

Privacy Front & Center

Meeting the Commercial Opportunity
to Support Consumers Rights



OMIDYAR
NETWORK

Fall 2020

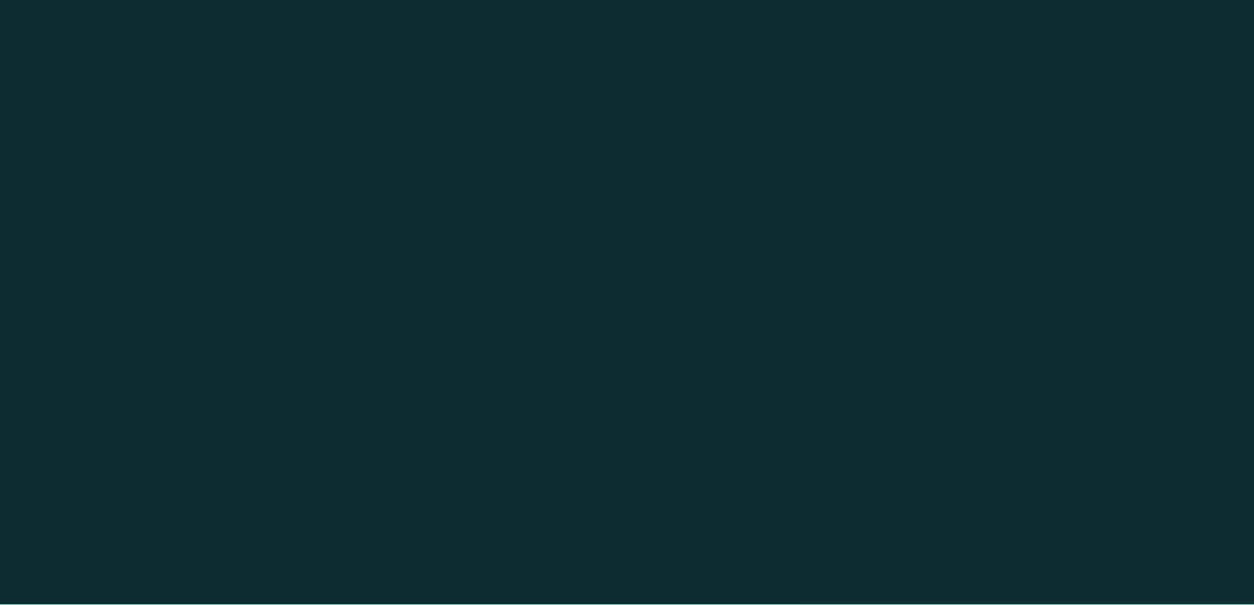
Consumer Reports in collaboration
with Omidyar Network

Contents

- 03 Section 1: Introduction
- 14 Section 2: The Evolution of Consumer Attitudes Around Data Privacy
- 34 Section 3: Consumer Attitudes Today
- 51 Section 4: Quantifying Consumer Preference
- 61 Section 5: Moving Toward a Market for Privacy
- 67 Appendix & Further Reading

Authors & Acknowledgements

This report was authored by Benjamin Moskowitz, Stephanie Nguyen, Michael Cohen, and Ginny Fahs. It is based on a literature review conducted by Justin Brookman and Katie McInnis; survey research and data analysis conducted by Kristen Purcell, Karen Jaffe, Debra Kalensky, Charu Ahuja, Monica Liriano, Michael Saccucci, Dina Haner, Kristen Dorrell, Nish Suvarnakar, Dirk Klingner and Amit Bhan. Thanks to Magdi Amin, Geoffrey MacDougall, Jesús Salas, Sarah Drinkwater, Shannon Miller, Elizabeth M. Renieris, and others for feedback and contributions to this report.



SECTION 1

Introduction

Privacy is what happens behind the scenes

privacy | 'prīvəsē |

noun

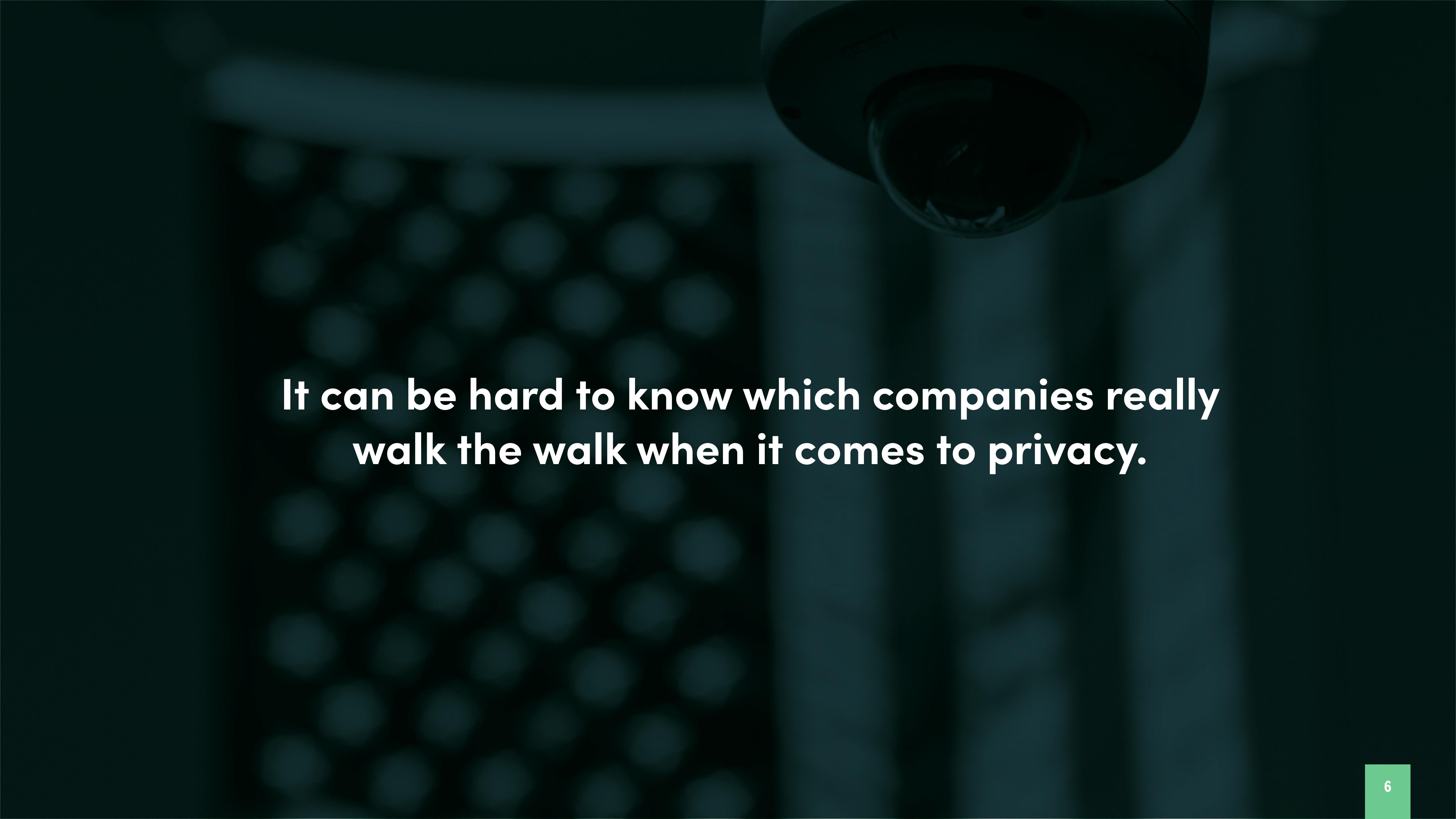
the state of being free from public attention

So it's natural that companies handle privacy privately

Privacy features are not typically marketed

Privacy tactics are usually kept secret

Companies say they care about privacy...but what does this mean?



**It can be hard to know which companies really
walk the walk when it comes to privacy.**



Yet the evidence shows that consumers increasingly care about their privacy.

And when companies compete on things that consumers care about – whether price, features, safety, or privacy – **everyone wins**.

This is what drives us at Consumer Reports

We exist to drive better outcomes for consumers by ensuring a fair, just, and high-functioning marketplace.

In a high-functioning marketplace, companies compete to win consumers along dimensions like price, performance, and features. We've been helping consumers choose on this basis since 1936.

Consumers increasingly demand that their products are private, secure, and treat them fairly



So Consumer Reports and Omidyar Network teamed up to examine evolving consumer attitudes toward privacy and quantify privacy's market impact.

Benefits exist for companies who compete and differentiate on privacy

**Historically, privacy has been seen as a liability.
Focusing on privacy means limiting downside risk.**

However, evidence suggests that technology companies focused on privacy and security will see significant upside.

The upside comes from **higher regard for brand** and **higher willingness to pay**.

A word about “willingness to pay”

Our goal is **not** to turn the right of privacy into a luxury good out of reach, but rather to harness competitive dynamics to raise privacy and data security standards.

However, we are interested in whether differentiation could be an opportunity for first-movers to capture market share or increase short-term willingness to pay.

Over time, we expect many privacy and data security features to become “table stakes” in which case first movers will innovate and raise standards further.

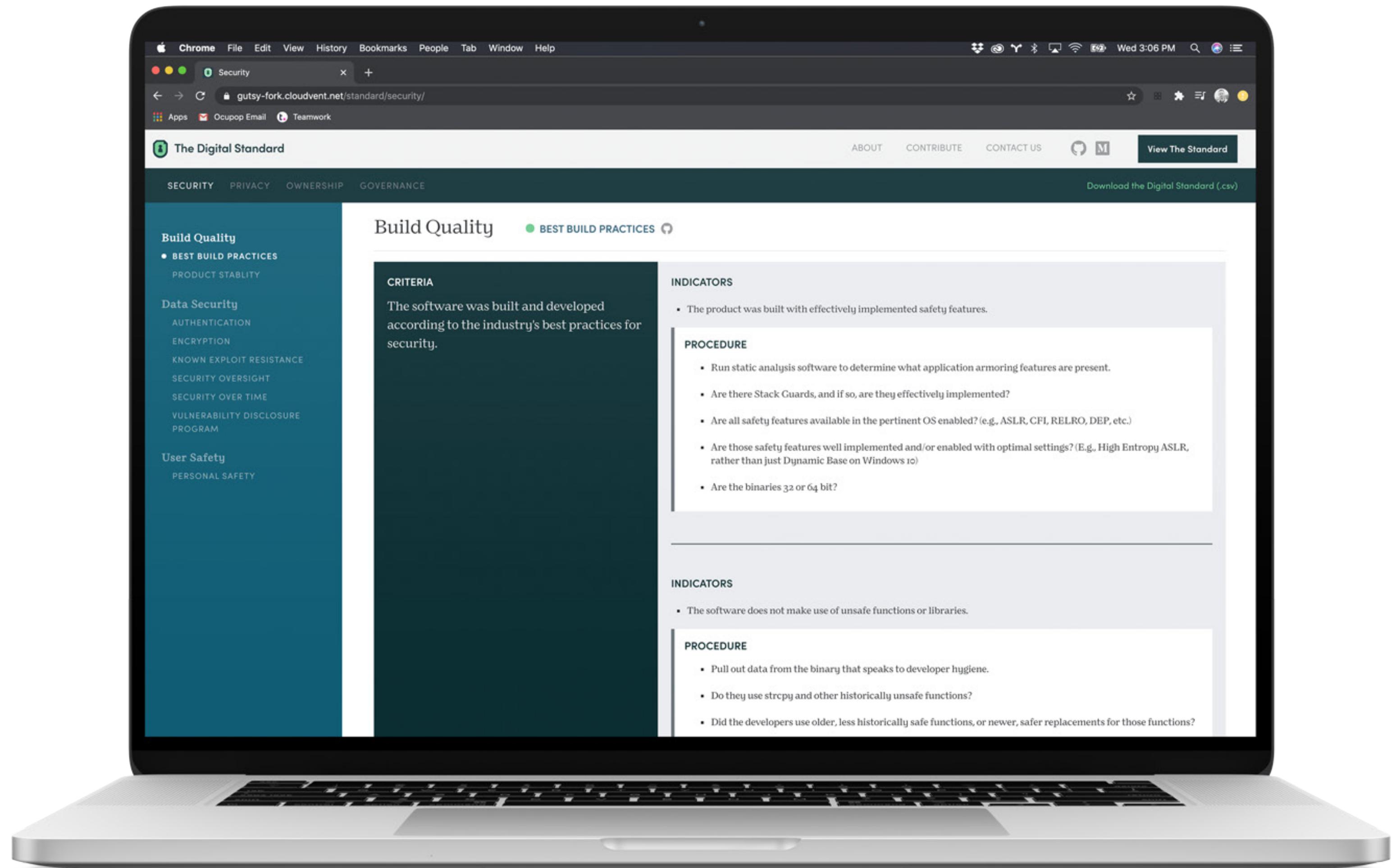


The
Digital
Standard

**Companies can use
The Digital Standard to
implement privacy in
product and service design,
among other values**

The Standard is

- A rubric articulating best practices in **security, privacy, ownership, and governance**
- An open source consensus reflecting expert viewpoints
- A way companies can prove their commitment to consumer values
- A roadmap to more secure products and higher favor with consumers



The evidence suggests real business impact when companies put privacy front and center

Trends are clear when we look at:

The history of consumer trends and demand for privacy and data security

How and when privacy and security inform consumers' purchasing behavior

How much consumers say they're willing to pay for better protection



SECTION 2

The evolution of consumer attitudes around data privacy

“Some have concluded that our society, quite simply, does not place much value on privacy.”

(Rubin and Lenard 2002)

**Has less privacy truly become
the new social norm over time?**

Consumers' privacy preferences are commonly misunderstood

MISCONCEPTION 1

"Consumers don't really care about privacy; the benefits of sharing & personalization outweigh the risks."

Privacy is not the opposite of sharing personal information; rather, it is control over sharing.

There are real benefits to sharing data, but consumers consistently report feeling a lack of agency and control over their data.

According to a recent Pew survey, just 9% of people believe they have "a lot of control" over the information that is collected about them, even as 74% say "it is very important to be in control."

MISCONCEPTION 2

"Consumers say they care about privacy, but their actual behaviors suggest privacy doesn't matter very much."

Privacy is highly contextual and involves a complex set of trade-offs that can mix tangible, intangible, and abstract qualities.

Privacy attitudes and privacy behavior are grouped too often.

These misconceptions conceal significant opportunities for companies to better meet consumers' values and preferences.

CR did a meta analysis to chart trends in public attitudes over 25 years:

1995–2004

Cautious Users

Early internet adopters

2005–2010

Confident Users

Wider adoption

2011–2015

Concerned Users

Growing awareness of tracking, privacy

2016–

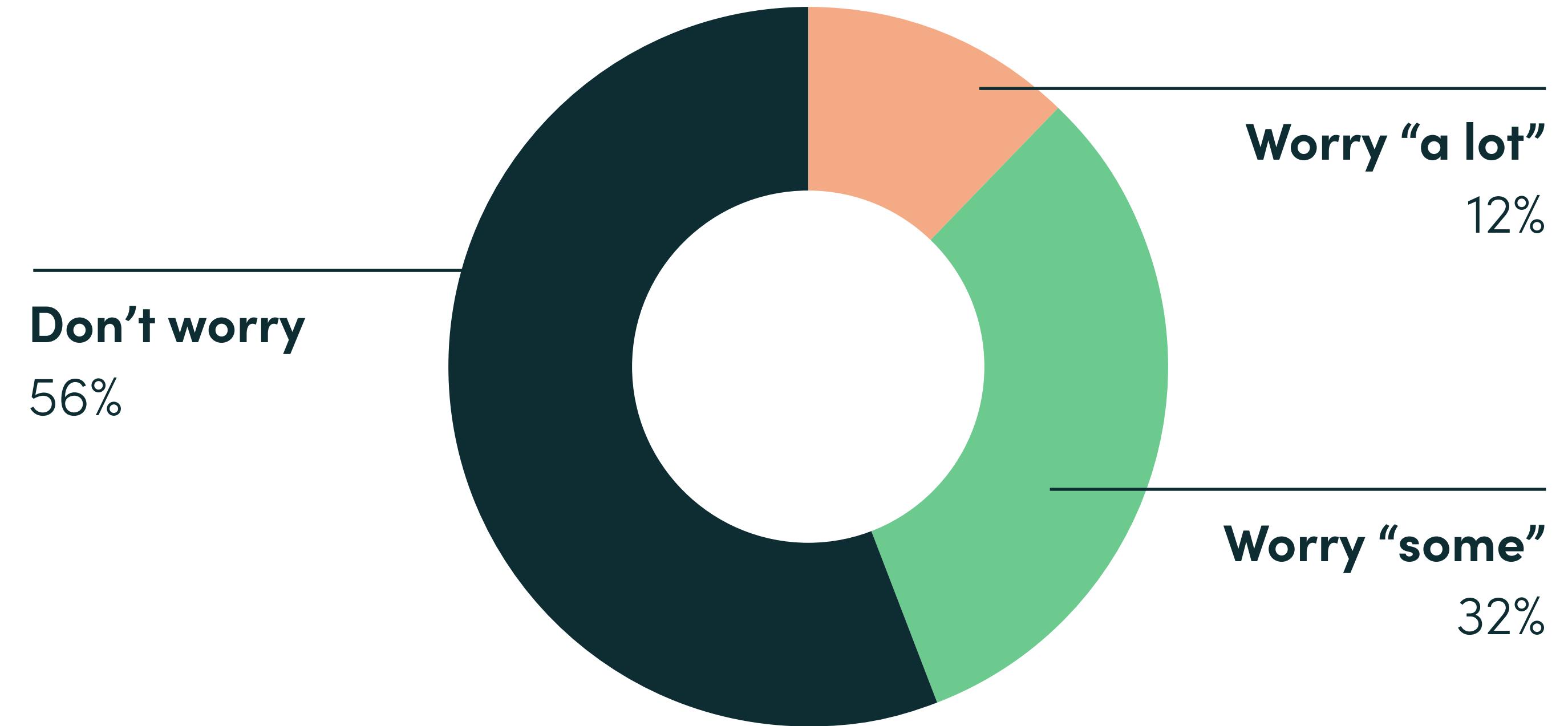
Critical Users

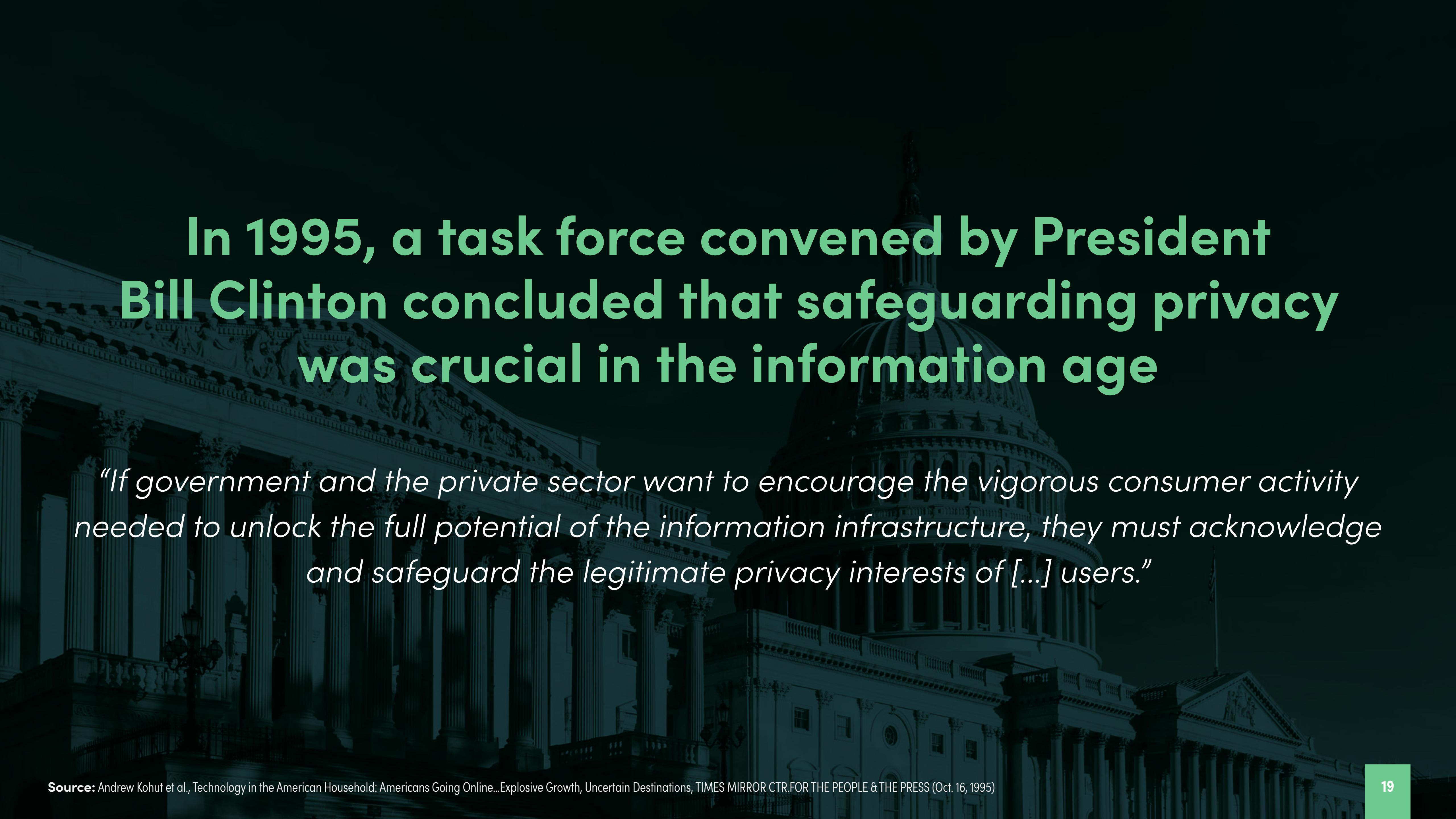
Consumer awareness leading to distrust

In 1995 when the internet was young, consumers were already worried about the impacts of technology on privacy

Fear of Internet Privacy Loss in 1995 Among Online Users

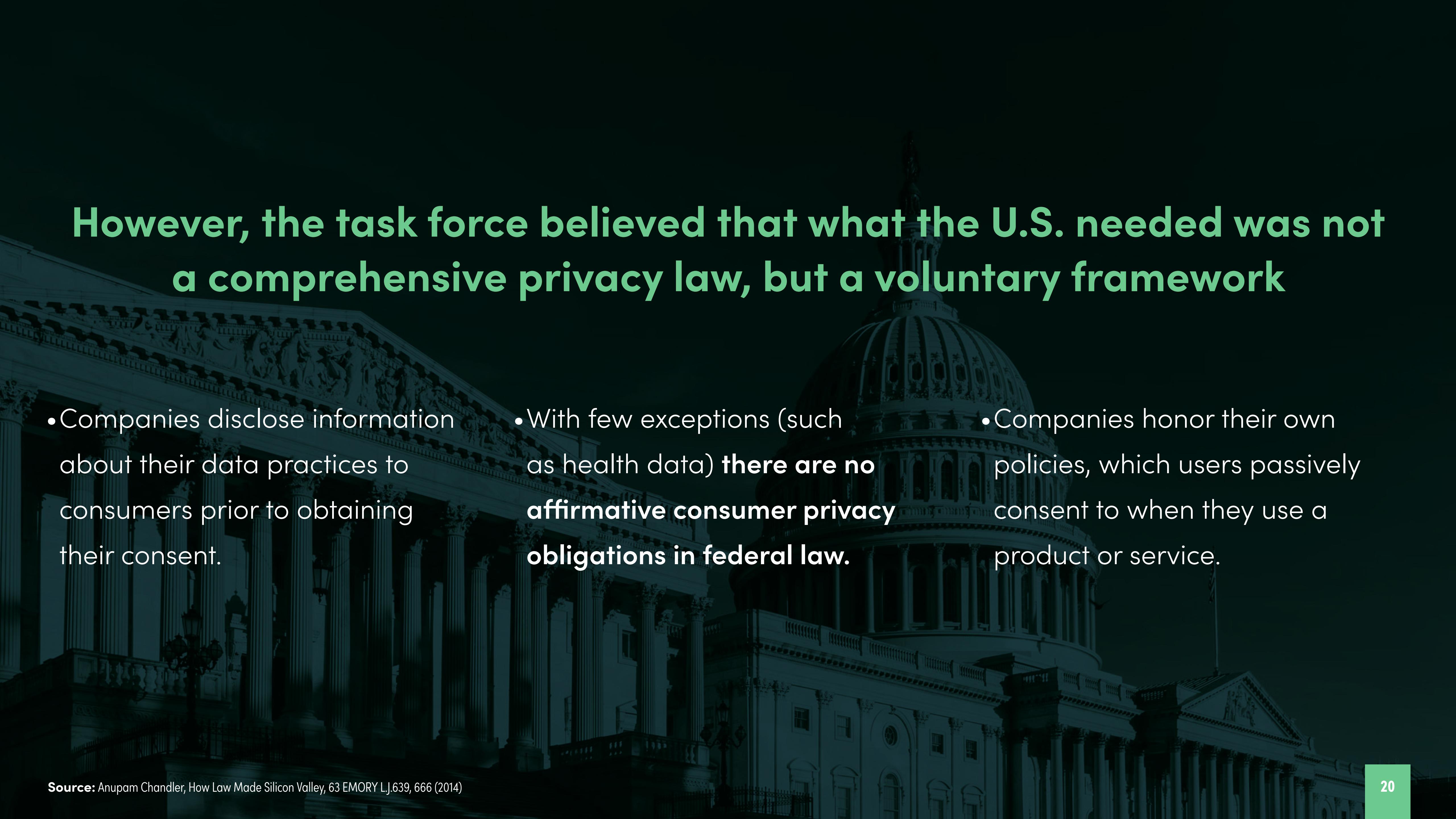
Almost half of online users worried “a lot” or “some” about loss of privacy.





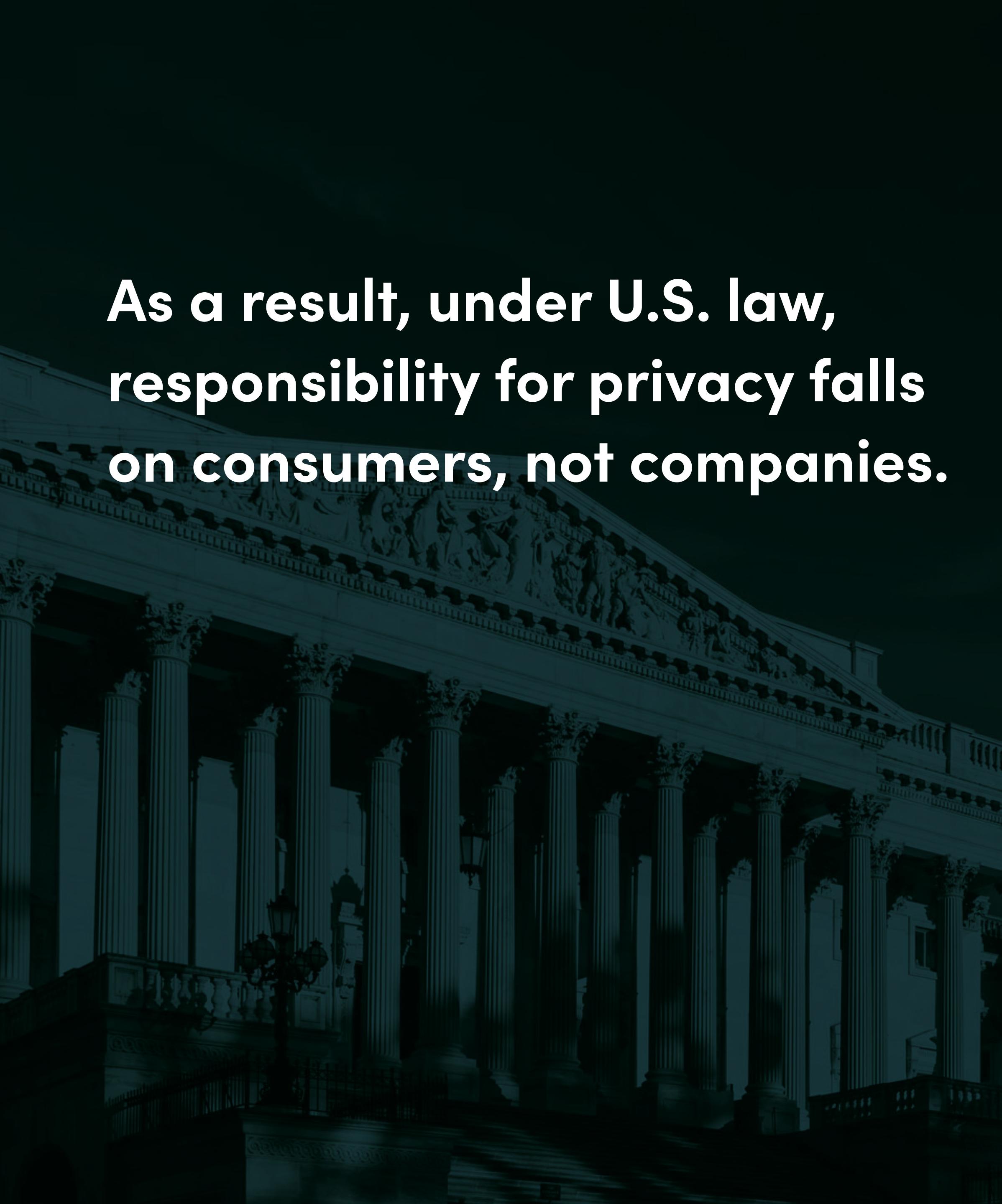
In 1995, a task force convened by President Bill Clinton concluded that safeguarding privacy was crucial in the information age

"If government and the private sector want to encourage the vigorous consumer activity needed to unlock the full potential of the information infrastructure, they must acknowledge and safeguard the legitimate privacy interests of [...] users."



However, the task force believed that what the U.S. needed was not a comprehensive privacy law, but a voluntary framework

- Companies disclose information about their data practices to consumers prior to obtaining their consent.
- With few exceptions (such as health data) **there are no affirmative consumer privacy obligations in federal law.**
- Companies honor their own policies, which users passively consent to when they use a product or service.



**As a result, under U.S. law,
responsibility for privacy falls
on consumers, not companies.**

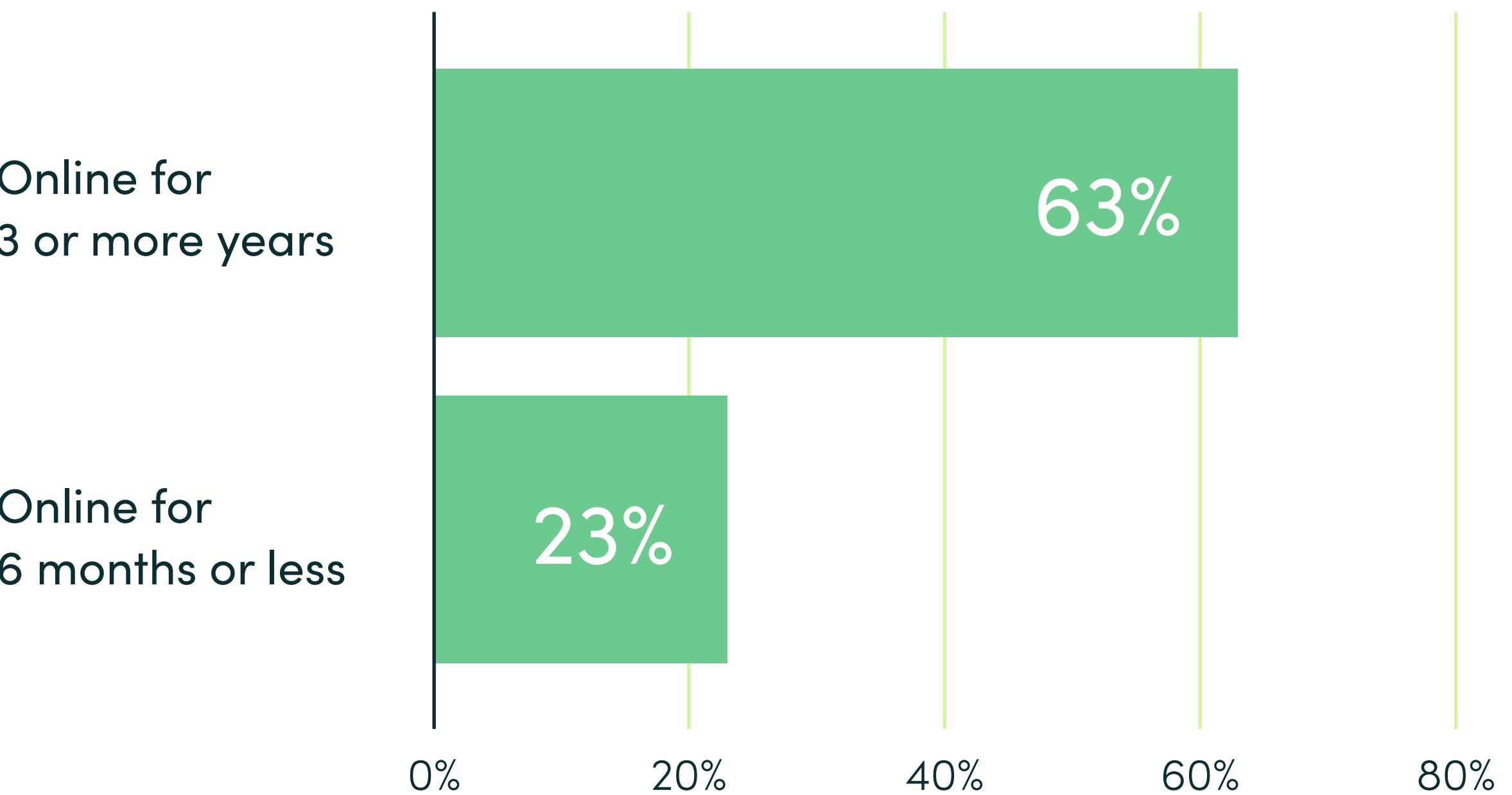
**To this day, the U.S. does not have a
comprehensive consumer privacy law.**

Practically it is almost impossible for consumers to fully consent to data collection and usage when they cannot keep pace with how advertisers, data brokers, and edge providers collect and leverage their data.

In the early 2000s, Americans demonstrated a growing awareness of tracking and data sharing and more than half of them were online

- 49% of consumers knew about cookies as a device for online tracking in 2002.
- Knowledge of cookies grew with maturity of internet use.
- In a 2002 survey, 76% of participants said they were uncomfortable with a company connecting data from internet cookies to email addresses in a targeted email campaign.

Knowledge of Cookies Based on Internet Use



Yet they still underestimated the lack of protection for their online activities, and the potential privacy and security risks

94% felt

“I have a legal right to know everything that a web site knows about me.”

57% believed

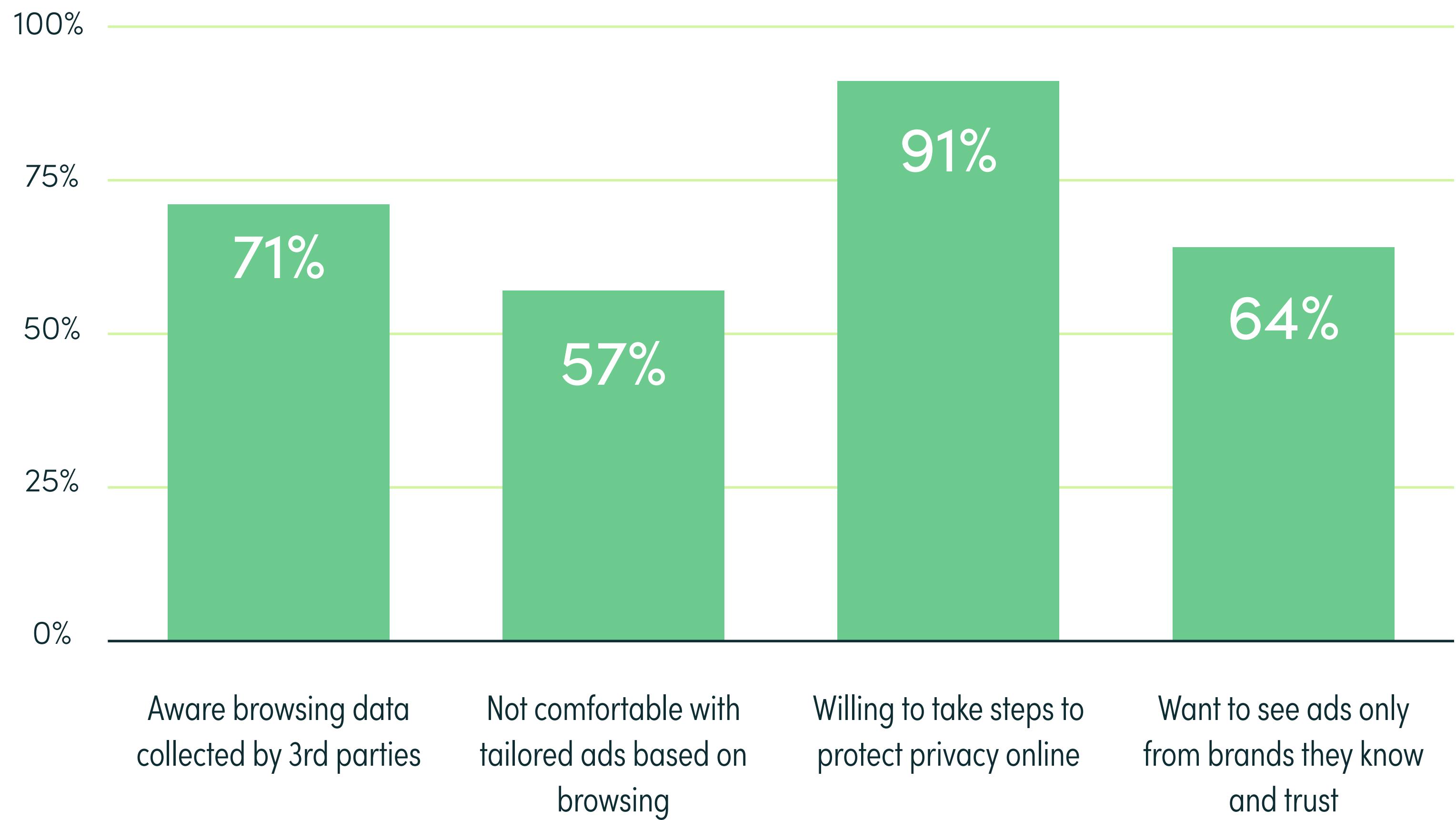
that if a company has a privacy policy, the company will not share information with other entities.

59% did not know

that websites collected information about them even without a registration requirement on the site.

**By 2008,
consumers'
knowledge of
online tracking
had grown again...**

Consumer Awareness and Attitudes About Behavioral Targeting



...but so had the sophistication of the online data sharing ecosystem

SEPTEMBER 2006

Facebook News Feed

Three days after releasing the feature, Facebook introduced privacy controls in response to public outcry.

JULY 2007

30M Facebook Users

More than half of all teens aged 12-17 had a social media profile.
66% of them limited access to their profile in some way.

NOVEMBER 2007

Facebook Beacon

Sent data from external sites to Facebook for targeting advertisements
Earlier in 2007, Facebook had changed its privacy policy to allow collecting information about users without their consent. Opt-out was no longer an option.

MARCH 2008

DoubleClick merger approved by FTC

Search information gathered by Google combined with browsing information gathered by DoubleClick paved the way for richer data sources that enabled highly targeted advertising

Source: Amanda Lenhart & Mary Madden, Social Networking Websites and Teens, PEW RESEARCH CTR.(Jan. 7, 2007); Amanda Lenhart & Mary Madden, Teens, Privacy, and Online Social Networks, PEW RESEARCH CTR.(Apr. 18, 2007); Bernhard Debatin et al.,Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences, 15 J.OF COMPUTER-MEDIATED COMM'C83, 83-108 (Oct. 2009); Andrew Romano, Facebook's 'News Feed', NEWSWEEK(Sept. 24, 2006; danah boyd, Facebook's Privacy Trainwreck, 14 CONVERGENCE13, 13-20 (Feb. 1, 2008); Vauhini Vara, Facebook's Tracking of User Activity Riles Privacy Advocates, Members, WALL ST.J.(Nov. 21, 2007; This org.known as the Digital Trust Foundation - operated from 2014-2019.

In the early 2010s, consumers saw a darker side of data sharing

2010

Julia Angwin revealed numerous ways companies track and mine information from consumers in her “What They Know” series

2013

Edward Snowden revelations made U.S. consumers more worried about being tracked by their government.

22% of adults said they had changed their tech usage patterns either “a great deal” or “somewhat” after the Snowden revelations.

Source: What They Know Series, JULIA ANGWIN; Julia Angwin & Tom McGinty, Sites Feed Personal Details to New Tracking Industry, WALL ST.J.(July 30, 2010); Emily Steel & Julia Angwin, On the Web’s Cutting Edge, Anonymity in Name Only, WALL ST.J.; Julia Angwin & Jennifer Valentino-DeVries, Race is on to ‘Fingerprint’ Phones, PCs, WALL ST.J.; What They Know: The Business of Tracking You on the Internet, WALL ST.J.; Public Perceptions of Privacy and Security in the Post-Snowden Era, PEW RESEARCH CTR.(Nov. 12, 2014); Lee Rainie & Mary Madden, Americans’ Privacy Strategies Post-Snowden, PEW RESEARCH CTR.

By 2016–2019, greater consumer awareness of tracking had spawned significant distrust

46%

of American consumers
believe their personal
information is less secure now
than it was 5 years ago

66%

of American consumers
do not trust the government to
protect consumers' interests

65%

of American consumers
say they are slightly or not at
all confident that personal
data is private

A slew of data breaches and scandals then further eroded consumers' expectation that their information could be kept safe and private



SEPTEMBER 2017

Equifax Data Breach

Revealed to have affected at least 148 million Americans.



MARCH 2018

Cambridge Analytica

Enabled the harvesting of private information from over 50M Facebook profiles without user permission



MARCH 2018

Marriott Data Breach

Exposed the data of 383M guests, including credit card, passport, email, phone, date of birth, and address

Source: Kaya Yurieff, Equifax Data Breach: What You Need to Know, CNN (Sept. 10, 2017); Equifax Data Breach Affected 2.4 Million More Consumers, CONSUMER REPORTS (Mar. 1, 2018); Cybele Weisser, Equifax Data Breach Puts Spotlight on How Credit Agencies Work, CONSUMER REPORTS (Oct. 3, 2017); Matthew Rosenberg, Nicolas Confessore, & Carole Cadwalladr, How Trump Consultants Exploited the Facebook Data of Millions, N.Y.TIMES (Mar. 17, 2018); Andrew Perrin, Americans are Changing Their Relationship with Facebook, PEW RESEARCH CTR. (Sept. 5, 2018); Chris Isidore, Marriott Hasn't Paid the Price for its Massive Data Breach, CNN (May 10, 2019)

Regulatory interventions have already begun

- On January 1, 2020 the nation's first comprehensive commercial privacy law, the California Consumer Privacy Act (CCPA), went into effect.
- CCPA is overwhelmingly popular, with 88% of California voters in favor and just 5% opposed.
- Under the CCPA, California consumers can:
 - Require that their personal information not be sold by specific companies
 - Get a copy of information that specific companies have about them
 - Request the deletion of their personal information

CCPA is California-specific, but other US states are working on similar new laws and initiatives.

Data privacy can feel like an arms race between an increasingly sophisticated consumer and companies trying to stay one step ahead

- Although consumers have gained tech literacy over time, they need to do ever more to protect the privacy and the security of their data
- Ongoing high-profile privacy revelations contribute to a sense of consumer helplessness
- Consumers remain concerned about their privacy but lack knowledge or meaningful choices

Half of consumers believe it's "part and parcel" of being online that people will try to cheat or harm them in some way.

We're at a critical juncture for consumer privacy in the U.S.

- **Notice and consent** has enabled a situation where the privacy practices of many products have drifted far from consumers' preferences.
- Consumers have believed for decades that they have **more rights and protection** online than they do.
- The **techniques to protect** user privacy have remained the same since the late 90s.
- The majority of consumers today know they are **not in control** of their data.
- There is a significant gap between **consumer understanding** of tracking technology & the **means to control** it.

Concern about the power of big tech and frustration from privacy scandals are increasing demand for both **regulation** and **consumer privacy solutions**.

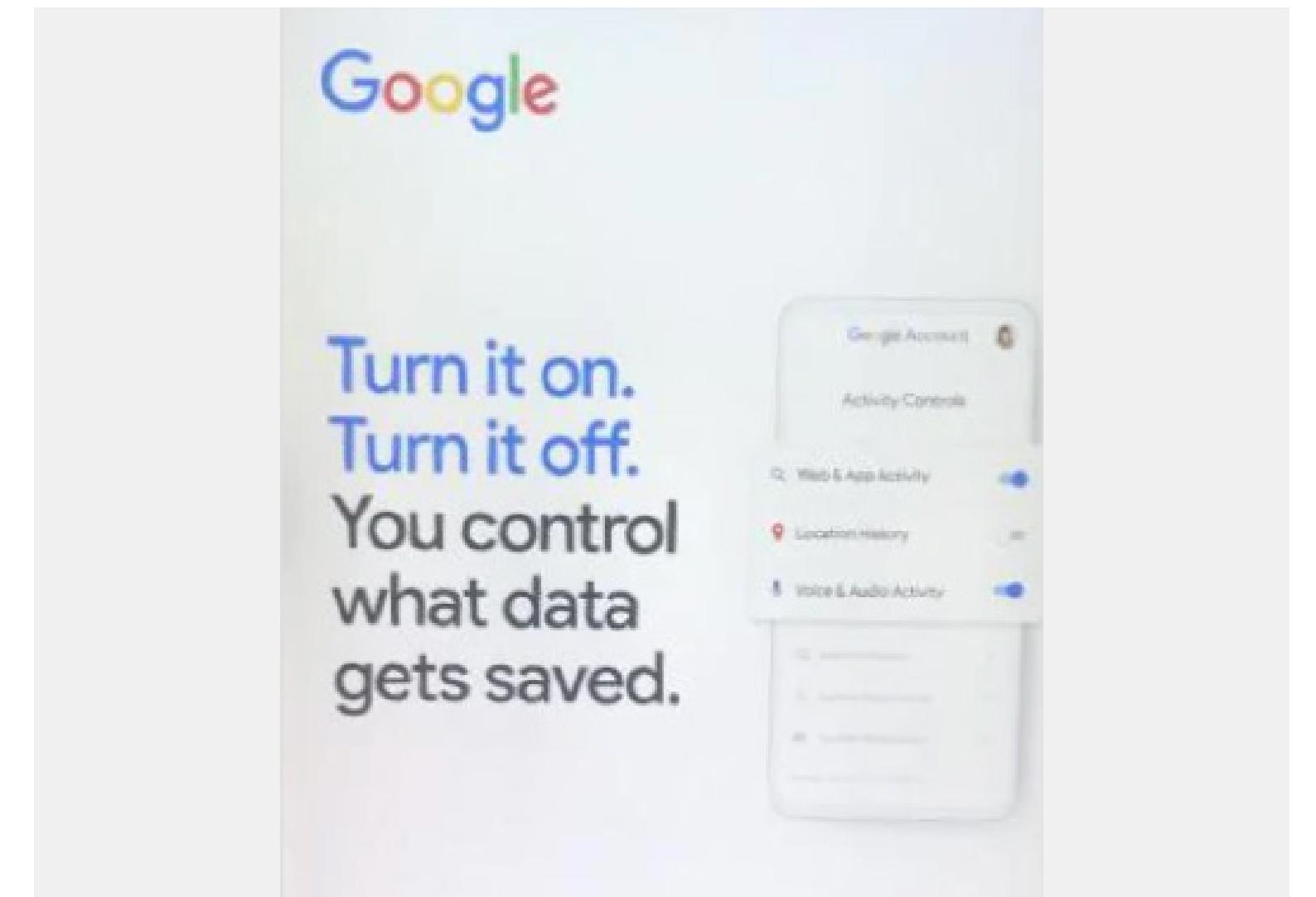
Marketing messages from big tech companies are starting to reflect consumers' privacy demands



Facebook CEO Mark Zuckerberg touting privacy features at April 2019 developer conference.



Apple iPhone privacy digital and billboard campaign, January 2019.



Google privacy settings print/billboard campaign, September 2019.



SECTION 3

Consumer Attitudes Today

**Nearly two thirds of smart product owners worry about loss of privacy
when buying them for their home or family**

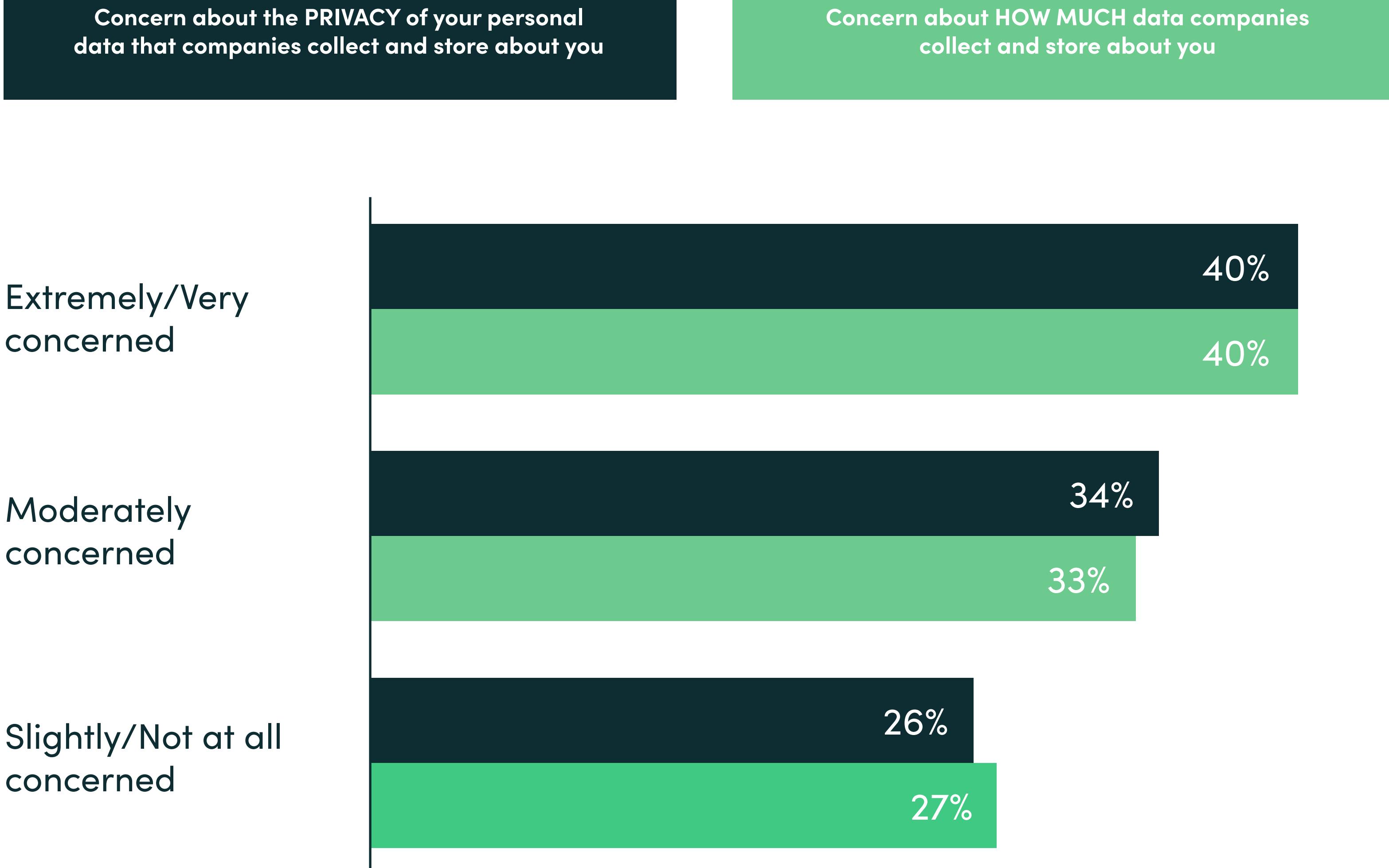
62% OF
SMART PRODUCT
OWNERS

said they worry about potential loss of
privacy when buying smart products

Three quarters of consumers are at least moderately concerned about the privacy of their personal data

Concern about how much data and about the privacy of personal data companies collect and store about you

Base: All respondents



96% of Americans agree that more should be done to ensure that companies protect the privacy of consumers

68% OF AMERICANS SAY...

Companies should be required to delete the data they have about you upon your request.

67% OF AMERICANS SAY...

There should be tougher penalties, such as high fines, for companies that don't protect your privacy.

64% OF AMERICANS SAY...

Companies should be prohibited from sharing data with third parties.

63% OF AMERICANS SAY...

Companies should be required to give you access to the data they have about you.

63% OF AMERICANS SAY...

There should be a national law that says companies must get your permission before they share your information.

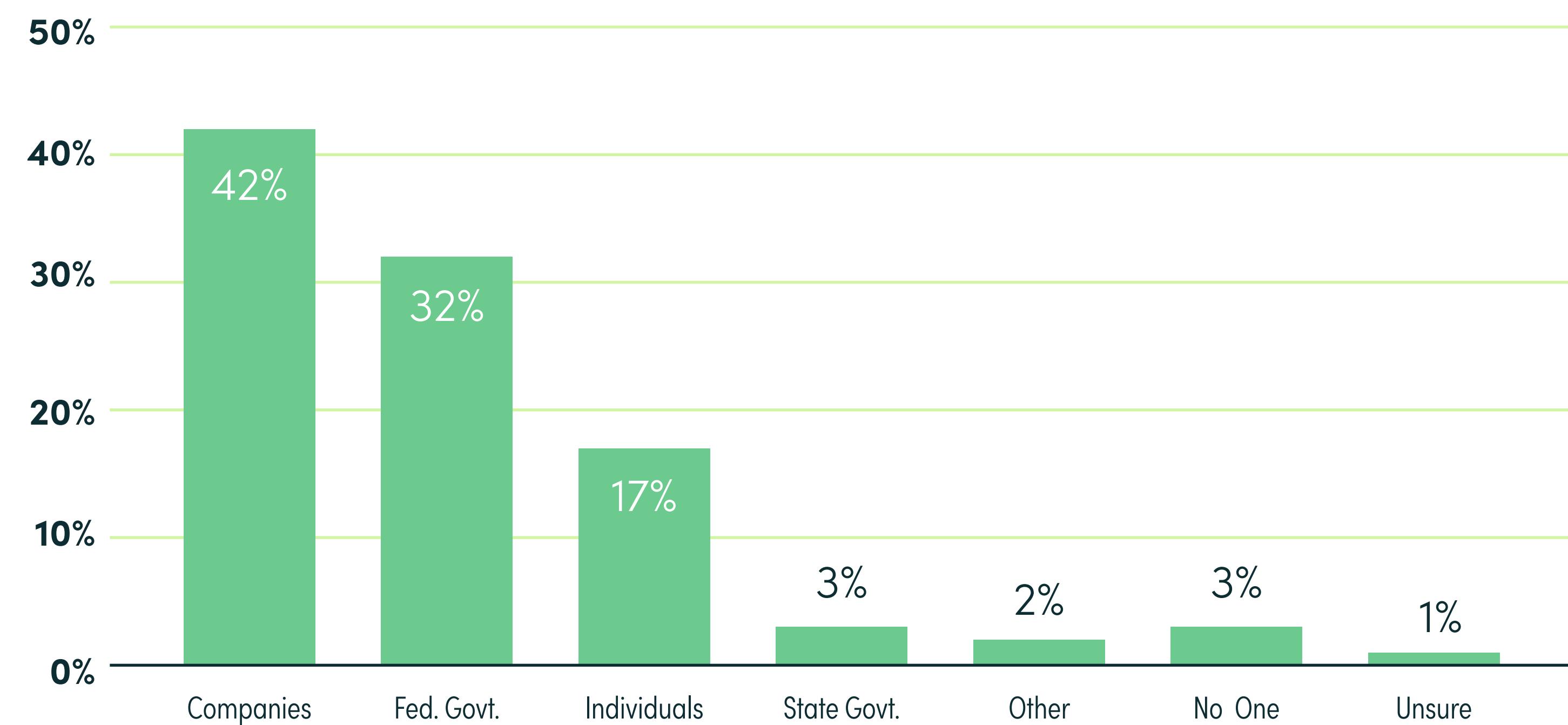
60% OF AMERICANS SAY...

Companies should be required to be more transparent about their privacy policies so that consumers can make more informed choices.

More consumers believe companies should be most responsible for user privacy than believe governments should.

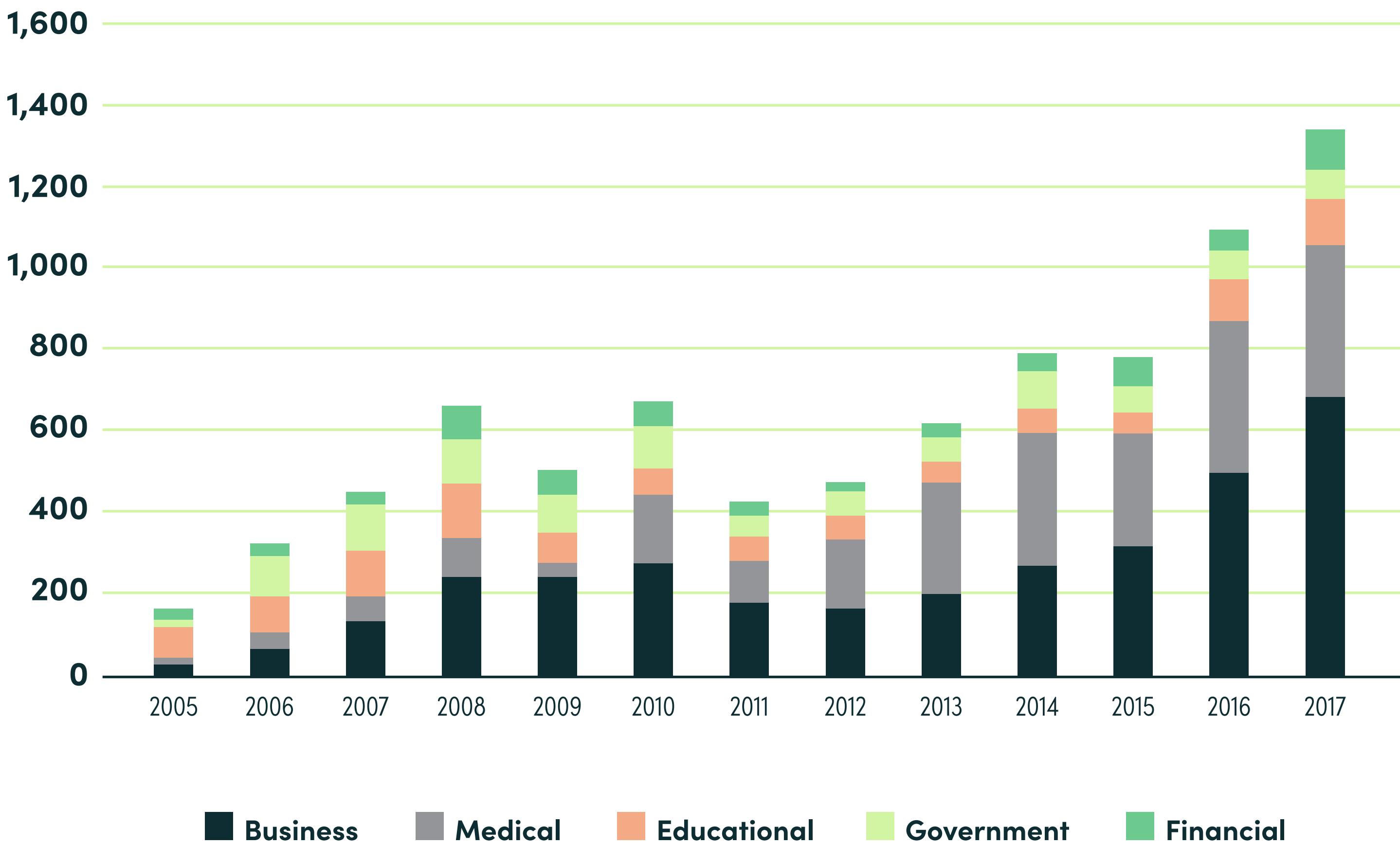
Over three-quarters of American consumers believe responsibility for protecting consumer privacy should not fall to individuals.

Who should be MOST responsible for protecting consumers' online privacy?



Data breaches are on the rise

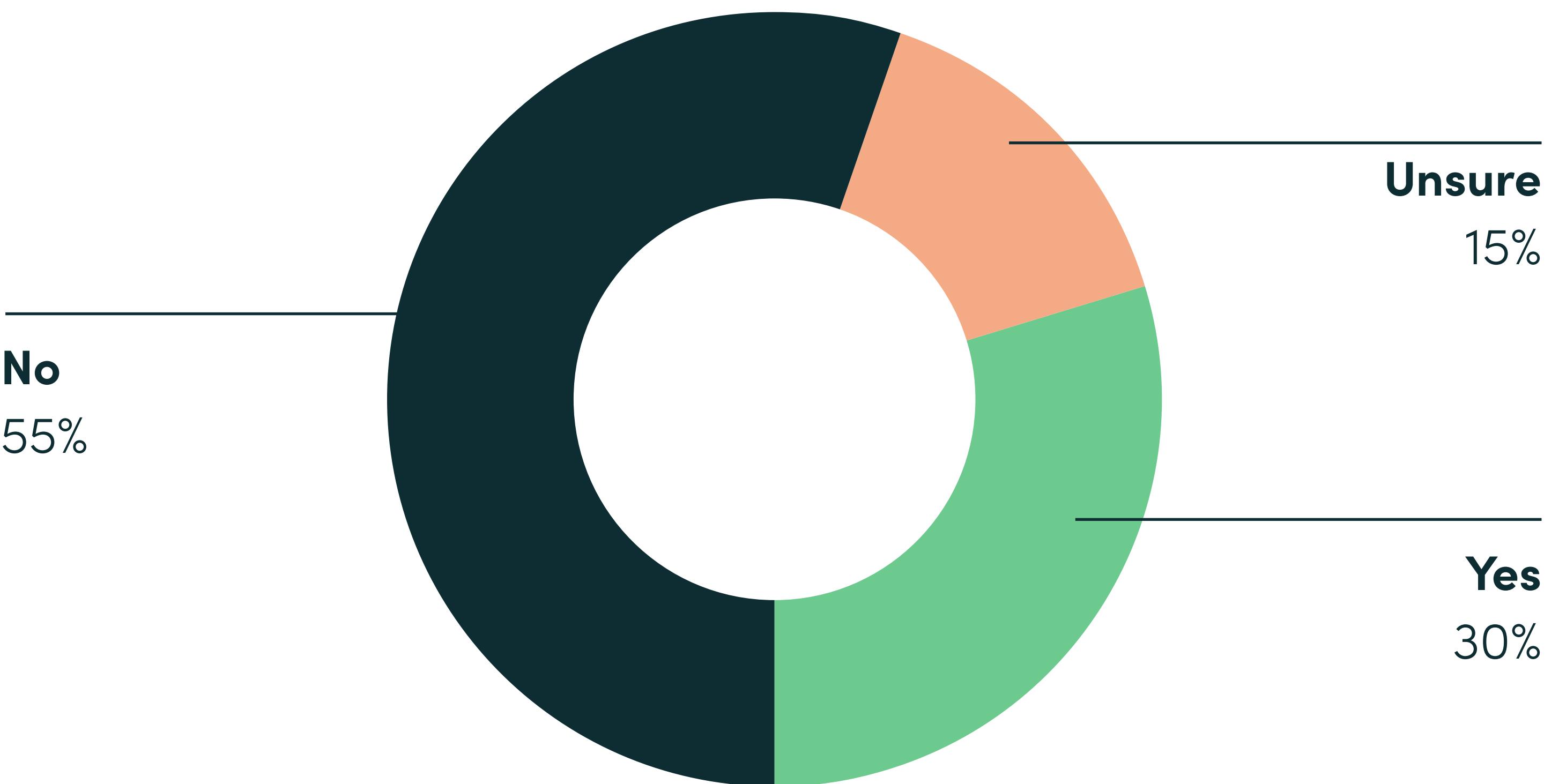
U.S. Data Breaches by Sector



Source: Identity Theft Resource Center

At least 30% of American consumers, and maybe as high as 45% have experienced a data breach

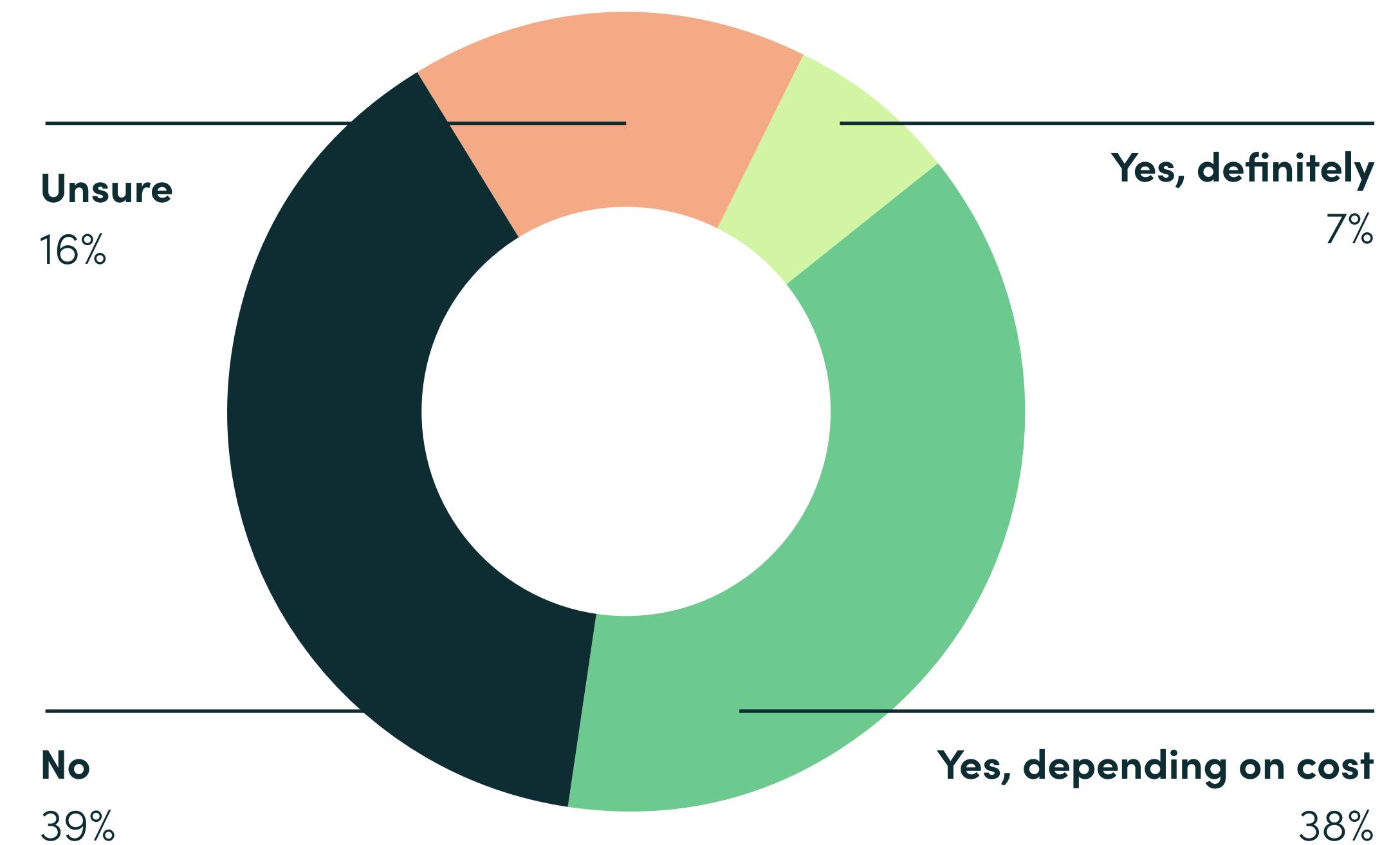
Have you ever personally experienced a data breach?



Consumers are willing to pay companies to be more responsible

Would you be willing to pay to use search engines such as Google, in exchange for these companies to STOP collecting, sharing, or selling your data?

45% of American consumers indicated a potential willingness to pay for online privacy



Privacy and security present sizable and rapidly growing opportunities

Consumer focus on privacy and security is rising.

Data privacy and security can be a point of beneficial product differentiation.

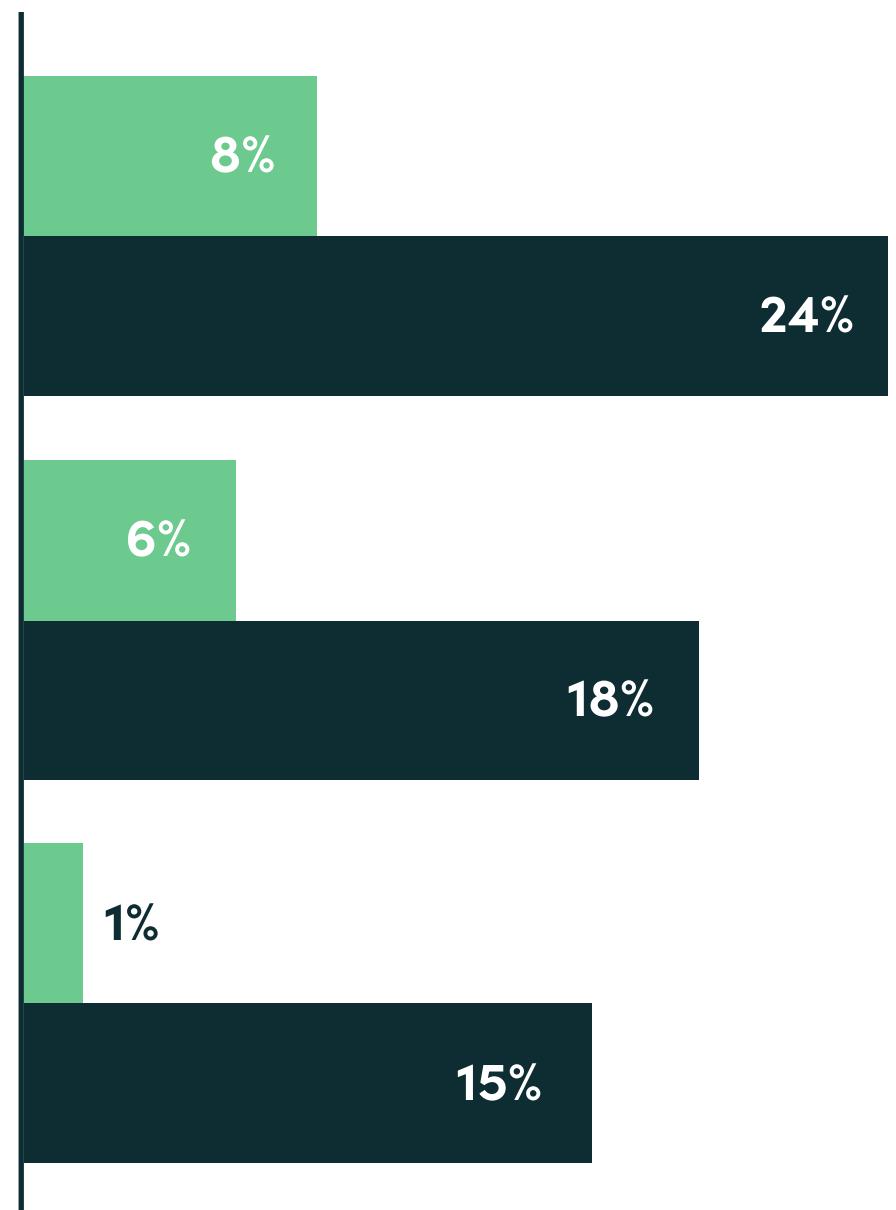
Benefits may come in the form of pricing power, profitability, market share, goodwill, talent attraction, or others.

With smartphones, perceived privacy & security factor into reasons Android users switched to an iPhone

Android users who have switched
from *an Apple to an Android*
in the past five years

- An Apple/Android is safer and has more security features than other phones
- Wanted a phone with better protections for my privacy so that my data isn't stored or accessed by anyone but me
- Wanted apps that are better vetted for security and privacy

Apple users who have switched
from *an Android to an Apple* in
the past five years



For those considering a switch to an iPhone from an Android, privacy or security reasons were cited by 4 in 10 Android users

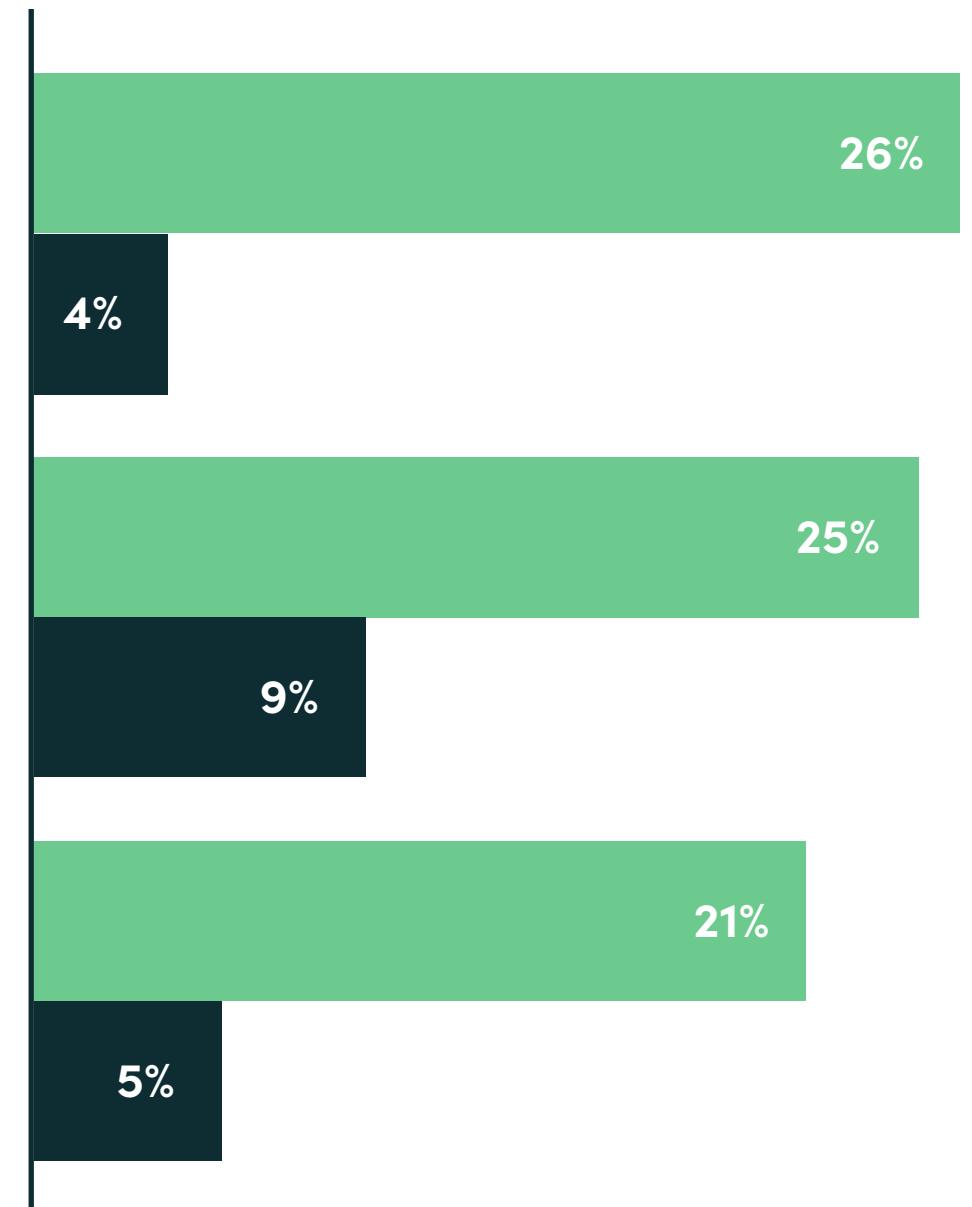
Android users who have considered switching to *an Apple* in the past five years

An Apple/Android is safer and has more security features than other phones

Want a phone with better protections for my privacy so that my data isn't stored or accessed by anyone but me

Want apps that are better vetted for security and privacy

Apple users who have considered switching to *an Android* in the past five years



“Concerned, non-switchers” could be
“low-hanging fruit” for conversion to products
with better privacy and security

Just as convenience carries switching power for Apple iPhone users, so too does privacy

Top reasons for recently switching type of phone

Convenience/Cost vs. Privacy-Driven Choices

Reasons why Android users have switched to iPhone

- 34% say “I want the same phone brand as family and friends”
- 24% say “An Apple iPhone is safer and has more security features than other phones”
- 21% say “The store where I bought it was providing good deals on iPhones”
- 20% say “I wanted a phone that would be compatible with other devices in my home”

Base: Apple iPhone users who have switched to an iPhone from an Android in the past five years

Reasons why iPhone users have switched to Android

- 39% say “I wanted a phone that I felt provided more value for the price”
- 36% say “I wanted a less expensive phone”
- 32% say “I wanted a phone with more options for flexibility and customization”

Base: Android users who have switched to an Android from an iPhone in the past five years

There is also staying power to privacy with Apple iPhone users, just as there is for convenience

Top reasons for not switching type of phone

Convenience vs. Privacy-Driven

Reasons why iPhone users have not considered switching to Android

- 41% say “It’s what I’ve been using for years and don’t want to learn a new operating system”
- 37% say “I have other Apple products and apps that are all synced up and it’s too costly, difficult, and time-consuming to start over”
- 28% say “I like the protections that an iPhone provides for the privacy so that my data isn’t stored or accessed by anyone but me”
- 27% say “I just haven’t thought about it. I’m happy with my iPhone”
- 23% say “I heard that an Apple iPhone is safer and has more security features than other phones”

Base: Apple iPhone users who have had their iPhone at least five years and have not considered switching to an Android

Reasons why Android users have not considered switching to iPhone

- 37% say “It’s what I’ve been using for years and don’t want to learn a new operating system”
- 33% say “I just haven’t thought about it. I’m happy with my Android”
- 18% say “I have other Android products and apps that are all synced up and it’s too costly, difficult, or time-consuming to start over”

Base: Android users who have had their Android at least five years and have not considered switching to an iPhone

Privacy and security are important factors in web browser choice, especially on desktop

Why do you typically use your preferred browser on each device?

- Smartphone
- Laptop
- Desktop

It's the default browser on my phone/desktop/laptop

It's what I've always used

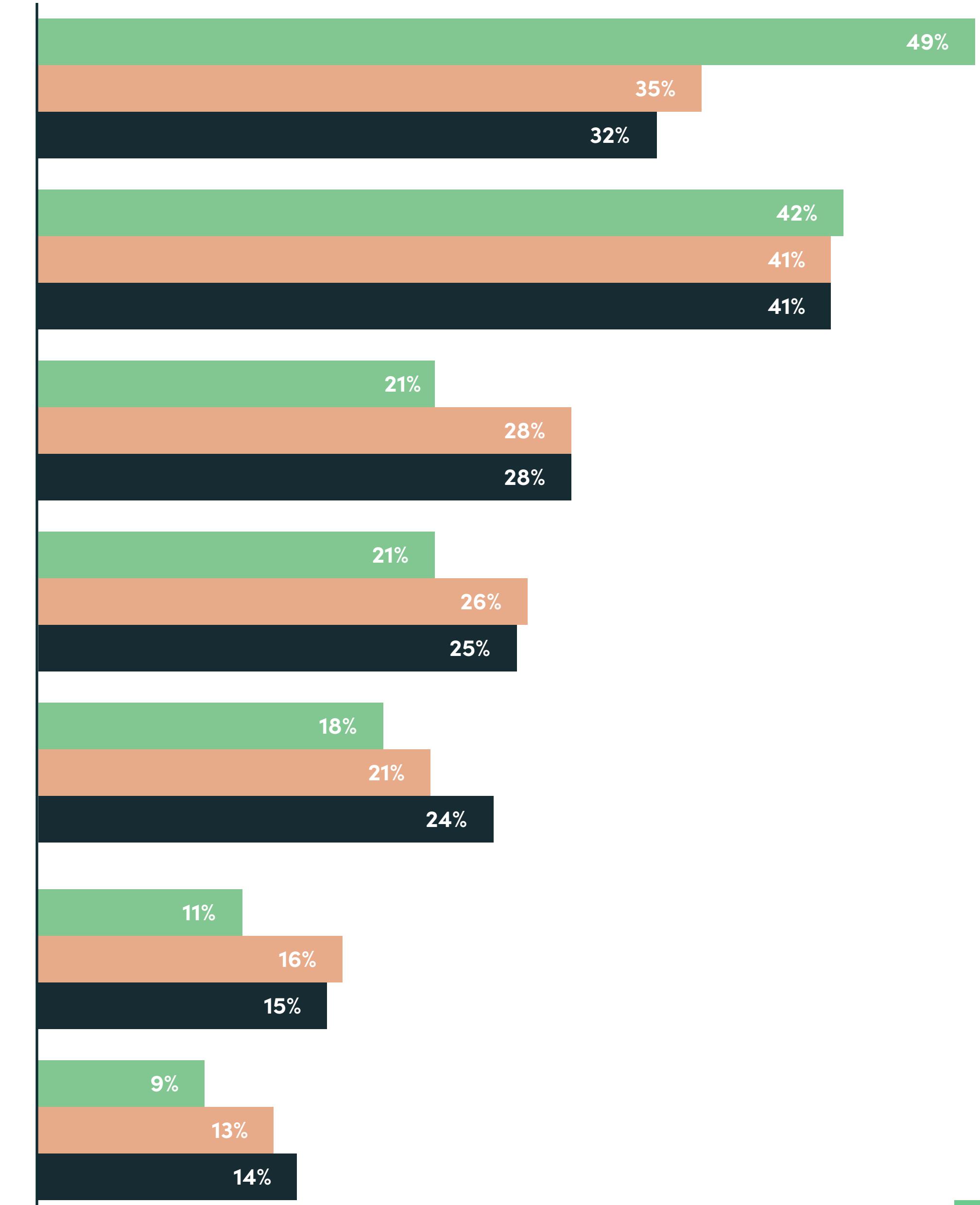
Faster than other web browsers

The interface is easier to use than others

Better than other browsers for maintaining my online security

Easy to customize settings to add extra layers of privacy and protection

More privacy tools so there is less data collection and tracking than other browsers





The privacy & security conscious consumer class seems to include more men and people of color.

Gender:

We define “more men” as a higher percentage of males than females.

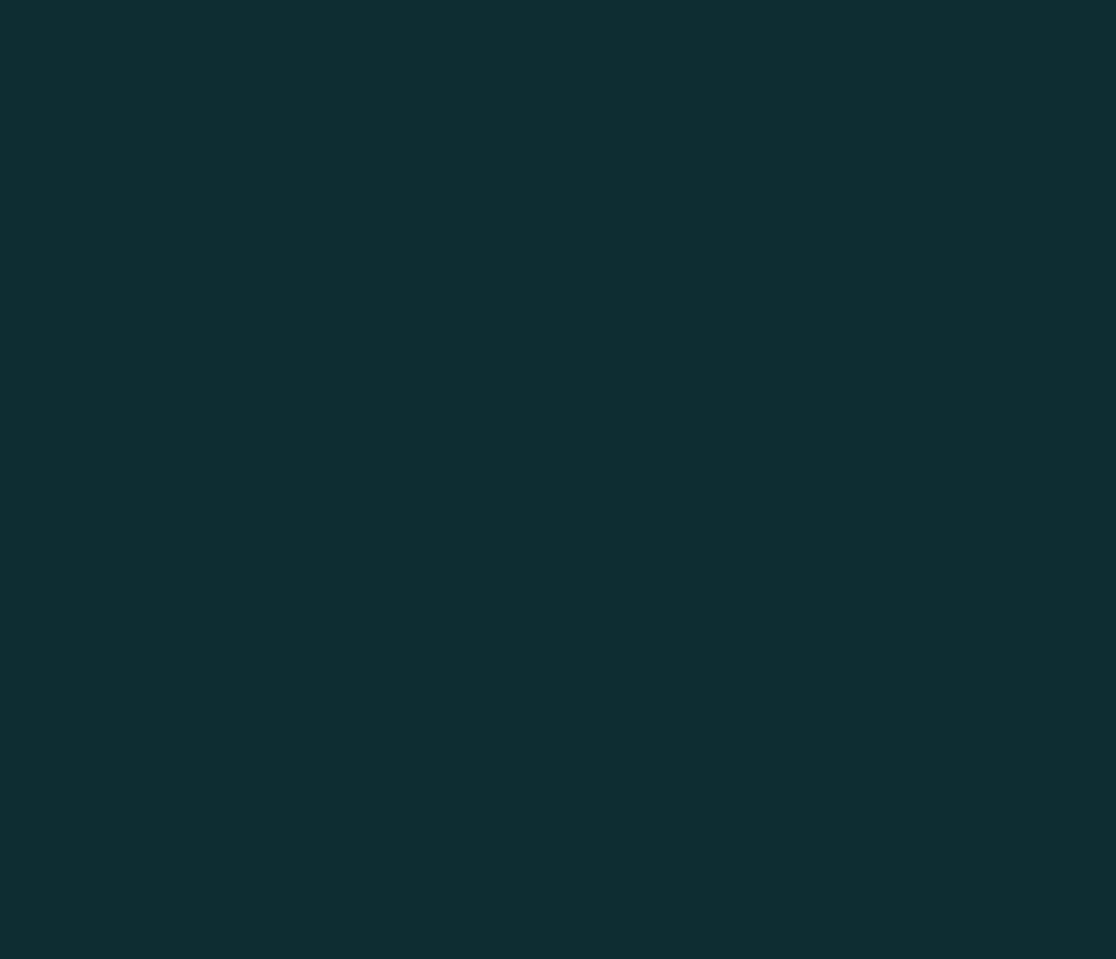
Race/Ethnicity:

We define “more people of color” as a higher percentage of Black, non-Hispanic and Hispanic Americans than white, non-Hispanic.

**We asked American Consumers
“Would you be willing
to pay to use search
engines such as Google,
in exchange for these
companies to STOP
collecting, sharing, or
selling your data?”**

And we learned:

- **Americans with higher incomes** are more likely to say they would consider paying depending on the cost...
- **A larger percentage of Black, non-Hispanic and Hispanic Americans** (11%) than White, non-Hispanic Americans (5%) say they would definitely pay...
- **Americans who are “extremely or very concerned” about the privacy** of the personal data companies collect and store about them are more likely to say they would pay or would consider paying depending on the cost...
- **A larger percentage of Americans who experienced a data breach** (52%) than those who have not (40%) would pay or would consider paying depending on the cost...
- **Americans who say they considered switching their phone type** for a privacy-oriented reason are more likely than those who haven’t to say they are willing to pay...



SECTION 4

Quantifying Consumer Preference

CR conducted a conjoint analysis to help quantify how consumers value privacy and security in purchasing behavior

Conjoint analysis is a technique to determine how people value different attributes (feature, function, benefits) that make up an individual product or service.

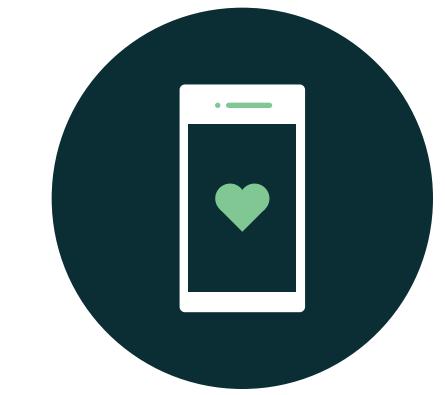
Consumer Reports conducted a conjoint analysis to drill into underlying consumer preferences in six product verticals across hardware and software.

The goal was to identify specific opportunities where companies might compete / differentiate.

We focused on product categories across hardware and software



VPNs



Health Apps



Security
Cameras



Smart
Speakers



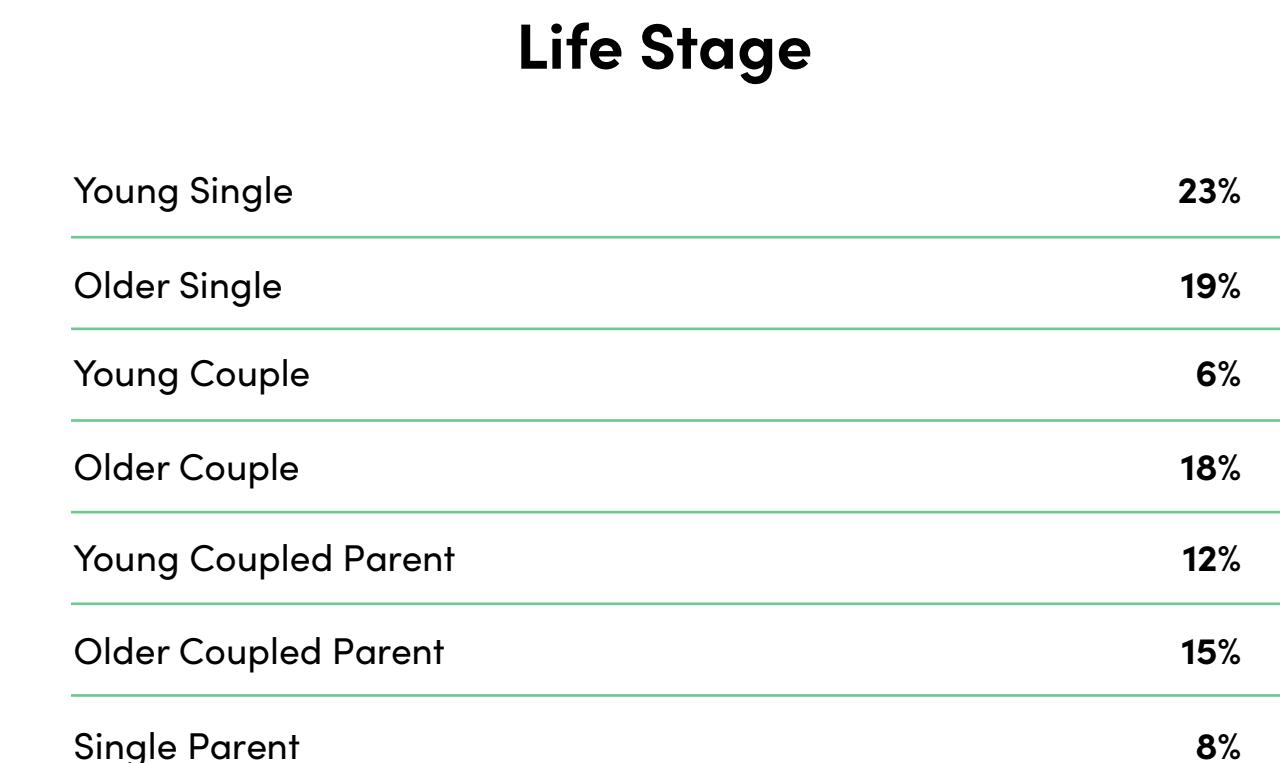
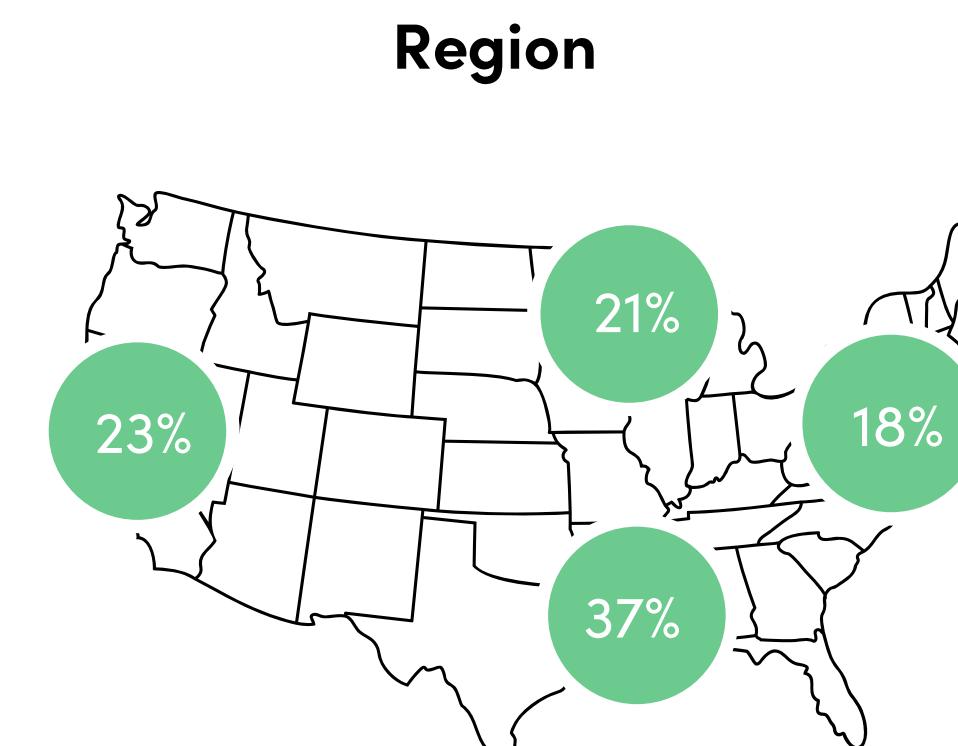
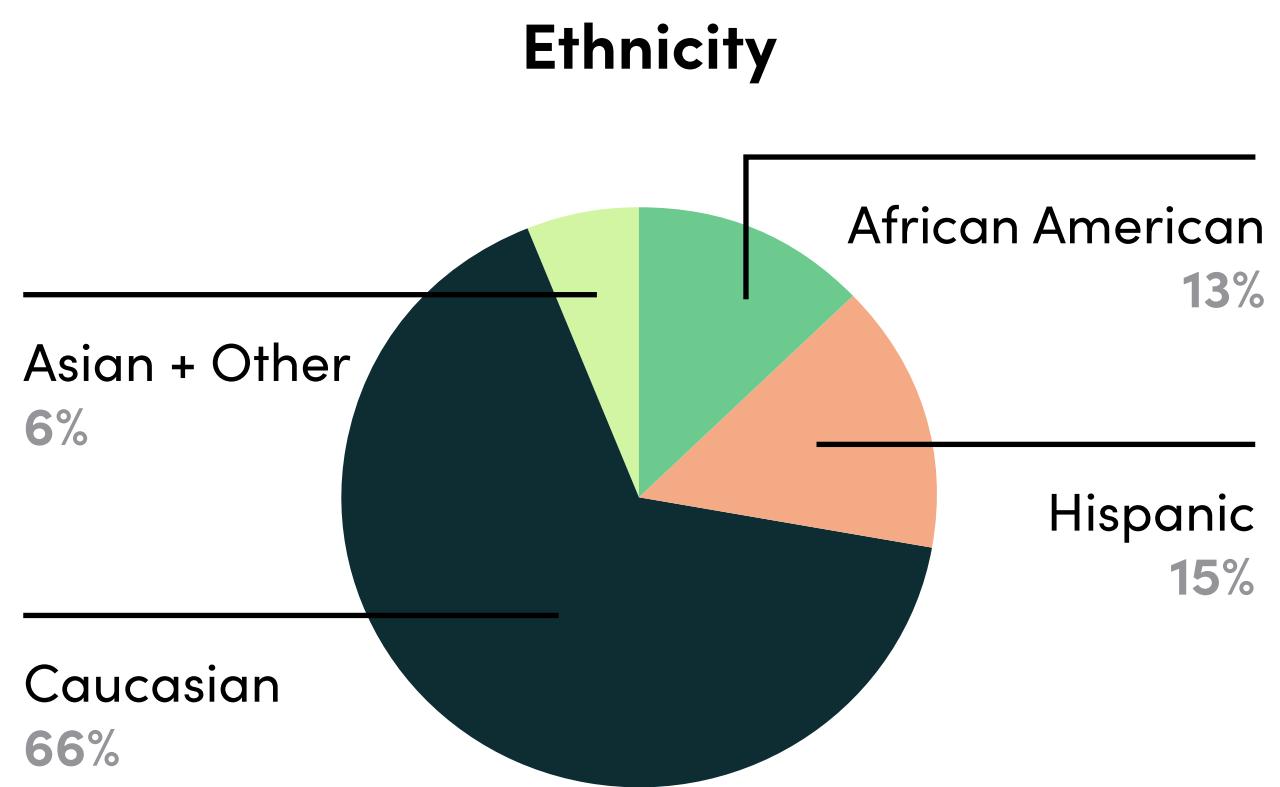
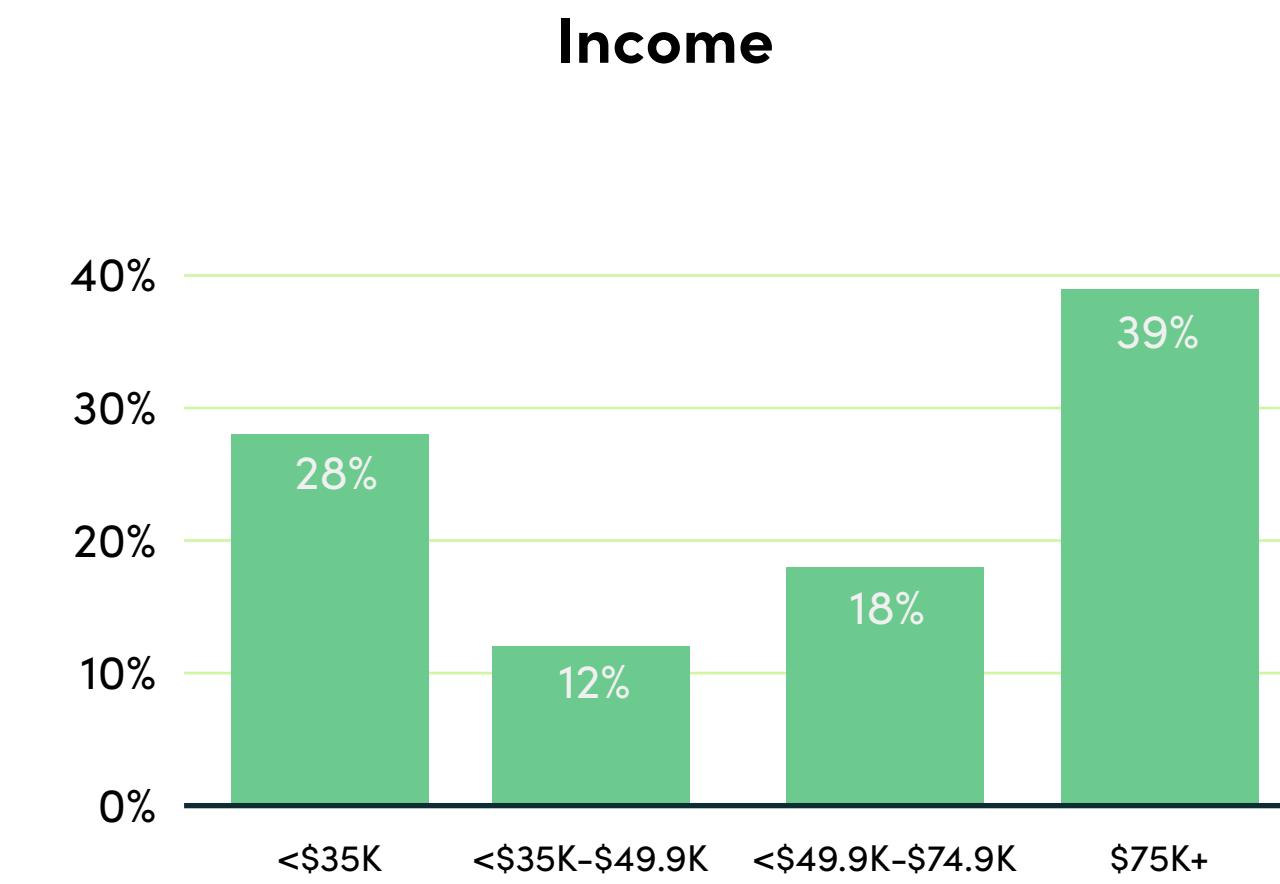
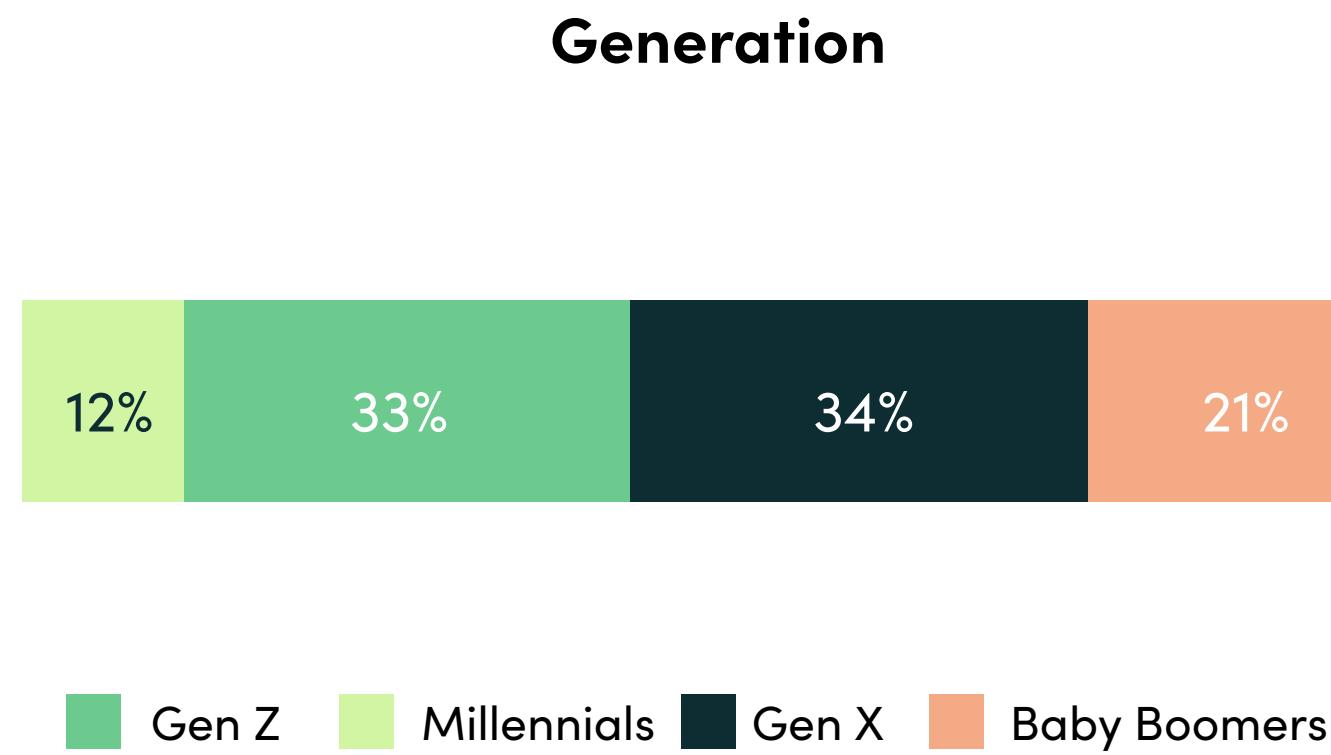
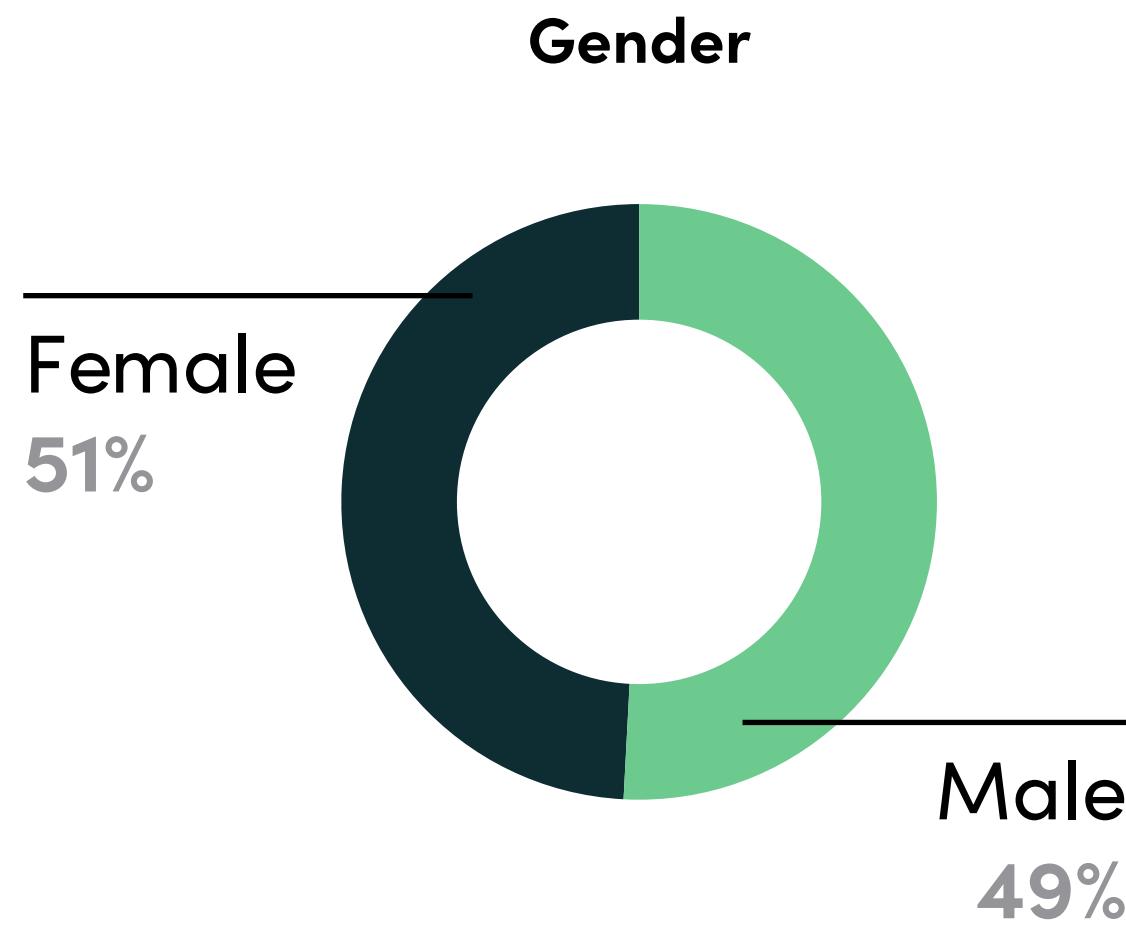
Streaming
Services



Cars

We also selected for product category representation across Health, Security, Entertainment, Technology, and Automobiles.

1,501 consumers participated



Each participant reacted to 10 hypothetical products.

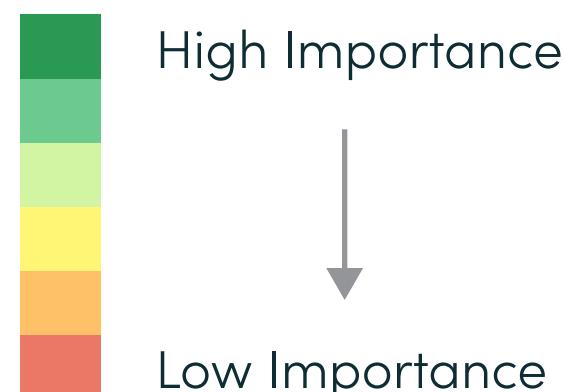
The hypothetical products were randomly generated and demonstrated varying product configurations based on pre-defined feature levels for:

- Price
- Reliability
- Performance
- Ease of Use
- Personalization
- Privacy
- Security

Across all products tested, price had the most impact

Privacy and security had broad impact and were prioritized over other features.

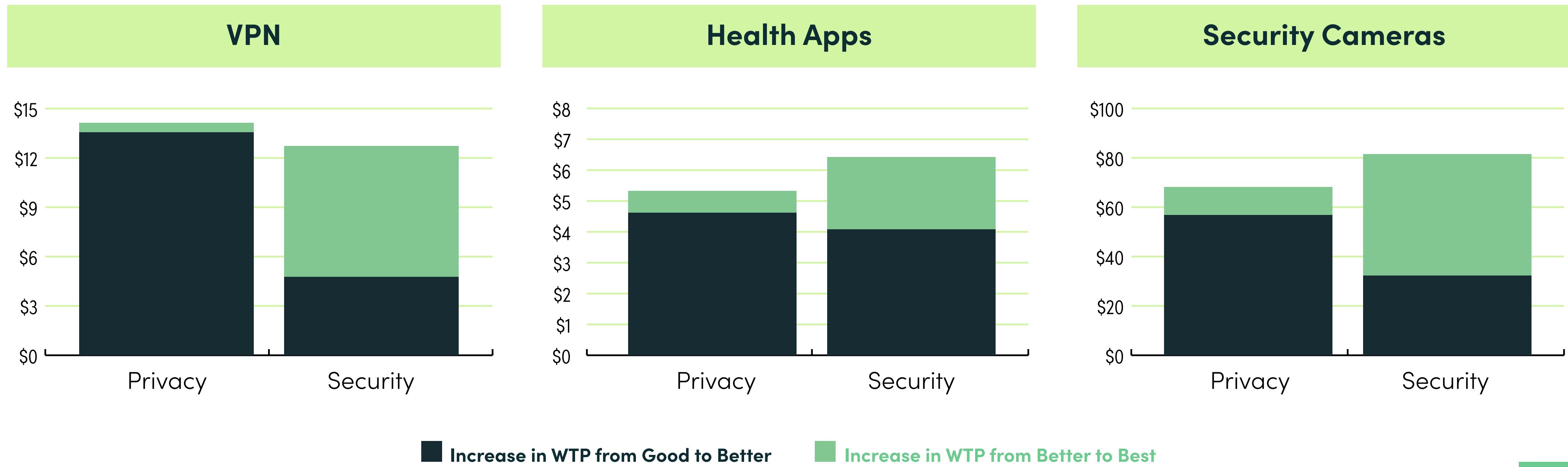
	VPN	Health	Security Cameras	Smart Speakers	Streaming Services	Cars
Price	236	190	153	253	201	287
Security	171	177	96	140	170	59
Privacy	160	135	79	118	118	107



Attribute Impact Scores: These scores are indexed Importance scores. An average impactful score would sit at 100, with scores above 100 having greater impact and below 100 having less. These scores are representative of importance at an entire feature level.

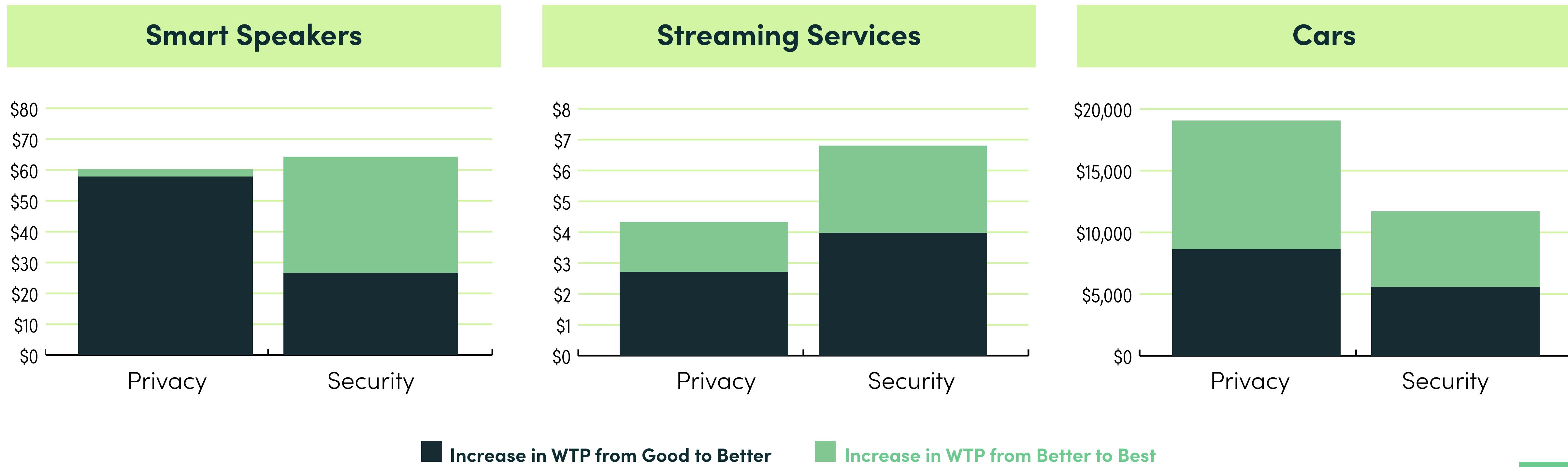
Across all categories, customers were willing to pay more for the better and best privacy features on the market

Customers also expressed a willingness to pay more for the better and best security features across all categories.



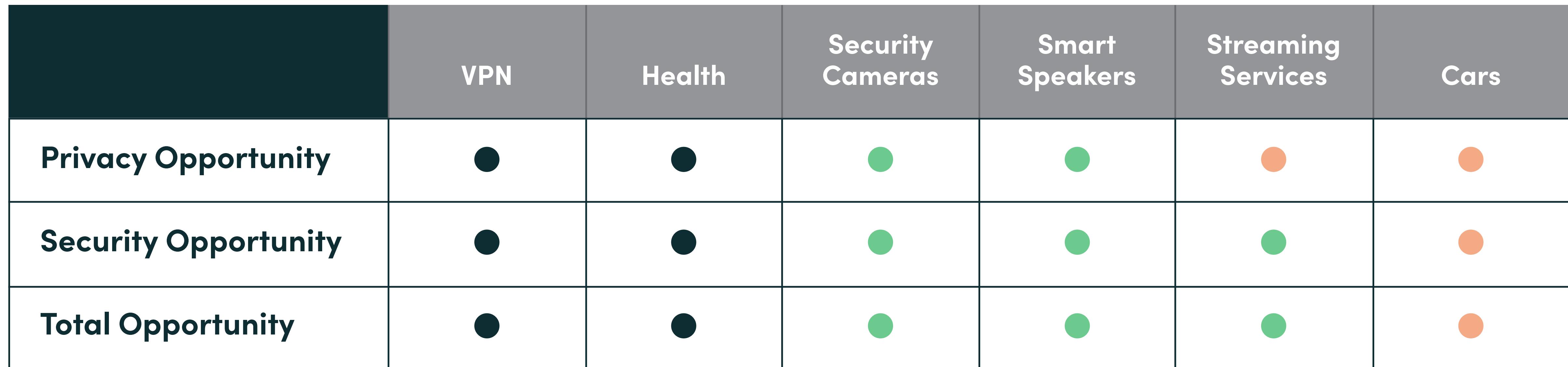
Across all categories, customers were willing to pay more for the better and best privacy features on the market

Customers also expressed a willingness to pay more for the better and best security features across all categories.



Software offerings showed a higher total opportunity around privacy and security than hardware offerings

○ HIGH ● MODERATE ○ LOW



Privacy and Security Opportunity determined based off of increase of WTP at "Best" level in comparison to the maximum price possible. Total opportunity determined by combination of those two metrics.

In conclusion, Health, Technology, and Security companies that prioritize consumer privacy and data security should see significant upside

Most consumers base their choices on convenience and cost factors, but nearly all remain concerned about privacy and security.

There are discernable customer classes that prioritize privacy and data security in their decisions.

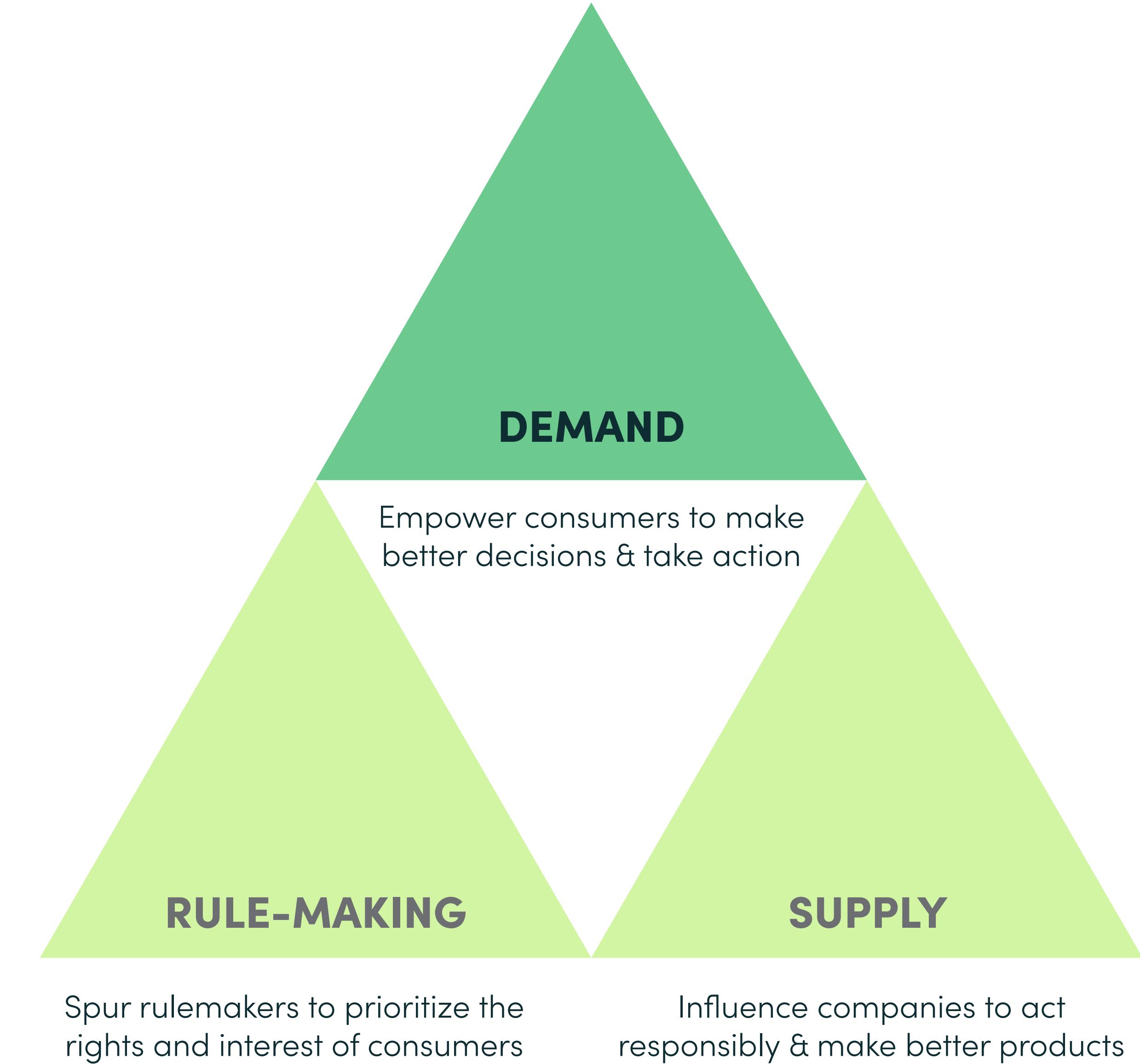
In four of the six product categories analyzed, privacy and security features had above average impact on consumer decisions.

A woman with long dark hair is shown from the chest up, looking down at her smartphone which she is holding in her hands. She is wearing a light-colored button-down shirt. The background is a soft-focus indoor setting.

SECTION 5

Moving Toward a Market for Privacy

With current market dynamics, privacy will continue to ascend



The regulatory tide on consumer privacy is already turning

Cultural and societal attitudes towards data privacy have irreversibly shifted.

100+ privacy and data governance-related laws introduced at state and federal levels since the 2018 California Consumer Privacy Act.

These laws could ultimately disrupt data-driven business models that rely upon the monetization of personal data.

Consumers increasingly care about privacy and security

3/4 of consumers are at least moderately concerned about the privacy of their personal data.

96% of Americans agree that more should be done to ensure companies protect consumers' privacy.

Consumers are willing to pay more for better privacy features across both hardware and software products.

Companies will see upside when privacy is front and center

And thus will find advantage in:

Differentiating with stronger
privacy and security features
than competitors

Building privacy and security
best practices into the product
development process

Highlighting privacy and
security in brand positioning

Privacy Front & Center

Meeting the Commercial Opportunity
to Support Consumers Rights



Contact

Ben Moskowitz

ben.moskowitz@consumer.org

Stephanie Nguyen

stephanie.nguyen@consumer.org

Appendix

Consumer Reports Research Tactics: meta-analysis, national surveys, and conjoint analysis

1. **Meta-analysis** of public opinion studies to chart changing consumer awareness and attitudes over a 25 year period (May 2020)

2. **A nationally representative multi-mode survey** to assess Americans' phone, web browser and app choices and usage, as well as consumers' expectations, concerns, and experiences with personal data privacy and security online (April 2020)

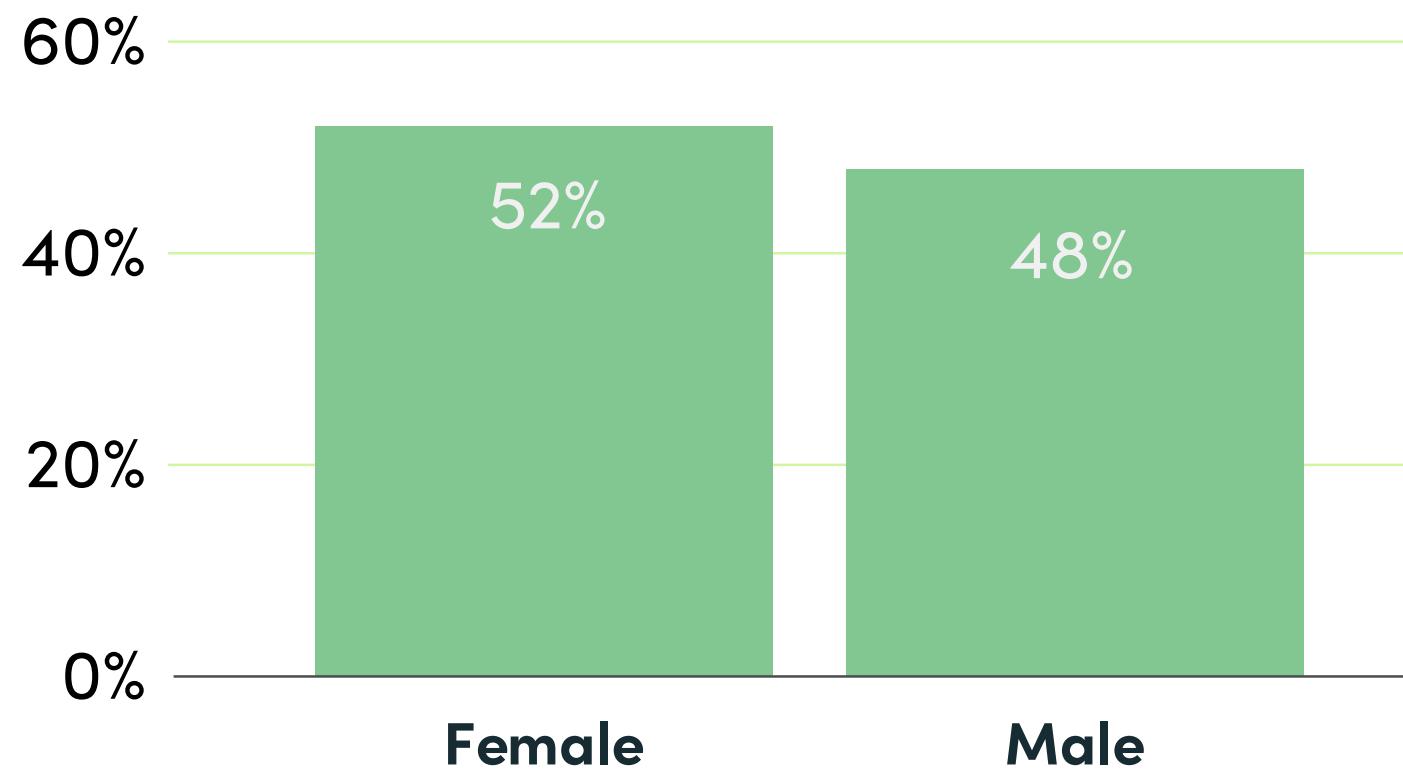
3. **A conjoint analysis** to chronicle consumers' purchasing considerations and willingness to pay for privacy and security (March 2020)

Research Timing & COVID-19

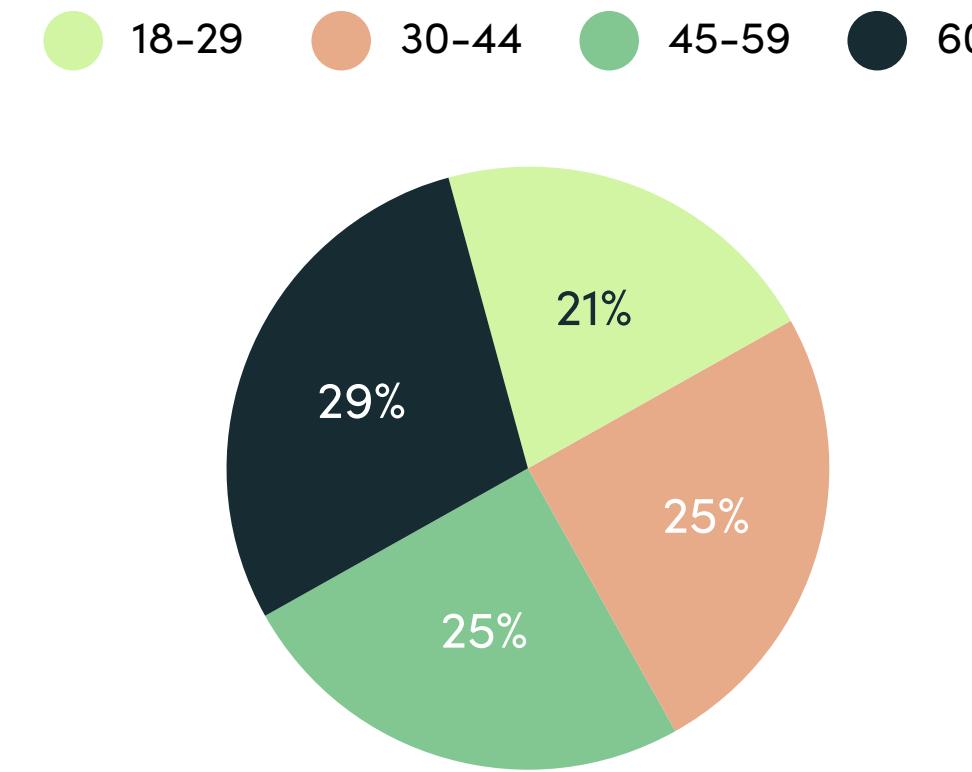
Parts of the survey research informing this report were conducted in March 2020 at the onset of the COVID-19 crisis. Though our findings may be subject to cyclical changes, the long-term trendlines on consumer attitudes toward privacy and security are consistent.

Consumer Reports Survey: Demographics (n=5,085 U.S. adults, fielded Feb 7 - 21, 2020)

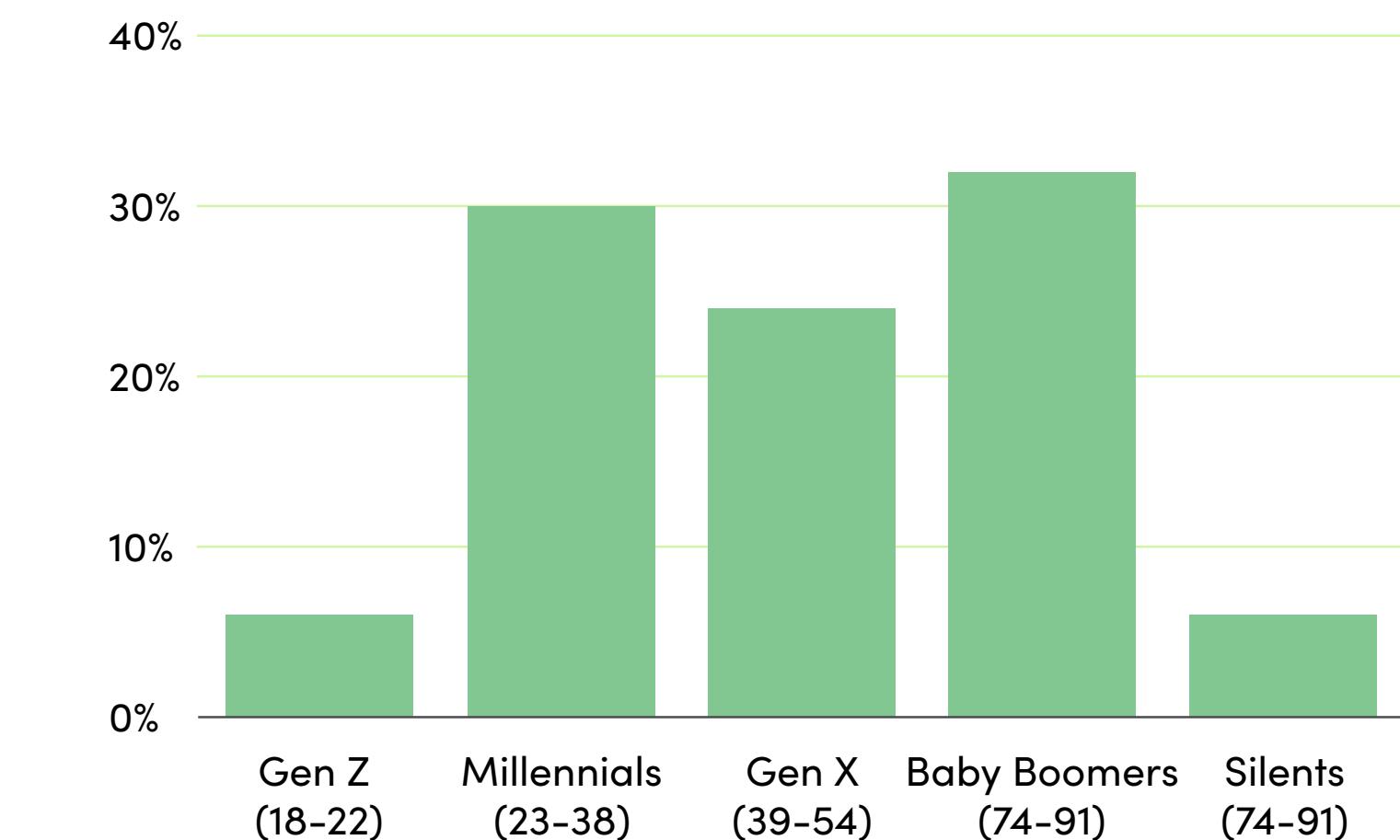
Gender



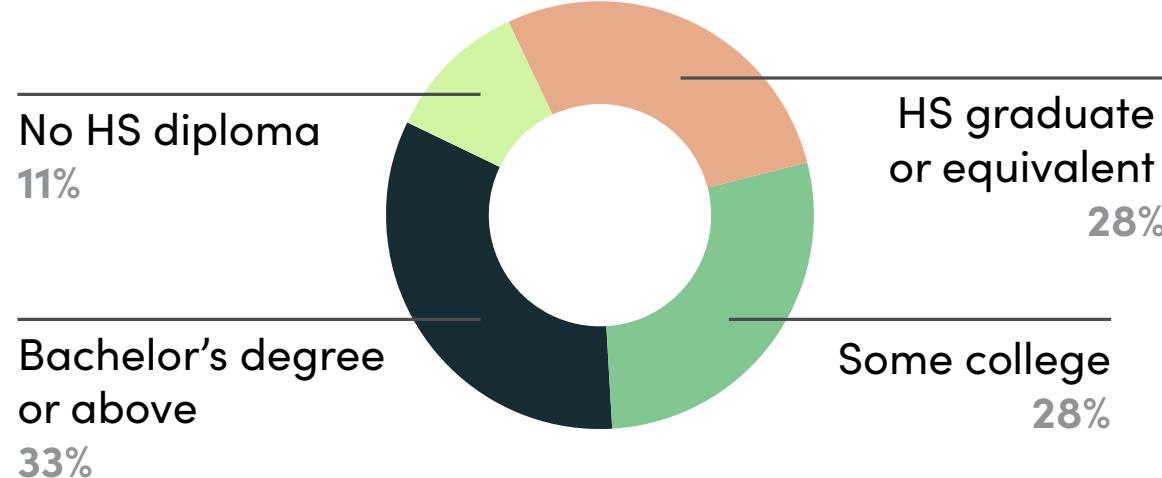
Age Cohorts



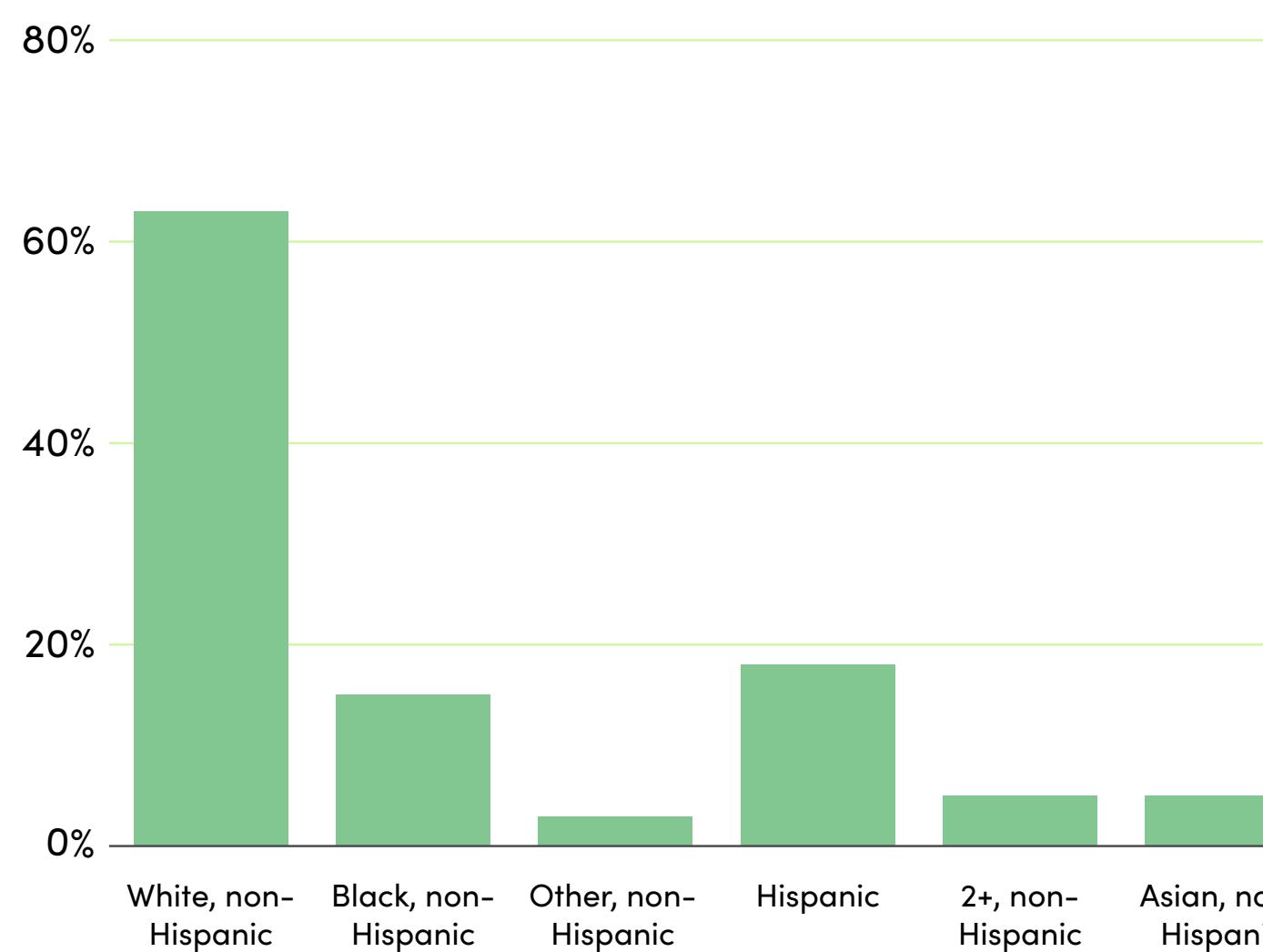
Generation



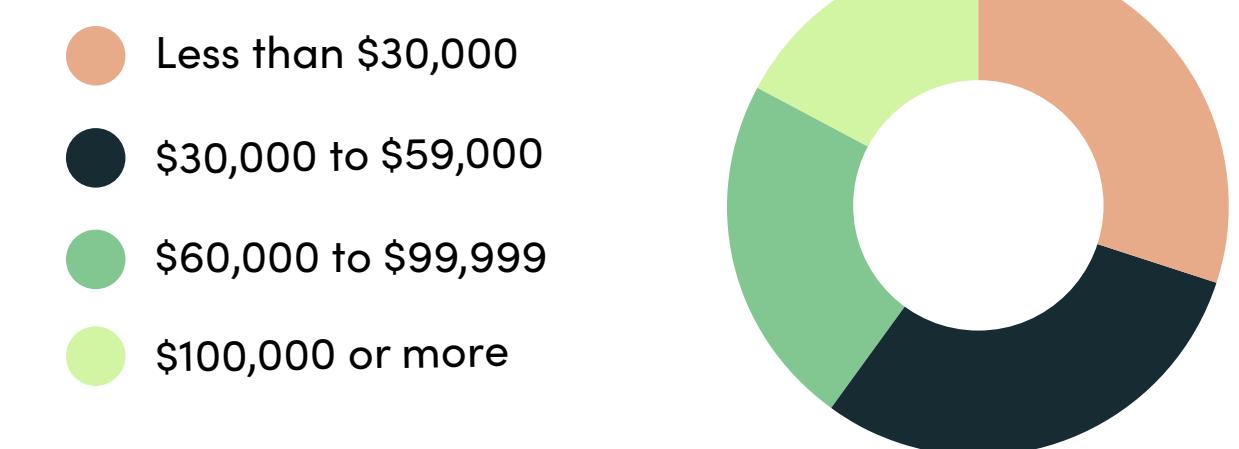
Education



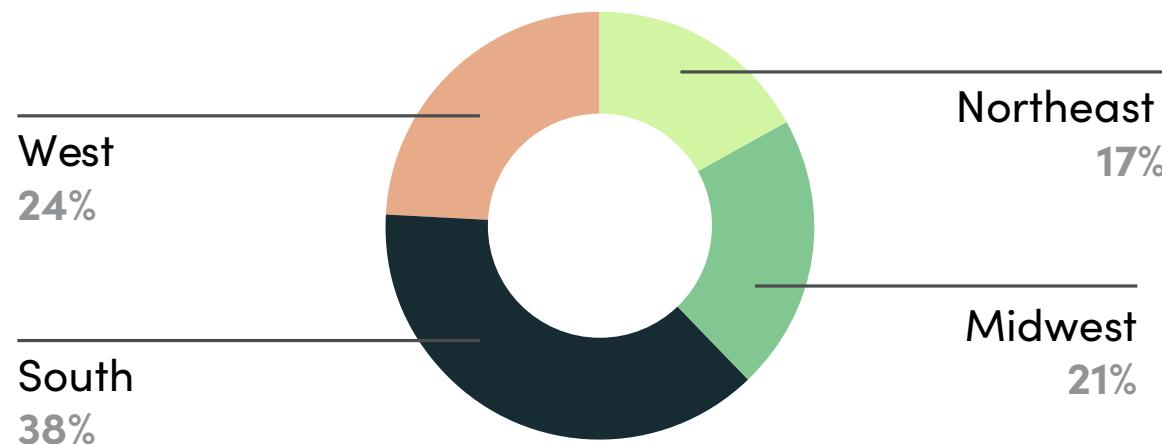
Combined Race Ethnicity



Household Income



Region



Metropolitan Area Flag



Consumer Reports Survey: Questions

The survey referenced in Section 3 asked consumers about:

- Concern about how much data and about the privacy of the personal data companies collect and store
- Concern about loss of privacy when purchasing smart products
- Experiences with data breaches
- Who should be most responsible for protecting the online privacy of Americans?
- What should be done to ensure companies protect the privacy of consumers?
- Willingness to pay to use search engines in exchange for these companies to stop collecting, sharing, or selling your data.
- How much, if at all, did privacy impact choices around
 - Web browser
 - Mobile messaging
 - Switching from Android to Apple or Apple to Android smartphones

Conjoint analysis: a tool to identify underlying consumer preferences

- Conjoint analysis is a survey-based statistical technique used in market research that helps determine how people value different attributes (feature, function, benefits) that make up an individual product or service.
- In a conjoint survey, set of potential products or services is shown to survey respondents to analyze how they make choices between these products to better understand “implicit valuations” or utility to people.
- Implicit valuations can be used to create market models that estimate market share, revenue and even profitability of new designs.

Previous (scholarly) applications of conjoint and/or discrete choice analysis around privacy valuations

- **Hann et al. (2007, p. 14)** used conjoint analysis to quantify the value individuals ascribed to website privacy protection and concluded that “among U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US\$30.49–44.62.”
- **Avoiding the Privacy Paradox Using Preference-Based Segmentation: A Conjoint Analysis Approach**
Kuzmanovic, Marija & Savic, Gordana. (2020). Avoiding the Privacy Paradox Using Preference Based Segmentation: A Conjoint Analysis Approach. *Electronics*. 9. 1382. 10.3390/electronics9091382.
- **The Personalization-Privacy Paradox and the Internet of Things**
Yoni Linden Maastricht University
- **The Value of Personal Information to Consumers of Online Services: Evidence from a Discrete Choice Experiment**
- **Investigating the Value of Privacy in Online Social Networks: Conjoint Analysis (2009)**
www.researchgate.net/publication/221599995_Investigating_the_Value_of_Privacy_in_Online_Social_Networks_Conjoint_Analysis

Conjoint Analysis: Benefits & Drawbacks

Benefits

- Realistic and similar to real situations in which respondents have to make trade-offs between conflicting factors.
- Preferences are measured indirectly, which can reduce the bias of strategic responses.
- Potential to experimentally uncover the hidden rules that individuals use to make trade-offs between products or services.

Drawbacks

- Even though interviews and context form the basis for the model, it is prone to the interpretation and view of the researcher and the characteristics of the limited sample of these interviews.
- The hypothetical nature of the study makes it difficult to determine conclusively whether individuals will, in actuality, pay to protect their privacy (e.g., the “intent-to-action” gap).

Consumer Reports Conjoint Analysis: Quantifying the Impact of Privacy and Security

Methodology

- Online, quantitative study
- 15 minute interview length
- Online survey featured a choice model covering 6 categories including VPNs, Health Apps, Security Cameras, Smart Speakers, Streaming Services and Cars

Sample

- N=1,501 respondents including combination of owners and intenders, with intenders capped at 20% of sample
- Nationally representative
- Age 18-69
- Non-rejecter to at least one category tested

Field Dates

- March 16, 2020 – March 27, 2020

Choice Model Details

- Model design included 10 total factors (e.g., Price, Privacy, Security, Reliability, etc.) tested across all products
- Each product included a maximum of 7 factors most relevant for that product
- In other words, 7 of 10 factors most relevant to a product were tested, though all 10 factors are covered across all products
- For each factor, 3 levels were tested (e.g., good, better, best); the number of levels for each factor will remained consistent across all products, with the exception of price which had 5 levels

Consumer Reports Conjoint Analysis: Category Decision

Combination of hardware and software products, where design and features could be differentiated.

Mainstream (and recognizable) established product categories where privacy and security would register as concerns.

Product categories undergoing CR evaluation as part of the Digital Standard initiative – opportunity to increase transparency and consumer awareness of where competitors differ.