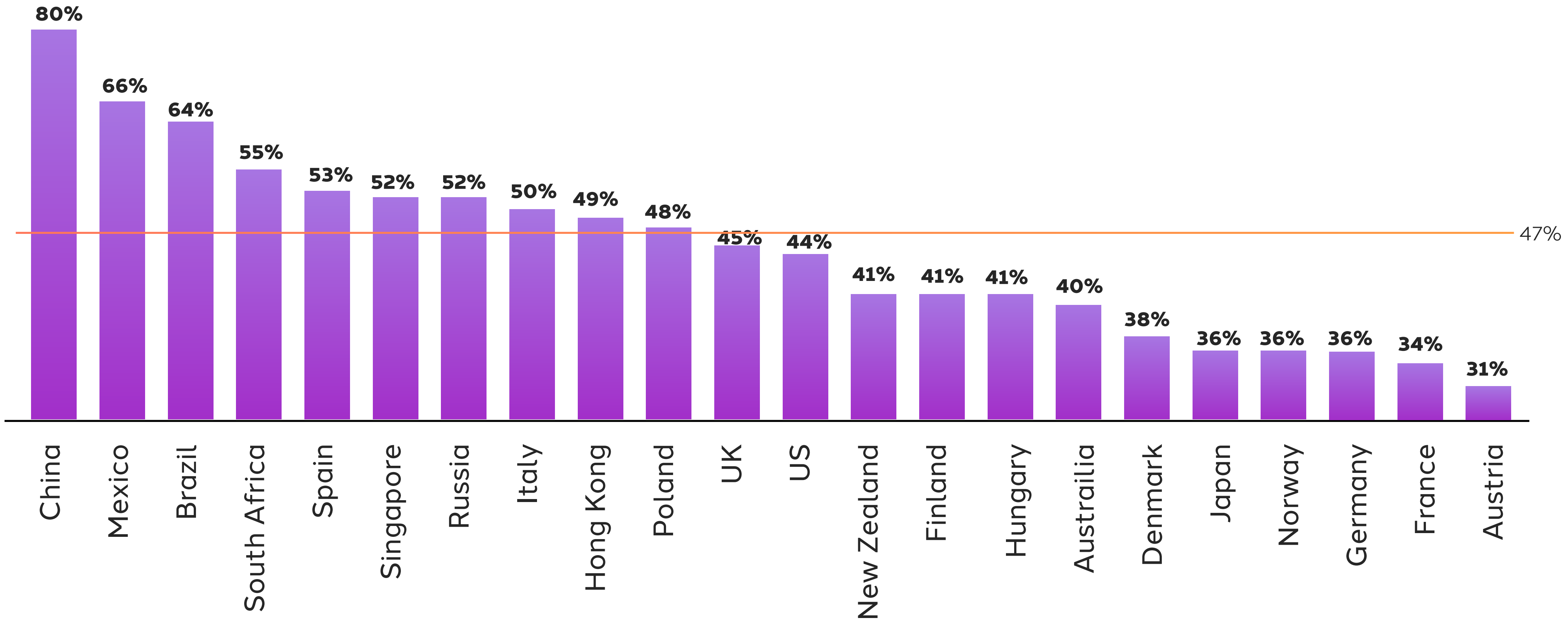
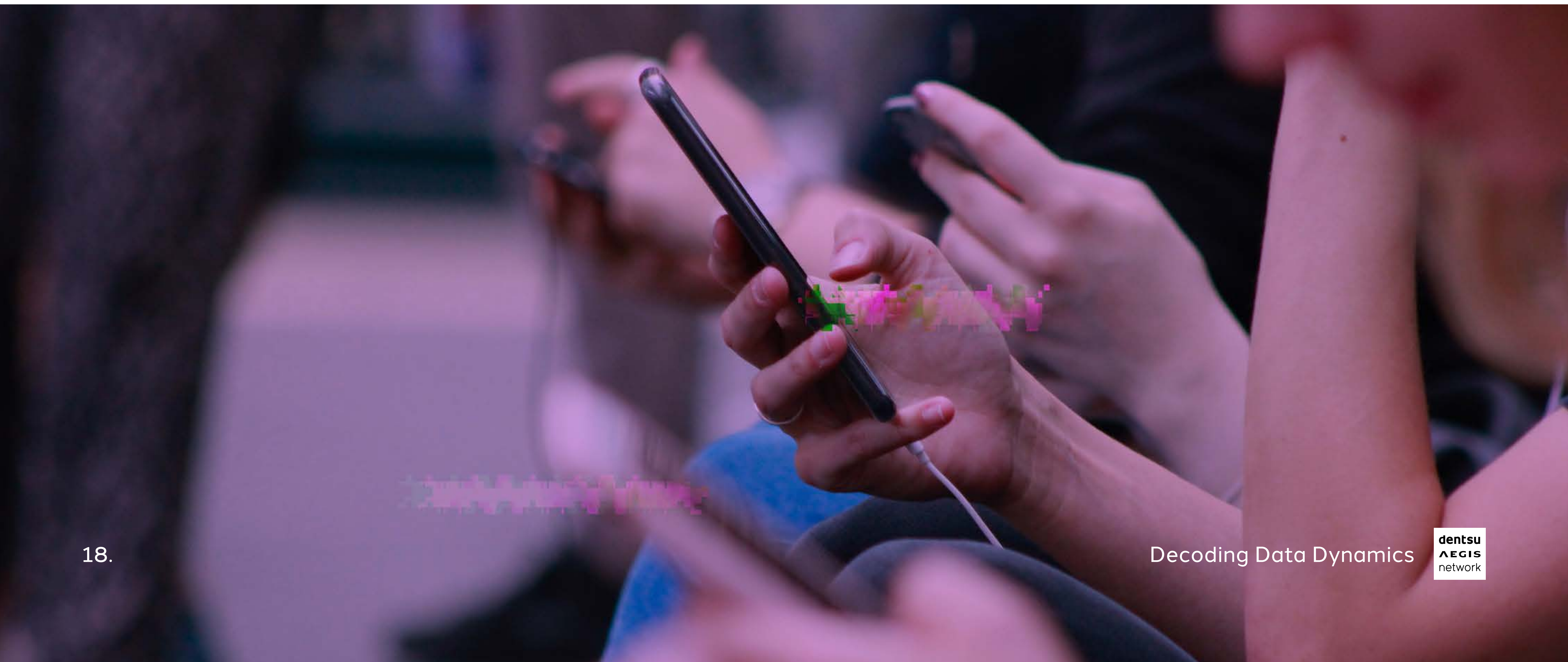


Figure 10: Almost half of people will expect to pay for products and services using facial recognition or fingerprint technology

In the future (i.e. next 2-3 years), I will pay for products/using services through facial recognition or fingerprint technology (% likely)



Source: Dentsu Aegis Network Digital Society Index Survey 2020

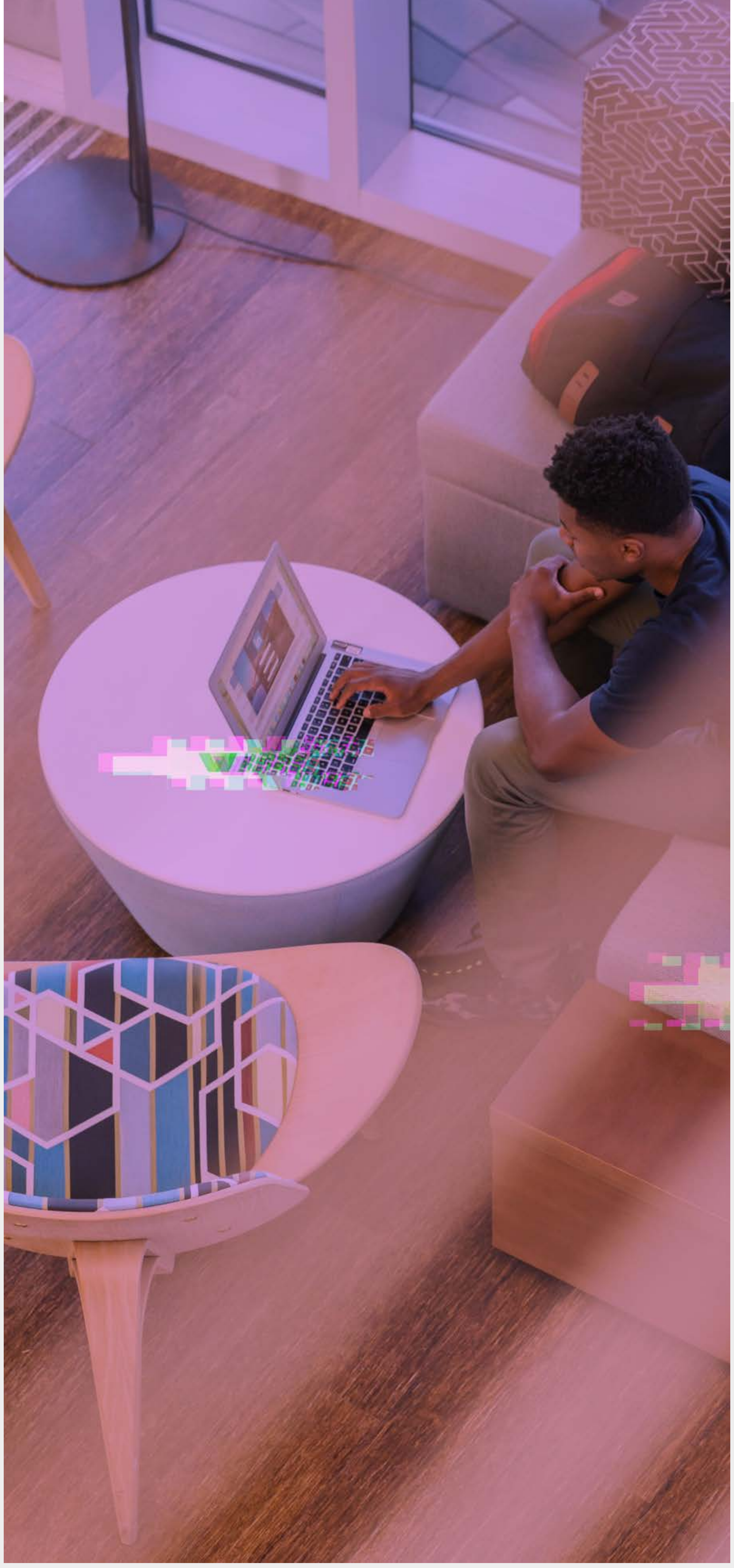


Scenarios

3. Looking ahead: Personal data scenarios for 2025

Despite some of the uncertainties surrounding consumer attitudes to personal data, what is clear is that adapting to these continuing trends will be critical to a business' long-term survival.

With the impact of the COVID-19 crisis on attitudes to personal data also still unclear, we've developed four scenarios to enable brands to explore the different possibilities for how the personal data landscape may unfold over the next five years. These scenarios will help brands to frame their thinking around personal data and navigate its opportunities and pitfalls. They are each intended to be equally plausible. Each scenario is presented through a short description and then a day in the life of an imagined consumer inhabiting that future world.



Why Scenarios?

- Scenario planning or development is a process that explores different scenarios that may happen in the future by identifying a specific set of key uncertainties.
- These scenarios provide a structure for thinking about—and a shared language for discussing—the impacts of and responses to potential future events.
- They help decision-makers to weigh up business risks and benefits and adapt current and future strategy accordingly.

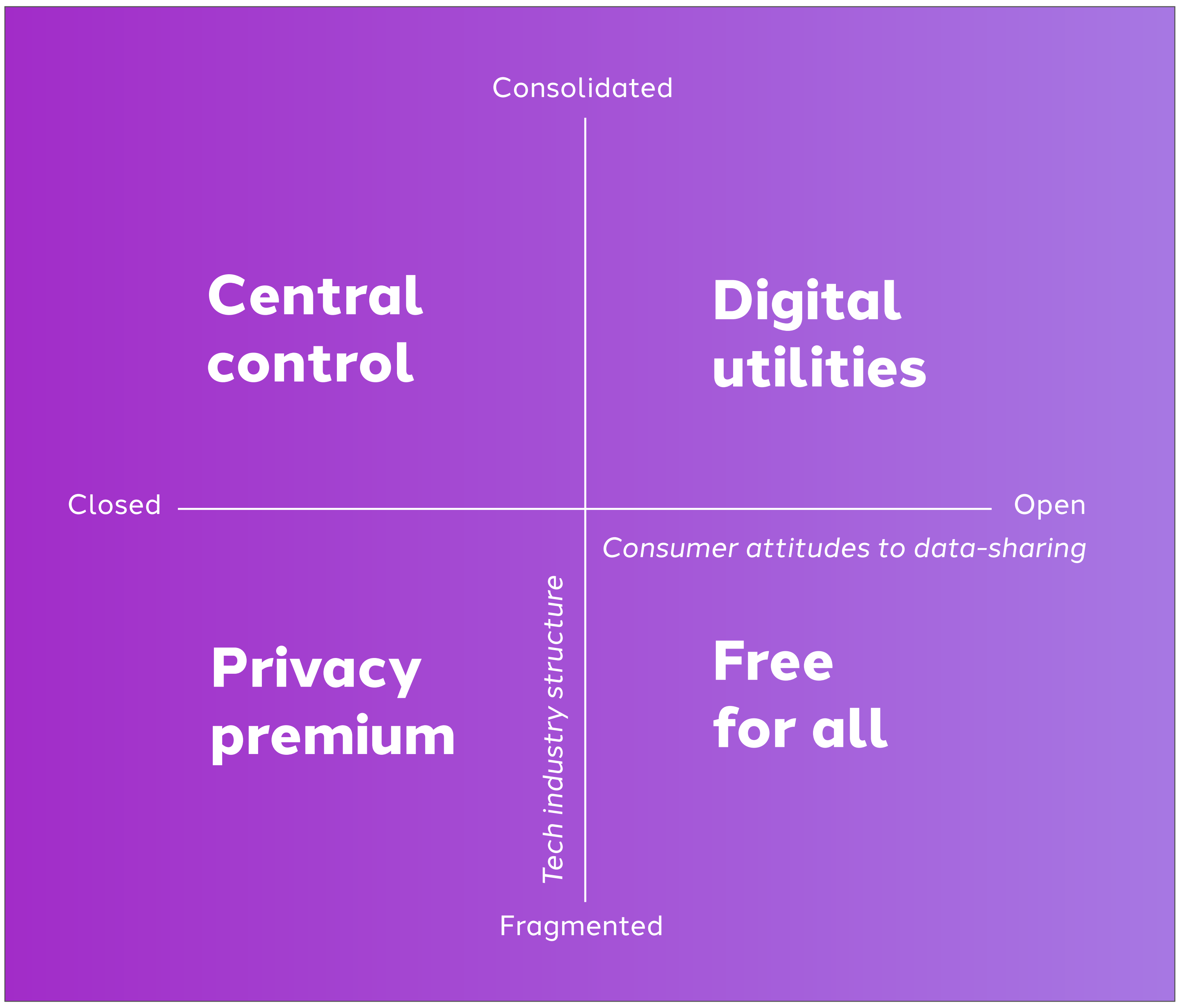
Methodology

To construct our scenarios, we ran a series of workshops with experts from across Dentsu Aegis Network—data protection lawyers, tech innovation and product development experts, client leads across creative, media and CRM, for example. We started by identifying a long list of future uncertainties facing business use of personal data, across the range of political, economic, social, technological, legislative and environmental factors. These were mapped by impact and uncertainty, with greater focus given to those uncertainties that we believe to be high impact but with a high level of uncertainty surrounding them.

We then explored the underlying drivers of these uncertainties and, after debate, discussion and refinement, arrived at two key drivers of uncertainty: consumer attitudes and behaviours towards sharing their data; and the overall structure and composition of the Big Tech industry, including the way in which it is regulated.

These two axes help us arrive at our personal data scenarios for 2025 (see Figure 11).

Figure 11: Our 2025 personal data scenarios



Source: Dentsu Aegis Network Analysis

Scenario 1: Central control

It's the year 2025. Consumers' trust in data-sharing is at an all-time low, following the great breach of medical data that followed the COVID-19 pandemic in 2020-21. Despite this lack of trust, Big Tech still reigns supreme, able to survive the economic recession brought about by market lockdowns and consolidating further into the 'big three' in 2022. These companies have invested heavily in walled gardens and privacy technologies, delivering unprecedented levels of data protection and limiting the amount of data-sharing. The UN Data Ethics Council was established in 2023, charged with ensuring consumer and citizen data rights are upheld around the globe. In response, brands are finally making personal data security their top priority and the number of data breaches are starting to decline.

A Day In The Life Of, Michael, aged 40, Sydney

*Stock photo used as representation of a potential consumer

Michael wouldn't trust someone with his data as far as he could throw them.

Like millions of others, his health records were stolen in 2021, his emails were hacked after his energy company lost his records in 2022 and he lost $3000 after his bank suffered a data breach in 2023.

Not surprising, then, that Michael is so pleased to see that the sanctions being brought in by the new UN Data Council are finally making CEOs sit up and take notice. Due to its gross negligence, one well-known consumer goods brand received a temporary ban from selling its products in a number of countries, including Michael's native Australia. About time too, Michael figured, until he realised that meant going without his favourite shaving foam for six months. It makes him wonder: perhaps consumers should be left to make their own minds up about whether to trust a brand?

Despite data breaches starting to decline, it seems to Michael that consumers are still being left with the short end of the stick. Now, companies are significantly less willing to share their data, even if it makes for a better customer experience. Most of the digital assistant apps Michael used to use are no longer running. A banking AI chatbot doesn't have a whole lot to chat about when your bank doesn't grant it access to your information.

For Michael, once (or more accurately, twice) burned, twice shy. He no longer saves his card details online, regularly clear his cookies and opts out of any location tracking on his smartphone. It's a lot less convenient, but it gives him a little peace of mind.

Last month, he even subscribed to a new privacy platform that tracks how a user shares their data online, verifies if their data is secure and automatically takes preventative measures on the user's behalf if their data is at risk. Still, Michael's not 100% reassured. Like many of the few innovations made these days, the platform is owned by the one of the 'big three' tech providers. Still, every little helps, right?

Scenario 2: Privacy premium

It's the year 2025. Countries have continued to enforce strict border controls since the COVID-19 crisis of 2020-21. Virtual borders have also been erected as a result of frictions between markets, like China and the US. With more people online following market lockdowns, Big Tech suffered the loss of millions of consumers following a major data breach in 2022. A number of governments even took legal action to break up their monopoly. Now, some countries enforce stringent data laws; others position themselves as 'data havens' that encourage data-sharing. In the post-Big Tech world, competition booms. Consumers may be worried about their personal data, but they have plenty of choice. To avoid being targeted like Big Tech was, brands are very protective of their customer data. Data-sharing across borders is highly regulated by governments and open data sources and partnerships are uncommon. To secure customer loyalty, all brands must demonstrate robust privacy strategies.

A Day In The Life Of, Julia, aged 33, Warsaw

*Stock photo used as representation of a potential consumer

Privacy is paramount for Julia.

Her personal data was hacked in 2022 when one of the world's largest tech companies suffered a colossal data breach. She lost very sensitive information, including health records, credit card numbers and passport details. Unsurprisingly, Julia is now very wary about her personal data's security, but she's thankful to be living where she is. She has friends abroad who aren't so lucky. She'd hate to live in one of those 'data haven' countries where lax data laws do little to protect consumers.

Although, Julia admits, a lack of data-sharing can have its drawbacks. With brands unwilling to risk breaking different national data regs, a number of planned open data schemes to support the COVID-19 response were abandoned and it took until 2024 before a vaccine was developed. Julia can't help thinking it's a shame. How can some of the world's biggest issues get solved if brands don't pull resources and innovate together?

When it comes to privacy technologies, however, innovation shows no signs of slowing down. Like most consumers nowadays, Julia only gives her loyalty to brands that walk the talk and truly put privacy at the top of their agenda. She now banks with a brand that uses blockchain so she doesn't have to share any personal data with a company when she makes a purchase.

Not that being a consumer in her country is all a bed of roses, either. Buying stuff online used to be the height of convenience, but now Julia spends so long trying to remember her countless passwords for different brand sites that she might as well pop down to the shops. And so now, she often does. Better to buy in-person or opt for smaller, local brands, she figures, than risk having her data hacked again.

Scenario 3: Digital utilities

It's the year 2025. Big Tech is now even Bigger. Their success led to the consolidation in the early 2020s of just a handful of Tech Titans. These companies have become the lifestyle partners of consumers the world over, providing a wide range of services that are tailored to their intimate, data-driven understanding of each individual. Consumers are happy to share their data, given the clear value exchange they receive. Regulation is light-touch these days, as consumers trust Big Tech to do the right thing. Big Tech developed its own Digital Ethics Alliance in 2023, which has helped to establish key principles and approaches governing data-led innovation. Part of that involves sharing personal data with NGOs and government agencies to address societal challenges, such as healthcare and the environment.

A Day In the Life Of, Anna, aged 22, Mexico City

*Stock photo used as representation of a potential consumer

Anna loves how seamless it is to be a consumer these days.

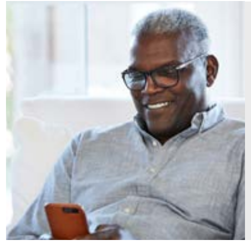
Take her music streaming platform. She switched to a Tech Titan a year ago. Now, while Anna listens to music at work or on the Metro, her search engine results, location data and smart billboards connect to give her real-time personalised promotions to nearby shops. That's how she got her new leather jacket half price—her friends are very jealous.

Life couldn't be easier now that one of the e-commerce Tech Titans branched out into healthcare and banking last year. Anna can now make purchases, transfer money and order prescriptions on one platform, with one username and one password. What's more, it's very transparent since the company acquired one of the world's top blockchain companies. So now, Anna receives a weekly overview of how her data has been used with clear directions on how to change permissions.

While the threat of a data breach remains, at the end of the day the benefits of sharing her data outweigh any risks in Anna's mind. Like many consumers since the COVID-19 pandemic, Anna has been passionate about using her data for good. Consequently, she has shared her medical data with the Tech Titans' new open data source scheme to enable health NGOs to use insights to develop more personalised care plans and treatments for patients.

Scenario 4: Free for all

It's the year 2025. The number of people online has permanently surged since the COVID-19 crisis of 2020-21, as consumers have found fulfilment in their virtual lives from the safety of their own homes. Happy to share their personal data to improve their online experience, consumer trust in data-sharing has rocketed the world over. People take confidence from their local regulatory intervention and a vast array of new tech services that have emerged since the Big Tech companies were broken up in most countries in 2022, following landmark legal cases in Europe and the US. Heralding a new era of competition and consumer choice, brands' focus is now back on consumer value—if there is a profit to be made from personal data these days, it now belongs to consumers. While the emergence of fledgling tech players provides new opportunities for hackers, brands are still happy to engage in open data schemes and partnerships with NGOs and government agencies to support purpose-led causes—and, hopefully, gain an edge.



A Day In The Life Of, Andrew, aged 55, Johannesburg

*Stock photo used as representation of a potential consumer

For Andrew, when it comes to personal data, things are looking up.

As a result of the COVID-19 pandemic, Andrew does most things online these days, from attending doctor appointments to buying his groceries, and he's willing to share his personal data for a superior customer experience. He trusts that his data is kept reasonably private, after his government took a firm stance on Big Tech—although some of his trust may be misplaced. With more people online than ever before, data breaches seem to be creeping up, now that consumers like Andrew are sharing data with a greater range of tech providers, and most governments are inclined to give out slaps on the wrists rather than crippling fines.

Andrew now subscribes to a platform start-up that enables him to easily earn money from selling his data to businesses, one of the many new tech products and services that has popped up in the last couple of years. It's not a big money-spinner, but he's pleased that, if there's money to be made from his data, he's the one earning it.

Open data partnerships have sprung up everywhere. Andrew is now selling his location history data so an environmental NGO and automotive brand can better understand his carbon footprint. He hopes it'll do some good, but data-sharing can be a bit of a minefield these days. As part of the deal, he's no longer allowed to sell this or any other personal data to other automotive brands—even if it's being used to support a purpose-led initiative.

New tech players bring benefits. Andrew takes advantage of the different online marketplaces to run his t-shirt business. Keen to outdo their competition, these platforms opt to take less profit share. Moreover, they offer free next-day delivery as standard—so he gets a good deal as a customer, too.

Recommendations

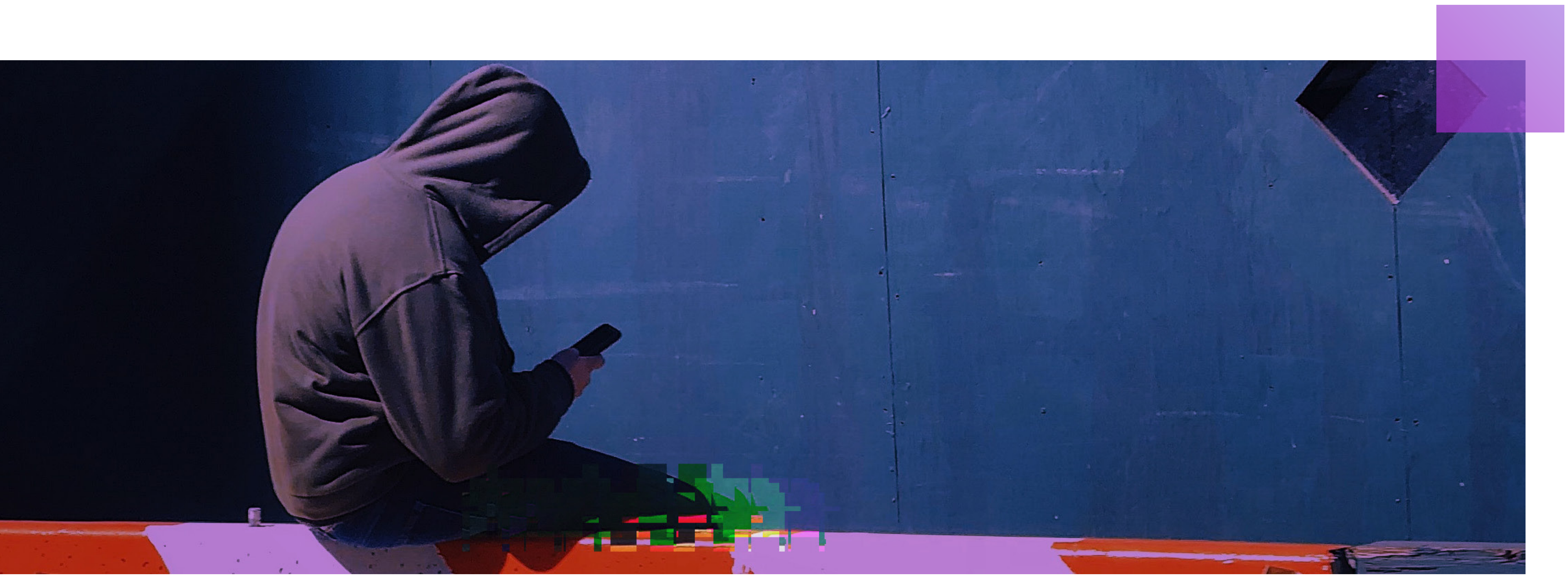
4. Brand actions to consider

These scenarios are neither designed to be inflexible nor mutually exclusive—in reality, each will manifest themselves to varying degrees in the coming years. Instead, they should shed light on how the factors driving the personal data landscape may evolve and help brands to make better-informed decisions in the future. Based on the trends and future scenarios identified, brands at a minimum need to do the following:

- Prioritise investment in data security to combat the ever-present risk of cyber-attacks and data breaches. This is not just about new technology, but ensuring that data security is part of your organisational and cultural DNA.
- Ensure that the right processes, workflows and roles are in place to make the most of your customer data. First-party identity and data, data management technologies and analytic capabilities act as enablers to gaining consumer insight and delivering valuable experiences, but they are not the entire solution.

For your organisation to achieve effective data management, it must focus on desired outcomes and how its data streams contribute to driving them.

- Build trust with consumers by being clear about the value exchange they will receive for sharing their data and by leveraging CRM capabilities. From providing promotions to tailored products and services, our analysis shows consumers expect to be asked for their consent. Prioritise transparency in your messaging so that your customers feel included and informed.
- Upskill employees to successfully navigate the changing data regulatory landscape. Your people cannot be expected to maximise data's value securely and legally without the right training. From virtual workshops to eLearning to instructor-led classes, facilitate a learning experience that works best for your teams and the type of content.



Beyond that, actions will vary depending on how events evolve and how far brands want to lean into the trends that underpin our scenarios. For example:

- In our **Central control** scenario, where a few key players dominate the data landscape and have constructed walled gardens that consolidate their position, brands able to procure first-party data and satisfy consumer concerns over personal data will have a competitive advantage. This would place a premium on first-party identity—the growth of a brand's universe of first-party CRM and digital records tied to a master, persistent ID—and exploring alliance and partnership opportunities.

  For example, American Express partnering with ad tech vendor Neustar, which brings together publisher's data with that of advertisers.[xii] Furthermore, within this context, a better long-term strategy to counter the control that few dominant players have over consumer data could involve building direct relationships with consumers through, for example, the development of app, content and commerce strategies.

- In **Privacy premium**, where privacy has evolved to be a fundamental source of competitive differentiation for all brands, a trusted relationship with customers is paramount. Successful strategies here would likely revolve around optimising and investing in loyalty programmes to build better customer relationships as well as enhanced product development to ensure privacy is strengthened by design. Apple is an example of a leading brand in this space, developing privacy features for its devices that tell consumers how apps may be tracking their data.[xiii]

  To successfully engage new customers, leveraging creative capabilities could also help build brand credibility and reliability. With some forms of data likely to be increasingly unavailable (e.g. cookie data), brands would want to ensure they retain a strong understanding of the customer. That means investing in first-party identity and data solutions (e.g. master ID and identity resolution), access to a range of data forms (e.g. privacy-safe offline data sources, panel data, attitudinal data etc.), as well as in the technologies and training to maximise this data's value.

- In **Digital utilities**, with consumers more open to sharing their data with a limited array of platform brands that support personal lifestyles, leveraging these large data partners to build your relationship with consumers would be key. This means partnering broadly across the Tech ecosystem, connecting brand consumer data into multiple ecosystems, and identifying and leveraging the key strengths of each. Use Big Tech's delivery platforms, targeting options and consumer environments to maximise impact in a coordinated, portfolio approach. In this approach, a key strategy will be the ownership, control and growth of first-party identity and data (e.g. CRM, site and app engagement) with the ability to match and connect this to Big Tech's universe of consumers.

  A bigger bet here could be to identify the Big Tech platform that best fits the brand objectives in terms of data handling and consumer engagement possibilities. Double-down on this single player, connect brand first-party CRM data to the ecosystem and leverage all aspects of the partner's targeting, delivery, and data infrastructure, seeking to gain benefit through depth, specialism, and the natural interconnectedness of the single partner's ecosystem.

- Last, in **Free for all**, a fragmented and competitive business environment makes it critical to ensure it's clear to customers the value exchange for sharing their data. For example, Killi is an app that pays consumers with cash for sharing their data, location, or providing insight about what ads they'd like to see. Brands such as McDonald's, GM, Danone and Staples have all signed up to participate, according to Killi.[xiv]

  Further options in this future would include decentralising brand and company architecture to enable more real-time messaging and micro-segmentation within markets, while concurrently looking for opportunities to automate and aggregate to increase your data scale. Taking bolder advantage of the open data ecosystem would necessitate greater focus on first-party identity resolution and privacy-safe data management, with scaled capture and blending of many data assets. That would create broad, deep, and dense data around each consumer as an organisation's "private first-party identity graph" that they own, versus ceding that capability to third-party Big Tech players, publishers and apps, for example. This would require brands to leverage open and shared consent mechanisms to provide consumers with appropriate controls and safeguards.

In addition to these recommendations, experts from across our network also give their perspectives on the key implications for brands from a creative, media and CRM perspective.

> *In a world where consumers are increasingly conscious of the value of their data, brands must design experiences that offer a compelling value exchange. Consumers must see the value in terms of utility, but more importantly must feel the value through delightful and relevant experiences.*
>
> *As controls on cookies tighten, contextual data becomes powerful. Real-time data on weather and traffic patterns, pollution levels and search patterns can enable highly relevant user experiences without feeling intrusive. As platforms like Apple become more transparent about how data is used (or abused), brands should start to think about the minimum personal data needed to make a meaningful connection.*
>
> *Finally, as interfaces evolve away from screen-based interactions, brands will handle ever more sensitive biometric data. The potential for social good is huge—start-ups are using AI to detect everything from heart disease to high blood pressure—but the responsibility will also be immense. A useful data mantra for us all might be our own version of the Hippocratic Oath: First, do no harm.*

Patricia McDonald
Chief Solutions Officer, Dentsu Creative

“Media is more important than it has ever been – to marketers, to consumers, to society. At the heart of all this promise sits the shared mutual trust of consumer data and how it is used to create value and good in equal measure for all involved. Brands have to manage the ever-increasing complexities of media, data, and privacy, which are key to building more relevant and accountable media experiences. More importantly than this, however, it is the key to bringing both brands and agencies together to passionately defend and advocate or consumers and their interests.

Bringing the brand and performance agendas together in an integrated approach to data and media is critical for brands to generate both long-term brand value and more immediate business performance. But none of this matters without also building and protecting the sacred trust of consumers, who come to brands seeking value. That's the mission to which brands and media agencies must mutually rededicate ourselves. And it's the only way we get to deliver the promise of the future to consumers in a way they can trust.”

Michael Epstein,
CEO Media Brands and Product

“*With privacy regulations increasing, third-party cookies disappearing, walled gardens like Google, Facebook and Amazon building their walls higher, and the growth of technology providers leading to continued consumer data fragmentation, brands need to take ownership and control of first-party identity and data as a sustainable competitive advantage to deliver the total customer experience.*

Like many leaders across almost every vertical who have amassed a large and stable universe of first-party IDs from direct-to-consumer business models and a focus on superior value exchange with consumers, brands will transform by placing first-party identity and data at the centre of their enterprise. With that comes the responsibility of proper data security and privacy measures, which will require new skills and capabilities. The first-party data management infrastructure powered by identity—and its ability to be interoperable with an ever-changing landscape of tech, data, and media—will take centre stage. These fundamentals, which would normally be relegated to CRM-driven businesses, will now become imperative for all organisations.”

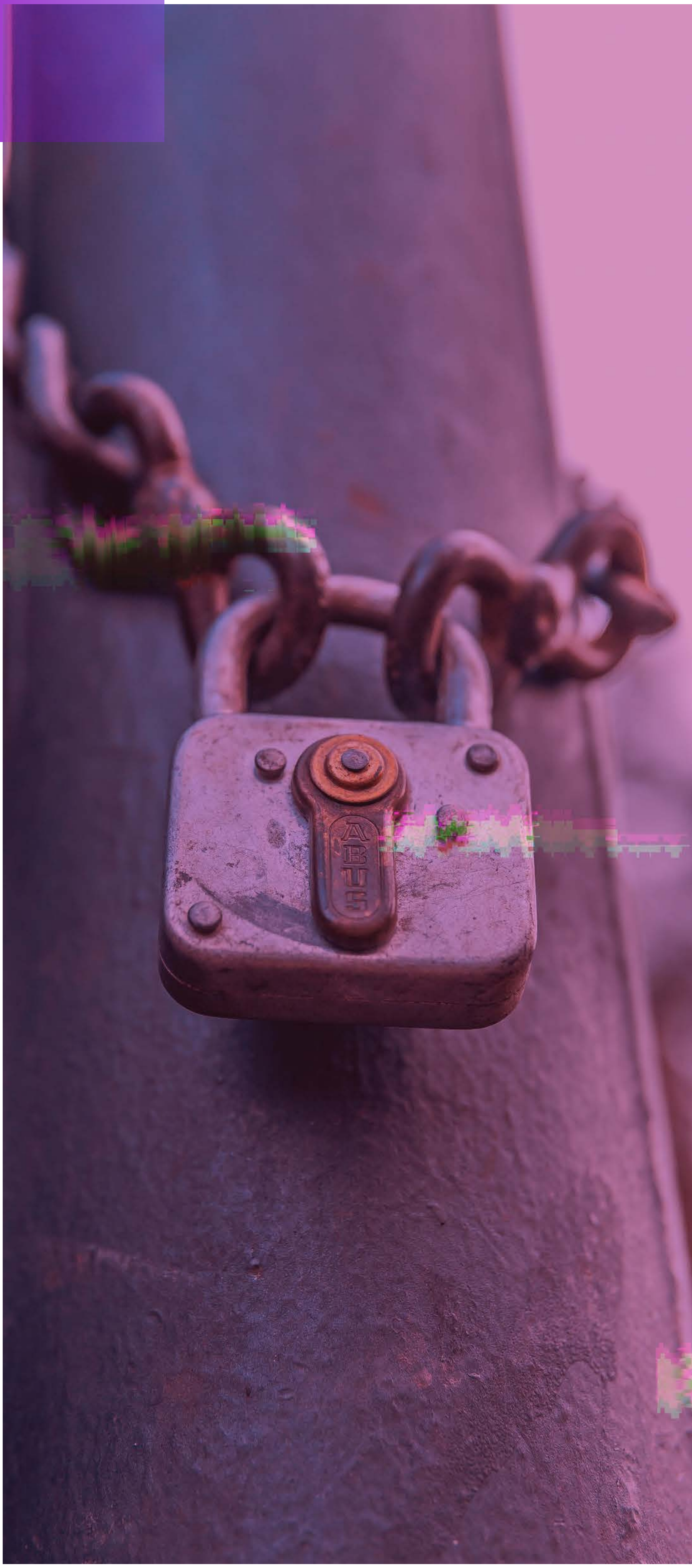
Gerry Bavaro,
Chief Strategy Officer, Merkury

5. Conclusion

The use of personal data has steadily climbed up the agenda of people, businesses and governments alike. The COVID-19 pandemic does not change this—if anything, the crisis highlights how personal data increasingly can be harnessed to enable our everyday lives in a virtual setting. Therefore, it is imperative that brands prioritise understanding the benefits and risks associated with personal data moving forward.

By exploring personal data through future scenarios, it becomes clear that there are many ways the data environment may yet be shaped by long-term trends, such as consumer concerns and data regulations, and the more immediate context of COVID-19.

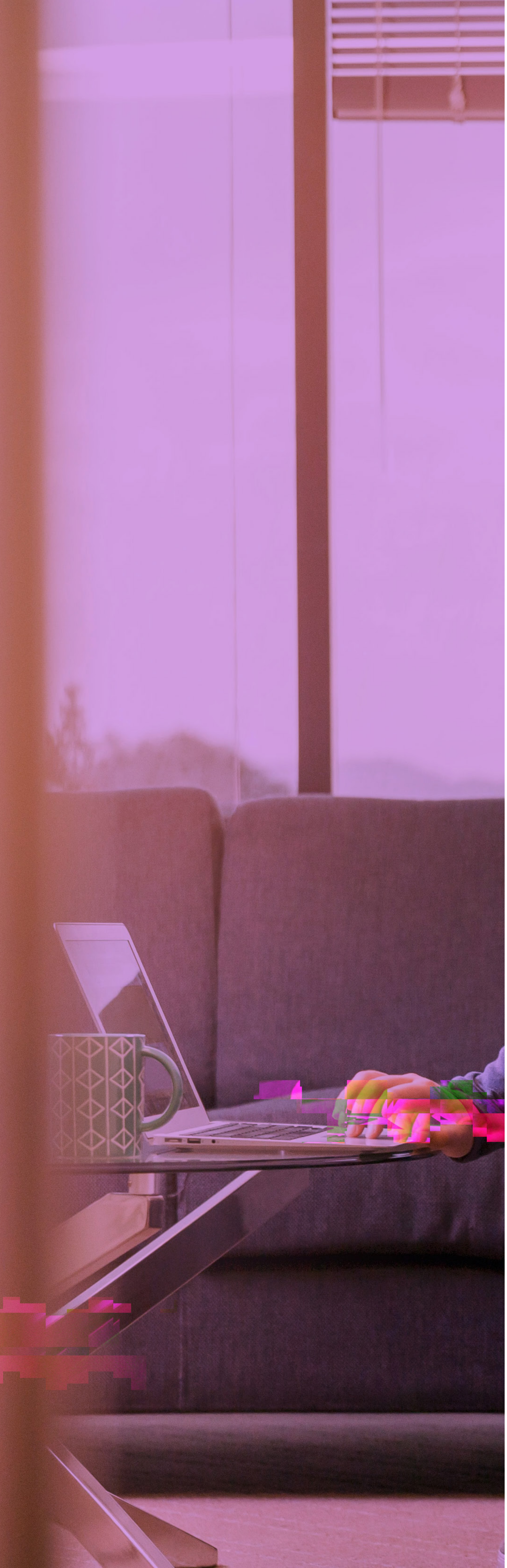
Brands have already demonstrated a quick ability to adapt during the current crisis. To maximise the opportunity that personal data represents, they must demonstrate the organisational agility and flexibility to respond to the data landscape, both today and tomorrow.



Acknowledgements

We would like to thank our many colleagues who have been involved in the development of this report from all parts of the business. At the risk of missing someone out, special thanks go to the subject matter experts who have shaped this report:

- **Gerry Bavaro** (Merkle)
- **Dan Calladine** (Carat)
- **Garreth Cameron** (Dentsu Aegis Network)
- **Michael Epstein** (Carat)
- **Louise Gordon-Jones** (Dentsu Aegis Network)
- **Anthony Groves** (Dentsu Aegis Network)
- **Damien Healy** (Dentsu Aegis Network)
- **Dirk Herbert** (Dentsu Aegis Network)
- **Patrick Hounsell** (Merkle)
- **Adam Lavelle** (Merkle)
- **John Lee** (Merkle)
- **Patricia McDonald** (Dentsu Aegis Network)
- **Christine McKinnon** (Carat)
- **Prashant Mehta** (Isobar)
- **Sanjay Nazerali** (Dentsu X)
- **Kara Osbourne** (Dentsu Aegis Network)
- **Rohan Philips** (iProspect)
- **Simon Rice** (Merkle)
- **Mahisha Rupan** (Dentsu Aegis Network)
- **Lauren Walker** (Dentsu Aegis Network)
- **Paul Wilson** (Vizeum)



References

[i] OECD, Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics, 23 April 2020

[ii] Forbes, Is COVID-19 Social Media's Levelling Up Moment?, 24 April 2020

[iii] Pew Research, Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, 15 November 2019

[iv] ZDNet, Zoom to iPhone users: We're no longer sending your data to Facebook, 30 March 2020

[v] Quicksprout, Checkout Process Design For High Conversion Rates, 8 January 2020

[vi] Digital Journal, Report finds only 1 percent reads 'Terms and Conditions', 29 January 2020

[vii] Dentsu Aegis Network, Digital Society Index survey 2020

[viii] Forbes, This startup wants to use your data to bet on the markets—and cut you in on the profits, 12 April 2019

[ix] Dentsu Aegis Network, Digital Society Index survey 2020

[x] Forbes, The Major Concerns Around Facial Recognition Technology, 25 September 2019

[xi] Dentsu Aegis Network, Digital Society Index survey 2020

[xii] Digiday, How American Express is preparing for a world without cookies, 6 November 2019

[xiii] Cnet, Apple's new iOS privacy updates will show how apps are tracking you, 22 June 2020

[xiv] Communicate, Redefining value exchange: give brands your data AND get paid for it, 12 August 2018

dentsu
AEGIS
network

About Dentsu Aegis Network

Part of the Dentsu Group, Dentsu Aegis Network is made up of eight leadership brands - Carat, dentsu X, iProspect, Isobar, dentsumcgarrybowen, Merkle, MKTG, and Vizeum and supported by its specialist/multi-market brands. Dentsu Aegis Network is Innovating the Way Brands Are Built for its clients through its best-in-class expertise and capabilities in media, digital and creative communications services. Offering a distinctive and innovative range of products and services, Dentsu Aegis Network is headquartered in London and operates in over 145 markets worldwide with more than 45,000 dedicated specialists.

www.dentsuaegisnetwork.com

For further information
please contact

Global head of thought leadership
tim.cooper@dentsuaegis.com