



Aleo

2024

Data privacy report

# Table of contents

Biographies	3
Bringing ZK to the masses <small>John Reynolds, Head of Product</small>	4
The perception of privacy is improving <small>Brennen Schlueter, CMO</small>	6
There's an appetite for privacy-focused solutions <small>Leena Im, Head of Global Policy and CSO   Aleo Ventures</small>	8
About Aleo + Acknowledgements	10

# Biographies

**John Reynolds**  
Head of Product

John Reynolds oversees Product for the Aleo Network Foundation. He has a diverse background encompassing years of experience as a cybersecurity professional. After over three years in the United States Air Force as a Cyber Operations Officer, he gained an understanding of the need to safeguard autonomous systems apart from central authorities, while simultaneously upholding privacy and fostering accountability.

**Brennen Schlueter**  
CMO

Brennen Schlueter is the Chief Marketing Officer at the Aleo Network Foundation. Before joining Aleo, Brennen led marketing at a Web3 project and spent a decade developing brands at advertising agencies like Wieden + Kennedy, Laundry Service, and TBWA\Chiat\Day.

**Leena Im**  
Head of Global Policy and CSO, Aleo Ventures

Leena Im is the Head of Policy at the Aleo Network Foundation, and CSO of Aleo Ventures. Prior to Aleo, she was at Meta as the Director of Strategy and Operations for the payments and commerce team. Previously, she was the Head of Payments and Blockchain policy at Meta and part of CFPB's startup years. Leena was a Fulbright Scholar in Indonesia and a UC Berkeley grad.

## Methodology

This survey was conducted between October 17th-20th, 2023 among a national sample of 2,217 adults. The interviews were conducted online and data was weighted to approximate a target sample based on gender, educational attainment, age, race, and region.

Results from the full survey have a margin of error of +/-2 percentage points.

# Bringing ZK to the masses

By John Reynolds, Head of Product

## Key data \*

- 67% of consumers indicated that they would definitely or probably switch to a product if there was an option to use a technology solution that was built with a focus on protecting data.
- Most people are willing to switch platforms/products should there be an incident where their data is exposed.
- Most people do not feel as though they have control over their data.

\* This data and all other information this report are from a survey commissioned by Aleo and conducted by Morning Consult

## Aleo's Analysis

Our research has found that sixty-seven percent of consumers are willing to switch to a product if it includes a data protection technology option. This number reflects something we knew anecdotally: People are increasingly worried about who controls their personal data. They want to protect their privacy from data brokers and large technology companies, highlighting the need for consumers to have choices.

While some customers are satisfied with their existing digital services, these services' privacy limitations are widely recognized. The growing awareness of potential digital risks is prompting even those who are content with their current setups to seek out alternatives that offer enhanced protection, but this isn't surprising. With the media covering data breaches, leaks, hacks, scams, and ransomware more extensively than ever, these risks are top-of-mind for the public.

### Data points

67%

Answered yes, if there were an option to use a technology solution that was built with the focus of protecting data, they would make the switch.

12%

Answered no, if there were an option to use a technology solution that was built with the focus of protecting data, they would not make the switch.

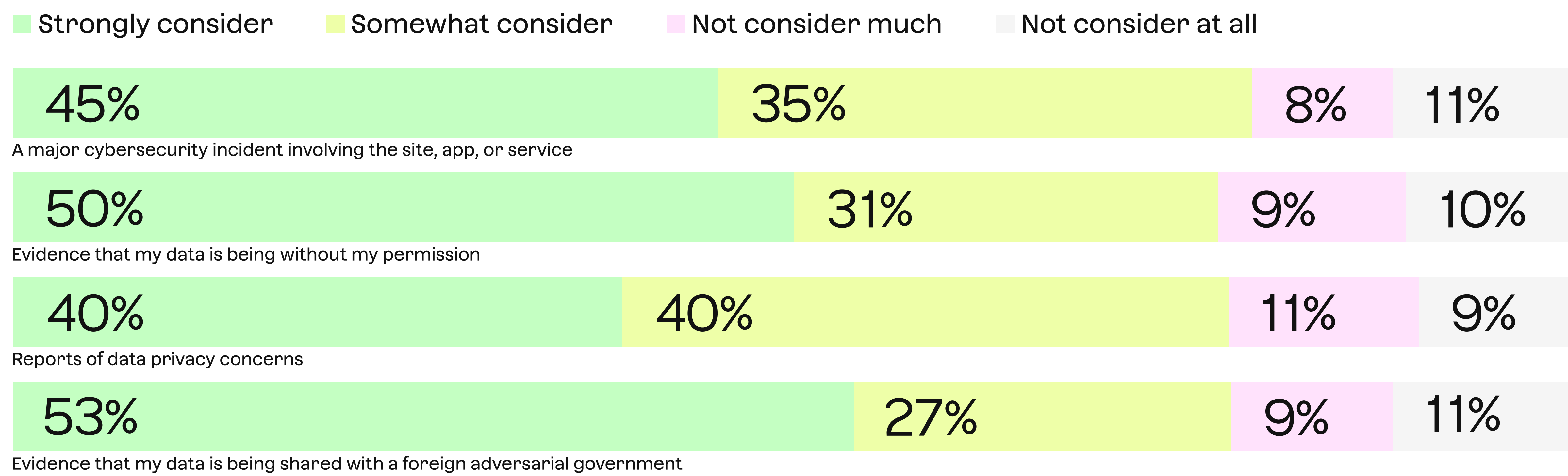
21%

Answered that they did not know or had no opinion on the matter.

Consumer sentiment is influenced by more than just news. Advertising for digital products that promise improved data security, increased awareness from global privacy laws like GDPR, and personal experiences have made people take privacy-focused solutions more seriously. This shift in consumer attitudes and behavior indicates a larger trend where the value of online privacy and security is increasingly recognized not as a luxury — but a fundamental right. As a result, companies that place a premium on protecting user data are gaining traction, marking a significant pivot in market dynamics towards privacy as a key differentiator.

### Event-based switching consideration

Survey participants were asked: If any of the following events occurred with an app, website, or social media service you use, to what extent would you consider switching to a new product?



The rise of privacy-centric platforms and services is a response to this changing landscape, where the demand for secure, transparent, and user-respecting alternatives is at an all-time high. This trend is expected to accelerate, with ZK technology offering promising avenues for enhancing privacy without compromising user experience. In this environment, Aleo aims to foster a platform that prioritizes privacy and security without sacrificing usability or accessibility. This aligns with the growing public demand for more secure digital experiences.

As digital technology becomes even more embedded in our daily lives, the call for user privacy and security becomes increasingly urgent. Companies and technologies that can address these concerns, offering robust solutions that protect user data by design, will not only lead the next wave of innovation but also rebuild trust in the digital ecosystem.

# The perception of privacy is improving

By Brennen Schlueter, CMO

## Key data

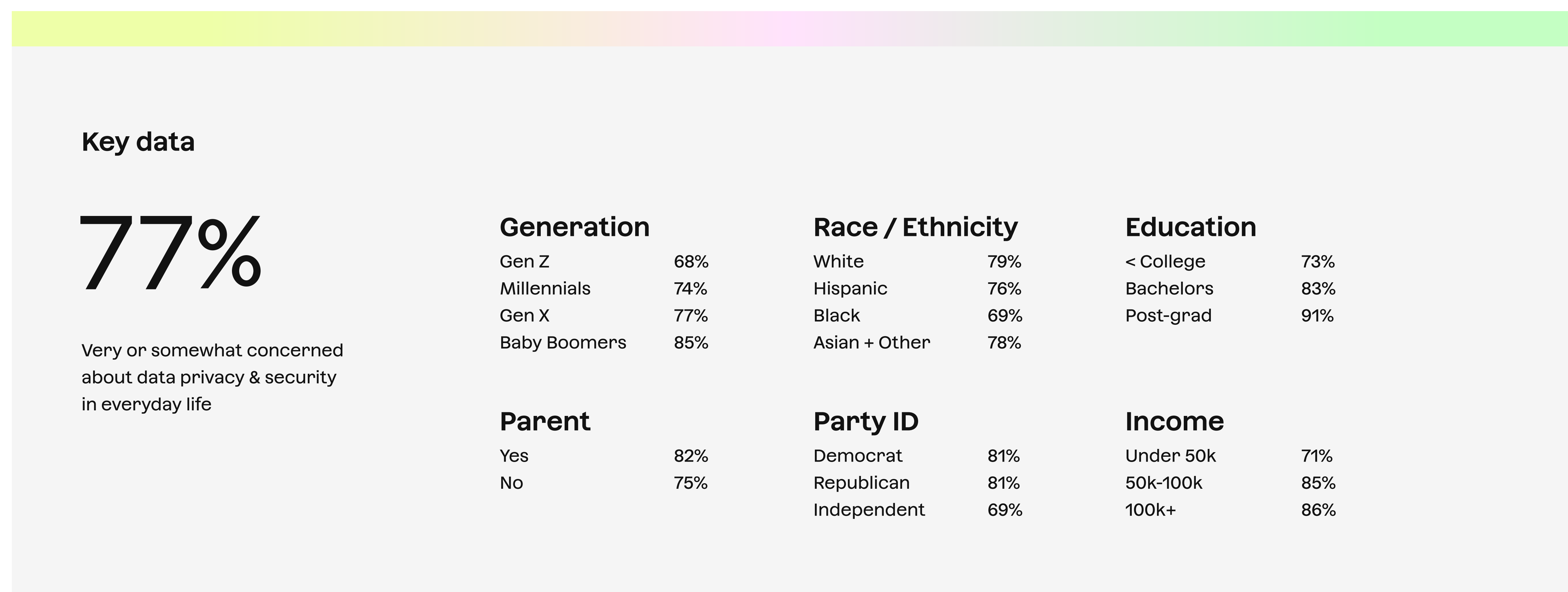
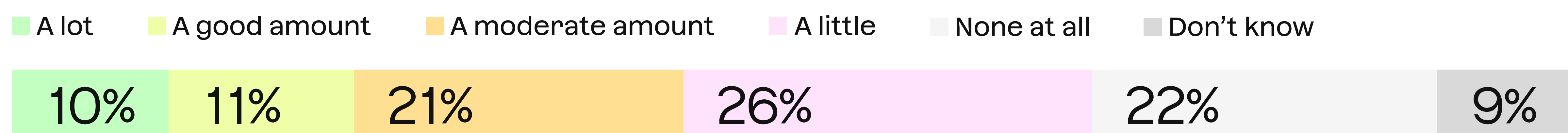
- Cryptocurrency companies are among the least trusted with regards to data privacy and security, with only 10% of respondents expressing a great deal of trust and 14% a fair amount.
- Concern about data privacy among different generations is as follows: Gen Z (68%), Millennials (74%), Gen X (77%), Baby Boomers (85%).
- Data privacy and security are considered the most concerning issues within the technology industry today, with 48% of respondents indicating it as a top concern.

## Aleo's analysis

Cryptocurrency companies encountered notable challenges to user trust in 2023. Only 10% of survey participants in our research voiced confidence in the industry's dedication to data privacy and security. The apprehension is particularly pronounced amongst older generations, incrementally increasing from GenZ to Baby Boomers, but regardless is seen as an issue for people of any age or background.

## Perceived individual control over customer data usage

Survey participants were asked: How much control, if any, do you feel you have over how tech companies use customer data they collect from you?



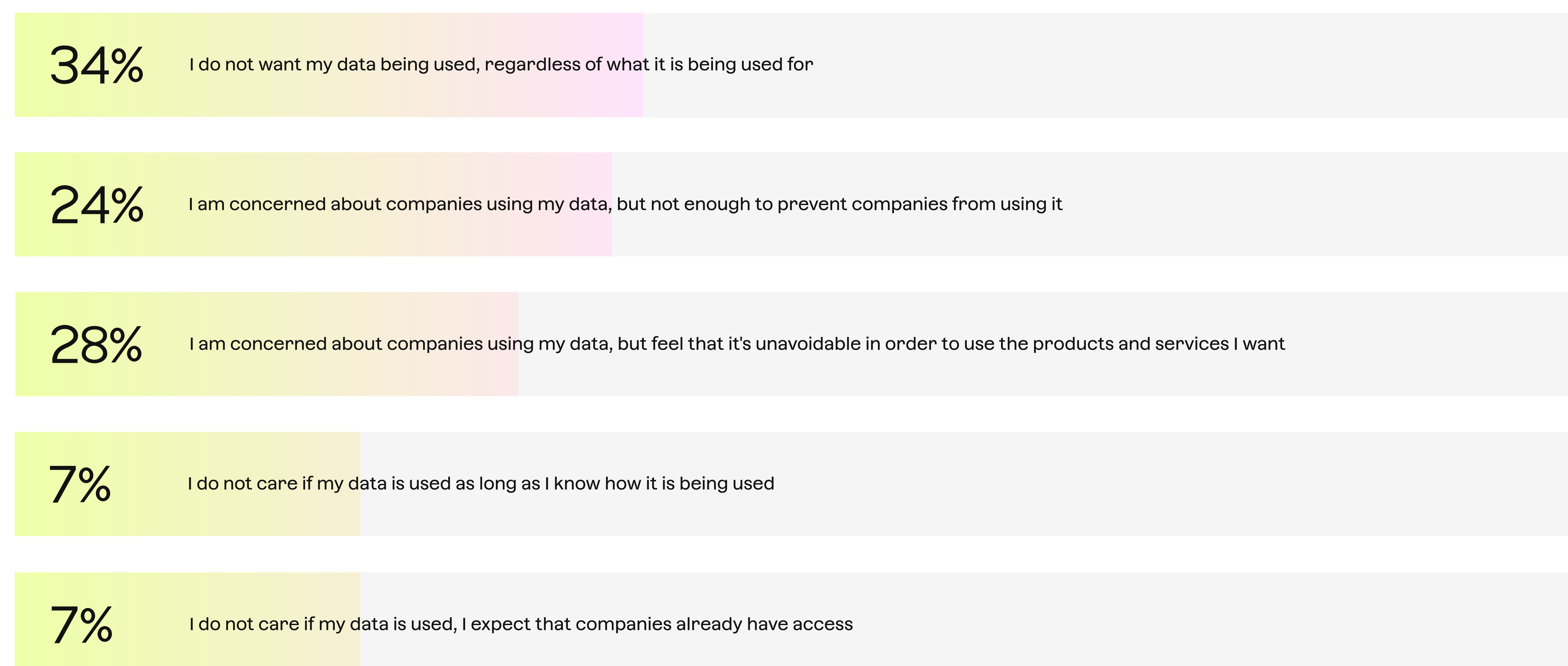
While evident in the Web3 space, data privacy and security concerns have plagued legacy Web2 technology companies, with nearly half of the surveyed respondents identifying privacy as their top worry. This concern is a reflection of the enduring dominance of Web2 products, which often offer only temporary fixes to privacy issues that arise, and a growing disappointment with blockchain technologies, which are sometimes perceived as speculative ventures rather than real-world solutions.

These numbers underscore the urgent need to rebuild faith through innovative solutions that prioritize user privacy. The expectation for retail and enterprise applications crafted with a privacy-first approach will become standard, with less tolerance for exceptions. With Aleo and other's efforts, 2024 will be remembered as the year when privacy became the cornerstone of innovation and user trust in the digital world. Simply put, privacy has gone from something users hope for to something they demand.

Few adults have a laissez-faire attitude towards data privacy; most are concerned about how their data is used, despite feeling like they have less control.

### Views on data privacy and security

Survey participants were asked: Which of the following statements fits best with your views on data privacy and security?



As we brace for this change, Aleo's upcoming mainnet launch stands at the forefront of digital privacy transformation. Enabling a new era of privacy-centric, permissionless, and easily programmable applications, Aleo will unlock scalable innovation with user trust front and center. By leveraging zero-knowledge proofs, Aleo uses cutting-edge cryptographic technology called zero-knowledge (ZK) to ensure transactions are verified without revealing any underlying sensitive information. This approach enables a level of privacy and security unmatched by traditional systems, allowing for the creation of digital applications that protect user data by design, ensuring only the necessary information is shared and nothing more.

The transition to a core expectation will ensure that the next generation of the internet won't simply repeat the mistakes of its predecessors but will pave the way for a future where privacy and security are embedded into the fabric of digital interactions, transforming how we engage with technology at every level.

# There's an appetite for privacy-focused solutions

By Leena Im, Head of Global Policy and CSO | Aleo Ventures

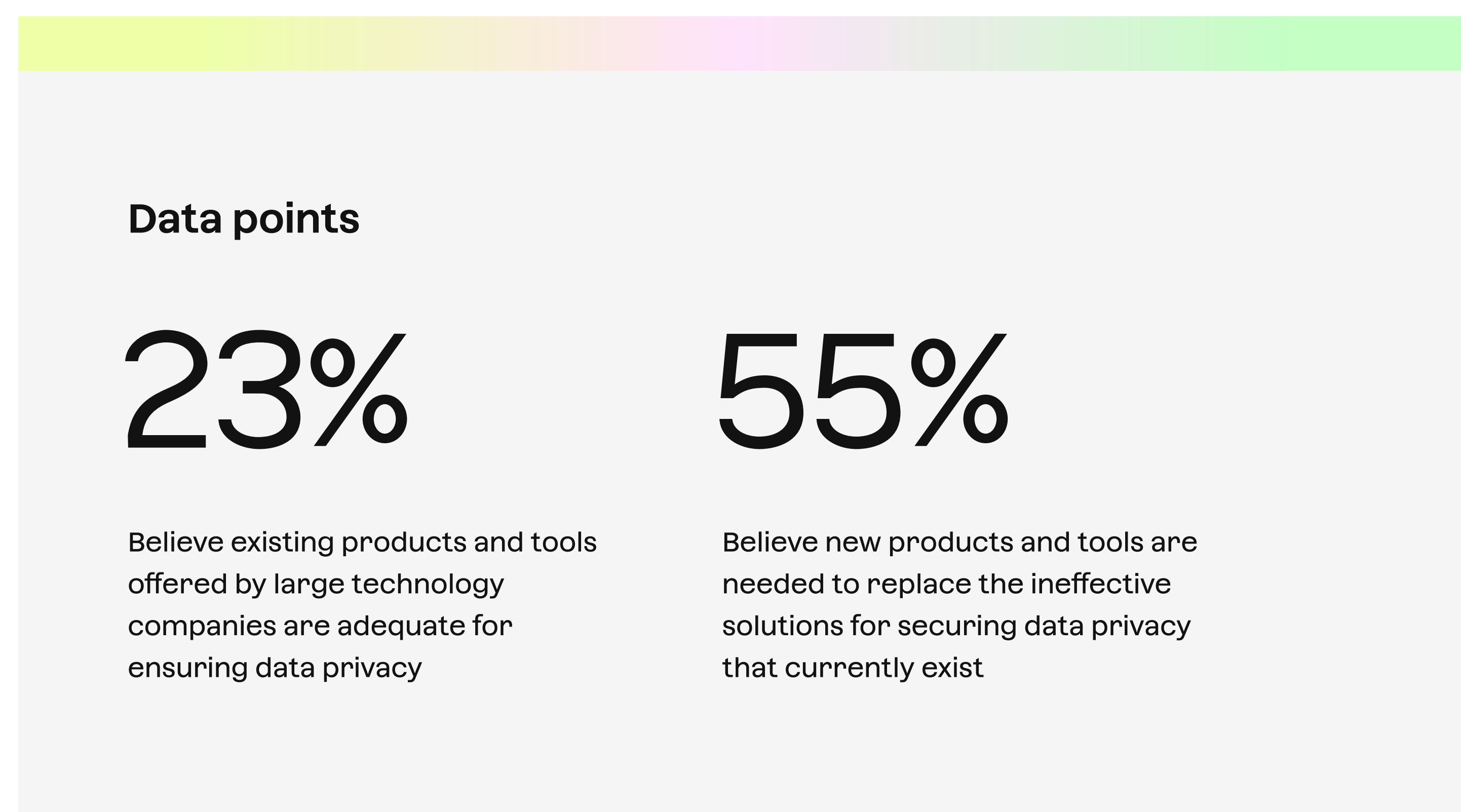
## Key Data

- 23% of respondents believe that existing products and tools offered by large tech companies are “adequate” for ensuring data privacy.
- 53% of those surveyed considered data privacy and security as a baseline expectation; having little influence on whether or not they think better of them for having these protections.
- 55% of respondents believe new products and tools are needed to replace existing, ineffective solutions for securing data privacy.
- Most people aren't familiar with technology companies' data collection processes.

## Aleo's analysis

2023 was a significant year for digital privacy, underscoring a persistent concern among users about their data privacy yet acknowledging a feeling of helplessness in effecting change. Despite the year passing with incremental privacy advancements, it presents an unmistakable opportunity to challenge and ultimately transform the privacy paradox — one where individuals express concerns over privacy yet continue to use services that compromise it.

This paradox persists. The current digital ecosystem is ripe for disruption by-products that prioritize privacy, signaling a pressing need for innovation in this space.

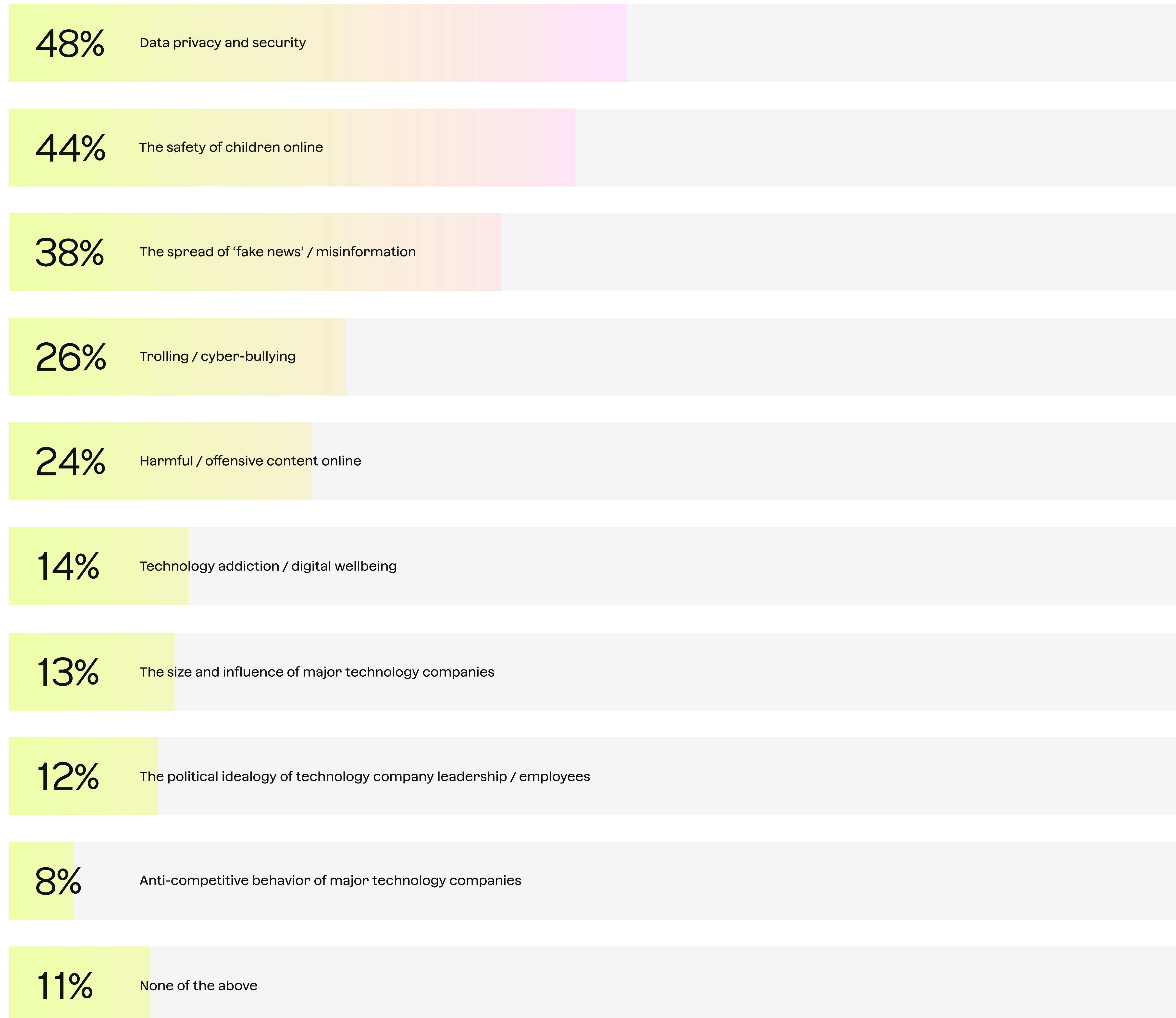


Regulatory developments are expected to be pivotal in shaping the privacy landscape. As regulators understand the nuanced threats and potential benefits associated with digital privacy, there will be a clearer distinction between harmful practices and those that genuinely enhance privacy. This understanding will likely lead to a regulatory environment that fosters the growth of privacy-focused technologies and products, offering them as viable alternatives to current market offerings. As such, 2024 promises to be a year where privacy moves from an afterthought to a central feature of digital products, driven by consumer demand, technological innovation, and supportive regulatory frameworks.



### Most concerning issues facing the technology industry

Data privacy is considered the most concerning issue facing the technology industry today.



Looking ahead, the focus will likely shift towards creating solutions that address tangible privacy issues, moving beyond theoretical discussions to practical applications in everyday life. The emphasis will be on developing products that solve real-world problems, such as enhancing age verification processes, streamlining Know Your Customer (KYC) procedures, and offering more effective ways to safeguard personal data. Blockchain technology, while crucial, will become an underlying layer rather than the main talking point, allowing the spotlight to shine on the solutions it enables rather than the technology itself. This shift will encourage a broader exploration of privacy-enhancing technologies, with tools like zero-knowledge proofs and platforms like Aleo leading the charge in introducing innovative products that strengthen privacy.

# About Aleo + Acknowledgements

## About the Aleo Network Foundation

Launched in January 2024, the Aleo Network Foundation aims to play an essential role in nurturing and supporting the Aleo Network's growing and decentralized open-source ecosystem. It focuses on promoting the use and adoption of zero-knowledge cryptography to empower and protect individuals and create new opportunities for developers to build products and services for the next-generation web. We're not just building technology — we're rebooting the internet.

## Acknowledgments

This survey was conducted with Morning Consult, a global decision intelligence company that specializes in online survey research technology. This report would not have been possible without their contributions.

## Contact us

Learn more about the Aleo Network Foundation by visiting [aleo.org](https://aleo.org), or reach out to us at [hello@aleo.org](mailto:hello@aleo.org)

For press inquiries, please contact [press@aleo.org](mailto:press@aleo.org)

Unless otherwise noted as a survey result, statements made in this report are based on Aleo's analysis and opinions of key takeaways from the survey.

# Aleo