

cassie

Privacy beyond borders

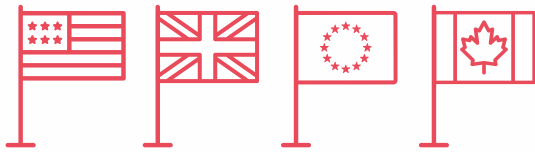
Insights from
around the world



Survey methodology and demographics

Survey conducted at 95% confidence, +/- 4% margin of error
Survey conducted from February 29, 2024 - March 12, 2024

Respondent qualifiers



Live in the
US, UK, EU, or CA

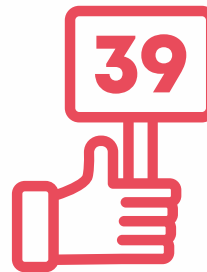


18+ Years of Age

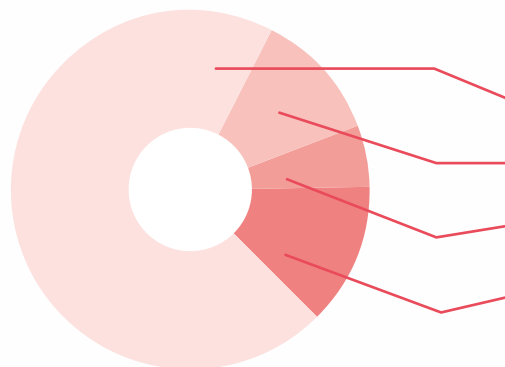
Respondents



Total number of
respondents



Average age of
respondent



66%	US
5%	UK
11%	EU
12%	CA

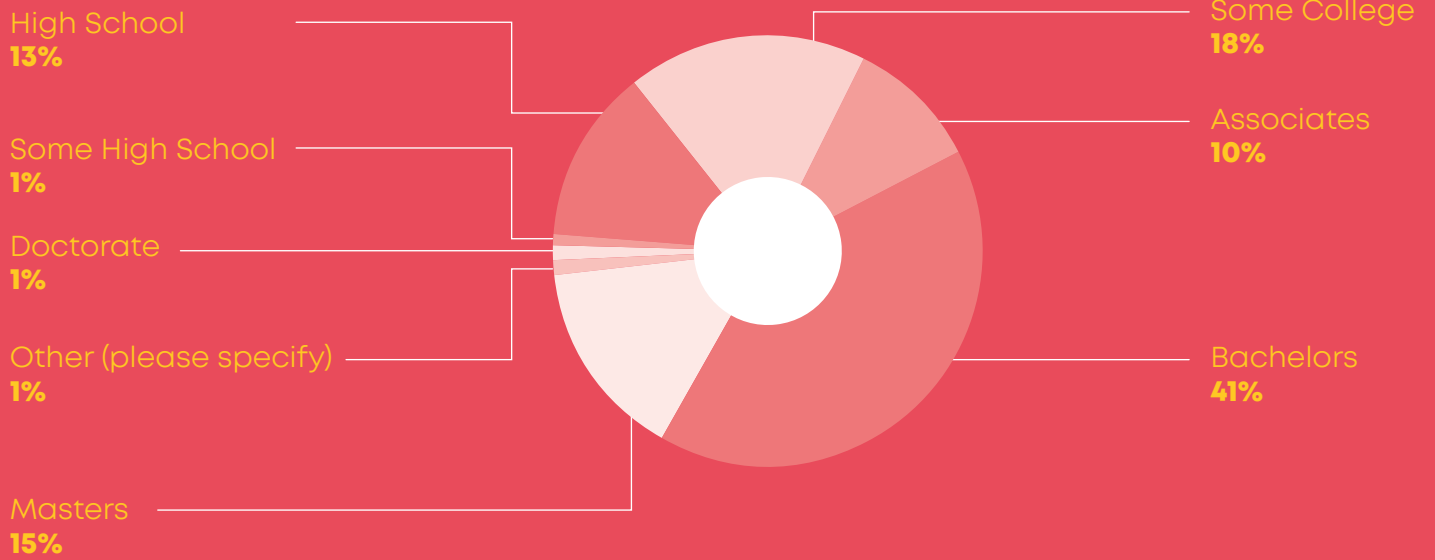
cassie

Demographics

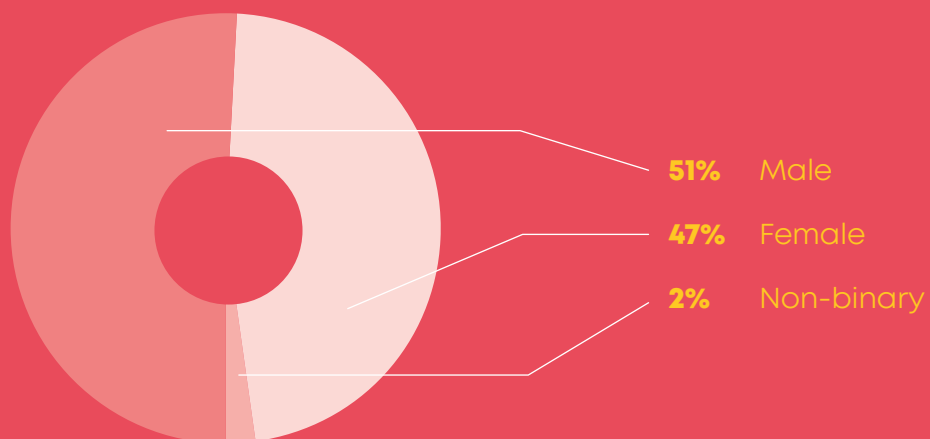




Education



Gender



Introduction



Global user preferences and privacy perceptions: Insights from around the world

As digital innovation drives technology to advance at a rapid pace, the implications on data privacy inevitably increase in parallel. With more digital touchpoints, comes more data collection.

Global businesses are racing to keep up – both with user expectations on personalization and privacy as well as the continuously evolving legislation around how data is managed.

Brands need to create seamless user experiences that transcend geographical boundaries without overstepping differing privacy regulations and risking fines.

In 2023, 137 out of 194 countries had put in place legislation to secure the protection of data and privacy. (UNCTAD)

That number only continues to grow, with new iterations coming into effect around the world in line with technological developments. The US alone has a patchwork of over 15 state-specific laws in place and plenty more to come.

Privacy laws have never been more important, with data transfers happening around the world through borderless networks.

Organizations need to consider the implications of legislation not just in their own country but around the world.

In this comprehensive report, we've surveyed people worldwide to understand global user preferences and the impact of regional privacy laws on their digital experiences.

Do US citizens care more about their data privacy than their neighbors in Canada?

Or across the pond to residents in the UK and Europe – who knows their rights when it comes to what businesses can do with their data?

By unlocking these regional nuances, brands can inform their digital strategy based on the delicate balance between meeting user demands and adhering to the ever-evolving legal frameworks in different regions.

cassie

Key findings



Online security is a increasing concern

93%

Of consumers are concerned about the security
of their personal information online

59%

Report that their concerns about data privacy
have **increased** over the last 12 months

Consumers are cracking down on their data privacy standards



97%

Believe there should be stricter penalties for companies that violate data privacy regulations

and

prefer to do business with companies that have a strong track record of protecting data privacy

Many feel like their rights are less important than dollar signs



92%

Believe that companies often prioritize profits over data protection

Yet the majority remain in the dark

A gauge graphic with a needle pointing to 73% on a scale from 0 to 100. The gauge is semi-circular and has a red background.

73%

Do not feel informed about their data privacy and protection rights

A gauge graphic with a needle pointing to 95% on a scale from 0 to 100. The gauge is semi-circular and has a yellow background.

95%

Wish companies were more transparent about their data collection and sharing practices

A gauge graphic with a needle pointing to 84% on a scale from 0 to 100. The gauge is semi-circular and has a teal background.

84%

Do not feel they have enough control over their personal data

Privacy concerns hit close to home



64%

Do not believe the
data privacy regulations
in their country
adequately protect
their personal data

But are not... ...confined by borders

85%

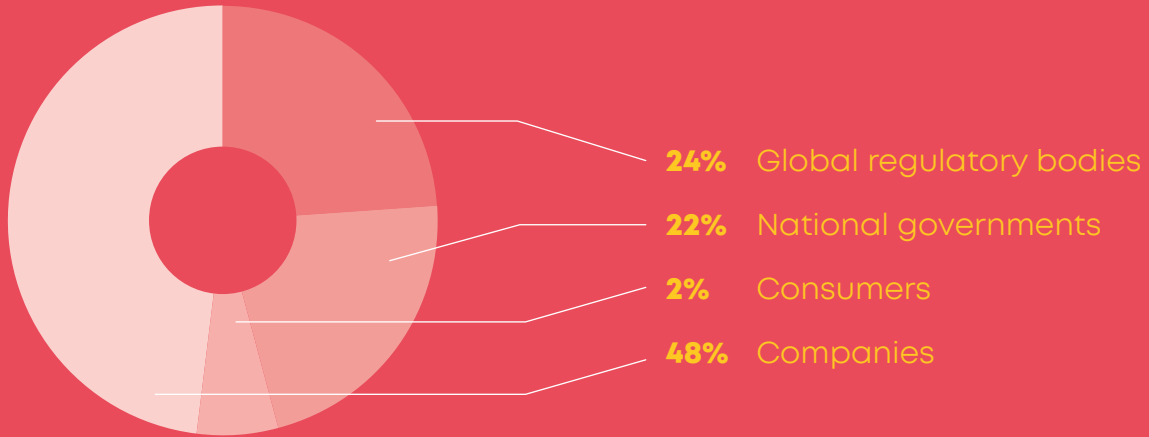
Are not confident in the consistency and effectiveness of data privacy regulations across different countries

94%

Agree that companies should adhere to the strictest data privacy regulations globally, regardless of the country in which they operate

Whose job is data privacy

According to our panel...



European consumers were **83% more likely** than US consumers to believe data privacy should rest in the hands of consumers

83%

US consumers were **55% more likely** than EU consumers to believe data privacy should rest in the hands of companies

55%

UK consumers were **45% more likely** than US consumers to believe data privacy should rest in the hands of global regulatory bodies

45%

So how can companies make consumers feel more comfortable



69%

Desire clear expectations of how their data will be used



69%

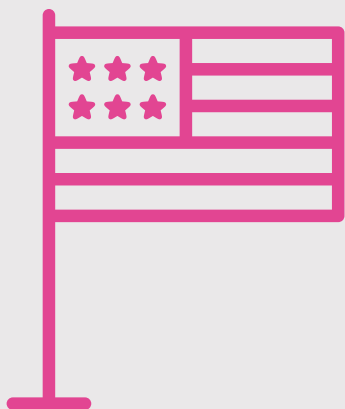
Want the use of encryption and secure data storage practices



68%

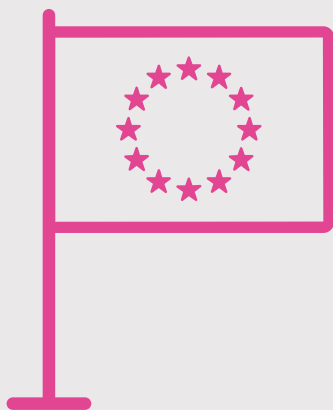
Would like the ability to control the types of data collected

But it goes beyond that – in a digital world, companies must consider global preferences



24%

US consumers were **24% more likely** than EU consumers to value the trustworthiness/reputation of a website



17%

EU consumers were **17% less likely** than average to value the use of encryption and secure data storage practices



When it comes
to privacy
**European
consumers**
run a tight ship

160%

European consumers were **160% more likely** than US consumers to never read a cookie consent popup before clicking a response

Likely - because they are

100%

More likely than US consumers to **never** click “accept all cookies”



UK consumers hold a high degree of trust in regulations – and prefer to work with companies that showcase compliance

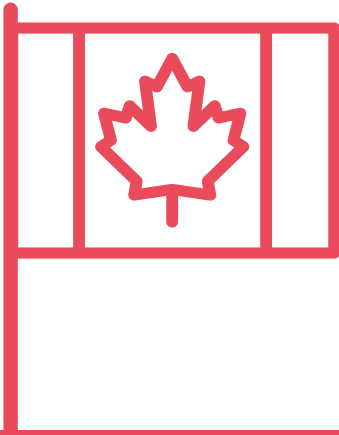
53%

UK consumers were **53% more likely** than US consumers to believe that their country's data privacy regulations adequately protect their personal data

and

34%

More likely than US consumers to feel more comfortable interacting with a website that showcases its compliance with data privacy regulations



While **Canadians** feel the least inclined to take matters into their own hands

57%

Canadian consumers were **57% more likely** than US consumers to feel not informed about data privacy regulations

**but
26%**

Less likely than US consumers to be willing to pay to preserve their privacy

**and
27%**

More likely than US consumers to feel that data privacy should be the responsibility of global regulatory bodies

And US consumers desire personalization



48%

Say that a lack of personalized content sways them to opt out of marketing emails from brands. US consumers place especially high value in personalization, as those in the US were **25% more likely** than those in Europe to say this

To share or not to share? consumers are split

49%

Prefer to select the specific types
of communications they receive

51%

Prefer to completely unsubscribe
or opt-out of all communications

To share or not to share? Consumers are split...

This near 50/50 split suggests a significant divergence in consumer preferences regarding communication engagement.

While nearly half of consumers prefer to have control over the types of communications they receive, the other half lean towards a complete opt-out of all communications.

While nearly half of consumers prefer to have control over the types of communications they receive, the other half lean towards a complete opt-out of all communications.

Businesses must carefully balance the desire for personalized engagement with the need to respect consumer autonomy and privacy preferences.

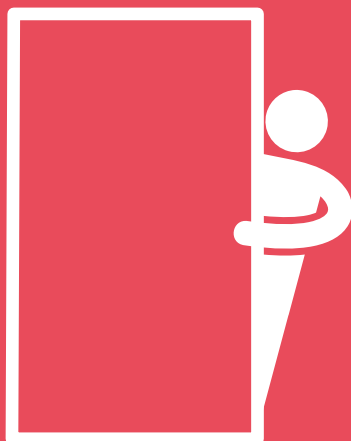
These findings underscore the importance of organizations offering **flexible communication options** that cater to individual preferences.

While some consumers appreciate targeted and relevant communications, others may prioritize privacy and choose to limit their interaction with brands altogether.

Understanding and respecting this diversity in consumer preferences is crucial for businesses seeking to build trust, enhance customer satisfaction, and foster long-term relationships with their audience.

By providing **granular preference controls** for selective communication and ensuring transparency in data usage practices, businesses can demonstrate their commitment to consumer choice and privacy and in turn, drive stronger engagement and conversion.

Where did all the data go? It might be hiding behind a private browser



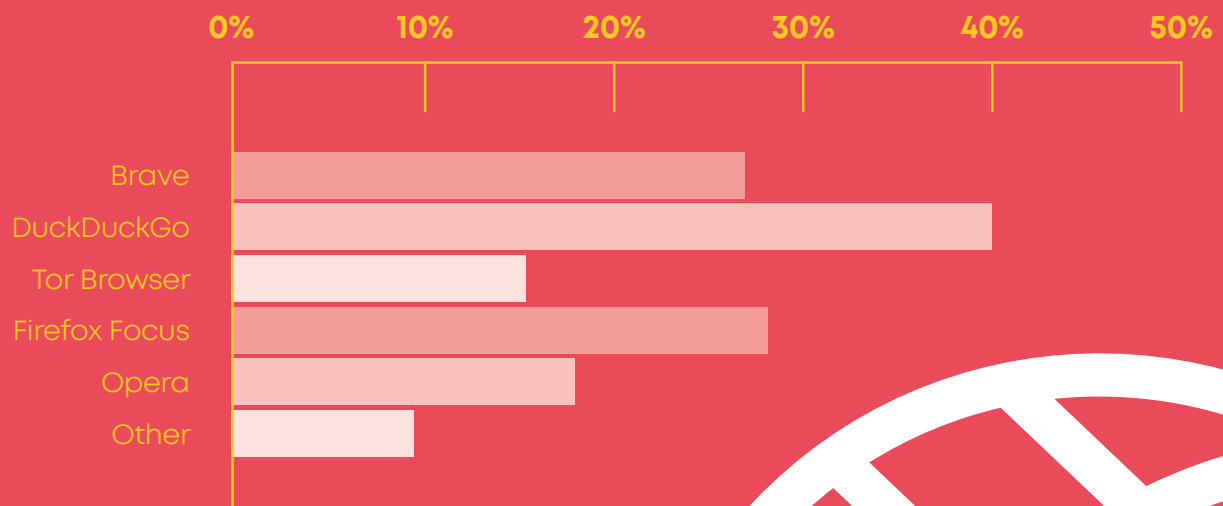
43%

Use a privacy-focused browser
(although UK consumers were **20% less likely**
than US consumers to report this behavior)

What's the most popular privacy-focused browser?



Online browsers



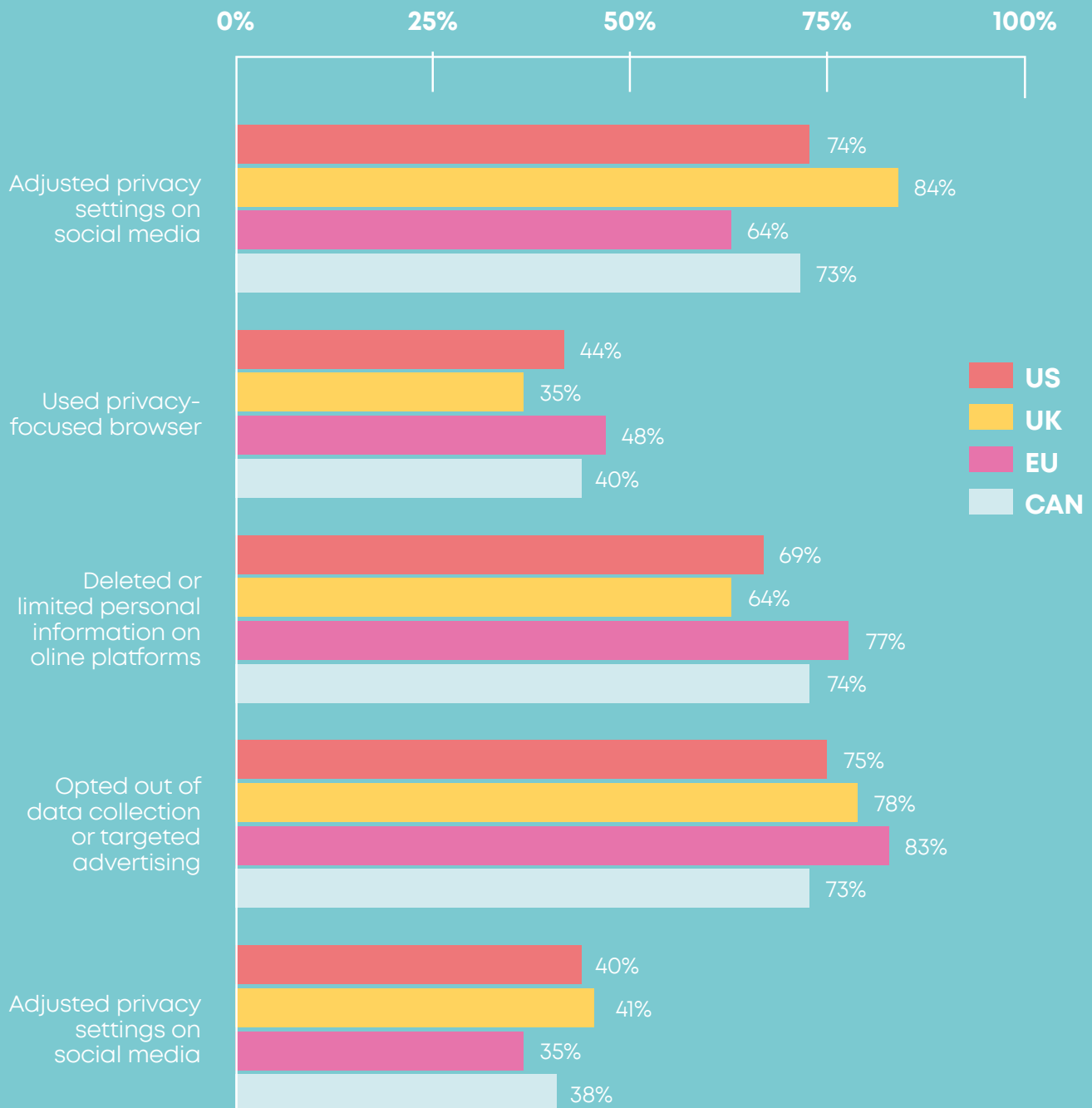
How else are consumers protecting their data?



97%

Of consumers have taken **at least one** action to protect their online data

How else are consumers protecting their data?



But one thing is unanimous - consent fatigue is high



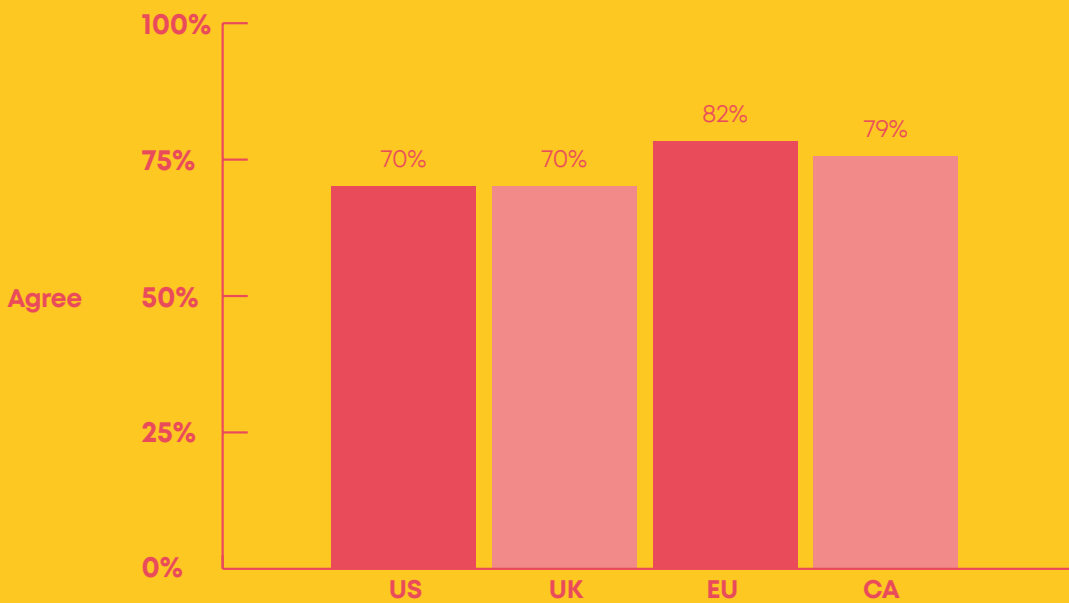
73%

Feel overwhelmed by the number of consent requests when using online services

But one thing is unanimous: consent fatigue is high

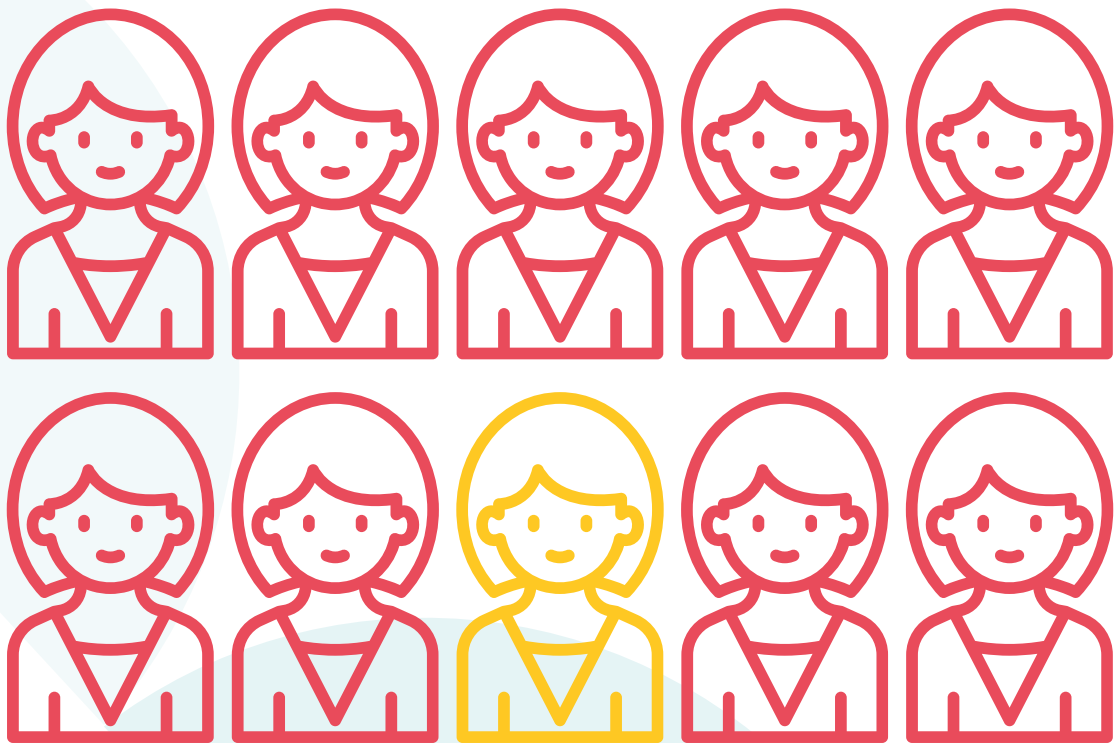


I feel overwhelmed by the number of requests for consent regarding my personal data when using online services



While concerns run rampant, information is hard to come by

9 out of 10



Consumers consider themselves to be
“uninformed” about data privacy

And even when
it's presented –
many consumers
find it challenging



33%

Rarely or never review
privacy policies before
using online services
or apps

and 62%

have consented to
data sharing without
considering the
consequences



30%

Rarely or never read a
consent pop up before
choosing a response

but 29%

always or often click
accept all cookies

In fact, the majority have gone against their gut feeling



67%

Of consumers have consented to cookies in order to view a website, even though they felt skeptical



**Only to face major
consequences**

Half

Of consumers that have consented without considering the consequences - have had their personal information leaked in a data breach

**It's time for companies
to lead the data
information charge
– before consumers
have to learn the
hard way**

63%

Of those who have faced consequences say the experience
changed the way they approach data consent

And swing the pendulum towards a solution that works for all

59%

Prioritize their online data privacy above all else and are willing to forego certain online experiences to maintain it

41%

Value the convenience and benefits of online services more than maintaining strict privacy over their data (Interestingly, Canadian consumers were **26% more likely** than those in the UK to say this)

Or risk losing business

53%

Of consumers have abandoned an online transaction due to concerns about a company's data security in the past 12 months – and US consumers were **25% more likely** than UK consumers to say this



Conclusion

These statistics paint a clear picture of the state of data privacy around the world: while online security concerns continue to surge, consumers are demanding stricter adherence to data privacy standards.

Despite this call for accountability, a significant majority feel that their rights are often overshadowed by corporate profit motives.

Alarming, a large portion of the global population remains uninformed about their data privacy rights, but they believe this responsibility lies with organizations.

Businesses need to prioritize transparency, empower consumers with more control over their data, and uphold rigorous privacy standards to foster trust.

But what about when it comes to regional perspectives?

The regional disparities in consumer attitudes towards online security and data privacy highlight the difficult environment that businesses must steer through in a globalized digital economy.

While US consumers prioritize website trustworthiness and value personalized content, European consumers demonstrate a meticulous approach to privacy, showing a heightened awareness of data consent and a preference for regulatory compliance when it comes to cookie banners.

Considering the UK is governed by just one set of privacy legislation, it's understandable that they feel more adequately protected than consumers in the US. Canadian consumers are somewhat trailing behind when it comes to feeling informed – potentially as they're one of the last of the regions surveyed to bring in more comprehensive legislation that

protects citizen's privacy rights. These findings underscore the imperative for organizations to adopt a tailored approach to user experiences alongside transparent data handling practices based on regional preferences and regulatory landscapes.

How can global brands improve user experiences without compromising on compliance?

This report signals a growing urgency for companies to prioritize transparency and accountability in their data handling practices.

A significant portion of consumers have experienced consequences that have fundamentally altered their approach to data consent, highlighting the tangible impact of privacy breaches on individual behavior.

A clear divide emerges between those who prioritize online data privacy above all else and those who value the convenience of online services, indicating a

complex balance between privacy concerns and the desire for seamless digital experiences. Businesses cannot afford to overlook these shifting preferences, as evidenced by the substantial number of consumers who have abandoned online transactions due to data security concerns.

This trend underscores the potential business repercussions of failing to address consumer apprehensions.

Companies face a pivotal choice: either **proactively lead the charge** towards more transparent and secure data practices or **risk losing consumer trust** and business opportunities.

As consumers become increasingly discerning and proactive in protecting their online privacy, companies must heed these warning signs and prioritize robust data protection measures to maintain competitiveness and build long-term customer loyalty.

Introducing Cassie

Cassie is a Consent and Preference Management Platform (CMP) that powers sustainable revenue growth by respecting individual choices and building stronger customer relationships.

Endorsed by Gartner, Cassie helps to ensure compliance, automates audit trails, and addresses the complex demands of high-volume data scenarios.

With unlimited metadata, Cassie captures and stores more information per data subject than any other CMP, providing new insights beyond behavioral data.

Cassie boosts engagement, sales, and loyalty through granular preference management, increasing marketing ROI while ensuring full consent audits required by legislation. Beyond compliance, Cassie drives better returns on marketing campaigns.

Cassie allows you to:

- Put customer preferences at the heart of your business
- Connect consent across all business, third-party platforms and channels
- Communicate with customers on their terms
- Ensure compliance by default
- Create a single source of truth

Book a Cassie demo to see that you can manage compliance according to your business rules.

[Book a demo](#)

Centralized Consent Management

If you'd like to learn more about how we can help you on your compliance journey, our team of dedicated consent and preference management experts will be able to guide you every step of the way.

UK Office

0800 368 7842
+44 20 4551 9501

US Office

+1 844 585 6264

Australia Office

+61 2 5119 5048

info@trustcassie.com

trustcassie.com/contact

cassie