Microsoft

iProspect

IN BRANDS WE TRUST

The Intersection of Privacy and Trust in the Age of the Empowered Consumer

2020 Consumer Privacy and Brand Trust Research by Microsoft Advertising in partnership with iProspect

FORWARD

We would be remiss to not acknowledge the unprecedented impact of COVID-19 and the potential for massive changes to how consumers view data ownership and privacy. The surveys analysed in this paper were completed prior to the global pandemic, but they still provide insights and opportunities for brands as well as a baseline for how consumer perceptions of privacy will change in the coming months and years.

The definition of privacy not only varies widely across consumer segments, it is constantly evolving. We're already seeing privacy impacts such as governments tracking mobile location data and the collection of aggregated and anonymised health data from smart devices. It's also likely that increased adoption of online interactions as a replacement for in-person transactions will drive increased knowledge of privacy agreements and the tangible value of data sharing across countries, age groups and other demographic segments.

One thing remains clear: It's critical that brands focus their privacy initiatives well beyond meeting the minimum legal requirements, educate and empower their consumers by being transparent and proactive, and deliver tangible value in exchange for personal data.

THANK YOU,

Misty Locke, Jeremy Hull, Christi Olson, Adrian Cutler

INTRODUCTION

The Intersection of Privacy, Customer Experience and Brand Loyalty

Data privacy is a hot topic among organisations in every industry. The amount of data that is generated and collected has grown exponentially over the past few decades — 90% of all existing data was generated in the last two years.[1] In 2020, 1.7 megabytes of data will be generated each second for every person on earth,[2] and by 2025, global data is expected to grow to 175 trillion gigabytes.[3]

It's no wonder 97.2% of organisations are investing in big data and AI for a variety of reasons,[4] including the ability to hone marketing outreach, segment target audiences, tailor advertising and offers, and generate relevant content and experiences that lead to high conversion rates.

But depending on their age, geographic location and experience, consumers have various levels of understanding about how their personal data is used and protected, and different tolerance levels about sharing it. As a result, new laws and regulations for data privacy are emerging to govern how organisations collect and use consumer data, which will have a significant impact on marketing organisations in every industry. Today's marketers are questioning what data they can legally collect, store and use - and how will they provide value and establish trust among a consumer audience that is bombarded with stories about data breaches and identity theft?

In this whitepaper, we share key findings and insights gleaned from the analysis of the Consumer Privacy and Data Survey by Microsoft and iProspect. The survey was conducted online by Toluna in December 2019 through January 2020. The survey had 23,867 responses from 16 countries across North America, South America, the European Union, Asia and Africa.

Building off the findings from the Toluna survey, we used the online research tool AskSuzy to engage with an additional 2,000 U.S. consumers in February and March 2020 to gain a deeper understanding of consumer understanding and perception of the California Consumer Protection Act (CCPA) that went into effect January 2020.

10 KEY FINDINGS

PRIVACY

1 87% of respondents say they believe data privacy is a right, not a privilege.

2 Nearly half (49%) of respondents think data privacy is a shared responsibility among businesses, individuals, governmental bodies and technology innovators.

3 Consumers in EMEA are more concerned about data privacy than consumers in other regions.

DATA COLLECTION

4 The vast majority (91%) of respondents are concerned about the amount of data companies can collect about them.

5 64% of respondents are concerned about the amount of data being collected, and of those with concerns, 72% have stopped using a product or service because of those concerns.

6 Nearly all respondents (88%) have either refused to give or provided false information when they were asked to provide personal info. Individuals have many reasons for refusing to share their data, with concerns about data security being the top selected.

Source: 2020 Consumer Privacy Research by Microsoft Advertising in partnership with iProspect

VALUE EXCHANGE

7 Only 24% see the value of personalisation as the result of sharing data, and just 15% feel they're getting good value from granting access to their data.

8 Millennials see more value in personalisation and expect to get more from agreeing to share their personal data than consumers in other age groups.

DATA BREACH

9 85% of consumers say their relationship with a company changed following a data breach, and 65% said they stopped doing business with that company altogether.

10 91% of customers who experienced a data breech reported decreased levels of trust with the companies involved.

Source: 2020 Consumer Privacy Research by Microsoft Advertising in partnership with iProspect

1 THE INTERSECTION OF PRIVACY AND TRUST

CAN PRIVACY BE DEFINED WITH CONSISTENCY?

Privacy is a broad term with strong emotional connotations. Most consumers feel it's a human right; we're entitled to live our lives the way we want and choose what information we share with others. Privacy begs a discussion of boundaries and personal space, as well as choice and freedom. Privacy is about being accountable for and respecting choices over the collection, control, use and distribution of personal data, as well as providing ways to manage those preferences.

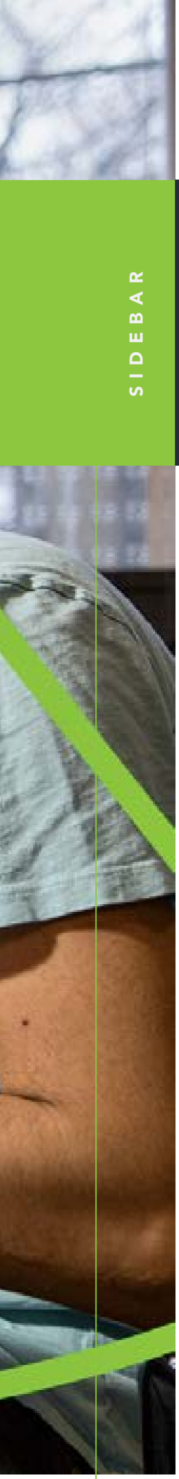
In this section, we explore the meaning of privacy, new and emerging data privacy regulations, and the impact of data privacy regulations and concerns for brands.

The Chameleon Nature of Privacy

Privacy is a chameleon because its meaning changes depending on a number of factors. Your nationality, culture, circumstance or situation all have an impact on how you view privacy and the boundaries you set around information you choose to share. An American citizen may feel more entitled to personal privacy and freedom than a Chinese citizen who's more accustomed to restrictive governmental regulations.[5] A Millennial who grew up sharing personal information on social channels may feel less concerned about personal privacy than a Baby Boomer who avoids social media. Other factors include the type of data in question, the purpose for sharing it, and the relative value exchange (what you get in return for allowing access to your data).

As digital technology continues to permeate our lives, data privacy has come to the forefront, with businesses and consumers all struggling to figure out exactly what it means—and how to handle it. Standard definitions of data privacy are based on practical concerns such as how data is collected, stored and shared with third parties, and whether individuals have the right to determine what, if any, of their personal data can be made public. These considerations have given rise to data privacy regulations such as GDPR in Europe and CCPA in California, the first of many that are sure to emerge globally.

But even these considerations can change depending on who is using the data in question and that depends a lot on one essential human emotion: Trust.



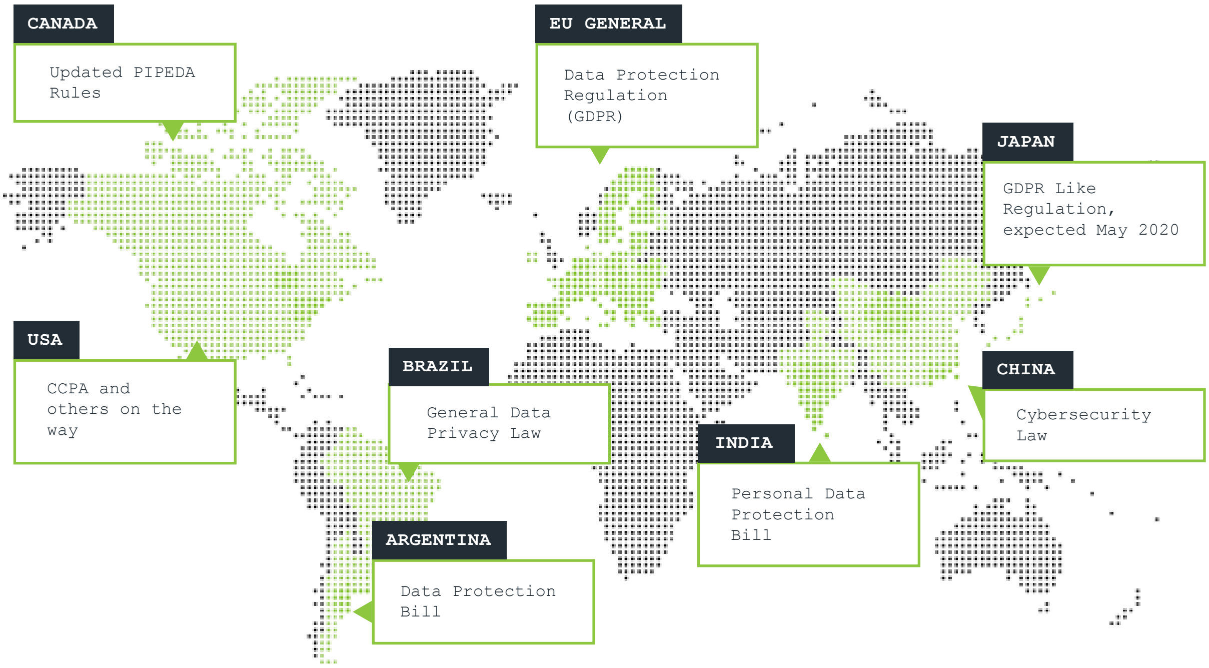
SIDEBAR

New Data Privacy Regulations Change the Game

Getting privacy right starts with understanding and abiding by the law. Here are summaries of recent data privacy laws that have been introduced globally:

FIGURE 1

Privacy Regulations Across the Globe



THE GDPR

The General Data Protection Regulation (GDPR) was enacted May 25, 2018 in the European Union, replacing the existing Data Protection Directive 95/46/EC. The new law is based on stricter directives around transparency, choice and accountability and is especially prescriptive in areas such as the content of privacy policies, data processing agreements and consent. If non-compliant, businesses can pay fines up to $23.5 million, or 4% of their global annual revenue. The GDPR also requires, in most cases, that businesses notify data protection authorities of any personal data breaches within 72 hours of the incident.

THE CCPA

Effective January 1, 2020, the California Consumer Privacy Act (CCPA) outlines new standards for data collection, as well as what happens to businesses who fail to protect user data. It grants California consumers rights to keep their data secure. The strictest data privacy standard enacted to date, the CCPA is likely to provide a blueprint for additional regulations, and the standard by which businesses build their privacy and data collection systems moving forward.

Other privacy protection laws:

- The Argentina Data Protection Bill (PDPA)
- The Brazil General Data Privacy Law (LGPD)
- The India Personal Data Protection Act (DPA)
- The Peoples Republic of China Cybersecurity Law
- The Australia Privacy Act (OAIC)

WHAT NOW?

Ultimately, the new laws put consumers in the driver's seat. They can demand to know what data companies have about them. They can ask companies to delete all of that data and be "forgotten." Or, they can allow companies to keep the data on record, but not sell it to anyone. Essentially, thanks to the new laws, brands are at the mercy of consumer choice when it comes to using data for marketing purposes.

The individual expectations of consumers are now part of the equation. Brands need to understand and respect consumers expectations of privacy. This includes what data and information a company collects, what a product or service should or is supposed to do and how personal data should be used to create that functionality.

Source: 2020 Consumer Privacy Research by Microsoft Advertising in partnership with iProspect

Data Privacy and Brands

Personal data can be used for great things, from predictive text to automatic reordering of products to personalised medicine. Privacy as it relates to brands is focusing on protecting data and creating controls that ensure the appropriate use of personal data. The use of personal data for marketing purposes is under a microscope as concerns around data privacy grow.

Marketing technology has evolved substantially in recent years, with more than 7,000 software applications and tools dependent on consumer data to help brands generate and convert business.[6] Personalisation in sales and marketing depends on access to consumer data and is, in itself, a controversial topic. Although consumers are beginning to expect a certain level of personalisation in the content they receive from brands, determining the point at which personalisation becomes intrusive isn't easy.[7] Brands need to walk a fine line between providing a personalised 1:1 experience and avoiding making consumers feel uncomfortable with hyper-personalised targeting.

To gauge consumers' threshold for personalisation—and to comply with data privacy regulations—brands must inform consumers about how they use their data. But simply sending them privacy policies is not always effective. According to our survey results, of the participants who acknowledge being asked to agree to a privacy policy online or in an app, only 22% confidently answered that they read the policy. This is hardly surprising considering for instance. the vast majority of the privacy policies of the most popular websites in the United States exceed the college reading level and can rarely be read in less than five minutes, according to The New York Times.[8] In their analysis, only BBC's privacy policy is equivalent to a middle school reading level.

And despite growing concerns over the ways in which brands use personal data for marketing and sales, only half of those asked to accept a privacy policy have stopped using a service or changed their purchase behavior because of privacy concerns. What's even more telling is 44% of consumers don't feel they really have a choice in accepting a privacy policy. If they don't accept, they fear they won't be able to use the product or service, or will have a limited experience with it.

FIGURE 2

Roughly half of consumers in North America and EMEA don't feel they have a choice when it comes to opting in and data collection

DO YOU FEEL YOU HAVE A CHOICE IN ALLOWING COMPANIES TO COLLECT DATA ABOUT YOU?

	ALL RESPONDENTS	NORTH AMERICA	EMEA	LATAM	APAC
YES	50.99%	50.54%	51.65%	41.01%	61.07%
NO	43.93%	49.46%	48.35%	36.37%	38.93%

FIGURE 3

91% of consumers are concerned about the data collected about them

ARE YOU CONCERNED ABOUT THE AMOUNT OF DATA COMPANIES CAN COLLECT ABOUT YOU?

(of the people who said No, they don't' have a choice, here is their sentiment and concern level)

	ALL RESPONDENTS	NORTH AMERICA	EMEA	LATAM	APAC
VERY + SOMEWHAT	91.09%	92.87%	89.57%	88.63%	92.56%
NOT CONCERNED	8.91%	7.10%	10.43%	11.37%	7.44%

Source: 2020 Consumer Privacy Research by Microsoft Advertising in partnership with iProspect

Yet concerns persist and can erode consumer trust in brands as evidenced by the fallout of recent major data breaches. For example, the Cambridge Analytica scandal in 2018, revealed that 87 million Facebook user profiles were compromised, driving Facebook's shares to fall more than 24% and the company to lose $134 billion in market value in just one week. Accenture reports that lack of trust costs U.S. companies $756 billion per year.[9]

Data privacy from the brand's perspective relates directly to business and financial success. Failing to comply with data privacy standards can result in steep fines and even legal consequences. Data breaches can damage a brand's reputation and, ultimately, impact market share and potential revenue. Importantly, customers are typically more willing to share their personal data if they trust that the environment is secure and companies aren't going to use their data in any unauthorised way.

SIDEBAR

What Data is Personal Data?

Personal data is more than personally identifiable information (PII), such as your home address or Social Security number. It's any data that is linked or linkable to a particular person. It can include any data linked directly or indirectly by reference to:

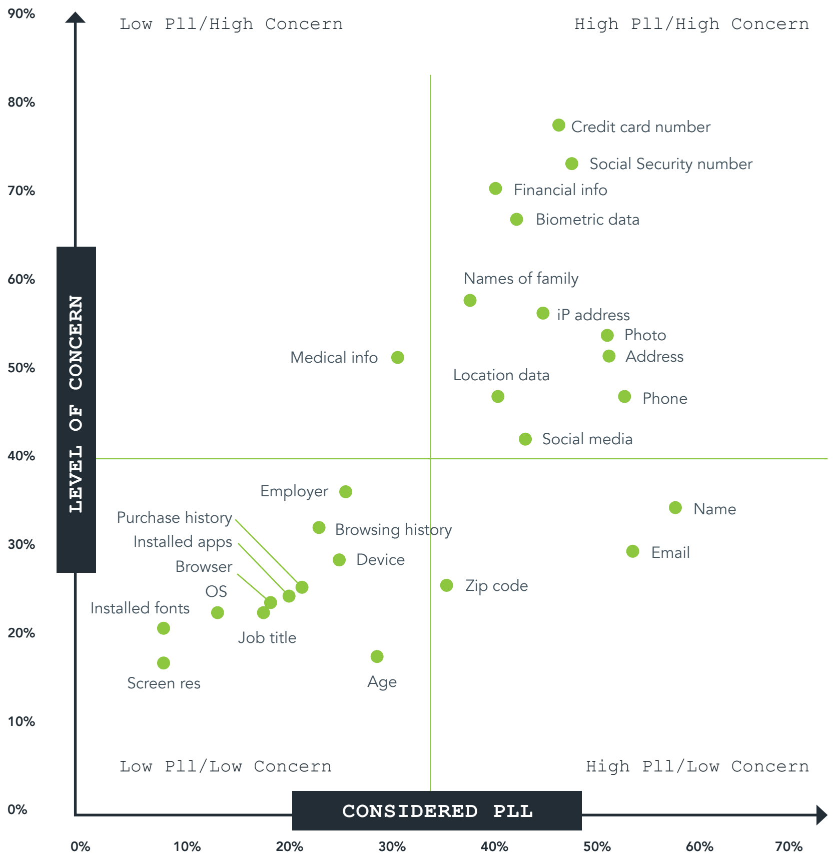
- An identifier, such as name, identification number, location data, an online identifier.
- One or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that individual.

Half of consumers responded that they felt like they have a choice in companies collecting personal information about them. The consumers who responded that they **don't** feel like they have a choice in companies collecting their personal data have significantly higher numbers when identifying data that can be combined together to create a digital fingerprint or PII, whereas consumers who feel like they **do** have a choice are more likely to share their information with companies they know. These consumers are also significantly more motivated by receiving compensation for their data.

A "**digital fingerprint** is a combination of data about a users web browser and computer (screen resolution, installed fonts, browser, device and installed apps) that can be used to uniquely identify and track individuals.

FIGURE 4

Which data consumers view as personally identifiable and the consumers' level of concern about sharing that data



Source: 2020 Consumer Privacy Research by Microsoft Advertising in partnership with iProspect

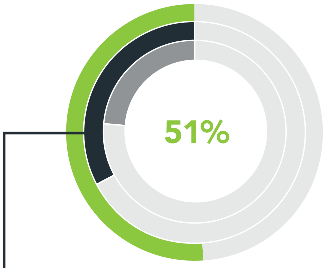
Figure 2 shows the cross reference between consumers level of concerns about sharing specific types of data and whether they consider that data to be personally identifiable information (PII) or not. The upper right quadrant represents the data consumers considered the most personally identifiable and where consumers have the highest level of concern with sharing. The bottom left quadrant represents the data consumers don't believe are personally identifiable and consumers have very low concern over sharing the data. While most of the data falls between these two quadrants, the survey responses highlight the consumer knowledge gap on data and data-driven identifiers used to create a digital fingerprint.

Marketers should expect that overtime consumers will become more savvy about how data can be combined to create digital fingerprints to track consumer behavior online.

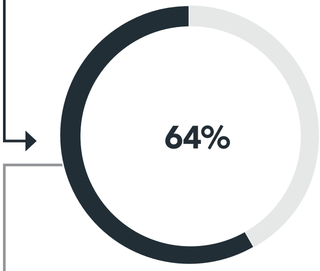
SIDEBAR

Are Consumers Willing to Share Data?

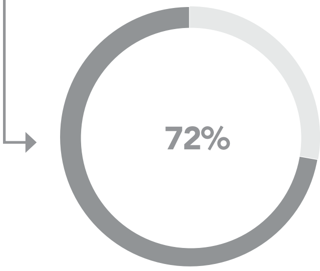
The short answer is yes. Of survey respondents, 51% say they will share basic information such as name and email. However, despite their willingness to share, 64% are concerned about the amount of data being collected. Of those who have concerns, 72% have stopped using a product or service because of those concerns.



51% say they will share basic information such as name and email.



64% are concerned about the amount of data being collected.



Of those who have concerns, 72% have stopped using a product or service because of those concerns.

> Customers are typically more willing to share their personal data if they trust that the environment is secure and companies aren't going to use their data in any unauthorised way.

Jeremy Hull, VP Innovation iProspect

Source: 2020 Consumer Privacy Research by Microsoft Advertising in partnership with iProspect

THE TAKEAWAY

Continued access to customer data despite growing privacy concerns can give brands competitive advantage, as they can fine-tune marketing outreach to better target audiences. Brands should proactively communicate compliance with new data privacy regulations to give customers peace of mind that their data is secure.

PURPOSEFUL PERSONALISATION

Done well, personalisation can be a powerful marketing tool and enhance the customer experience — but it must be purposeful. Personalising every aspect of the customer experience simply because it's possible can come off as intrusive, leaving customers feeling as if their privacy has been violated. Understanding your target customer's preferences is an important step in planning what experiences to personalise.

> **Make sure your customers understand why data is needed and what they get in return. If your customers aren't able to see the benefit – you need to rethink what you are doing. This could mean doing a better job articulating and showing your customers how you are using data to create more personalised and better customer experience or making sure that you really are using the data you collect.**

Christi Olson, Microsoft Advertising Marketing

But creating an amazing brand experience goes beyond having data for personalisation. Purposeful personalisation means you understand what your target audience values when connecting with your brand and make data-driven decisions about how to deliver the experiences they value most. Brands must continue to refine what they know about perceived value and leverage insights and technology to create experiences that make people feel increasingly connected to the brand. It's this deepening connection that leads to ongoing loyalty, increased engagement and trust, and, ultimately, better business outcomes.

We asked survey participants what types of personalised experiences would warrant sharing personal data. In general, our findings indicate that consumers are more willing to provide access to their data for personalised discounts and pricing, free samples and upgraded shipping options, but less willing to provide access for recommendations, automated reordering, or personalised customer service (see Figure 6).

FIGURE 6

The purpose behind personalisation matters:

WOULD YOU BE WILLING TO SHARE YOUR PERSONAL DATA WITH A COMPANY OR BRAND IN EXCHANGE FOR:	GLOBAL TOTAL		NORTH AMERICA		EMEA		LATAM		APAC	
	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO
Personalised rewards or discounts on frequently bought items or services	57.45%	42.55%	52.99%	47.01%	52.89%	47.11%	72.76%	27.24%	52.89%	47.11%
Personalised pricing (% off, money back)	56.86%	43.14%	51.83%	48.17%	53.13%	46.87%	72.47%	27.53%	51.28%	48.72%
Personalised recommendations	34.57%	65.43%	31.39%	68.61%	30.35%	69.65%	42.73%	57.27%	35.81%	64.19%
Personalised alerts and notifications	33.86%	66.14%	33.97%	66.03%	30.2%	69.8%	36.71%	63.29%	36.49%	64.13%
Expedited purchasing/ checkout options	38.8%	61.2%	38.58%	61.42%	32.44%	67.56%	48.04%	51.96%	39.26%	60.74%
Automated reordering of frequent purchases	29.9%	70.1%	30.28%	69.72%	26.1%	73.9%	32.43%	67.57%	32.86%	67.14%
Free or upgraded shipping options	51.44%	48.56%	48.42%	51.58%	46.9%	53.1%	61.44%	38.56%	51.06%	48.94%
Free samples of products or services	55.82%	44.18%	52.51%	47.49%	50.7%	49.3%	69.6%	30.4%	52.63%	47.37%
Free access to a service	54.07%	45.93%	49.02%	50.98%	48.93%	51.07%	70.04%	29.96%	50.33%	49.67%
Free access to content	47.16%	52.84%	42.38%	57.62%	43.36%	56.64%	59.71%	40.29%	44.7%	55.3%
More personalised customer service	40.28%	59.72%	34.93%	65.07%	35.64%	64.36%	52.61%	47.39%	39.99%	60.01%
To help a company improve their products or services	44.24%	55.76%	38.86%	61.14%	37.86%	62.14%	58.2%	41.8%	44.95%	55.05%
Automatic and recurring payments	42.28%	57.72%	42.1%	57.9%	37.72%	62.28%	54.09%	45.91%	37.06%	62.94%
Access to purchase history	31.15%	67.85%	32.94%	67.06%	29.64%	70.36%	31.39%	68.61%	36.16%	63.84%
Ability to set and manage appointments	34.55%	65.45%	37.62%	62.38%	33.36%	66.64%	32.12%	67.88%	35.89%	64.11%
Access to healthcare records	34.76%	65.24%	36.4%	63.6%	29.33%	70.67%	43.34%	56.66%	32.51%	67.49%
Access to service data	33.37%	66.63%	31.54%	68.46%	30.11%	69.89%	38.2%	61.8%	35.26%	64.74%
Access to educational records	35.36%	64.64%	32.98%	67.02%	29.62%	70.38%	49.3%	50.7%	32%	68%
Service or appointment notifications	35.58%	64.62%	38.64%	61.36%	32.83%	67.17%	31.74%	68.26%	39.99%	60.01%

Source: 2020 Consumer Privacy Research by Microsoft Advertising in partnership with iProspect

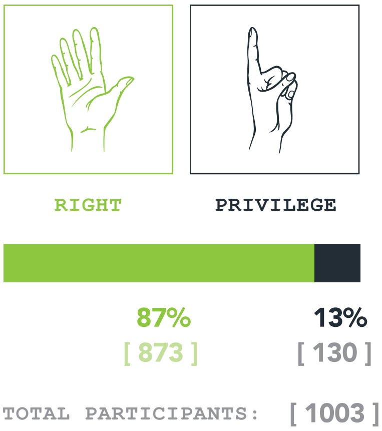
The Data Privacy Spectrum: Is Privacy a Privilege or a Right?

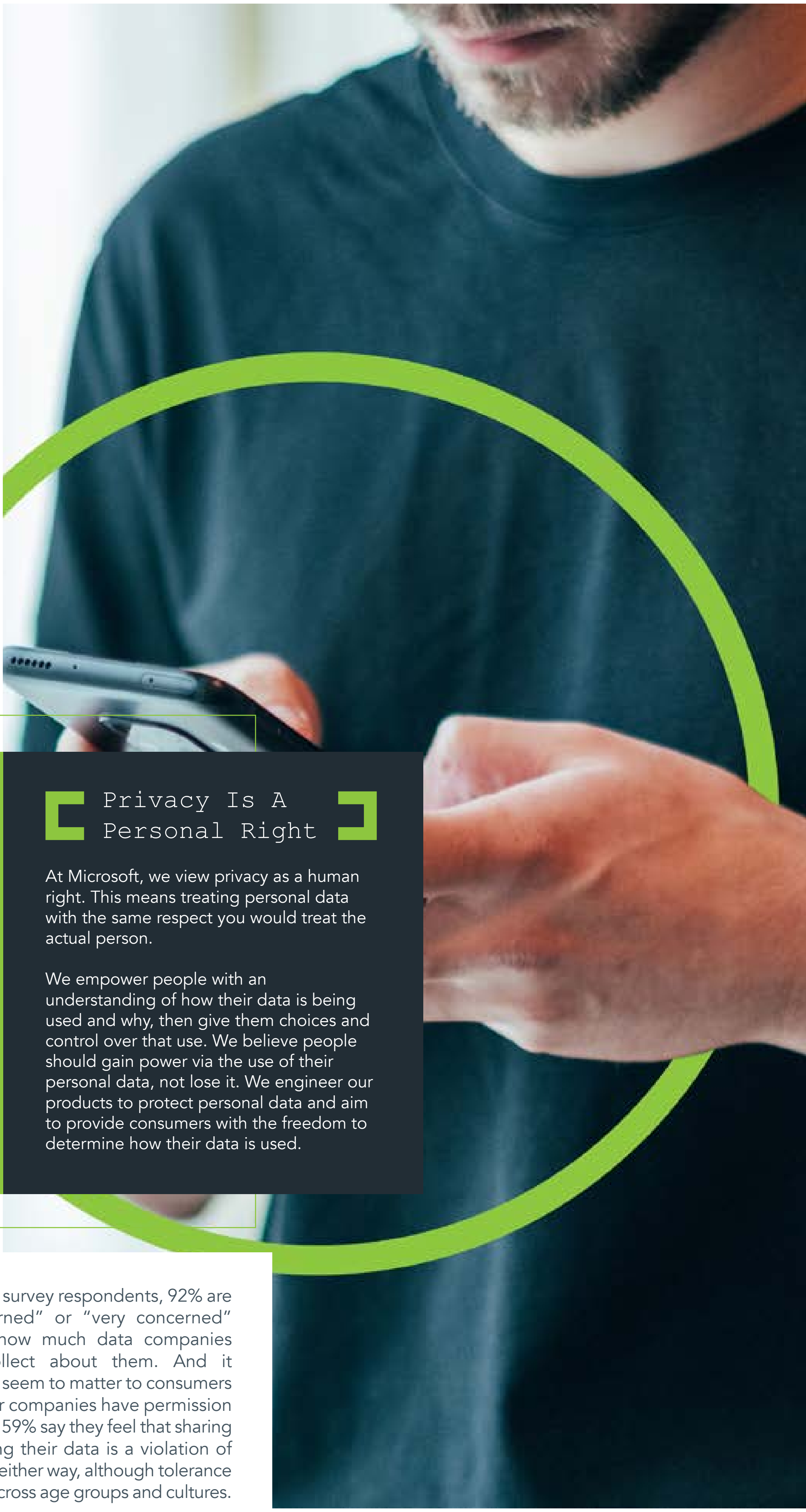
Although most would agree that they value data privacy, people have different expectations around how brands use their data, and different opinions about whether data privacy is a privilege or a right. While some feel that once they give a company permission to use their data, anything goes, others feel that selling personal data is a privacy violation under any circumstances.

FIGURE 7

Most consumers believe privacy is a right.

DO YOU BELIEVE PRIVACY IS A RIGHT OR A PRIVILEGE?





SIDEBAR

Privacy Is A Personal Right

At Microsoft, we view privacy as a human right. This means treating personal data with the same respect you would treat the actual person.

We empower people with an understanding of how their data is being used and why, then give them choices and control over that use. We believe people should gain power via the use of their personal data, not lose it. We engineer our products to protect personal data and aim to provide consumers with the freedom to determine how their data is used.

Various factors influence perceptions and expectations around data privacy. What seems fair and comfortable to some people may seem threatening to others. We sought to better understand consumer expectations and their perception of the value they receive from personalisation against their level of concern for sharing data.

Among survey respondents, 92% are "concerned" or "very concerned" about how much data companies can collect about them. And it doesn't seem to matter to consumers whether companies have permission or not – 59% say they feel that sharing or selling their data is a violation of privacy either way, although tolerance varies across age groups and cultures.

Data Privacy is a Shared Responsibility

As a society, we're increasingly reliant on the Internet for our everyday activities. We depend on a variety of online services and software apps to perform daily tasks. We've become dependent on mobile connectivity and digital assistants in our homes, at our workplaces and on the go. Data is the lifeblood behind this way of life, and few would be willing to give up this data-driven lifestyle.

Journalists started poking fun at our data-driven lifestyle more than a decade ago, as soon as it became clear that the personalized services consumers were expecting would require a new level of data collection and insight. A 2009 video from The Onion is a good example[10] -- it suggested those who opt out of Google's data policies may as well be banished to a remote part of the world and give up contact with humanity. While this exaggerated viewpoint is humorous, today it's not far from the truth. It's difficult to operate in modern society without using Google or Amazon. Even basic services such as healthcare and utilities increasingly drivie consumers online.

While businesses have a duty, both legal and ethical, to respect and protect the privacy of their customers, they are not solely responsible for it. Consumers must also be cognizant of the information they share, make an effort to understand how their data is being used, and make good decisions about whether or not to give businesses access to that data. The responsibility for data privacy also falls in part on governmental bodies who must draft legislation specifying the penalties for mishandled or misused data.

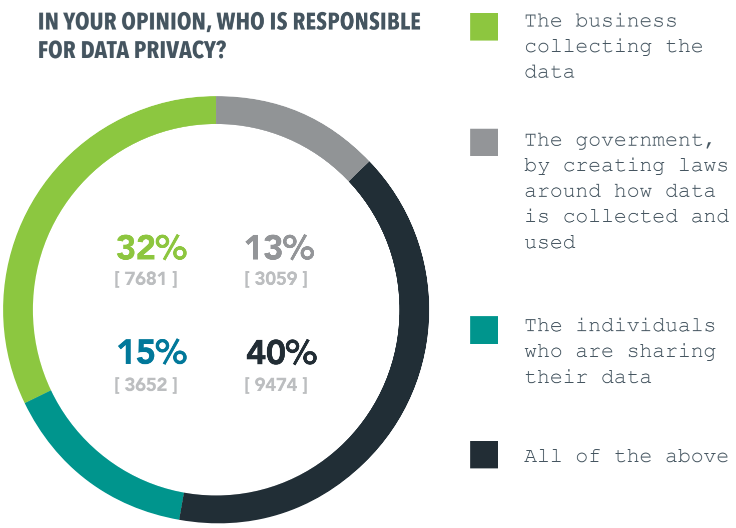
But the chain of responsibility doesn't end there. The technology innovators who develop software and solutions that leverage our data must also be held accountable. They must design in capabilities that enable businesses to offer consumers choices about how their data is used, if at all.

And if businesses must give consumers the right to opt out of sharing their data, they must also be prepared to provide a service that doesn't require data. This is where the value exchange discussion gets complicated. Consumers who opt out of all data sharing cannot access the apps and services their smartphones are designed to deliver. Still, they have the right to opt-out, and companies must provide something in exchange if they are to retain the consumers' business.

Consumers seem to understand that data privacy requires collaboration among the government, individuals, business and technology innovators (see Figure 6). Of those surveyed, nearly half (40%) think data privacy is a shared responsibility.

FIGURE 8

Data privacy is a shared responsibility



Source: 2020 Consumer Privacy Research by Microsoft Advertising in partnership with iProspect

Here's how each group can step up to accept responsibility and accelerate change:

BUSINESSES:

Twenty-six percent of survey respondents believe businesses are responsible for data privacy. Consumers expect businesses to not only know and follow data privacy legislation, but act as trusted leaders. To this end, businesses must be transparent and proactively educate consumers about how their data is being used when they use their products and services. Businesses must communicate clearly, concisely and repeatedly with customers about their rights concerning personal data. Internally, they must build a culture of respect and data stewardship as part of a customer-first mindset, not only to stay compliant with data policies but to build and maintain consumer trust.

INDIVIDUALS:

There's an old saying that goes, "If you're not paying for a product, you are the product." In the value exchange for personal data, everyone gets something, and everyone must give up something. Individuals are active participants in the exchange of personal data and services, and as such, have a responsibility to learn how their data will be used. In today's data-driven society, consumers cannot be unwitting bystanders; they must understand their options, ask questions and make informed decisions about sharing personal data.

GOVERNMENTAL BODIES:

Data is a powerful tool, and it can be used for good (improved customer service, convenience and personalisation) or bad (political propaganda, theft and fraud). To enable the good and prevent the bad, governments must walk a fine line when creating data privacy legislation, protecting citizens' rights while making sure their policies aren't so restrictive that innovation comes to a halt. To achieve this balance, collaboration with businesses and consumer advocacy groups is necessary.

TECHNOLOGY INNOVATORS:

Technologists often innovate and disrupt markets before slow-moving legislation can catch up. A creative, new capability or service on a consumer's smartphone may have far-reaching implications for consumers that the engineers designing it can't possibly know or imagine. Before introducing technology innovation to market, technologists have a responsibility to examine the potential impact, and take data privacy trends and legislation into consideration as they build out their product roadmaps.

SIDEBAR

Collaboration on a Global Scale

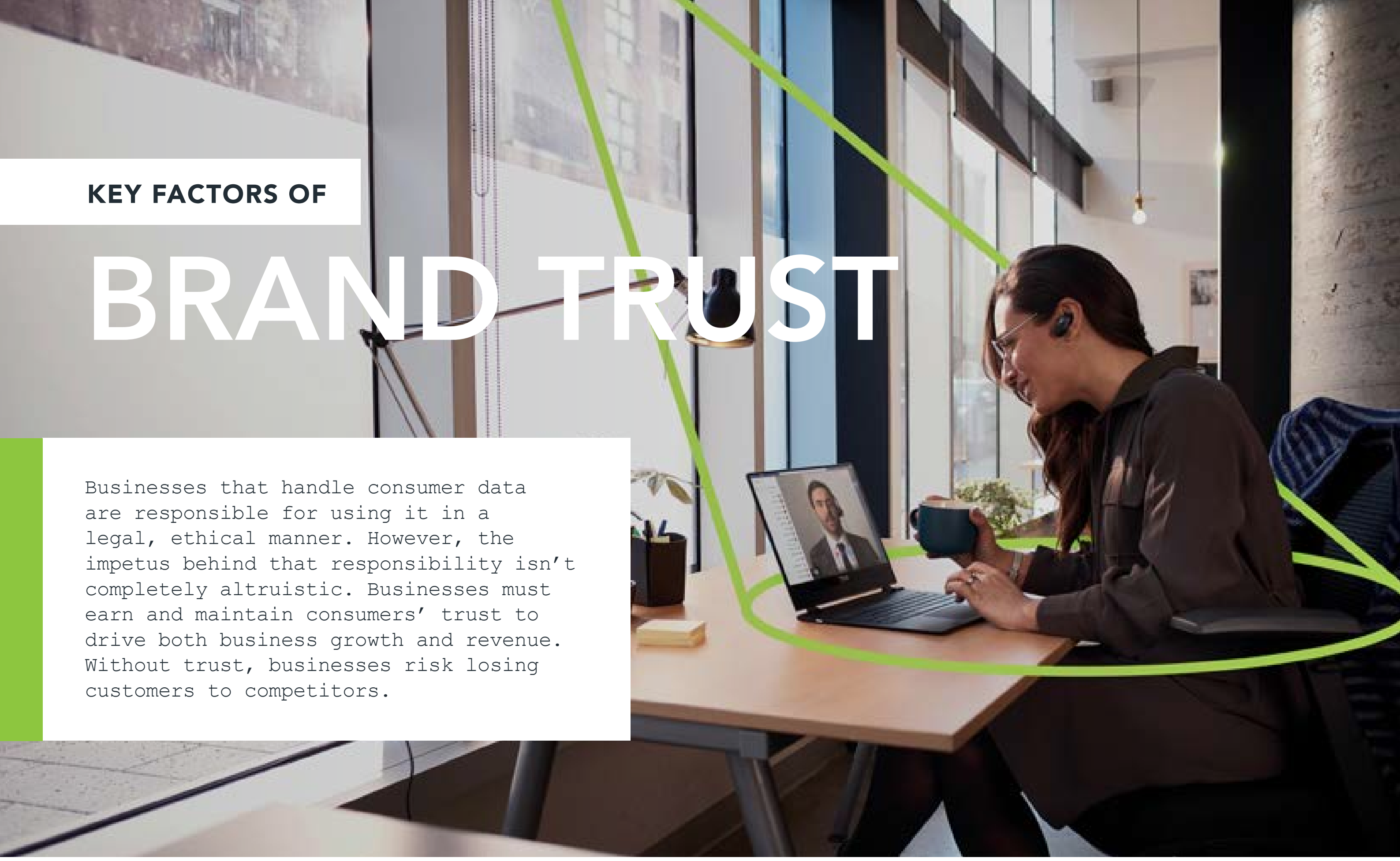
Data privacy regulations vary by country and region, however business is increasingly global. Although local in scope, privacy laws such as CCPA and GDPR have implications for data privacy and collaboration worldwide. Additionally, new regulations will emerge as these standards begin to take hold, and businesses must be prepared to adapt.

THE TAKEAWAY

Getting data privacy right can't be accomplished in siloes. It requires close collaboration between consumers, businesses, governmental agencies and technology innovators.

Privacy compliance is essential. It's up to businesses to understand the laws around data privacy and to comply with them at scale, and businesses have to determine the level of scale so that consumers can:

- **View** personal data collected about them (or their device / services)
- **Know** how personal data is being used, shared or sold
- **Delete** personal data
- **Edit** or correct personal data
- **Limit** or restrict the use of data
- **Access** or export data in a usable format



KEY FACTORS OF BRAND TRUST

Businesses that handle consumer data are responsible for using it in a legal, ethical manner. However, the impetus behind that responsibility isn't completely altruistic. Businesses must earn and maintain consumers' trust to drive both business growth and revenue. Without trust, businesses risk losing customers to competitors.

Trust isn't static, and businesses have to put long-term strategies in place to inspire consumer trust and advocacy. Such strategies have many components. Businesses must:

- Actively engage with consumers to build a relationship.
- Listen to and act on customer feedback about their business, products and services.
- Adhere to regulations around data privacy and protection.
- Be transparent about how they're using customer data, as well as about any mistakes they've made or breaches that have occurred, and what they're doing to remediate the issues.

The business value of brand trust cannot be underestimated. According to a Brand Keys report,[11] a loyalty increase of 7% can boost lifetime profits per customer by as much as 85%, and a loyalty increase of 3% can correlate to a 10% cost reduction, depending on the sector.

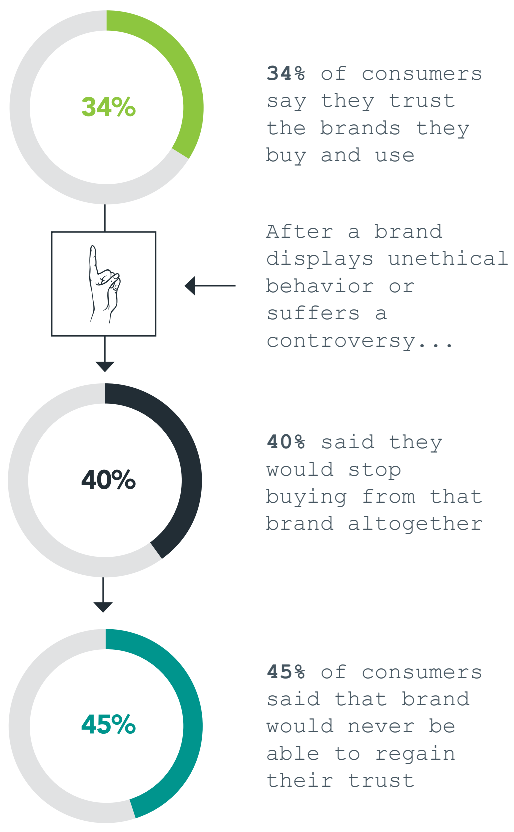
Yet today's businesses must operate in an environment that supports the open, frequent and very public exchange of feedback and opinions. Long gone are the days of "Mad Men," when brands had complete control over how consumers perceived them. Online reviews and ratings give consumers immediate access to customer feedback about a brand, business location or product. Today's consumers trust others' online recommendations as much as they do personal recommendations,[12] and more than 90% of people consult online reviews and ratings before choosing a business.[13]

As a result, today's consumer holds the majority of the power over brand perception and trust. Brands must constantly monitor and act on customer feedback and be completely transparent about their operations and intentions, or risk losing that trust.

When it comes to data privacy, businesses have a long way to go to earn consumers' trust. According to Edelman's Brand Trust Survey, just 34% of consumers say they trust the brands they buy and use.[14] After a brand displays unethical behavior or suffers a controversy, 40% said they would stop buying from that brand altogether and 45% of consumers said that brand would never be able to regain their trust.

FIGURE 9

Businesses have to earn consumer trust



Source: 2020 Consumer Privacy Research by Microsoft Advertising in partnership with iProspect

Quantifying Brand Trust

iProspect's formula for measuring consumer trust has three key components:

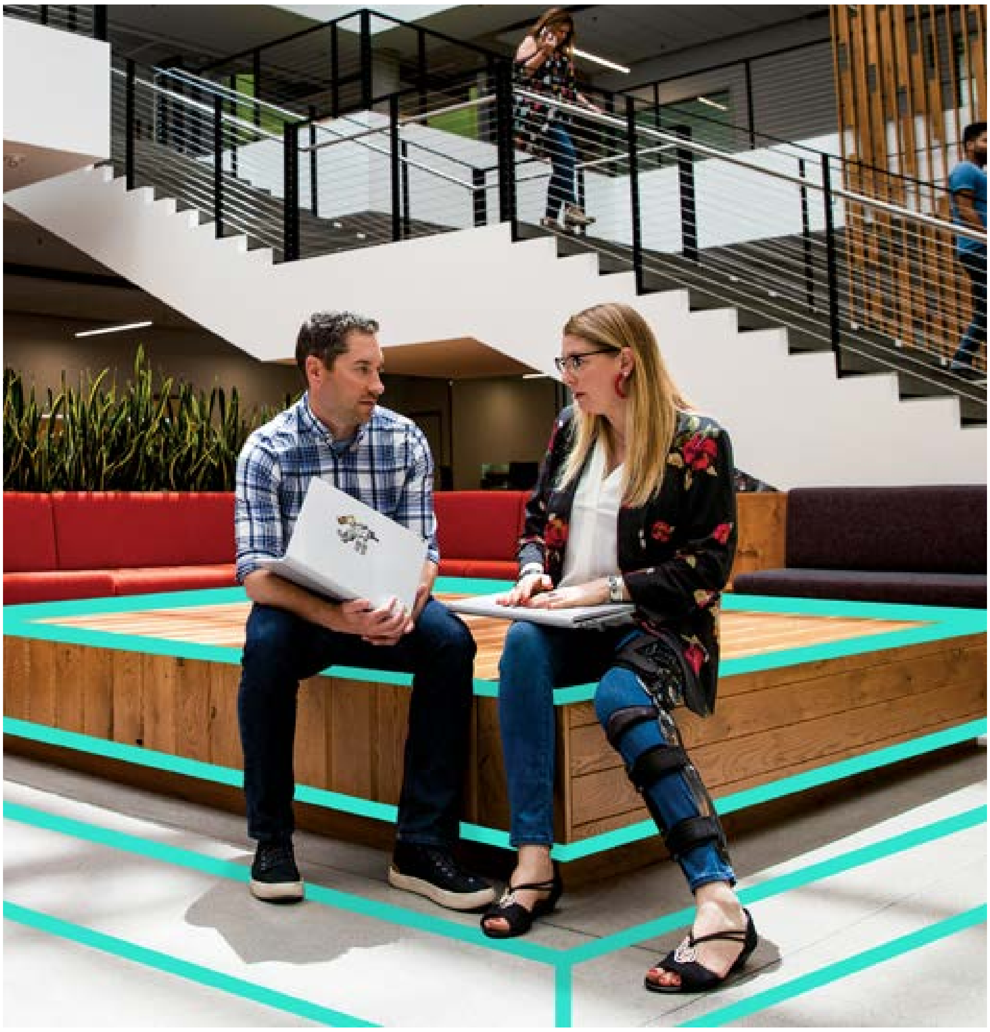
Trust = Credibility + Relevance + Reliability.[15]

These factors have implications on how businesses view and handle data privacy.

Credibility is the capacity to be perceived as competent and legitimate. This factor ties back to customer sentiment and a business's ability to deliver on customer expectations. Whatever a business is selling, they must convince consumers they understand the value of the product or service and deliver on its potential value.

The second factor, relevance, refers to a business's ability to resonate with consumers. The business must listen to and act on customer feedback and requests, to deliver products or services customers need and want. Otherwise, customers may think the business doesn't understand their needs and move on. A second, important aspect of relevance is the ability to meet customers' needs at the right time and place. Google's "micromoment" concept illustrates this requirement.[16] Today's consumers want instant gratification and real-time access to goods and services. If you're not able to meet their need the moment it arises, they'll go elsewhere.

The third factor is reliability, or a business's capacity to provide an experience that consistently and conveniently meets customer expectations across every interaction with a brand. When brands are consistent, customers feel confident that whenever their need arises, the brand will be there to fulfill it.



WHERE DOES DATA PRIVACY FIT INTO THIS EQUATION?

A **credible** business takes the necessary precautions to protect consumer data. Businesses who are transparent about how they use personal data and provide access to and information about privacy policies at play are more credible than businesses who hide their policies or try to "trick" consumers into accepting policies before they fully understand them.

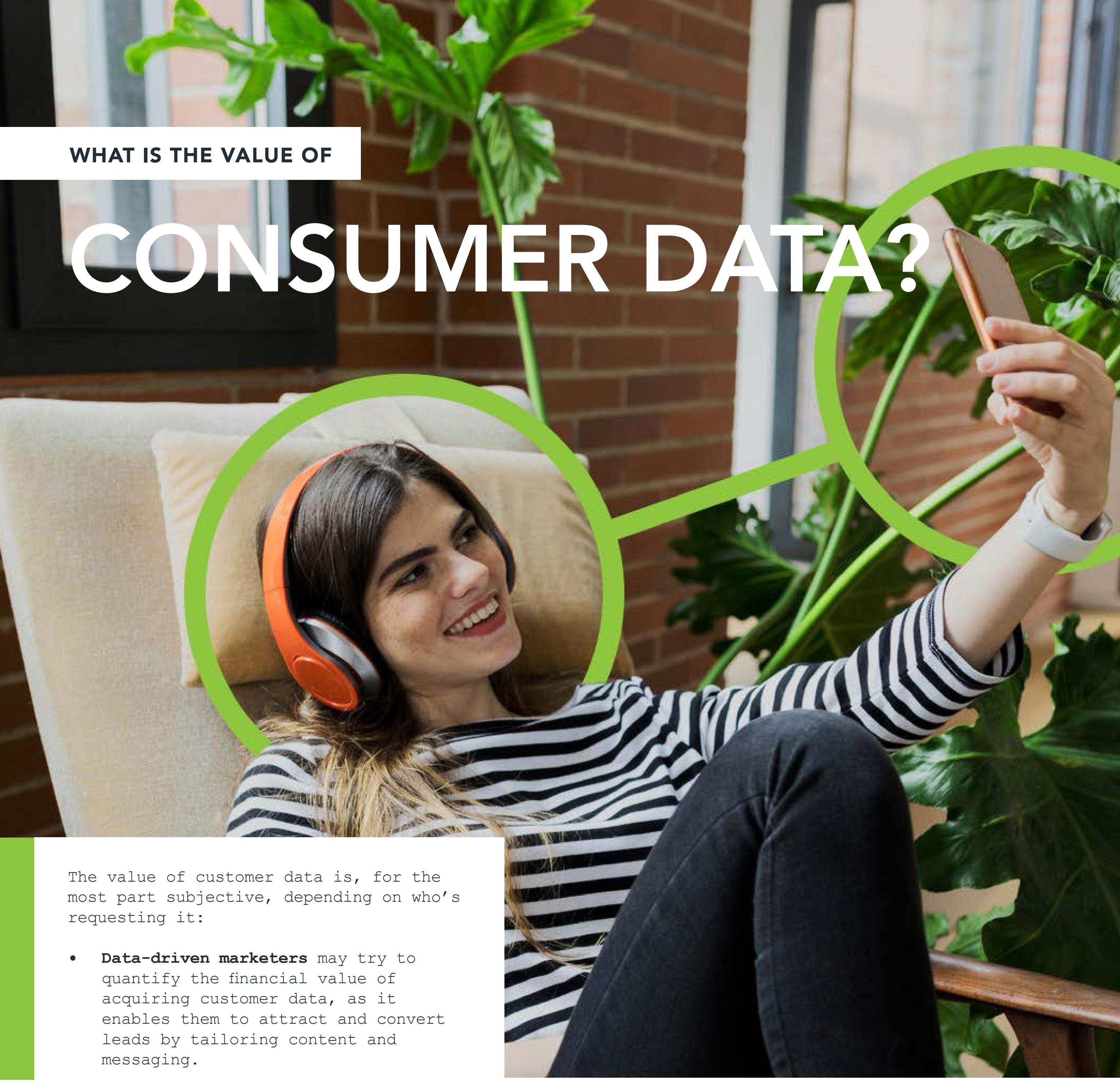
A **reliable** business does what it says it will do -- whether that means delivering promised products and services, or following through with actions pertaining to personal data. If a business's privacy policy states that it will not sell a customer's data, customers must be able to rely on the business to keep their promise.

Relevance comes from delivering on customer expectations. But relevance is a double-edged sword. With new data privacy laws governing, and in many cases limiting, the ways in which businesses can use customer data, businesses have less power to leverage that data to create the personalised customer experiences consumers now demand. Eighty percent of consumers are more likely to make a purchase when brands offer personalised experiences.[17] But if they don't provide access to their personal data, this is impossible. Businesses cannot create targeted, relevant content and messaging to drive and convert new business without the benefit of consumer data. That's why the ability to build and maintain consumer trust is essential to competitive advantage.

Customer trust ultimately boils down to the value customers receive versus the risk they must take to engage with a business. In any transaction, there's a value exchange, and the perceptions around this value exchange govern consumers' comfort levels for sharing personal data.

2 THE PRIVACY VALUE EXCHANGE

WHAT IS THE VALUE OF CONSUMER DATA?



The value of customer data is, for the most part subjective, depending on who's requesting it:

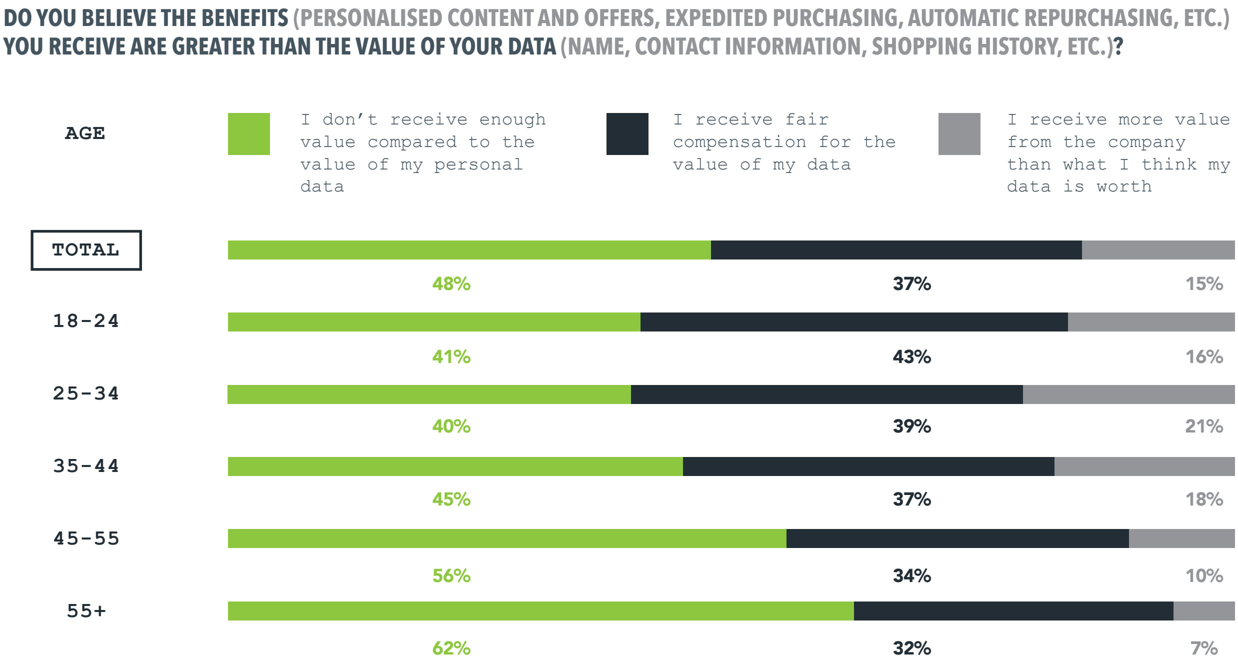
- **Data-driven marketers** may try to quantify the financial value of acquiring customer data, as it enables them to attract and convert leads by tailoring content and messaging.
- **Data aggregators** place a high value on customer data, because they can sell to other businesses to use for marketing purposes.
- **Publishers** value user data because it helps them create relevant content and experiences.
- **Governmental bodies** need consumer data for a variety of reasons, including national security and law enforcement, public health, voter registration and statistics that help determine legislation.

Meanwhile, consumers may feel their data has intrinsic value. After all, their data defines them. What constitutes a data point for a marketer, an address, for example, is someone's home. A middle name may have been passed down for generations. People may actively work to keep other personal information private from people in their daily lives, but be willing to share it with a business if the perceived value is high enough, and if they trust that business to keep it private.

The true value of data, then, lies in the exchange: What does one party give up, and what does the other receive? According to our findings, 15% of customers feel they're getting good value from granting access to their data. What do they find valuable? Survey respondents seem to think free services and health records are valuable tradeoffs for private data access. Notably, belief in the value of sharing personal data appears to decrease with age across all geographies.

FIGURE 10

Younger consumers tend to have higher perceived value for sharing their personal data



Source: 2020 Consumer Privacy Research by Microsoft Advertising in partnership with iProspect

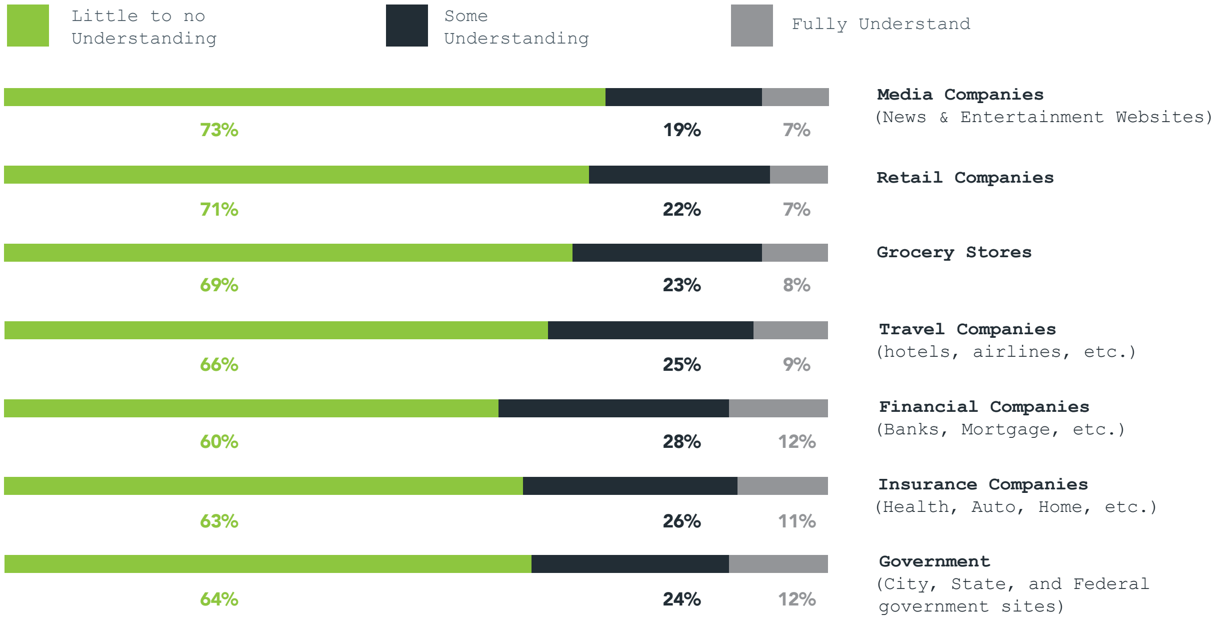
Perceived value of the exchange of data for services depends on many factors. Some products and services are hyper-personalised by nature. For example, consumers accept the fact that financial institutions must have access to a range of private personal data to deliver products such as mortgage and home equity loans, personal loans, credit, and access to mobile banking apps. Businesses in other industries can provide sufficient value with much less data. For example, a retail business that sells women's clothing typically markets toward a broader demographic within that market segment. They may base inventory orders on the average size, weight, height and age of a typical customer, but they don't need to know data points such as household income, occupation or whether or not a customer is a homeowner.

However, our findings reveal is that regardless of the industry at least two-thirds of consumers don't understand how their data is being used. Consumers seem to have a better understanding of how financial service companies, insurance companies and government may use their data, but they don't understand how companies in the media, retail and grocery industries use data and information.

FIGURE 11

Regardless of the industry at least two-thirds of consumers don’t understand how their data is being used

HOW WELL DO YOU UNDERSTAND HOW THE FOLLOWING TYPES OF COMPANIES ARE USING YOUR PERSONAL DATA?



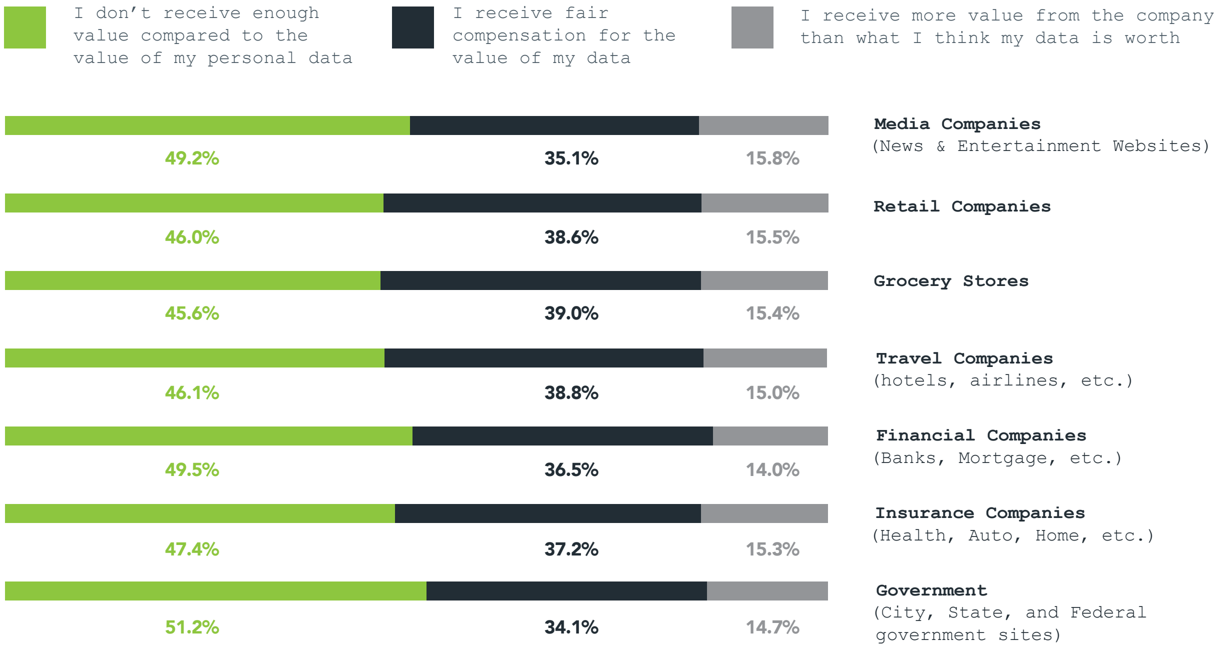
Source: 2020 Consumer Privacy Research by Microsoft Advertising in partnership with iProspect

Regardless of the industry, our findings reveal that roughly half of all respondents don’t feel the benefits they receive from sharing their data are as valuable as their personal data.

FIGURE 12

Roughly half of consumers don’t feel the benefits they receive are as valuable as their personal data

DO YOU BELIEVE THE BENEFITS (PERSONALISED CONTENT AND OFFERS, EXPEDITED PURCHASING, AUTOMATIC REPURCHASING, ETC.) YOU RECEIVE ARE GREATER THAN THE VALUE OF YOUR DATA (NAME, CONTACT INFORMATION, SHOPPING HISTORY, ETC.)?



Source: 2020 Consumer Privacy Research by Microsoft Advertising in partnership with iProspect

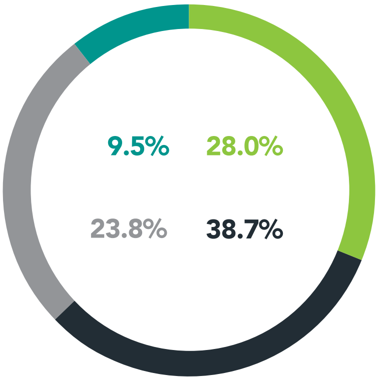
An Imbalance in the Value Exchange Breeds Distrust

When an imbalance exists in the value exchange, it causes a disconnect between brands and consumers, and often, customers don't understand the value of the exchange. In fact, 66.7% of survey respondents said they have little to no understanding about how their data is being used by companies. When asked if respondents provide personal information 40% said they refused to provide data because the company either didn't disclose or they didn't understand how the data was going to be used.

FIGURE 13

Two-thirds of consumers don't understand how their data is being used.

HOW WELL DO YOU UNDERSTAND HOW COMPANIES ARE USING YOUR PERSONAL DATA?



- 🟩 I have no understanding of how my data is being used
- ⬛ I understand very little about how my data is being used
- ▨ I understand a great deal of how my data is being used
- 🟦 I fully understand how my data is being used

Source: 2020 Consumer Privacy Research by Microsoft Advertising in partnership with iProspect

Similarly, there is not a consistent view on the value of specific types of consumer data, and if the value of data differs based on country and type of data. According to their whitepaper, "How Much is Privacy Worth Around the World and Across Platforms?," the Technology Policy Institute attempted to measure individuals' valuation of online privacy across a wide range of countries and data types. The paper states, *"Quantifying the value of privacy is necessary for conducting any analysis of proposed privacy policies."* Their research found significant differences across countries and platforms for different types of data.[18]

The gap in understanding between consumers and marketers on how data is used can breed distrust. Below are verbatim explanations we received from our survey respondents as to why they don't share their personal data:

> **"**
>
> **Something occurs / comes up in the communication that makes me suspicious**
>
> **On checking information about the company I discovered it was not based in the same country where I live**
>
> **I give permission for one purpose and at some later date the information is given to someone else for a completely different purpose**
>
> **I don't want organisations giving out my name to other organisations**

If consumers don't see value in providing their personal data, businesses cannot personalise the customer experience because they don't have enough information to understand what the customers want. Content may be irrelevant or uninspiring, or, more likely, delivered to the wrong audience at the wrong times. This can also happen if data is inaccurate or unusable, for example, if businesses don't have effective data management processes and solutions in place to cleanse and normalise the data, or if customers who don't trust the business provide false information to get the functionality they want.

When an imbalance exists, engaging with customers in meaningful ways is left to chance, and customers can become uninterested or, worse yet, disenchanted with the brand. Additionally, when businesses give away too much for too little, they don't realise adequate ROI and may not have the resources to continue to deliver on customer expectations for new products and services.

When customers realise they're losing value by opting out of privacy policies, do they opt back in? Generally, consumers report their concerns when they recognise an imbalance, but they self-report low levels of behavior change. Eighty-five percent of people reported their "relationship changed" with a company after a data breach, but only 50% of those reporting their relationship changed altered their behavior. The other 50% continued interacting with the company in the same manner as they did prior to the breach. Although our survey didn't measure behavior patterns, we can surmise that the overriding attitude is, "I care, but I'm resigned to the issue."

However, that can change over time, as new players with broader basic functionality enter the market. Consumers are likely to remain loyal to the brand that gives them only one choice for only as long that brand's product or service is the only option.

The end result of an imbalance in the value exchange for personal data is the loss of brand trust. Consumers who don't get what they expect from brands for providing their personal information are less likely to trust the brand with their future business.

Does Data = Experience?

Our survey results indicate consumers understand the connection between data and the experience they have with a website or app, but feel that companies should provide a good experience regardless of the amount of data they share. In fact, 79% of people reported they believe companies should provide the same experience on a website or app if they opt out of sharing their data as they do to individuals that opt in.

Below are some verbatim explanations we received from respondents as to why they feel they should receive the same experience:

Our privacy is a right, just as is due process. It's our right as a citizen of the United States of America.
(Male, 63)

Because it is a legal right, but it should not have repercussions.
(Female, 48)

I don't think my data should be used as a bargaining chip for accessing information on a website. Doesn't seem very fair to me.
(Male, 30)

I believe that as long as we are sharing SOME data, we should be entitled to the same experience and features.
(Male, 21)

They may not be able to give me an experience as closely tailored to me, but it is my choice not to give them information. The quality of the service, however, should be equally as good.
(Female, 24)

Respondents who feel they should NOT receive the same experience seem to have a better understanding of the relationship between data and functionality. Verbatim response included:

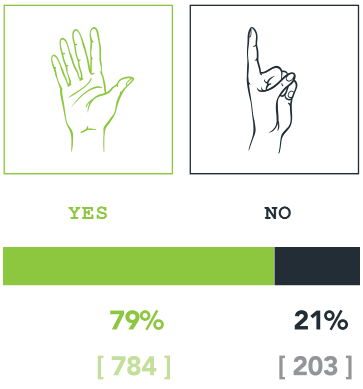
Everything costs something. If we don't pay with money, then we pay with something else. If I'm not willing to pay with money or information, then I don't deserve the same experience as those that do.
(Male, 40)

If you don't share your location or specific information/data, it's impossible to have the same experience. They ask for your info for a reason to give you a certain experience, so if you decline that then that's on you.
(Female, 19)

FIGURE 14

Almost 80% of consumers believe opting out of sharing data should change the digital experience

IF YOU OPT OUT OF SHARING YOUR DATA, DO YOU BELIEVE YOU SHOULD RECEIVE THE SAME EXPERIENCE (ON A WEBSITE OR IN AN APP) **AS THE INDIVIDUALS WHO SHARE THEIR DATA?**



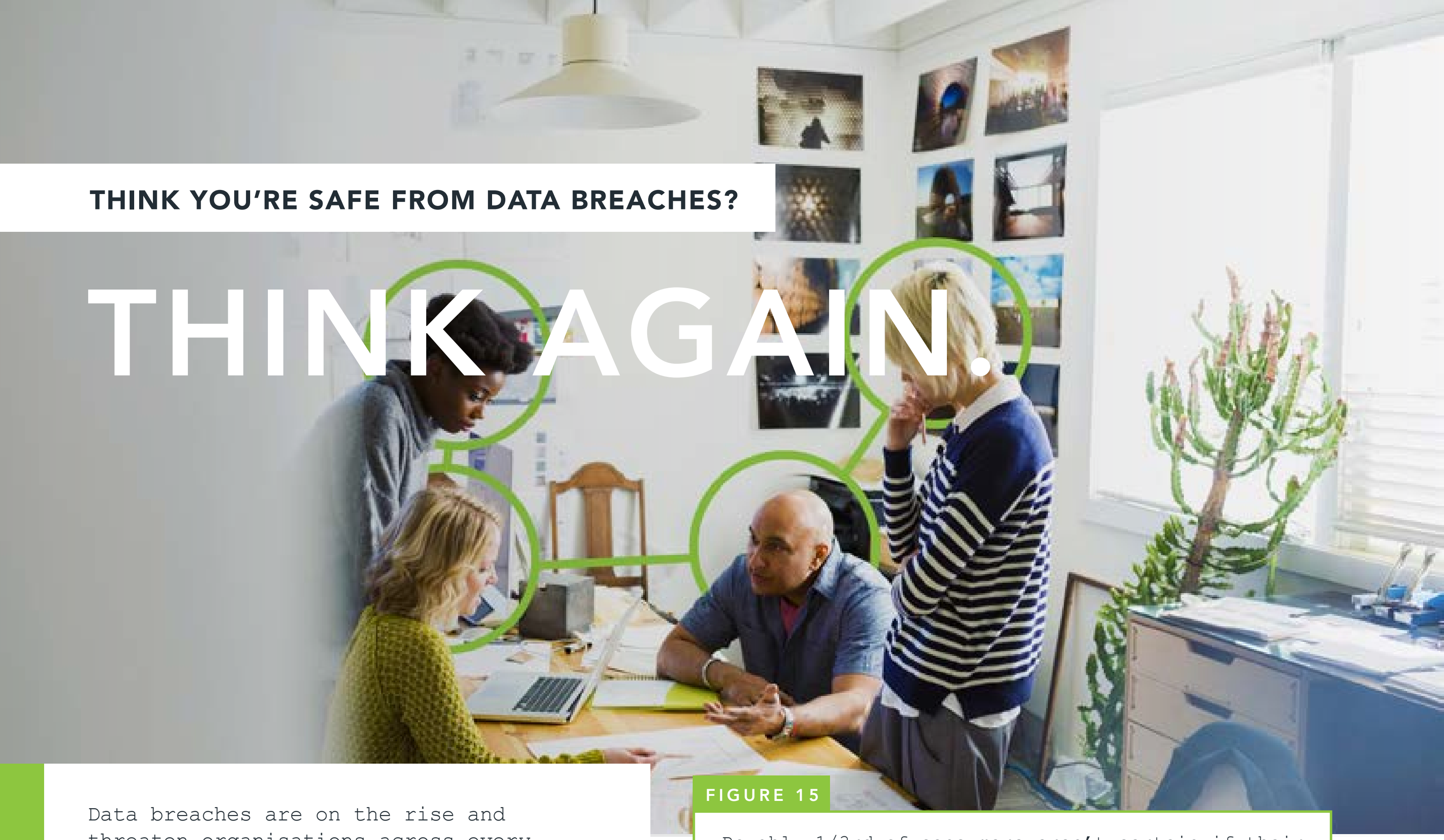
TOTAL PARTICIPANTS: [987]

Source: 2020 Consumer Privacy Research by Microsoft Advertising in partnership with iProspect

THE TAKEAWAY

It's important to communicate very clearly what customers are receiving in exchange for their data. Providing an explanation as to why a lack of data will impact the experience can help clear up confusion and build trust, while also helping to convince consumers to share more of their data. Additionally, brands should develop alternate yet quality customer experiences with their websites and apps that don't require full data access, in order to retain customers who choose to opt out of sharing data.

3 BUILDING BRAND TRUST: ACTIONABLE STEPS TO PREPARE FOR AND SURVIVE A DATA BREACH



THINK YOU'RE SAFE FROM DATA BREACHES?

THINK AGAIN.

Data breaches are on the rise and threaten organisations across every industry. According to a report by Risk Based Security,[19] the total number of breaches was up 33% in 2019 from the previous year, and the total number of records exposed more than doubled, up 112%. Based on our survey results, 29% of respondents have had their personal data compromised in a data breach. An additional 31% don't know whether or not their data has been compromised. Given these dramatic increases, one thing is clear: It's not a matter of "if" an organisation will suffer a data breach — it's when. No one is immune; we are all at risk.

The price an organisation pays is high. IBM Security's recent Data Breach Report cites the cost of an individual breach has risen 12% in the past five years to $3.92 million per incident, on average.[20] These totals take into account the multi-year financial impact of a breach and the cost of regulatory compliance but exclude the high price of reputational damage. More than 64% of survey respondents whose data was compromised in a data breach stopped doing business with that company.

FIGURE 15

Roughly 1/3rd of consumers aren't certain if their data has ever been compromised in a data breach

HAS YOUR PERSONAL DATA EVER BEEN COMPROMISED IN A DATA BREACH?

	YES	NO	I'M NOT SURE
AUSTRALIA	27.71%	37%	35.29%
INDIA	44.52%	35.32%	20.16%
UNITED STATES	44.44%	32.76%	22.8%
CANADA	30.55%	39.68%	29.76%
SOUTH AFRICA	22.11%	34.65%	43.23%
UNITED KINGDOM	28.23%	43.9%	27.87%
GERMANY	12.54%	46.34%	41.11%
FRANCE	18.7%	46.83%	34.46%
NETHERLANDS	19.01%	42.36%	38.63%
SPAIN	19.42%	48.54%	32.04%
MEXICO	23.18%	46.7%	30.12%
COLOMBIA	21.95%	46.83%	31.22%
CHILE	17.19%	45.29%	37.52%
ARGENTINA	16.35%	39.05%	44.6%
JAPAN	45.93%	23.35%	30.72%

Source: 2020 Consumer Privacy Research by Microsoft Advertising in partnership with iProspect

Consumers' perceptions about companies involved in a breach change. Our findings revealed that 85% of consumers say their relationship with companies changed following a data breach, and 65% said they stopped doing business with that company altogether. Furthermore, of those whose personal data was involved in a breach, 56% say they trust companies involved in data breaches less.

A mishandled data breach can have far-reaching and lasting impact on organisations who must now work hard to regain consumer trust and, in the meantime, lose business to competitors who are perceived to be safer — or who handled a breach better.

FIGURE 16

How consumers actions changed after a data breach

HOW, IF AT ALL, DID YOUR RELATIONSHIP CHANGE WITH THE COMPANY INVOLVED IN THE BREACH? (Select all that apply)	STOPPED PURCHASING PRODUCTS OR SERVICES FROM THE COMPANY	STOPPED USING SERVICES OR UNSUBSCRIBED FROM SERVICES FROM THE COMPANY	UNINSTALLED AN APP BECAUSE OF PRIVACY CONCERN	ADJUSTED THE PRIVACY SETTINGS FOR THE DATA I SHARE	USED ANY FORM OF SOFTWARE TO REDUCE HOW MUCH DATA I SHARE (E.G., BROWSER EXTENSION, VPN)	REQUESTED FROM A COMPANY TO ACCESS, MODIFY OR ERASE THE DATA THEY MAY HAVE ON ME	IT DIDN'T.
AUSTRALIA	37.85%	37.54%	36.62%	41.54%	30.77%	35.69%	12.31%
INDIA	37.32%	44.93%	36.96%	46.01%	44.20%	47.46%	05.80%
UNITED STATES	40.25%	32.91%	30.19%	38.26%	25.57%	27.20%	15.87%
CANADA	23.87%	20.21%	18.49%	30.53%	16.34%	18.06%	30.53%
SOUTH AFRICA	55.22%	46.27%	43.28%	47.76%	32.84%	37.31%	08.96%
UNITED KINGDOM	36.18%	33.77%	25.97%	33.02%	27.27%	27.46%	11.32%
GERMANY	43.06%	38.89%	31.94%	31.94%	34.72%	38.89%	05.56%
FRANCE	30.71%	28.35%	32.28%	33.86%	14.17%	23.62%	11.02%
NETHERLANDS	28.76%	19.61%	31.37%	32.68%	17.65%	22.22%	26.80%
SPAIN	39.17%	37.50%	45.00%	34.17%	24.17%	41.67%	04.17%
MEXICO	52.55%	43.07%	43.07%	53.28%	21.17%	21.90%	03.65%
COLOMBIA	59.26%	48.15%	45.93%	50.37%	21.48%	31.11%	05.19%
CHILE	56.73%	48.08%	50.00%	43.27%	20.19%	25.96%	09.62%
ARGENTINA	50.49%	41.75%	49.51%	48.54%	21.36%	25.24%	05.83%
JAPAN	45.83%	36.67%	22.08%	29.58%	12.29%	24.38%	14.38%

Note: Percentages noted in the chart above do not include the percentage of respondents who added their own response, and include a .05 - 5% margin of error.

Source: 2020 Consumer Privacy Research by Microsoft Advertising in partnership with iProspect

Fortunately, there are specific steps you can take to minimise the impact of a data breach and mitigate the damage caused in the aftermath. Following are best practices for preparing for the inevitable data breach and managing the fallout effectively.

Before the Breach

1 PLAN AHEAD.

Don't wait until the breach happens to have appropriate procedures in place. Work with IT and security personnel to understand your network environment and potential vulnerabilities. Make sure your information security policies for data management are understood and in place, and determine how you'll enable employees to access data following an incident. Take inventory of any contractual obligations you may have with customers who may be impacted by a breach.

2 ASSEMBLE A RESPONSE TEAM.

Identify ahead of time the individuals in your organisation who will set established procedures in motion when the breach occurs. Your team should include an executive sponsor to serve as the primary point of contact between the company and its board of directors. Other essential team members include individuals from the IT, security, risk management and legal teams, and a public relations professional who can activate external communications. Identify a team leader who can coordinate the group's efforts and keep everyone on track.

3 UNDERSTAND THE REGULATIONS.

Data privacy regulations are evolving all the time, so it's critical to have a solid understanding of which regulations apply to various categories and types of breaches. Some violations have to be disclosed immediately, while others should be kept confidential to give law enforcement bodies time to identify and apprehend fraudsters. Knowing what response is required for the various types of incidents will help eliminate confusion and expedite a response.

4 EDUCATE EMPLOYEES.

It's important to ensure all employees know how to respond should a breach occur. They should have a good understanding of what to do if they suspect a breach, including who to contact and what facts to report. Simply bringing the potential for a data breach to your employees' attention can help build a culture of security and risk management, reducing the possibility of a breach.

5 EDUCATE YOUR CUSTOMERS.

Most privacy policies are clear as mud. Consumers don't want to decipher legalese, it's confusing and time-consuming. Make sure you communicate your privacy policies in clear, concise language, and do it more than once. Develop relevant assets such as blog posts, eBooks or email campaigns informing customers of newly enacted policies or policy updates, to demonstrate you're knowledgeable about data privacy and that you care about the security of your customers' personal data.

6 TAKE CONTROL OF THE MESSAGE.

How you communicate to your employees, customers and the public that your organisation experienced a data breach can have an enormous impact on your reputation and whether or not customers continue to trust your brand in the future. Consider an omnichannel strategy that includes email, text, search ads, website and other ways to disseminate your response. As crafting the message and designing deliverables can take time, create templates in advance and drop in tailored copy with specific details, as needed.

7 DOCUMENT YOUR PLAN OF ACTION.

All of the action items listed here should be formalised and distributed to all critical stakeholders. Data breaches are stressful and taxing on an organisation, and a written plan of action will simplify the reponse process and reduce stress, while ensuring no step is missed and no detail overlooked.

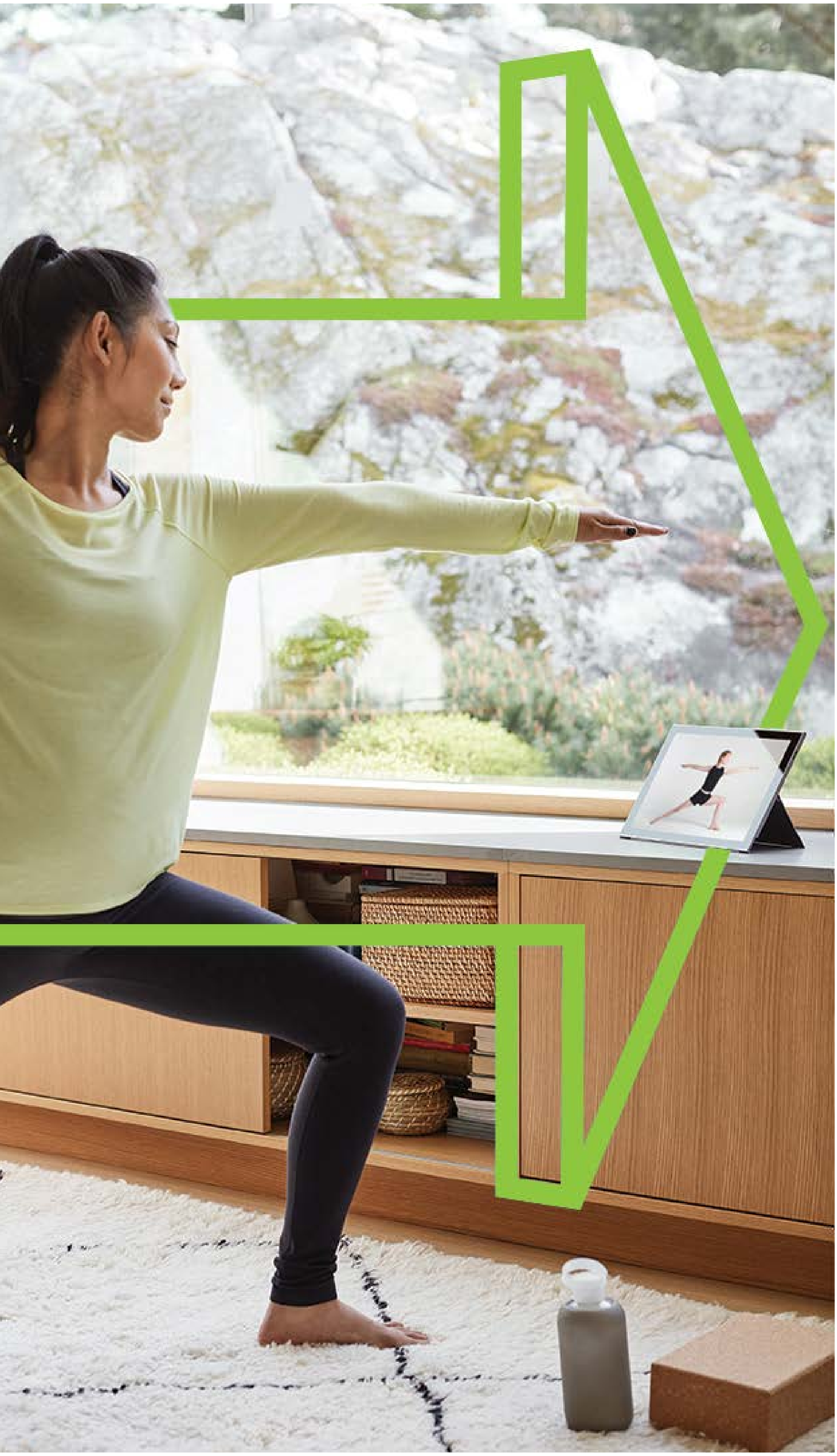
8 BUILD TRUST IN ADVANCE.

Nothing protects an organisation from the reputational damage of a data breach better than a solid reputation. If your customers trust you and think positively of you, they'll be more willing to forgive you when a breach occurs. Basic reputation and CX management strategies such as engaging with customers on social media and reviews sites, requesting and responding to feedback, and proactive communication strategies will strengthen their trust ahead of time, helping to keep you in good standings with your customers and the public, despite the incident.

SIDEBAR

Use SEO to Take Charge of Public Perception

Create a page on your where you own the message and provide ways for consumers to engage directly with you. Make sure the page is discoverable for the most commonly searched keywords related to your brand and the issue. Use SEO best practices to optimise the page and content for keywords related to the breach. You can also buy keyword-based advertising to ensure that your message ranks among the top results in search queries about the incident.



After the Breach

1 ACKNOWLEDGE THE BREACH AND ADMIT THE MISTAKE.

According to our findings, 56% of respondents learned about a data breach from news or media, and only 39% learned of the breach through direct communication with the company that experienced the breach. Learning about the problem from a third party causes consumers to lose trust; 66.82% were concerned that the company did not engage directly via phone call, email or physical mail to notify them of the data breach.

Providing regulations allow you to discuss the breach publicly, don't hide the issue. Leverage your communications plan to proactively reach out to customers and inform them of the problem. Own up to the mistake and apologise for compromising their private data. Then, explain what actions you plan to take to remediate the issue and prevent further breaches.

2 BE TRANSPARENT ABOUT REMEDIATION.

Communicate to customers through multiple channels how your organisation plans to compensate for the breach, whether that's through financial means or by putting in place new measures to protect customer data. You can provide updates throughout the process to reassure customers that you're working on the issue.

3 PERFORM RECONNAISSANCE AND COMMUNICATE LESSONS LEARNED.

It may take some time, but eventually your IT and security teams will determine the root cause of the breach, along with the extent of the damage and lessons learned. Share your findings with your customers to continue to rebuild trust and reaffirm your commitment to keeping their data private and secure.

4 THE NEW VALUE EXCHANGE

CONCLUSION

There is a growing imperative to get data privacy right, not only for security purposes but to meet changing consumer expectations for brand interactions. Marketers need to understand consumers perceptions in order to meet and address their concerns and take into account the various factors that influence opinions and preferences around data privacy. This will require a concentrated effort on the part of brands to facilitate open and clear communications around data collection and usage.

We believe education and communication will be key in the effort to earn consumer trust, and the resulting credibility will make consumers feel both comfortable sharing their data and cognizant of the value they receive in exchange.

ABOUT THE AUTHORS

JEREMY HULL

As SVP, Innovation at iProspect, Jeremy works with iProspect's clients developing new advertising solutions that incorporate emerging technologies, leverage ever-changing platform features, and most importantly, address evolving consumer behaviors and expectations. He provides both thought leadership around changing trends and specific plans that ensure brands can continue to connect with individuals and deliver performance across digital and physical experiences.

In 2013, Jeremy was inducted into the ClickZ Digital Marketing Hall of Fame, and in 2017 he was recognised as the Bing Executive of the Year. Over the past twelve years Jeremy has delivered transformative business results for dozens of the world's top brands, including General Motors, adidas, Choice Hotels, T-Mobile, Under Armour, The Neiman Marcus Group, Hilton Worldwide, Michael Kors, Microsoft, NRG, and Staples.

Outside the office, Jeremy is a talented bassist and can often be found playing for a crowd at a local jazz lounge.

MISTY LOCKE

Misty Locke is responsible for iProspect's global vision and strategic direction, as well as maintaining the firm's industry relationships. Co-founder of Range Online Media in 2001, Misty served as President and led the award-winning company through its acquisition in 2009 by Aegis PLC (later acquired by Dentsu).

As a founding member of the global iProspect leadership team, Misty is committed to closing the gap between today's iProspect and its future potential. Misty has more than 20 years of digital and performance marketing experience with a reputation for passionately focusing on building brands and people. She is dedicated to creating an industry environment built on opportunity and accountability, driven to overdeliver on client expectations and committed to developing authentic and personal relationships with clients and partners alike. Misty also heads the Female Foundry initiative globally which drives diversity and inclusion in business.

CHRISTI OLSON

Christi is the Head of Evangelism for Search at Microsoft with over a decade of experience in Digital Marketing leading both in-house and agency teams across the retail, travel, automotive and consumer electronics industries. Christi serves on the Advisory Boards for the Paid Search Association, the Internet Marketing Association, and the University of Idaho School of Business. Christi has been recognised as one of the top 25 most Influential Paid Search experts annually since 2014 by PPCHero and additionally is a recognised global speaker on Digital Marketing Strategy, Search, and Cognitive AI. She is a published author in the Applied Marketing Analytics Journal and regularly contributes to Forbes, AdAge, Marketing Profs, Search Engine Land and Search Engine Journal.

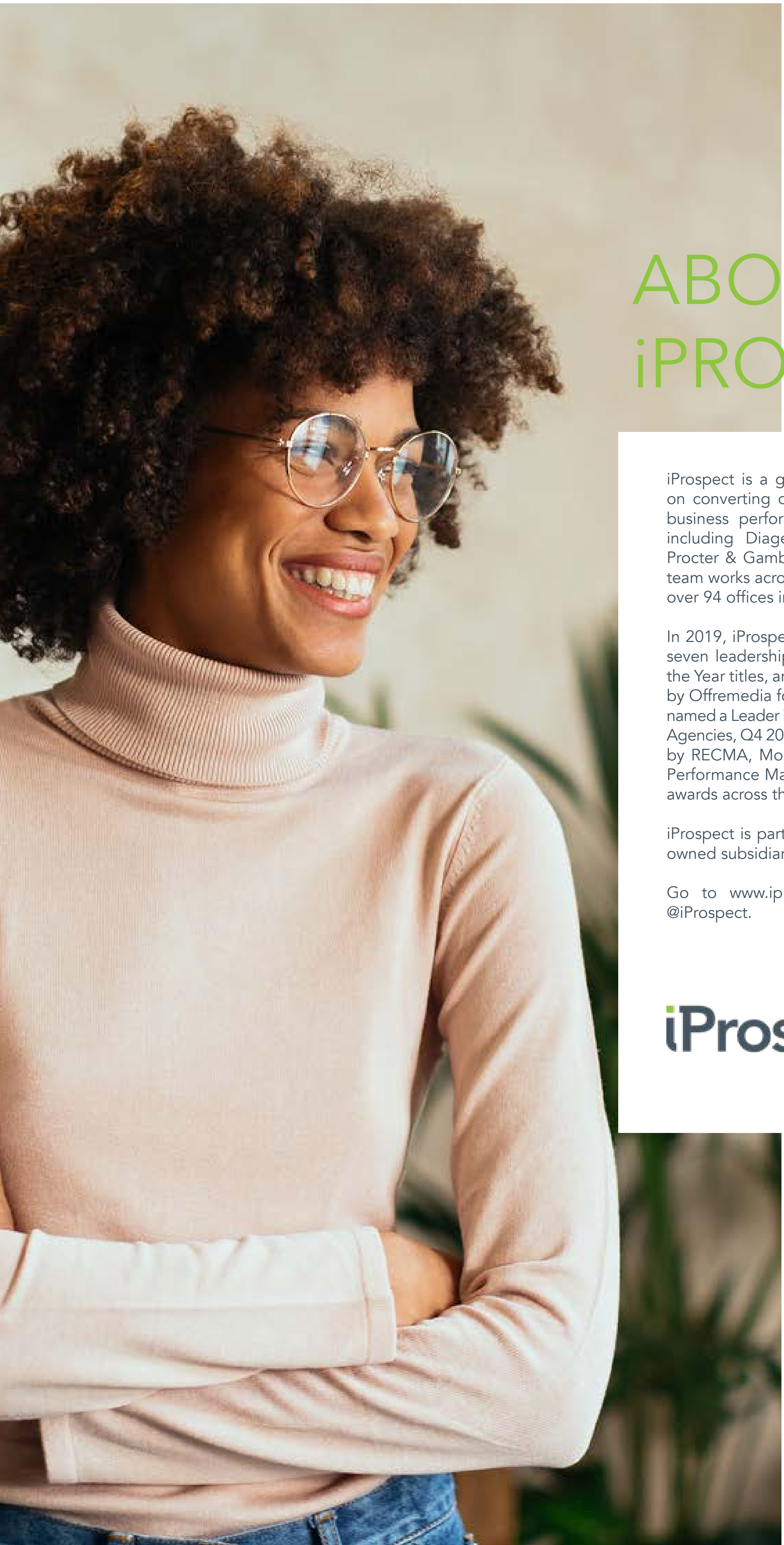
ADRIAN CUTLER

Adrian is the Director of Global Agencies for Microsoft Ads based in London. He joined Microsoft to bring an "outside-In" view to Microsoft Ads with a clear perspective in how to truly obsess about our customers. Prior to joining Microsoft, Adrian successfully ran profitable paid search and performance media teams in Zenith Optimedia Performics and Dentsu Aegis iProspect, where he moved client side to build an in-house digital team from scratch.

Adrian is a regular keynote speaker, award judge and panelist at industry events such as Cannes, Adweek, SMX and DMEXCO. Adrian is deliberate in always demystifying AI and showing how not only can it save the greatest and most precious commodity to humanity, time, but also how its place in the world can empower us all to truly amplify what we are naturally capable of through our own Human Ingenuity.

As a Fellow of the Royal Society of Art, Commence and Manufacturing, he takes the greatest pride in seeing humanity collaborate with each other and how tech can advance this collaboration.

Adrian is a father, husband, lives in Sussex and works in London.



ABOUT iPROSPECT

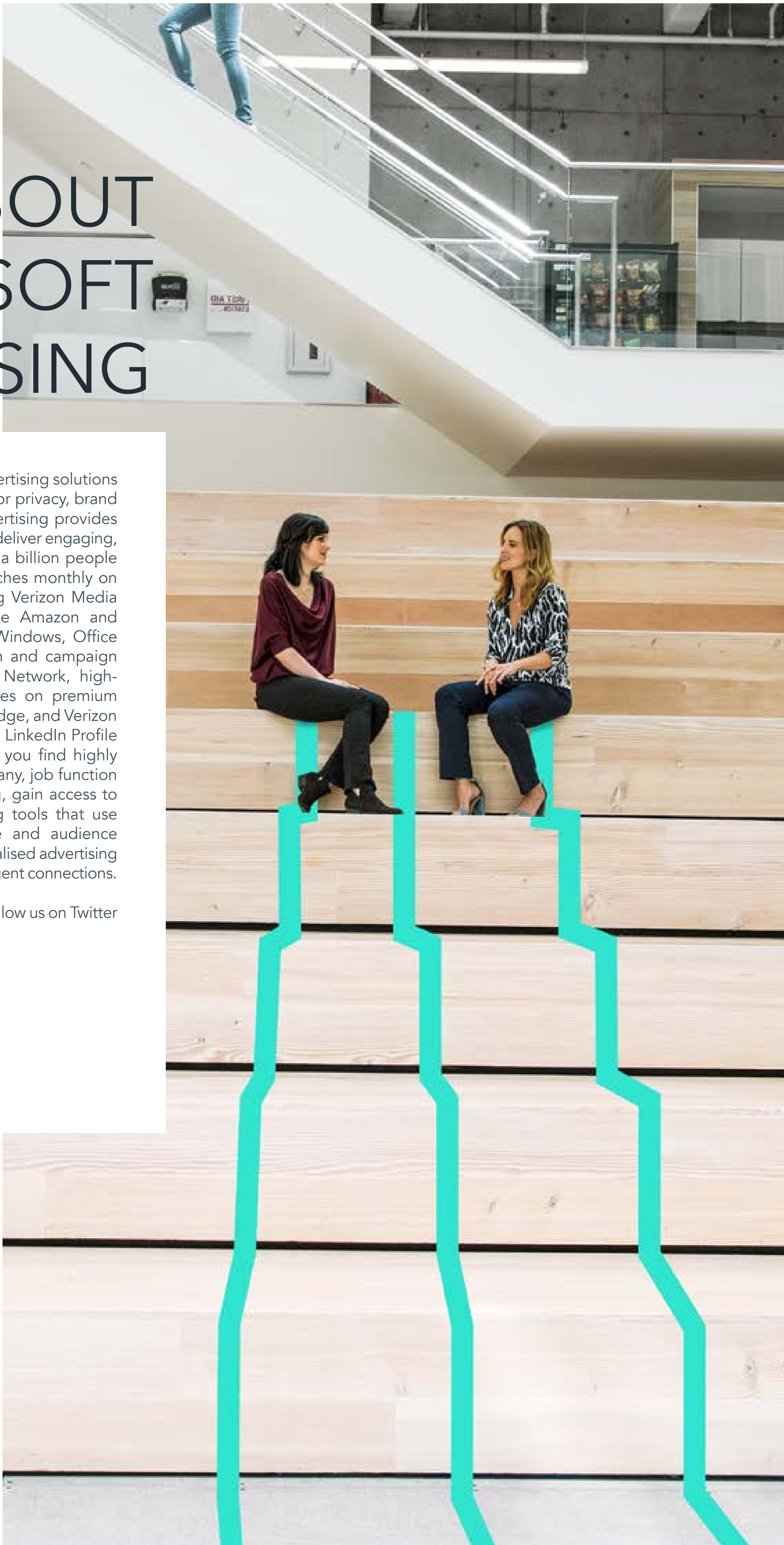
iProspect is a global, award-winning agency – focused on converting consumer intent into action and driving business performance for the world's largest brands, including Diageo, Hilton, Burberry, General Motors, Procter & Gamble, Gucci, and Microsoft. The iProspect team works across a network of 4,600 employees spread over 94 offices in 56 countries.

In 2019, iProspect won more than 160 awards including seven leadership recognition awards and 15 Agency of the Year titles, and was named Media Agency of The Year by Offremedia for the third consecutive year. iProspect is named a Leader in The Forrester Wave™: Search Marketing Agencies, Q4 2017, #1 Global Digital Performance Agency by RECMA, Most Effective Agency at The International Performance Marketing Awards, and took home six Effie awards across the globe in 2019.

iProspect is part of the Dentsu Aegis Network, a wholly owned subsidiary of Dentsu Inc.

Go to www.iprospect.com or follow us on Twitter @iProspect.

ABOUT MICROSOFT ADVERTISING



Represent your brand at its best with advertising solutions guided by an uncompromising respect for privacy, brand safety, and data security. Microsoft Advertising provides intelligent solutions that empower you to deliver engaging, personalised experiences to over a half a billion people worldwide. Bing powers billions of searches monthly on the Microsoft Search Network, including Verizon Media properties (AOL, Yahoo), platforms like Amazon and Apple, and on Microsoft services like Windows, Office and Microsoft Edge. Extend your reach and campaign performance with Microsoft Audience Network, high-quality native placements across devices on premium sites like MSN, Outlook.com, Microsoft Edge, and Verizon Media. Only Microsoft Advertising offers LinkedIn Profile targeting on search and native to help you find highly relevant audiences based on their company, job function and industry. With Microsoft Advertising, gain access to in-depth insights, intelligent advertising tools that use AI to improve campaign performance and audience targeting solutions to create more personalised advertising experiences. Microsoft Advertising. Intelligent connections.

Go to www.about.ads.microsoft.com or follow us on Twitter @MSFTAdvertising

Microsoft

RESOURCES

1. IBM Marketing Cloud, “10 Key Marketing Trends For 2017 and Ideas for Exceeding Customer Expectations”, Page 2,” Cited in a Research Brief by Media Post, December 22, 2016, https://www.mediapost.com/publications/article/291358/90-of-todays-data-created-in-two-years.html

2. Domo, “Data Never Sleeps 6.0”, 2018, https://www.domo.com/learn/data-never-sleeps-6

3. David Reinsel, John Gantz, John Rydning, “Data Age 2025: The Digitization of the World From Edge to Core”, November 2018, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

4. NewVantage Partners LLC, “Big Data Executive Survey 2018”, from NewVantage.com, January 2018, http://newvantage.com/wp-content/uploads/2018/01/Big-Data-Executive-Survey-2018-Findings-1.pdf

5. Michael Fertik, “In the Future, Everything Will Have a Number - What’s Yours?”, Forbes; April 2, 2019, https://www.forbes.com/sites/michaelfertik/2019/04/02/in-the-future-everything-will-have-a-number-whats-yours/#51fd2330970c

6. Scott Brinker, “Marketing Technology Landscape Supergraphic (2019): Martech 5000 (actually 7,040)”, Chiefmartec.com; April 2019, https://chiefmartec.com/2019/04/marketing-technology-landscape-supergraphic-2019/

7. Retail Customer Experience, “Consumers expect personalization, reveals report”, April 8, 2019, https://www.retailcustomerexperience.com/news/consumers-expect-personalization-reveals-report/

8. Kevin Litman-Navarro, “We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.”, New York Times, June 12, 2019, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html

9. Erica Perry, “Lack Of Trust Costs Brands $2.5 Trillion Per Year: Study,”, Social Media Week, February 6, 2018, https://socialmediaweek.org/blog/2018/02/lack-trust-costs-brands-2-5-trillion-per-year-study/

10. The Onion, “Google Opt Out Feature Lets Users Protect Privacy By Moving To Remote Village”, YouTube, April 11, 2009, https://www.youtube.com/watch?v=lMChO0qNbkY

11. Brad Smith and Carol Ann Browne, Foreword by Bill Gates, “Tools and Weapons: The Promise and the Peril of the Digital Age”, Penguin Press, New York, Sept 2019

12. Customer Think, “Brand Keys 2019 Customer Loyalty Engagement Index Identifies Secret to Lasting Loyalty” February 5, 2019, http://customerthink.com/brand-keys-2019-customer-loyalty-engagement-index-identifies-secret-to-lasting-loyalty/

RESOURCES

13. BrightLocal, "Local Consumer Review Survey", BrightLocal, December 11, 2019, Link: https://www.brightlocal.com/research/local-consumer-review-survey/

14. Diana Kaemingk, "20 online review stats to know in 2019", Qualtrics.com, April 9, 2019, https://www.qualtrics.com/blog/online-review-stats/

15. Ethan Jakob Craft, "5 Key Takeaways From The 2019 Edelman Brand Trust Survey", Ad Age June 18, 2019, https://adage.com/article/digital/5-key-takeaways-2019-edelman-brand-trust-survey/2178646

16. Dan Hagen, "The Trust Equation," iProspect, February 5, 2019, https://www.iprospect.com/en/global/news-and-views/news/the-trust-equation/

17. Google, "The Basics of Micro-Moments", May 2016, https://www.thinkwithgoogle.com/marketing-resources/micro-moments/micro-moments-understand-new-consumer-behavior/

18. Epsilon, "New Epsilon research indicates 80% of consumers are more likely to make a purchase when brands offer personalized experiences", January 9, 2018, https://us.epsilon.com/pressroom/new-epsilon-research-indicates-80-of-consumers-are-more-likely-to-make-a-purchase-when-brands-offer-personalized-experiences

19. Jeffrey Prince and Scott Wallsten, "How Much is Privacy Worth Around the World and Across Platforms?", Technical Policy Institute, New York, January 2020, https://techpolicyinstitute.org/wp-content/uploads/2020/01/Prince_Wallsten_How-Much-is-Privacy-Worth-Around-the-World-and-Across-Platforms.pdf

20. Risk-based Security, "Data Breach QuickView Report 2019 Q3 trends", Issued November, 2019, https://pages.riskbasedsecurity.com/hubfs/Reports/2019/Data%20Breach%20QuickView%20Report%202019%20Q3%20Trends.pdf

Microsoft

iProspect