MARKETING

Privacy Matters:

How Different Generations Think about Their Data

What marketers need to know to build trust with consumers

Introduction

Marketers have long counted on consumers to provide their personal information in exchange for something of value, such as a discount, access to a perk or just more-personalized content. Yet, an increasing demand for transparency around how brands use data and data governing legislation — such as the EU's General Data Protection Regulation (GDPR), the California Consumer Protection Act (CCPA), and Brazil's General Data Protection Law (GDPL) — indicate a shift in consumer attitudes toward privacy.

We surveyed 1,000 consumers to better understand the ways their attitudes toward privacy have shifted. This report lays out striking generational divides and provides insight into the strategies companies can implement to build consumer trust in an era of changing expectations.

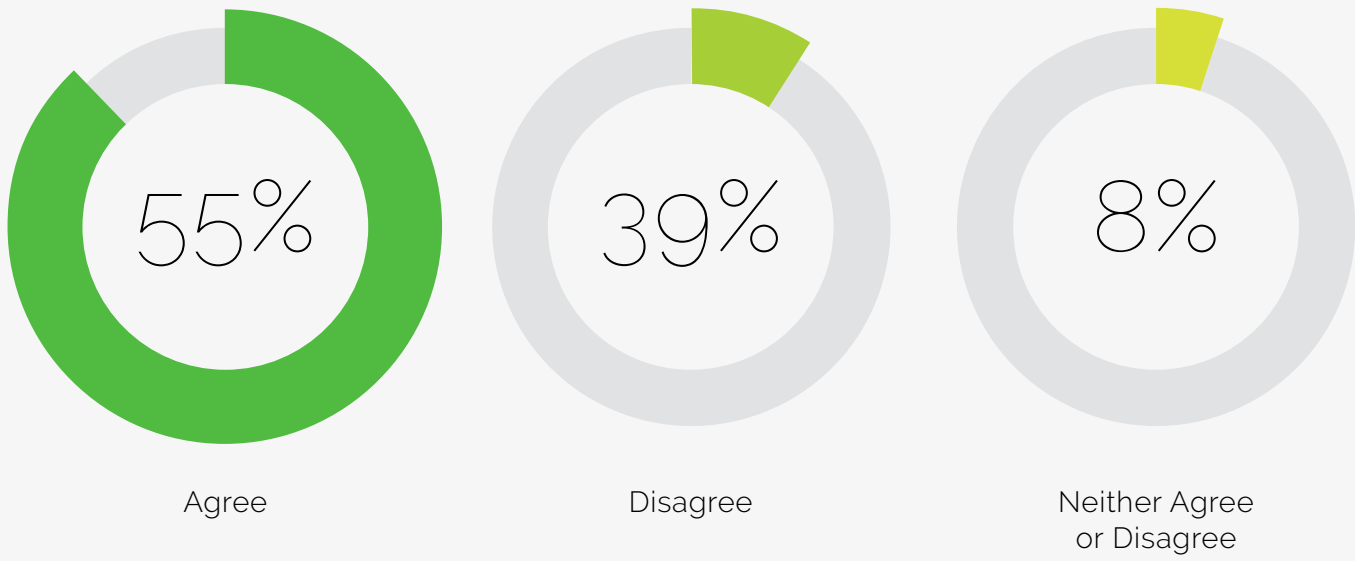
Section 1: A rising focus on privacy

Consumers of all ages are increasingly focused on their data and how it is used.

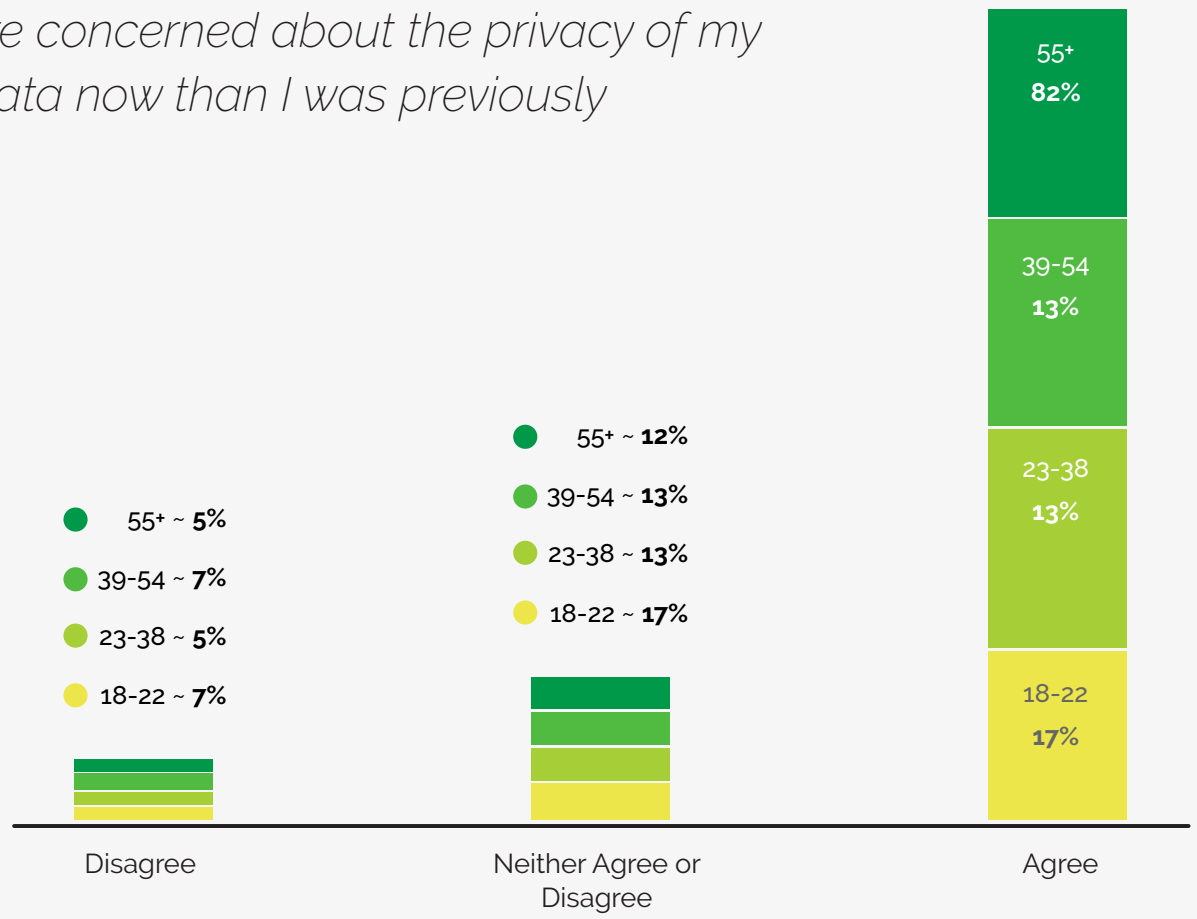
Eighty-eight percent of the consumers we surveyed are concerned about the privacy of their data. And that concern is growing. An overwhelming 80% of consumers say they are more concerned with their data's privacy than they used to be.

Privacy concerns are prevalent across all ages, and on the rise.

I am concerned about the privacy of my data



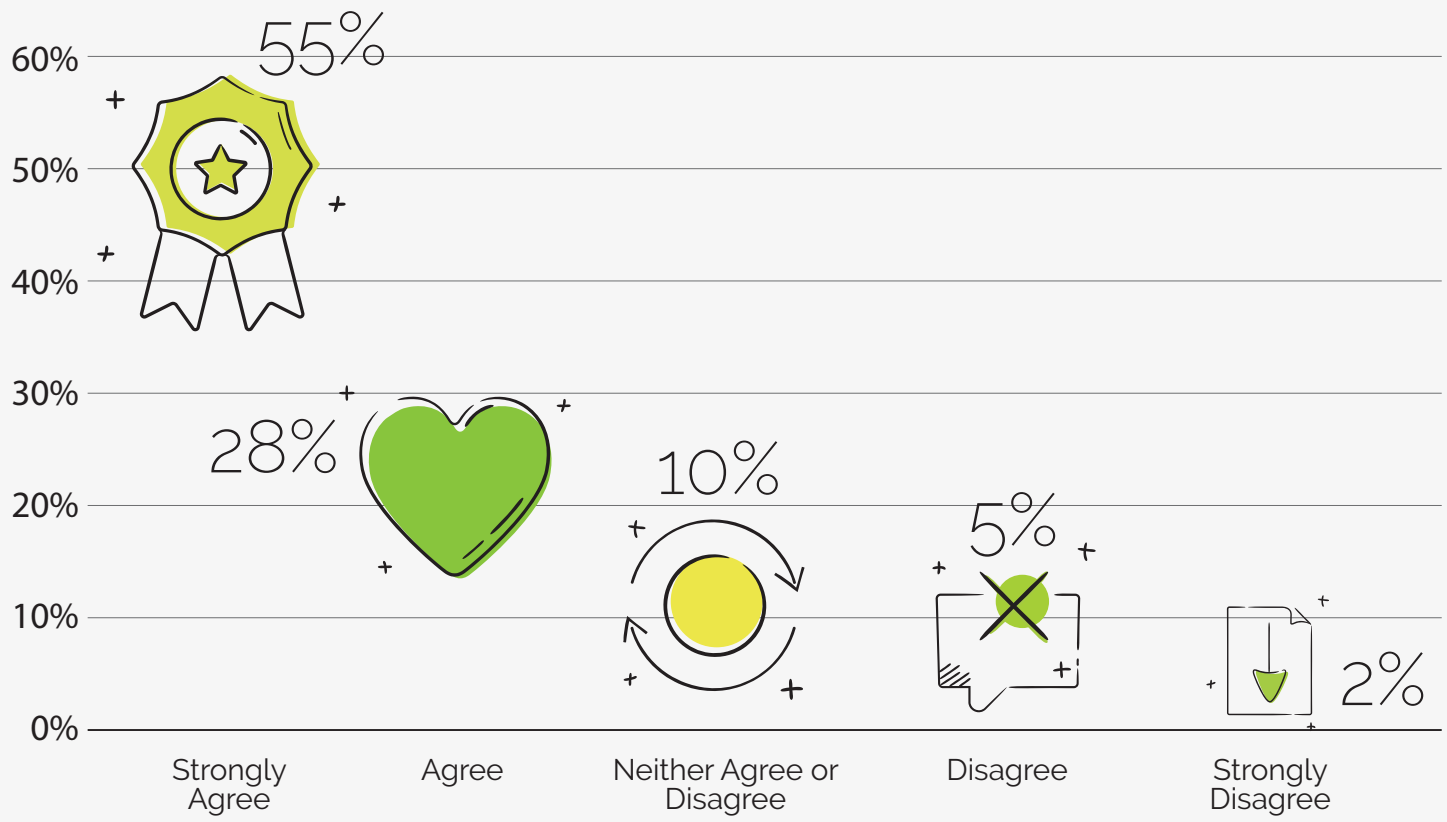
I am more concerned about the privacy of my data now than I was previously



The survey shows that while respondents expect companies to protect their data, many consider it a risk to provide personal data and credit card information to businesses.

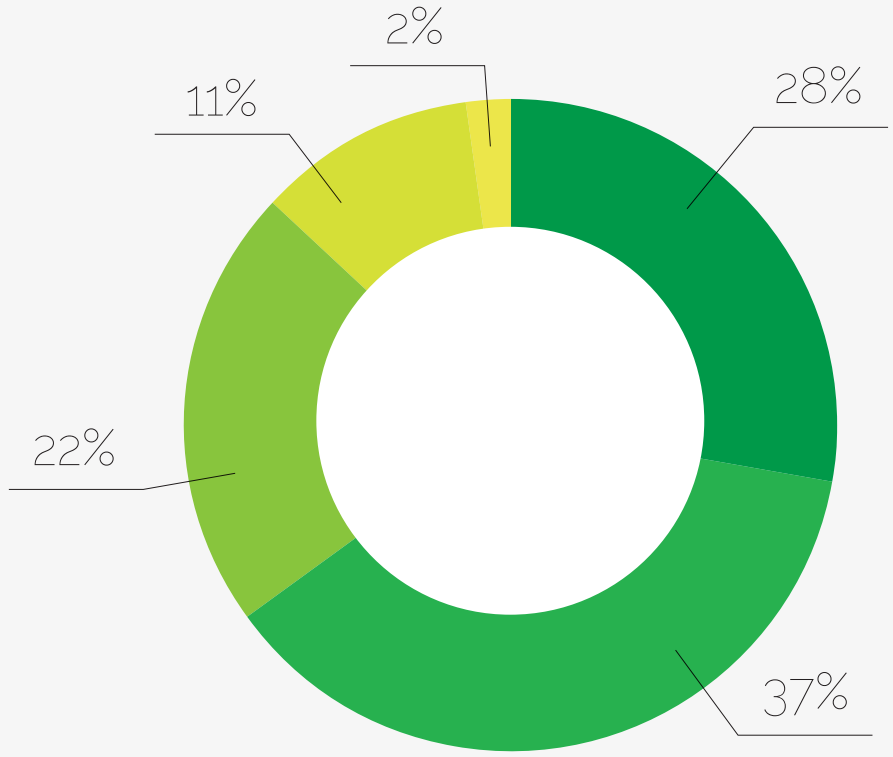
Although consumers expect companies to act responsibly with their data, they understand there is still a risk.

I expect the companies I do business with to keep my data secure



I consider it a risk to give a company my personal information (i.e. Full name, email and phone number)

- **28%** – Strongly Agree
- **37%** – Agree
- **22%** – Neither Agree or Disagree
- **11%** – Disagree
- **2%** – Strongly Disagree



Turning insights into action

Make data governance policies clear and ironclad

An intentional approach to data governance and ethical data management protects consumers' privacy even as it encourages businesses to become more efficient. Yet many companies are still playing catch-up when it comes to data governance. For example, according to the 2018 Global State of Information Security Survey (GSISS), only 51% of businesses maintain an accurate inventory of the collection, transmission and storage of employee and customer personal data.[i]

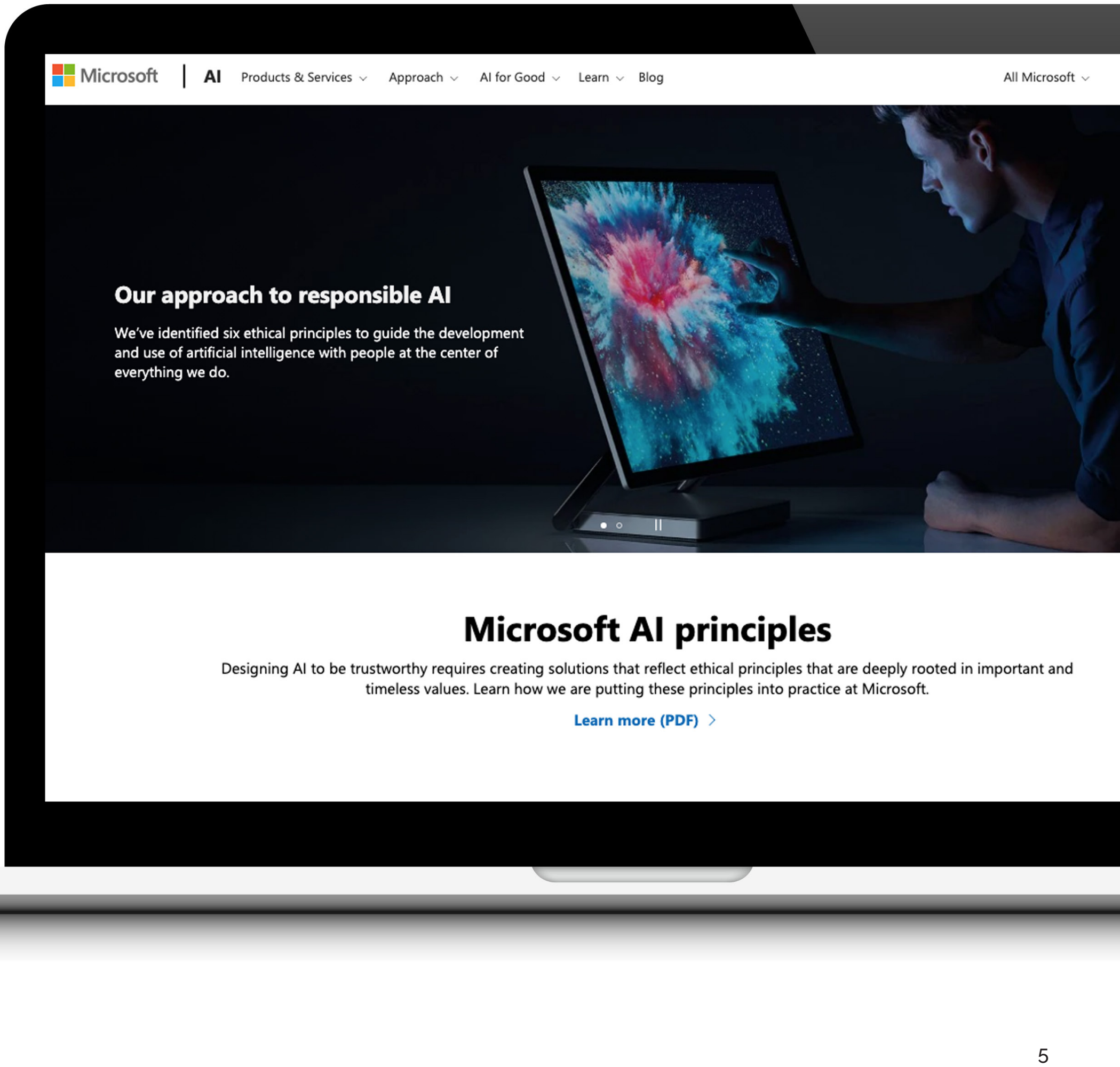
Brands that develop a clear strategy for how they will use data, why they need it, which data they need to collect, and how long they should keep it will save time and valuable resources. In addition, clearly communicating how a brand respects and protects customer data goes a long way toward easing consumer concerns.

Brand example: Microsoft

As many technology companies experience consumer suspicion, Microsoft is embracing privacy consciousness. Under the guidance of CEO Satya Nadella, Microsoft has made their commitment to privacy a central tenet of business growth.

In 2019 the company was named one of the 10 most reputable companies in technology by the Reputation Institute. Microsoft showed the highest year-over-year increase in reputation rating.[ii]

The brand provides consumers and businesses with clear communication about privacy and ethics through a number of channels. For example, their Trust Center offers in-depth information about the brand's approach to data security and privacy, while their AI website highlights the brand principles that guide their approach to developing ethical artificial intelligence.



In addition, Microsoft's swift action and communication[iii] after data from their call-center logs was exposed demonstrates one way brands can weather a data leak. The company provided detailed information about what caused the issue, what kinds of data were exposed, how the company fixed the problem, and how their standard operating procedures (redacting personal information from call logs, for example) had protected their customers' privacy despite the breach.

Microsoft

Microsoft Security Response Center

Report an issue | Security Update Guide | About MSRC

Access Misconfiguration for Customer Support Database

MSRC / By MSRC Team / January 22, 2020 / Misconfiguration, Privacy

Today, we concluded an investigation into a misconfiguration of an internal customer support database used for Microsoft support case analytics. While the investigation found no malicious use, and although most customers did not have personally identifiable information exposed, we want to be transparent about this incident with all customers and reassure them that we are taking it very seriously and holding ourselves accountable.

Our investigation has determined that a change made to the database's network security group on December 5, 2019 contained misconfigured security rules that enabled exposure of the data. Upon notification of the issue, engineers remediated the configuration on December 31, 2019 to restrict the database and prevent unauthorized access. This issue was specific to an internal database used for support case analytics and does not represent an exposure of our commercial cloud services.

As part of Microsoft's standard operating procedures, data stored in the support case analytics database is redacted using automated tools to remove personal information. Our investigation confirmed that the vast majority of records were cleared of personal information in accordance with our standard practices. In some scenarios, the data may have remained unredacted if it met specific conditions. An example of this occurs if the information is in a non-standard format, such as an email address separated with spaces instead of written in a standard format (for example, "XYZ @contoso com" vs "XYZ@contoso.com"). We have begun notifications to customers whose data was present in this redacted database.

We are committed to the privacy and security of our customers and are taking action to prevent future occurrences of this issue. These actions include:

- Auditing the established network security rules for internal resources.

Search ...

Follow MSRC

Categories

BlueHat (178)
Japan Security Team (872)
MSRC (910)
Security Research & Defense (363)

Tags

advisory (60) | ANS (47) | Attack (43) | Attack Vector (68) | BlueHat Security Briefings (55) | Community-based Defense (65) | Defense-in-depth (38) | EcoStrat (34)

Section 2: Consumer attitudes on privacy are not always consistent

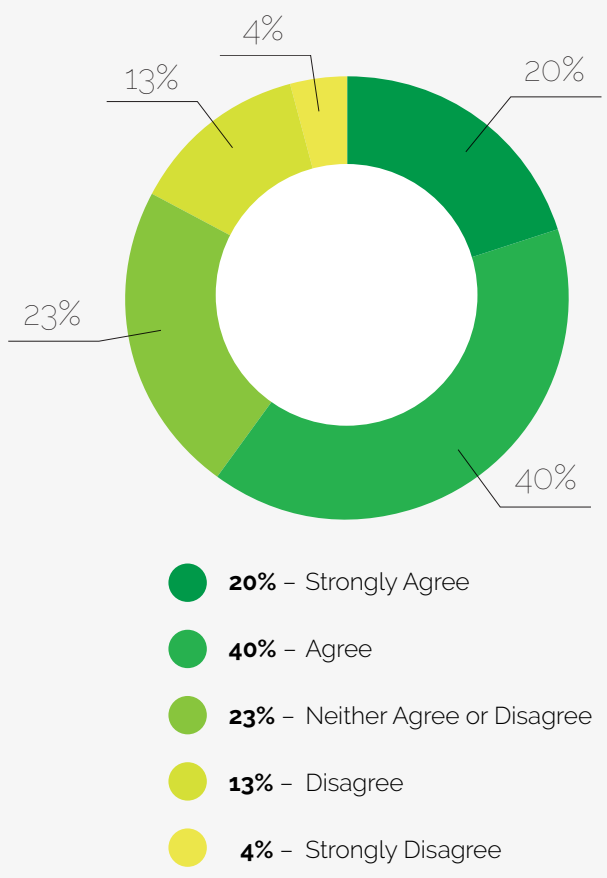
While consumers are more concerned about privacy than they used to be, many survey takers across generations believe that we already live in an era where privacy no longer exists.

That may mean that some consumers accept the way businesses use data to improve customer experience and – in turn – generate more revenue.

However, 57% of consumers across all ages (weighted slightly towards senior generations) are alarmed when they see a product they searched for online advertised on social media – indicating a lack of understanding of common marketing tactics that use consumer data to improve targeting and ad relevance. What might otherwise be viewed as helpful information is making some consumers wary.

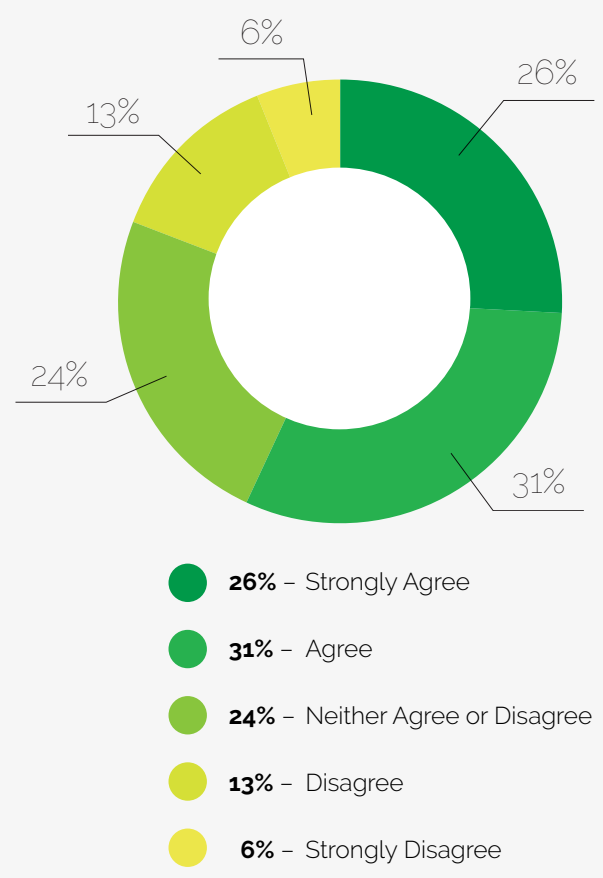
Regardless of age, the majority of respondents agree there is no privacy in the digital age.

I believe that in today's hyper-connected world, privacy doesn't/can't exist



Although advertising previously searched products is common and basic marketing technique, most people are still find it surprising and concerning.

I am alarmed when I see an advertisement for a product on social media after searching for it online



However, across all ages (weighted slightly towards senior generations), 57% of consumers said they are alarmed when they see a product they searched for online advertised on social media.

This indicates consumers' lack of understanding about common marketing tactics that utilize consumer data to improve targeting and ad relevance. What might otherwise be viewed as a helpful information is making some consumers wary, in part due to lack of understanding about how their data is being used.

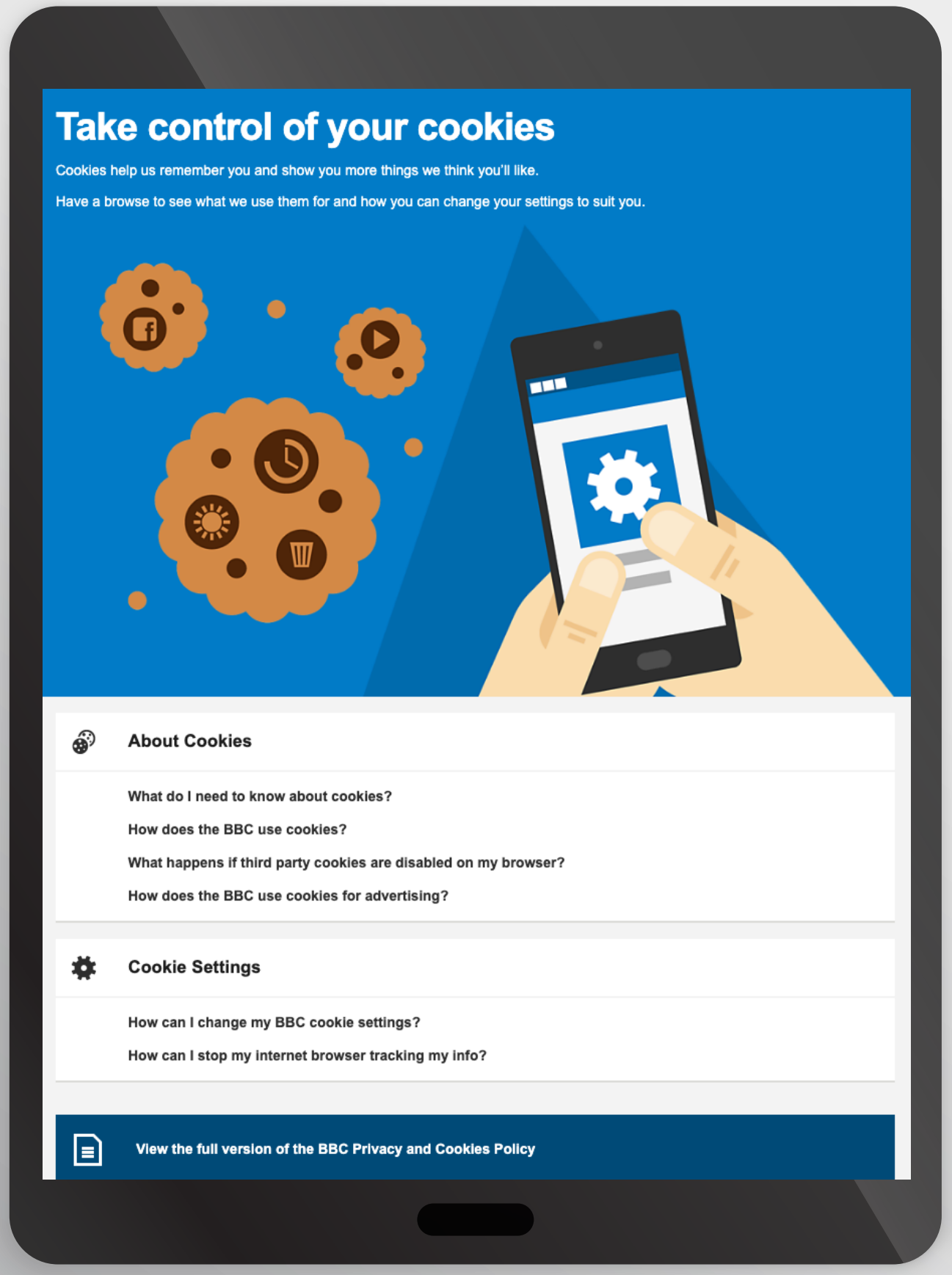
Turning insights into action

Ease consumer confusion and give them more control
Brands should keep in mind that consumers' attitudes about privacy can sometimes be based on fearful feelings that spring up in the absence of a basic understanding of common marketing practices. Easing consumer confusion by clarifying up front how data will be collected and used can help build trust and foster goodwill. In addition, giving consumers more control over their data will boost confidence in a brand's ability to protect customer privacy.

Brand example: BBC (British Broadcasting Corporation)

The BBC makes it easy for consumers by giving their audience a detailed account of how the brand uses cookies to remember them. Moreover, the network puts power back into consumers' hands by enabling them to adjust their cookie settings to control the information BBC collects about them.

BBC



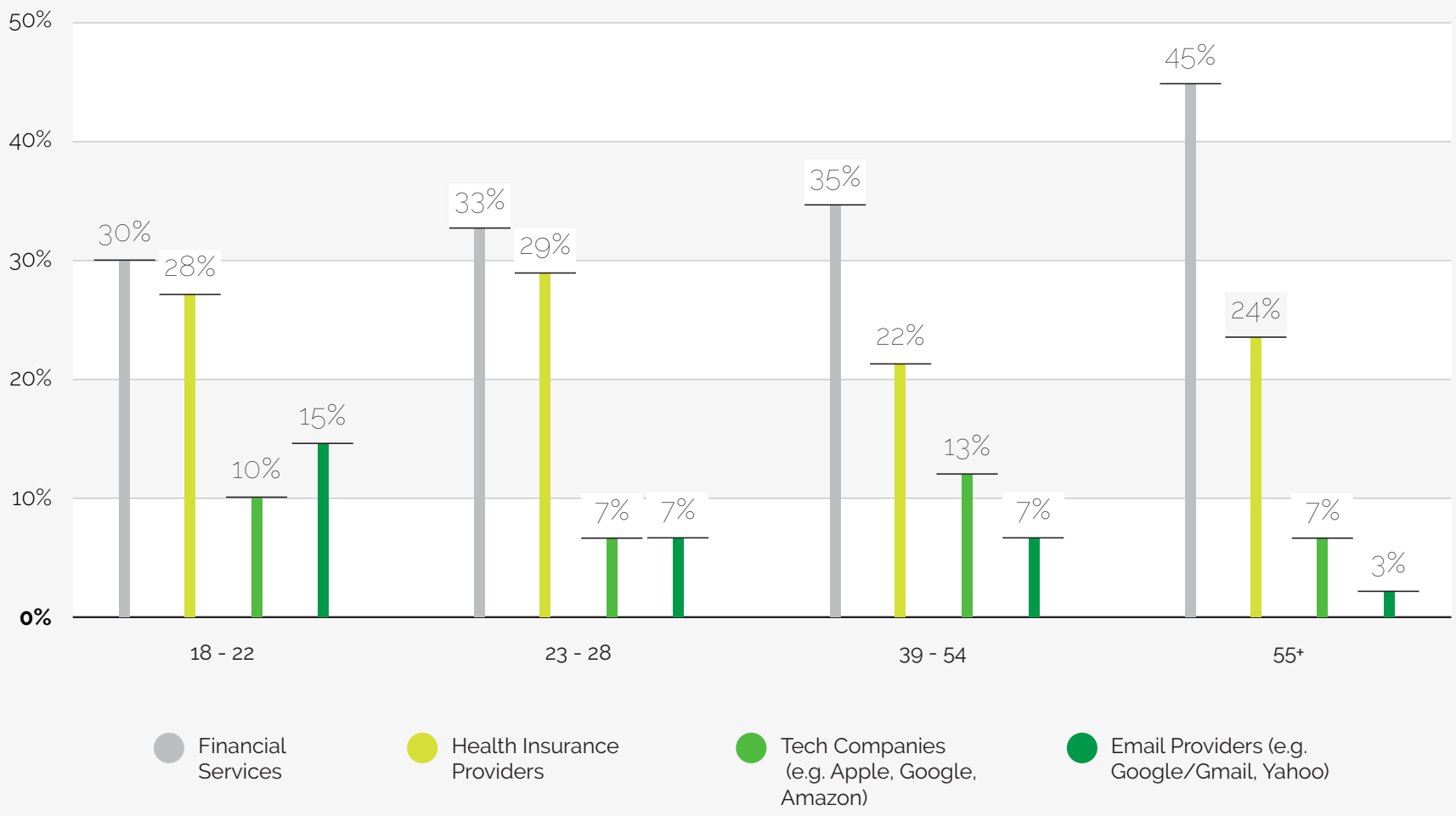
Section 3: Traditional industries are most trusted

Our research revealed that not all industries spark the same level of concern — and that generational attitudes vary based on a company's sector. Among senior age groups in particular, financial services and healthcare are considered the most worthy of trust.

Younger generations also consider these traditional industries the most trustworthy, although to a slightly lesser extent. Younger generations trust newer industries, such as email providers and tech companies, more than older generations do.

Older generations are much more trusting of financial services and healthcare providers with their data than they are with technology companies.

Industry most trusted with personal data



Finance and healthcare's status as most trustworthy can be credited to their long-standing reputation and familiarity, as well as the fact they are held to a higher standard through strict data regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA). Traditional industries also tend to focus on their reputations for safety and security, while a number of companies in the technology sector have made headlines for pushing the limits of consumer privacy.

Turning insights into action

Regulation and compliance can help improve consumer trust
74% of cyber security professionals believe compliance requirements are a “very” or “extremely” effective way to keep data secure.[iv] While marketers often view privacy legislation as the enemy, because it may limit marketing efforts, consumers see it as a source of security. It is possible for brands to employ innovative marketing strategies while honoring consumers’ desire for privacy. When brands explain the ways they comply with regulations and protect customer data, consumers are often more willing to consent to sharing their data.

Brand example: HIPAA compliant marketing

An agency that provides consumer engagement solutions for health insurance plans worked with Infogroup and Yes Marketing to implement a new HIPAA-compliant marketing database, campaign, and analytics solution. The result proves that even heavily regulated industries can use advanced technologies to employ modern marketing strategies. Because the agency runs multiple databases with sensitive first-party data unique to each of their health-insurance clients, they emphasized data security and compliance when choosing a vendor and technology solution. Their new HIPAA-compliant marketing technology has enabled their health plan clients to improve personalization and customer satisfaction while providing new tools for acquisition, retention, and building loyalty.

HIPAA COMPLIANT

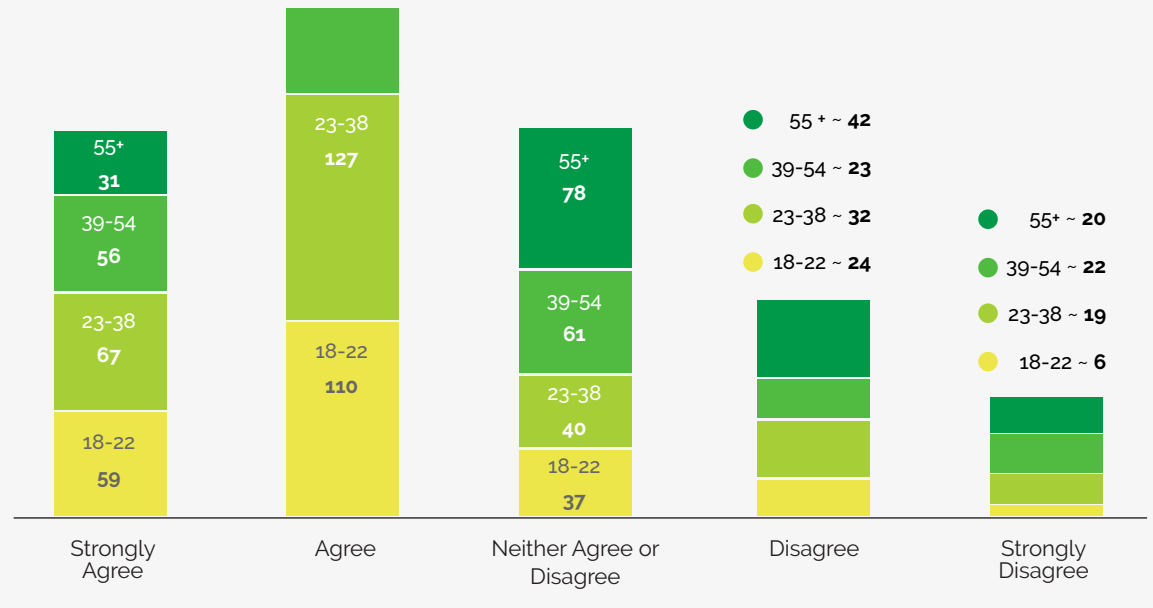
Section 4: Privacy and new technologies

Privacy may be a concern, but it’s not a deal breaker when it comes to interacting with new technologies for security and convenience. Younger generations are, unsurprisingly, the most comfortable engaging with new technologies and platforms. However, older generations are also open to using new technologies - with many reporting they are somewhat comfortable or on the fence.

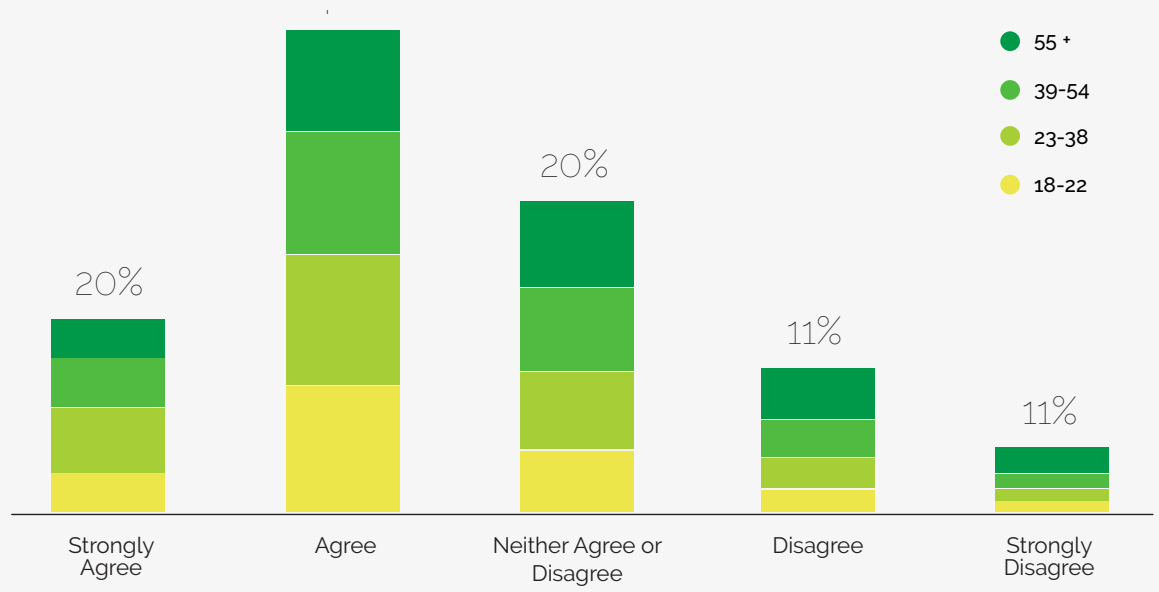
Consumers across generations are using new security technologies like face- and thumbprint-recognition to protect themselves – with 61% saying they either strongly agree or agree that they are comfortable using these technologies.

Older generations are less comfortable with newer technology services than their younger counterparts, but they are not completely turned-off to the idea.

I am comfortable using a phone or personal computer with face ID or thumbprint recognition

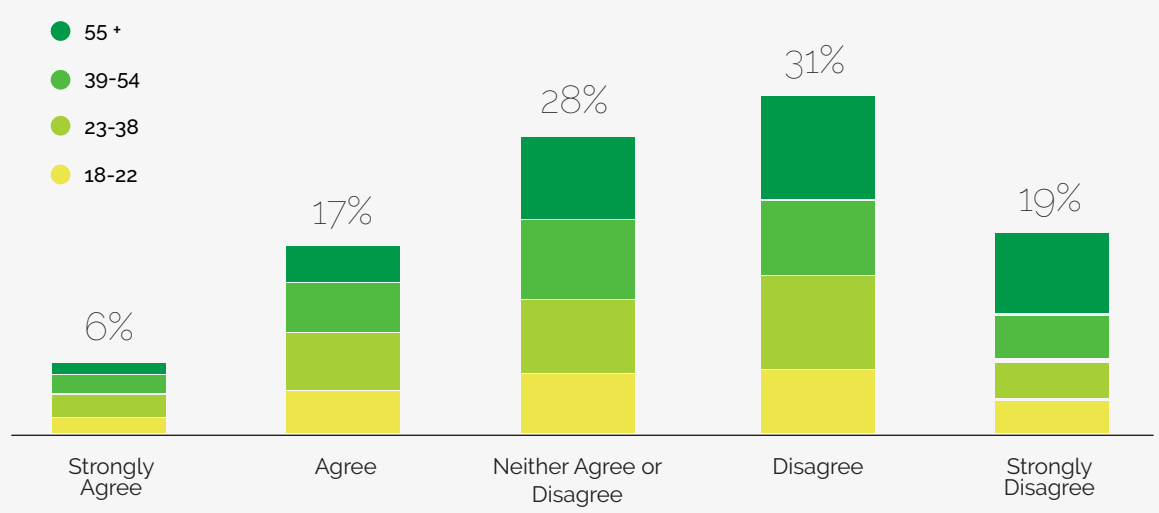


I am comfortable using online financial services



Older groups are most often distrustful of voice services.

I believe it's okay to trust voice services hardware and software (e.g. Alexa, Siri, Google) with sensitive informaiton



Voice-recognition technologies, such as Amazon's Alexa and Apple's Siri, present a particularly promising area for innovation, even if most consumers still use them for activities like playing music or turning off the lights. These actions encompass a small fraction of voice's capabilities, which include sending money and purchasing products. Consumer wariness of sharing sensitive information on voice-service hardware may be stalling growth in this area.

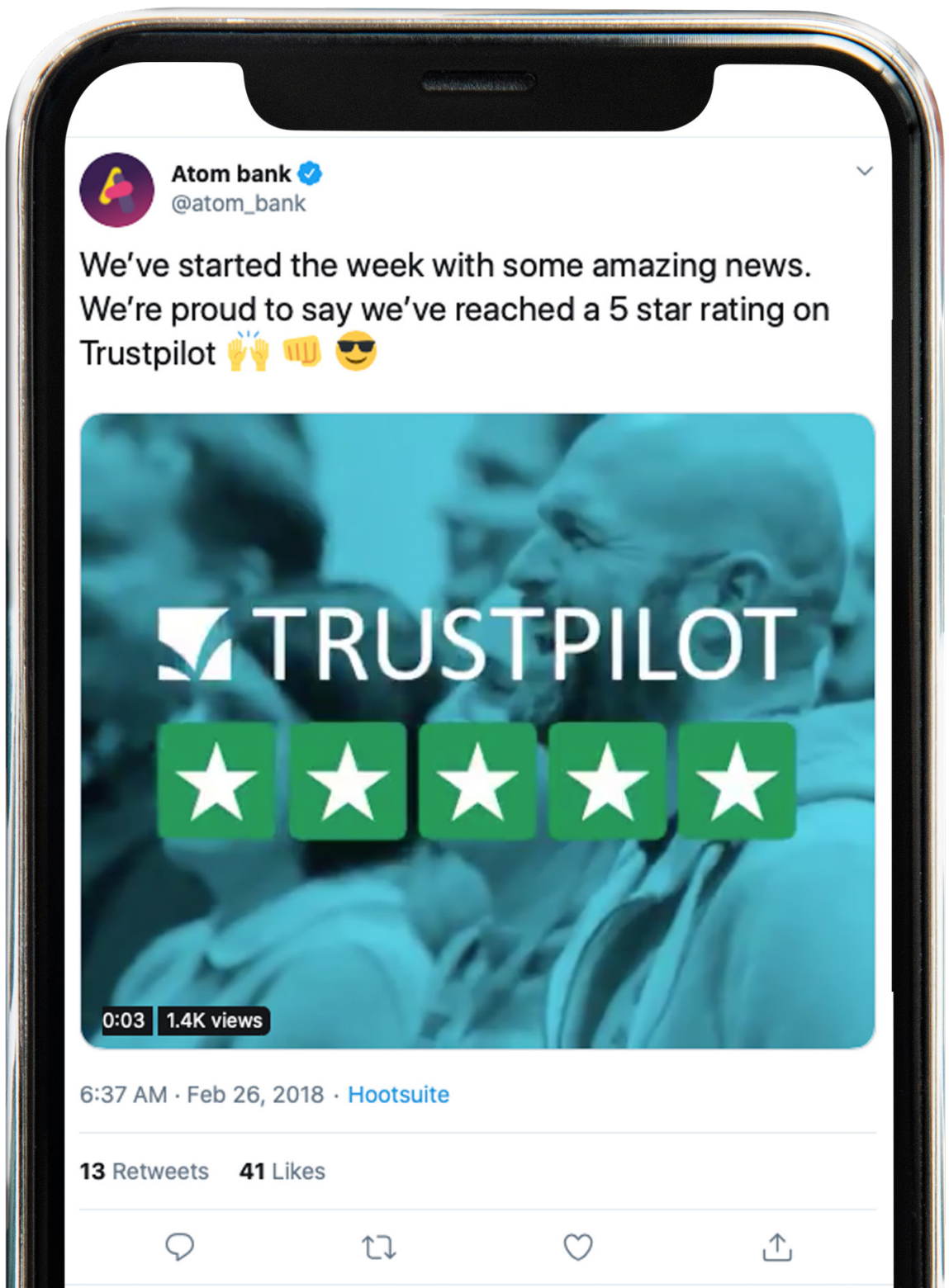
Turning insights into action

Make transparency a core brand value
A focus on transparency can help marketers rebuild consumer trust. Pledges not to sell data to third parties can inspire confidence. Alternatively, being upfront about the fact that data may be commercialized in exchange for incentives, including improving the customer experience, can also build trust. In today's environment, privacy and security are competitive advantages that set businesses apart.

In addition, brands can work to meet consumers where they are when it comes to technology. Young customers may demand the latest bells and whistles, while older ones may choose more traditional ways of interacting with the brand.

Brand example: Brand example – Atom Bank

Blending a new-school approach with an old-school industry's respect for data protection, Atom Bank, the U.K.'s first all-digital banking service, has become a major disruptor in the financial services industry. The brand's success derives from a dedication to data transparency as part of their core brand identity. Atom Bank Chief Marketing Officer Lisa Wood explains, "Trust is absolutely embedded into our marketing strategy and built into the culture of the company, so that everything we do is about building trust and transparency with our consumers. Transparency is one of our design standards, one of the things we hold ourselves accountable to when designing our Atom proposition."[v]

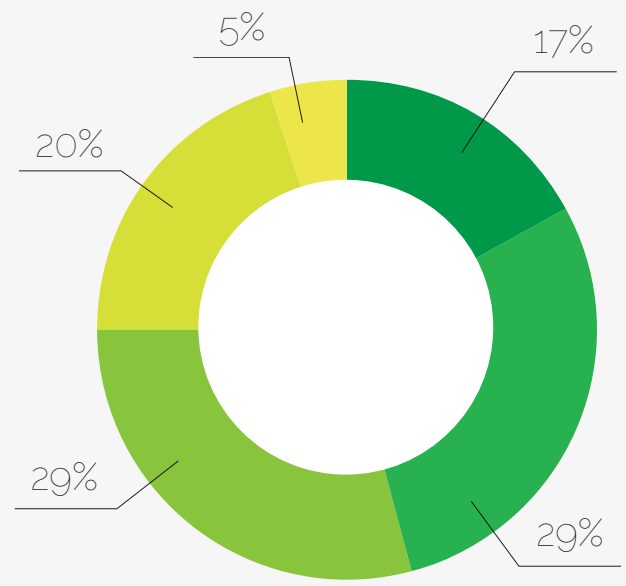


Section 5: How consumers protect their data

Most respondents across age groups say they are careful about what device they use to share sensitive information

I'm more careful when using my desktop computer vs. a mobile or app-based program to share sensitive information

- **17%** – Strongly Agree
- **29%** – Agree
- **29%** – Neither Agree or Disagree
- **20%** – Disagree
- **5%** – Strongly Disagree



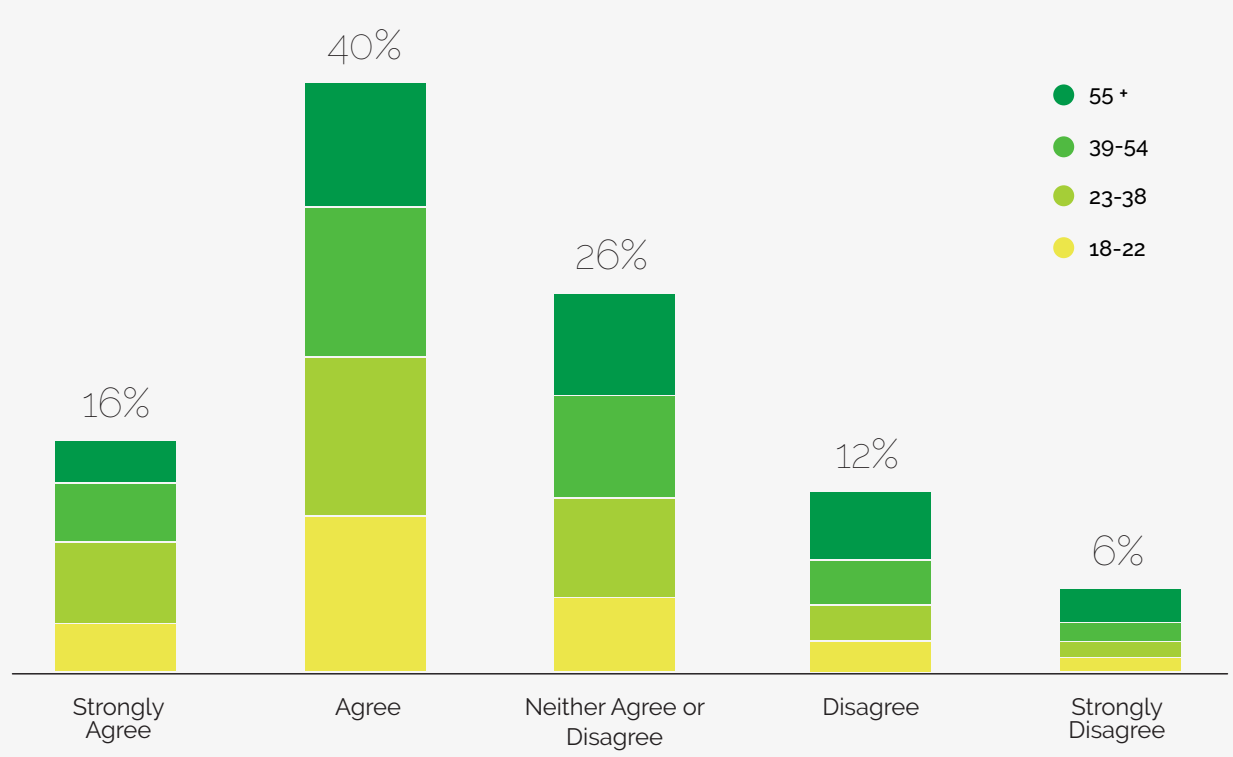
All respondents, especially adults over 55, indicate they are taking more action to protect their data. They are more careful than before about sharing sensitive information online, such as full name, email and phone number.

Consumers are also more thoughtful about using a desktop computer versus a mobile app when sharing sensitive information, believing the difference to be important to their data's security.

Another story emerges around social media. Baby Boomers (55+) are quick to say they restrict their social media use in order to avoid exposing personal information. However, Facebook's user data shows that people over 55 tend to be heavy users of the platform and baby boomers register the highest growth in adoption of Instagram and WhatsApp.[vi]

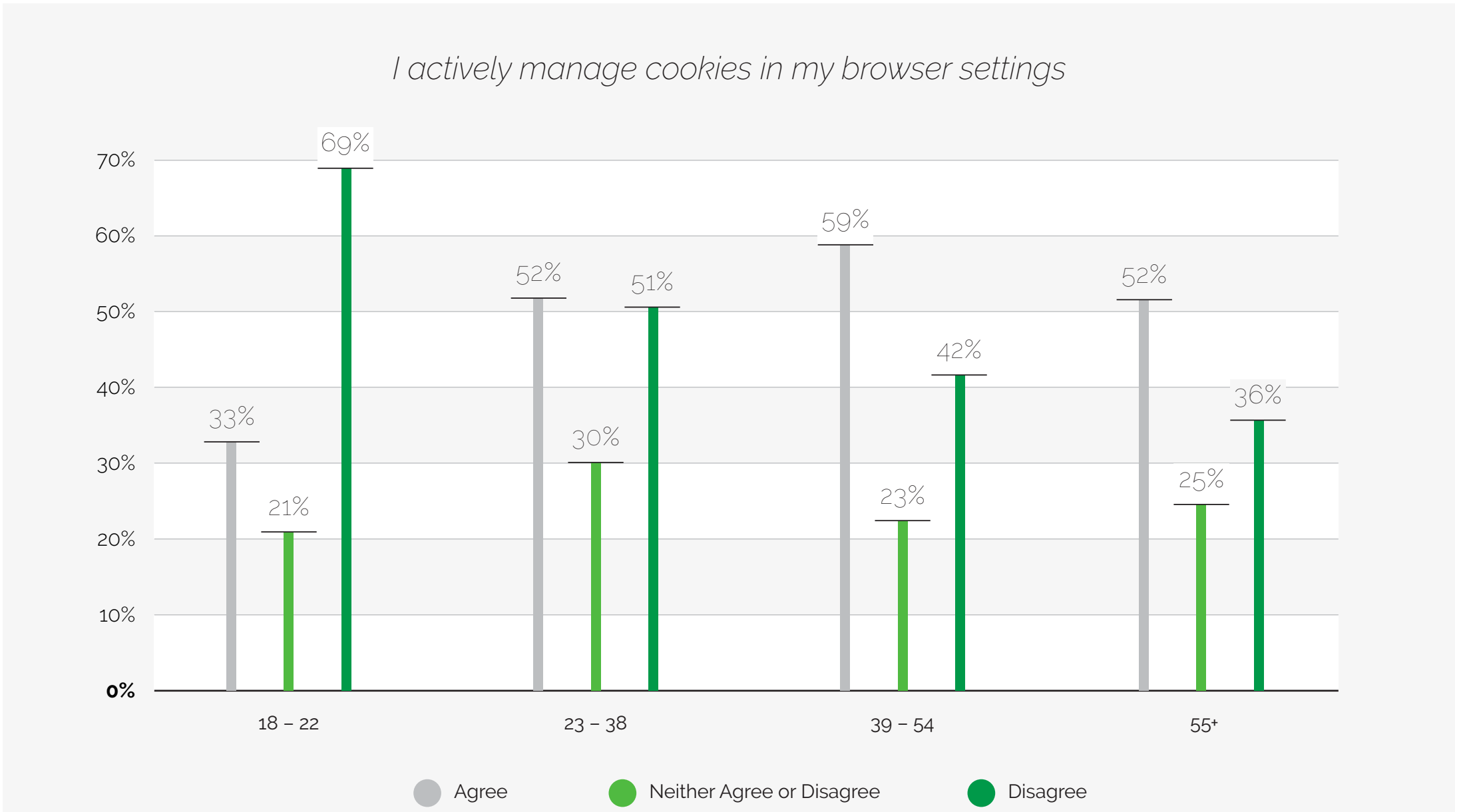
More than half of respondents say they restrict social media use for privacy reasons.

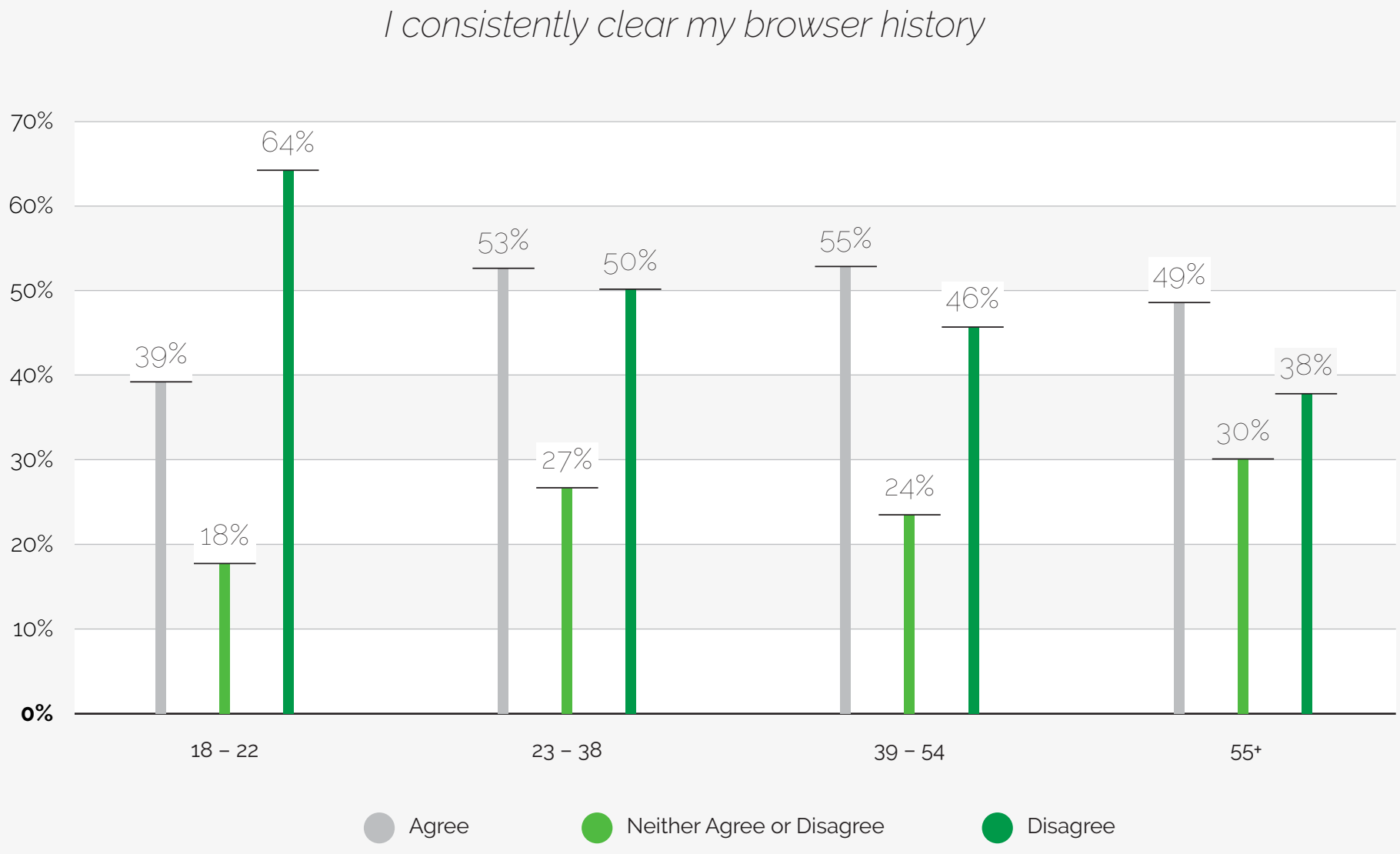
I'm more careful when using my desktop computer vs. a mobile or app-based program to share sensitive information



In addition, respondents, particularly older groups, say they are taking more action to protect their data by managing, disabling, and clearing browser cookies.

A greater proportion of older respondents say they are taking action by clearing their browser history and cookies.

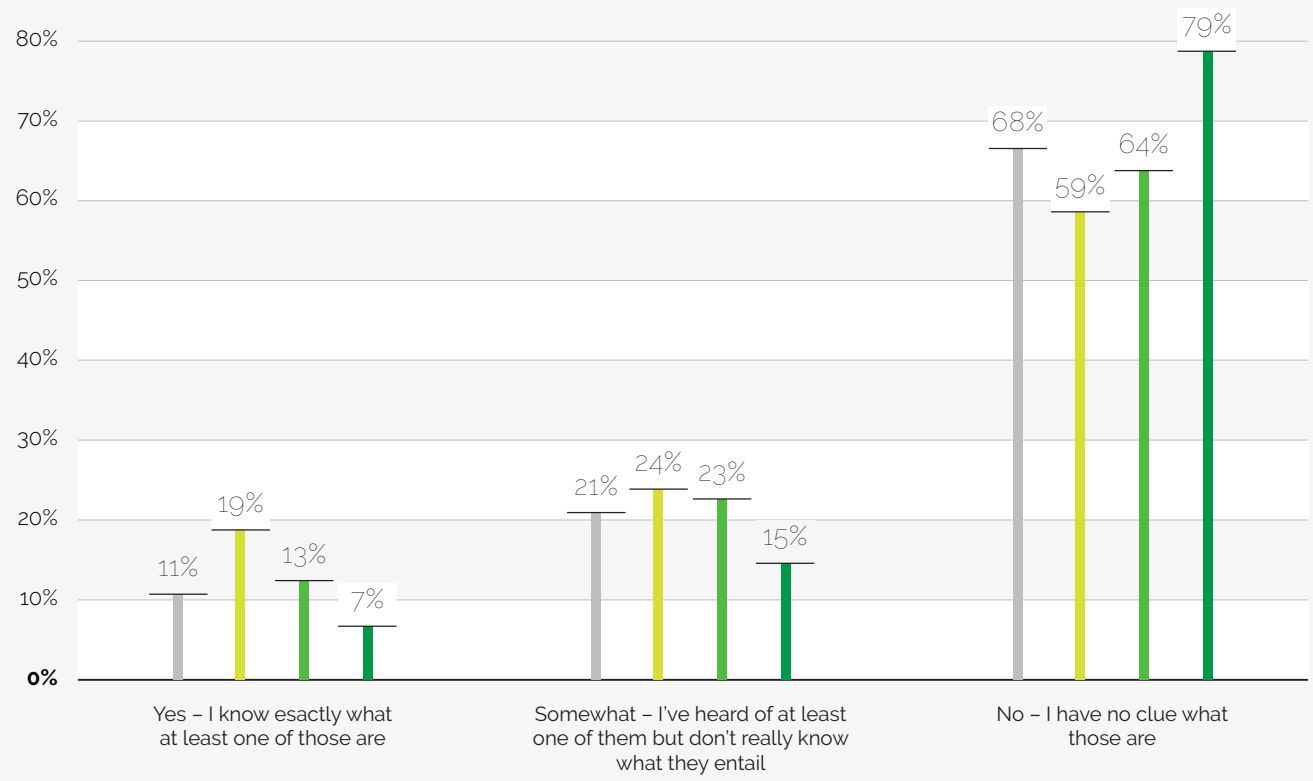




Even as they make new efforts to protect their privacy, consumers could do more to learn about their privacy rights, including the upcoming California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). As it stands, very few survey takers knew about these regulations.

The majority of respondents, particularly among older age groups, have no knowledge or understanding of data protection legislation.

As it relates to data security, do you know what CCPA or GDPR is

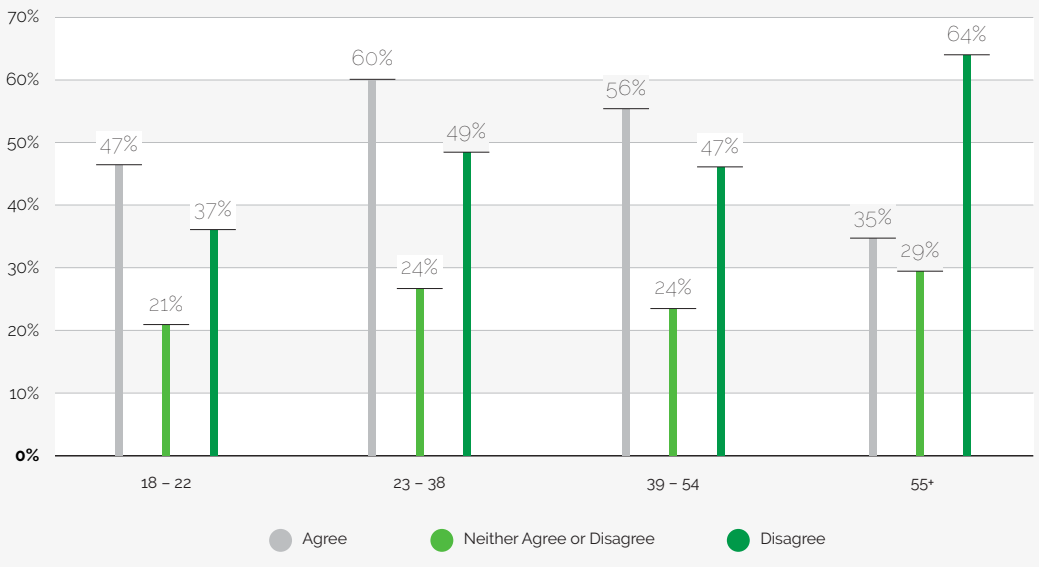


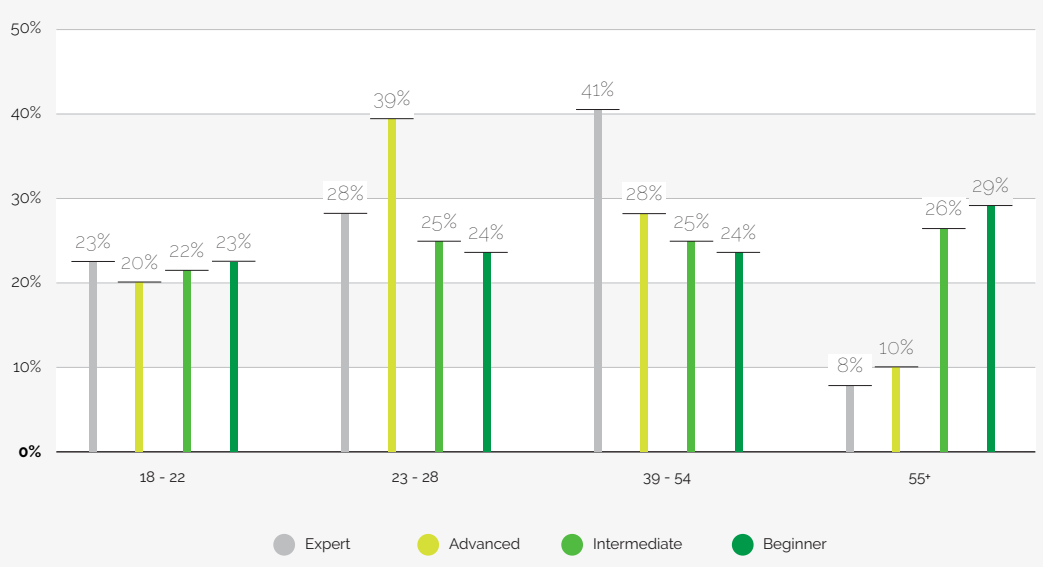
Although most people are taking more action to protect their data than they used to, they don't necessarily feel confident that their actions are effective. While younger survey takers are more likely to say they are confident in their ability to keep their data safe, few consider themselves experts.

So there's an opportunity for organizations to help consumers of all ages to keep their data secure. Even the more tech-savvy generations are looking for a hand.

Middle-aged survey respondents say they feel most confident, and most capable of protecting their data.

I have confidence in my ability to keep my data safe





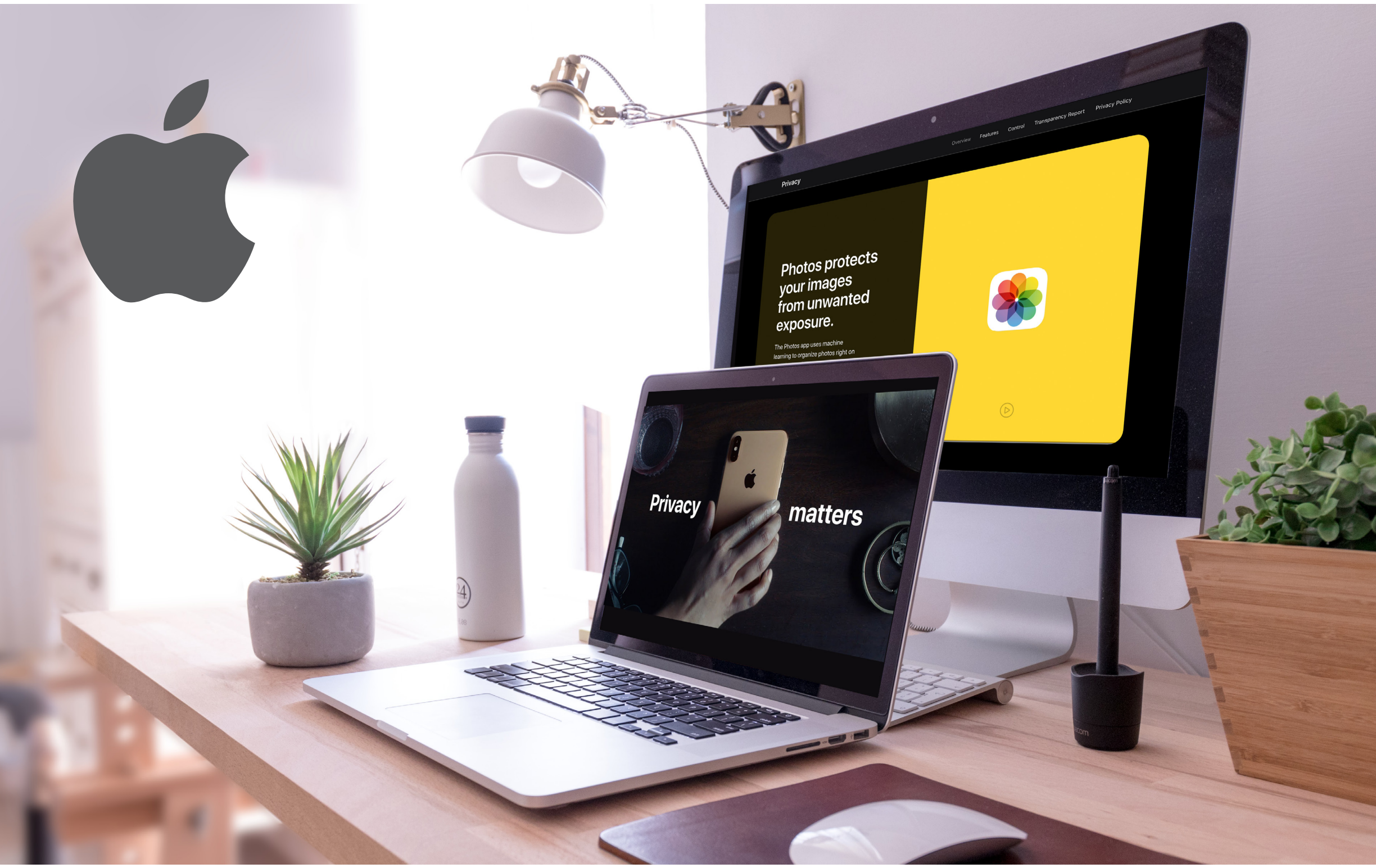
Turning insights into action

Adapt to changing consumer demands
Consumers of all ages are taking proactive measures to protect their data. Against this backdrop, hard-to-decipher privacy policies win no awards. Rather than hinder privacy-seeking users or ignore the trend altogether, savvy companies can make their commitment to data protection a selling point. Communications that are designed to put customers at ease, updated privacy policies that give consumers more control, and technologies that help keep identities and data safe (e.g., authentication tools), are powerful ways to create (or rebuild) trust.

Brand example: Apple

While Apple has been criticized for their secrecy and has faced criticism over data privacy and Siri recordings[vii], the tech brand is demonstrating that it's never too late to turn over a new leaf in consumer privacy.

Apple has made multiple changes over the past few years to adapt to increasing consumer demands for privacy. The brand introduced a new privacy portal at the end of 2018 that enables users to download all of the information Apple retains about them and/or delete their account data entirely. Their updated privacy pages also provide clear communication about how the brand protects consumer data. Apple also launched an iPhone campaign highlighting consumer privacy with the tagline: "If privacy matters in your life, it should matter to the phone your life is on."

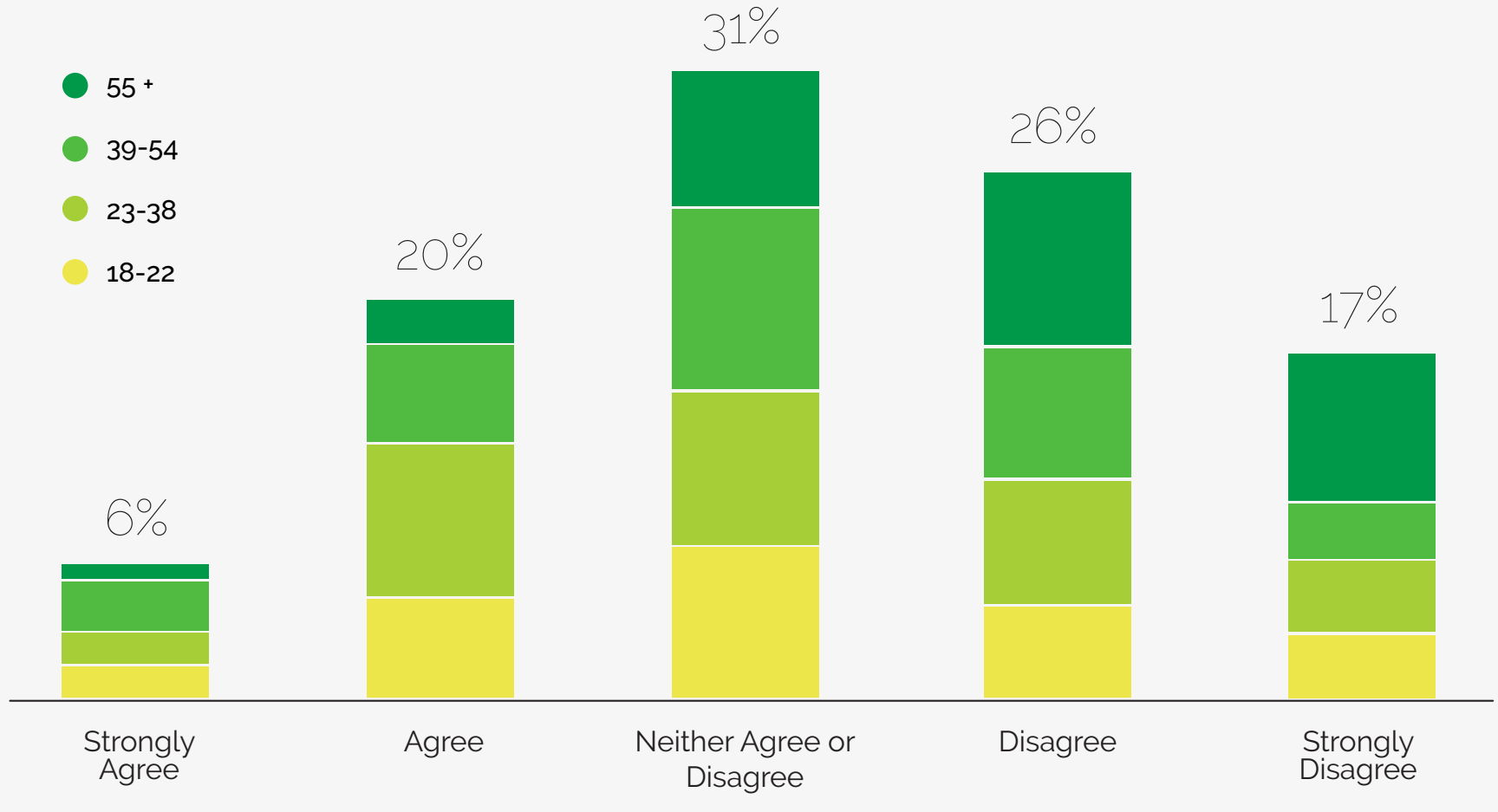


Section 6: Seeking value for data

The ease with which consumers once traded personal data for tangible benefits increasingly conflicts with consumer anxiety over privacy. High-profile data breaches and heightened awareness of unethical data uses, such as the Cambridge Analytica scandal, have lowered people's tolerance for risk.

Older generations are less comfortable with newer technology services than their younger counterparts, but they are not completely turned-off to the idea.

I am happy to trade personal information for a tangible benefit (e.g. a deal, free gift, special offer)



Increasingly, users want to know that the value they receive for sharing their data will outweigh the risk of that data being compromised. As consumers increasingly prioritize privacy and security, they will select their digital services with greater care.

Turning insights into action

Provide REAL value to customers
Marketers should shift their data collection practices to cater more to the consumer than to their marketing programs. Companies can avoid reputational harm from data collection by clearly communicating both the value they offer consumers in exchange for their information and the ways they use that information.

Brand example: General Motors

GM's OnStar system uses wireless technology to capture data directly from each vehicle to detect abnormalities, provide routine maintenance reminders, and improve customer experience.[viii] OnStar collects data on location and driving behavior to provide roadside assistance, safety and vehicle alerts (exceeding speed limits, hard-braking events, car battery draining), and trip insights. Consumers are willing to trust GM with this type of data in exchange for peace of mind.

Conclusion

Our survey suggests that if consumers of all ages had greater trust that companies would protect their data, they would engage with brands more intelligently and more often. As consumers continue to expect more privacy protection, companies may rise and fall based on their ability to earn and retain trust. Brands can start building trust right away by focusing on transparency, disclosure, and user control, and by addressing the concerns of each generation.

Key Takeaways

- Consumers are focusing on data security, now more than ever
- Consumers want to reap the benefits of personalization in marketing, but are wary of how brands obtain and use their data
- Consumers trust traditional industries the most
- Consumers of all ages prioritize protecting their data, even when they are happy to trade personal data for convenience and an enhanced experience

About the survey

Infogroup used SurveyMonkey to conduct a national survey of 1,072 people in September 2019. The age breakdown is as follows:

18-22	23-38	39-54	55+	Prefer not to say
236 respondents	285 respondents	274 respondents	261 respondents	16 respondents

[i] https://www.pwc.com/gx/en/news-room/press-releases/2018/organisations-are-not-doing-enough-to-protect-data-privacy.html

[ii] https://insights.reputationinstitute.com/reptrak-reports/why-tech-is-not-only-a-matter-of-innovation

[iii] https://msrc-blog.microsoft.com/2020/01/22/access-misconfiguration-for-customer-support-database/

[iv] https://www.helpnetsecurity.com/2019/03/13/data-management-challenges/

[v] https://econsultancy.com/why-trust-transparency-are-crucial-components-of-brand-success/

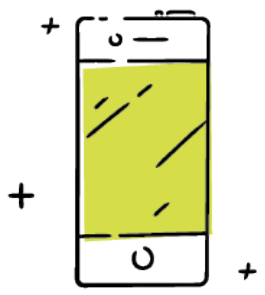
[vi] https://www.weforum.org/agenda/2019/10/social-media-use-by-generation/

[vii] https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings

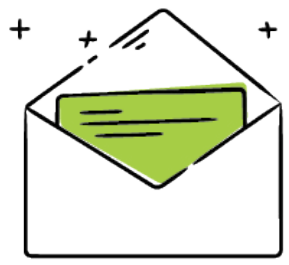
[viii] http://customerthink.com/big-data-the-key-to-delivering-value-to-customers/

Was this content helpful?

Yes | Somewhat | No



Phone
1.877.937.6245



Email
marketing@yesmarketing.com

Website
yesmarketing.com