MIT Technology Review Insights

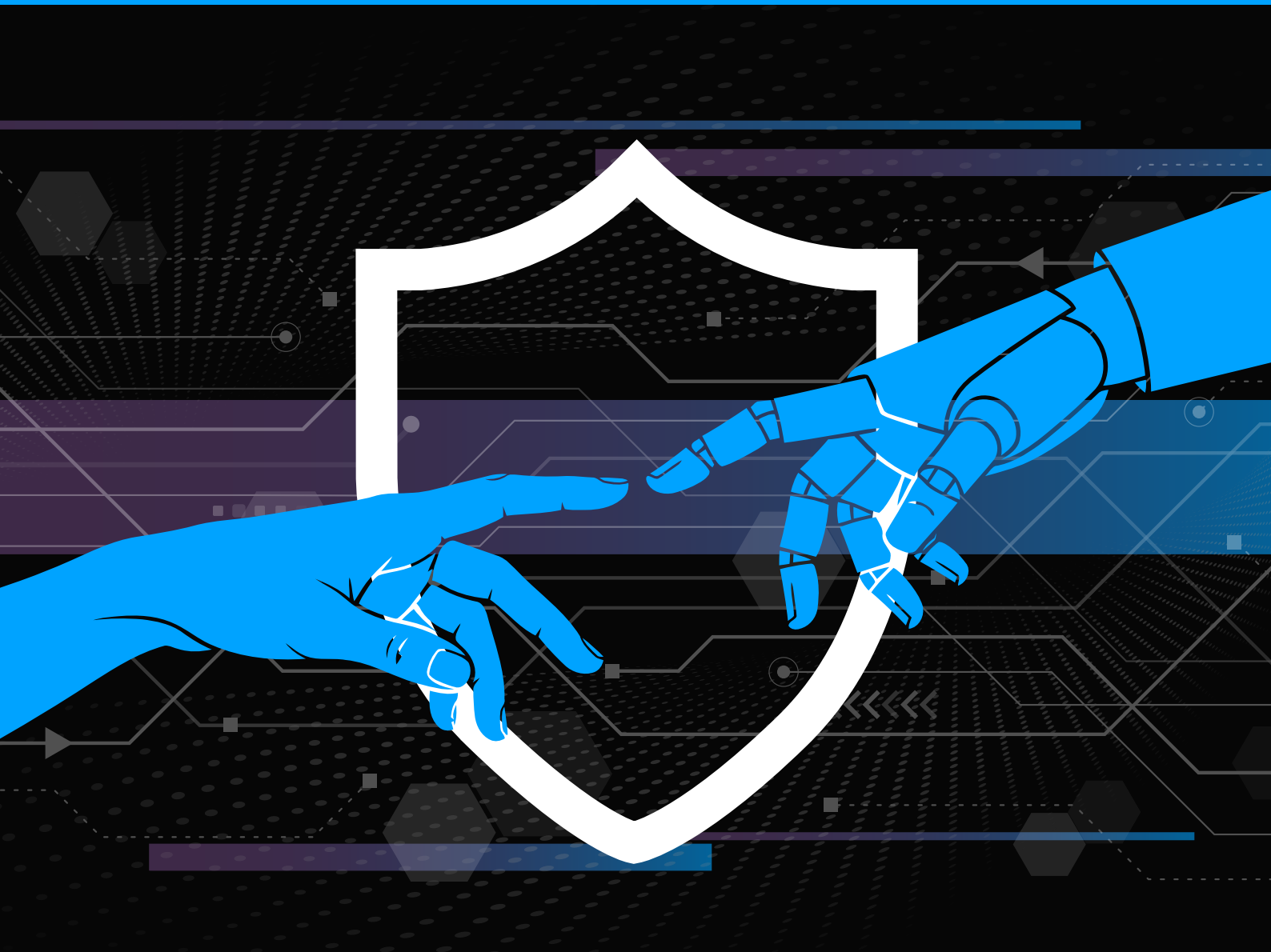
Produced in partnership with

USERCENTRICS

Cookiebot by Usercentrics

Reimagining data consent as an ongoing relationship rather than a one-time compliance concern.

Building trust in the AI era with privacy-led UX



Preface

"Building trust in the AI era with privacy-led UX" is an MIT Technology Review Insights report sponsored by Usercentrics, parent company of Cookiebot. The findings and perspectives presented here draw on research and in-depth interviews with industry experts and practitioners whose work sits at the intersection of privacy technology, digital marketing, consumer analytics, and trust. Stephanie Walden was the author of the report, Laurel Ruma was the editor, and Nicola Crepaldi was the publisher. The research is editorially independent, and the views expressed are those of MIT Technology Review Insights.

We would like to thank the following contributors for their time and insights:

- **Tilman Harmeling,** Strategy and Market Intelligence, Usercentrics
- **Enza Iannopollo,** Vice President and Principal Analyst, Forrester
- **Max Lucas,** Senior Consultant and Managing Director, DWC Consult
- **Adelina Peltea,** Chief Marketing Officer, Usercentrics
- **Jeff Sauer,** Co-founder and CEO, MeasureU

Contents

Foreword

The moment you ask a customer for their data is one of the most consequential moments in the brand relationship. Get it right and you earn trust, consent, and the high-quality first-party data that powers personalization and responsible AI. Get it wrong and you lose customers who rarely return.

That is the insight behind "Building trust in the AI era with privacy-led UX," our report with MIT Technology Review Insights, informed by Usercentrics research and expert interviews across privacy technology, digital marketing, and consumer analytics. It makes the case plainly: privacy is not a constraint on growth. It is a prerequisite for it.

The urgency is real. Our research found that 77% of consumers do not fully understand how their data is being collected and used. AI is raising the stakes further. More than half of users (59%) are uncomfortable with their data being used to train AI models. And unlike a browsing session that can be cleared or a preference that can be adjusted, AI training carries a permanence consumers instinctively sense. With more than 20 U.S. states now operating under distinct privacy frameworks, and enforcement agencies actively demonstrating they will use them, the compliance surface for any brand is no longer manageable through point solutions.

The organizations that build transparent consent infrastructure now will be best positioned to deploy AI responsibly and at scale. Privacy is also moving from a one-time consent event to a managed data relationship. One where what you ask for, when you ask, and how you use the answer all compound into measurable business outcomes: opt-in rates, data quality, and the signal fidelity that makes personalization and AI outputs actually work. That is also why Usercentrics has been investing in the connective layer between consent infrastructure and the AI tools organizations are already deploying, so that privacy decisions made at the point of consent actually travel with the data through its lifecycle, including into AI systems.

This report gives you a practical roadmap for making that shift, anchored in the TRUST framework, five principles for operationalizing privacy-led UX across the customer journey:

- **Translate:** plain language, matched to the moment
- **Reduce:** fewer consent barriers, higher opt-in conversion
- **Unify:** consistency across every touchpoint
- **Secure:** transparent data flows, end-to-end
- **Track:** measure trust through opt-in rates, data quality score, and downstream model performance

The organizations building that infrastructure now, across consent, AI governance, and first-party data quality, are the ones who will have something to work with when the regulatory and competitive environment tightens further. This report shows you how to join them.

Adelina Peltea
Chief Marketing Officer, Usercentrics

01 Executive summary

The practice of privacy-led user experience (UX) is a design philosophy that treats transparency around data collection and usage as an integral part of the customer relationship. An undertapped opportunity in digital marketing, privacy-led UX treats user consent not as a tick-box compliance exercise, but rather as the first overture in an ongoing customer relationship. For the companies that get it right, the payoff can bring something more intangible, valuable, and durable than simple consent rates: consumer trust.

The opportunities of privacy-led UX have only recently come into focus. Adelina Peltea, the chief marketing officer at Usercentrics, has seen enterprise sentiment shift: "Even just a few years ago, this space was viewed more as a trade-off between growth and compliance," she says. "But as the market has matured, there's been a greater focus on how to tie well-designed privacy experiences to business growth."

And it turns out that well-designed, value-forward consent experiences routinely outperform initial estimates.

Touchpoints for privacy-led UX often include consent management platforms, terms and conditions, privacy policies, data subject access request (DSAR) tools, and, increasingly, AI data use disclosures.

This report examines how data transparency builds trust with customers; how this, in turn, can support business performance; and how organizations can maintain this trust even as AI systems add complexity to consent processes. Key findings include the following:

- **Privacy is evolving from a one-time consent transaction into an ongoing data relationship.** Rather than asking users for broad permissions up front, leading organizations are introducing data-sharing decisions gradually, matching the depth of the ask to the stage of the customer relationship. Companies that take this tack tend to gather both a larger quantity and higher quality of consumer data, the value of which often compounds over time.

- **Privacy-led UX is a prerequisite for AI growth**. The consumer data that organizations gather is rapidly becoming a core foundation upon which AI-powered personalization is built. Organizations that establish clear, enforceable privacy and data transparency policies now are better positioned to deploy AI responsibly and at scale in the future. This starts with correctly configured consent mode across ad platforms.

- **Agentic AI introduces new levels of both complexity and opportunity.** As AI systems begin acting on users' behalf, the traditional consent moment may never occur. Governing agent-generated data flows requires privacy infrastructure that goes well beyond the cookie banner.

- **Realizing the advantages of privacy-led UX requires cross-functional collaboration and clear leadership.** Privacy-led UX touches marketing, product, legal, and data teams – but someone must own the strategy and weave the threads together. Chief marketing officers (CMOs) are often best positioned for that role, given their visibility across brand, data, and customer experience.

- **A practical framework can support businesses in getting it right.** Organizations must define their data collection and usage strategies and ensure their UX incorporates data consent, including a focus on banner design. Following a blueprint for evaluating and improving privacy-led UX supports consistency at every consent touchpoint.

02 Digital trust and AI

Most internet users today understand that nothing online is truly free. Every app downloaded or service subscribed to, every search query answered, involves a trade. A growing number of consumers are aware they are participating in a "value exchange" in these scenarios, says Tilman Harmeling, strategy and market intelligence at Usercentrics. "Even apps or services that look 'free' are never neutral to the data behind them," he observes.

And yet, most people still don't precisely know what they are exchanging. A recent Usercentrics report finds that more than two-thirds (77%) of consumers do not fully understand how their data is being collected and used by brands.[1]

Introducing the TRUST framework

Usercentrics has developed the TRUST framework, a blueprint for evaluating and improving privacy-led UX at every customer touchpoint. It serves as the organizing logic for practical guidance throughout this report:

- **Translate** privacy prompts and notices in plain language. Match the communication to the moment. Contextual cues delivered at the right stage of the customer journey are far more effective than dense disclosures presented all at once.
- **Reduce** friction without reducing choice. Design consent interfaces that give genuine equal weight to all options (accept, decline, or customize). Make controls accessible in one or two clicks.
- **Unify** the privacy experience across touchpoints. The consent banner is just one part of a larger ecosystem that includes DSAR tools, preference centers, product permissions, and AI-interaction disclosures. Inconsistencies between these touchpoints undermine trust. Brand consistency in design and language should run through all of them.
- **Secure** data flows end to end, including third-party integrations and AI tools. Map out where consent signals go. Ensure AI tools do not become shadow data processors operating outside the visibility of users or internal governance teams.
- **Track** trust signals and optimize continuously. Establish executive sponsorship and cohesive KPIs across teams. Measure more than just opt-in rate. Track churn, retention, engagement, complaint rates, DSAR volume, and "learn more" click-through rates. A/B test every meaningful change.

That awareness gap translates into both preventive and reactive behaviors from consumers seeking to reclaim control. Proactively, this may look like downloading ad-blocking software or using a VPN. According to Forrester research, more than 90% of consumers used at least one tool to safeguard their digital privacy in 2025.[2] On the reactive front, some actions are small but telling at scale, such as more users declining cookies or tightening their privacy permissions.

"Most people are like, 'Okay, yeah, I know that they're tracking, I'll only do the minimum or I'll accept it. I just want to get to what I want to go to,'" says Jeff Sauer, co-founder and CEO of marketing data company MeasureU. But this can lead to frustration with elements like cookie banners, where users just try to ignore them. "People ask, 'why are cookie banners there?' Even though they are meant to protect you, they feel like a hindrance," Sauer adds.

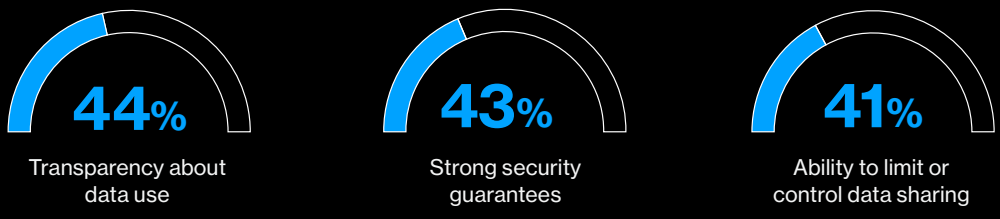
Other consumer responses are more consequential. Transparency is the single most powerful driver of customer trust, according to Cisco's 2026 Data and Privacy Benchmark Study.[3] When transparency breaks down entirely, so can the relationship. The fallout is particularly acute in the aftermath of a public trust violation, notes Enza Iannopollo, vice president and principal analyst at Forrester. "If a company is in the news because of a data breach, one of the first reactions we see among consumers is, 'I want to be forgotten. I don't want you to have my data,'" she explains.

Once severed, consented data relationships rarely return. According to the Thales 2025 Digital Trust Index, 82% of customers have abandoned a brand in the previous year due to data privacy concerns.[4] And, according to a 2025 survey by market research firm YouGov, two-thirds of UK adults stop buying entirely from companies that lose their

Figure 1: The privacy gap: Consumers are uncertain about how their data is being used, what their rights are, and who to trust.

Source: Compiled by MIT Technology Review Insights, based on data from "The State of Digital Trust in 2025," Usercentrics, 2026[6]

Figure 2: Transparency, security guarantees, and the ability to control data sharing are crucial for building trust with consumers.



Source: Compiled by MIT Technology Review Insights, based on data from "The State of Digital Trust in 2025," Usercentrics, 2026[7]

trust. One in five (21%) say they would never trust the brand again.[5]

Trust and opportunity in the agentic AI era

AI is expanding the surface area of data collection faster than most organizations' privacy policies were designed to handle. Agentic AI, now moving from hypothetical to real-world deployment, introduces an especially thorny set of considerations. Where generative AI asks users to make a conscious choice about what to share with a chatbot or copilot, agentic AI systems act on a user's behalf. They can book, purchase, communicate, and make data-sharing decisions without explicit user input at each step.

For privacy-conscious brands, staying ahead of the curve requires rethinking consent systems before agentic tools go live. In an agentic environment, the central consent question shifts from, "Does the user understand what they're agreeing to?" to, "Who is consenting on behalf of the user, to what, and when?" In many cases, the traditional consent moment never occurs at all.

This has profound implications for data governance and enterprise accountability. Organizations deploying agentic AI need infrastructure capable of specifying what agents can access and how user preferences propagate through automated systems. But today, few organizations have fully reckoned with that reality.

Understanding the tech behind privacy-led UX

Privacy-led UX requires infrastructure that can enforce user choices consistently across every data flow. An emerging set of technical tools is giving organizations the ability to minimize what data leaves their environment, control how it is routed, and ensure consent signals are respected end to end.

Server-side tagging is one development in this arena. Rather than firing tracking scripts directly in a user's browser (where data can leak to third parties in uncontrolled ways), organizations route data through their own servers first. This enables them to send only the minimum data necessary to each downstream partner; block or filter outbound data when consent is not present; reduce uncontrolled third-party data leakage; and maintain a clearer audit trail of what was shared, with whom, and under what conditions.

Sauer explains the practical value: "Going to server-side tagging means you can send the conversion to Meta, but you're not violating that person's privacy in the same way because it's not identifiable. You're getting rid of the flaws of the old way of doing things and also having more control over your data."

A harder challenge – and perhaps a more pressing one – is what happens when the data flows are not initiated by a user at all. Agentic AI systems act independently of human oversight, often exchanging data with external platforms and services without triggering any recognizable consent touchpoint. Most organizations have not yet built the governance to manage this; they lack visibility into what their agents are accessing, let alone controls for enforcing user preferences across those interactions.

Model Context Protocol (MCP) represents one emerging approach to that problem. The protocol provides a standardized framework for managing how AI systems exchange information with external platforms. A policy layer built on top of MCP is designed to enable what data an agent can access and share, creates the foundation for logging those interactions for audit purposes, and allows organizations to begin governing user consent preferences through automated systems.

It is, however, early days; while the tooling exists, awareness is still low. "MCP is less than one year old," notes Peltea. "While adoption is increasing, most businesses aren't yet aware that this problem exists, let alone that tools to address it are emerging."

The window to get ahead of the governance gap in agentic AI systems is open but narrowing. Getting the architecture right before it is urgently needed is one of the most consequential privacy decision an organization can make.

The governance challenge takes a different shape when AI agents deploy not on behalf of users, but on behalf of businesses, such as querying, processing, and acting on personal data without a visible consent moment. In these scenarios, the question is not whether a user understands what they are agreeing to, but whether the organization deploying the agent has the infrastructure to enforce consent preferences in real time, across every system the agent touches. This is the more immediate enterprise challenge, and the one that requires consent architecture to be embedded at the integration layer – not bolted on after deployment.

On an optimistic note, the growing ecosystem for data collection is also an opportunity. Every chatbot interaction, copilot query, or personalized recommendation is a valuable signal of customer preferences and behavior, and an opportunity to demonstrate that a brand can be trusted with those insights.

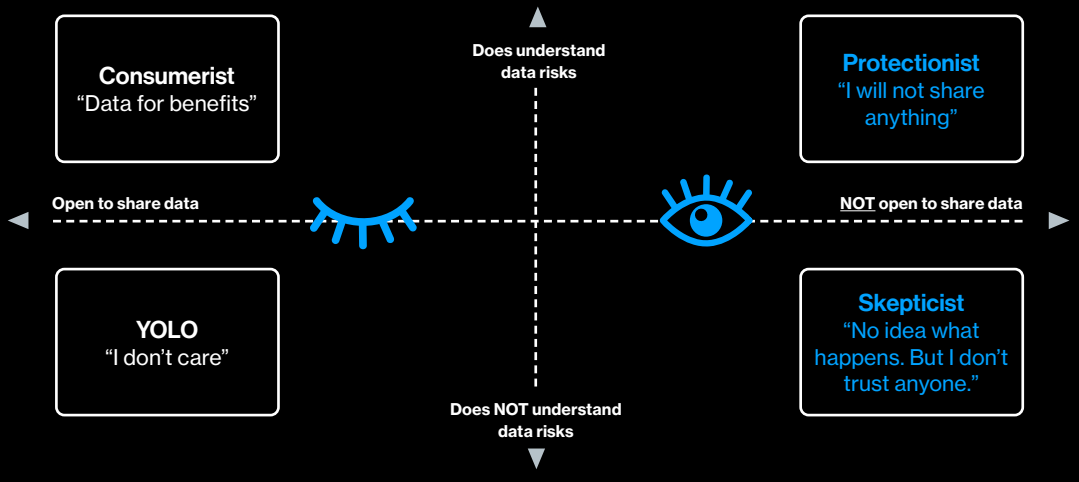
The trust persona matrix (and why it matters)

Not all users approach privacy the same way. Usercentrics has identified four broad consumer trust personas that shape how individuals engage with privacy experiences:

- The **Consumerist** is willing to share data in exchange for tangible benefits and a better experience.
- The **Protectionist** is highly cautious and privacy-focused, requiring a lot of reassurance before engaging.
- The **Skepticist** distrusts most data practices and is uncertain about whether sharing serves their interests.
- The "you only live once" (**YOLO**) cohort is largely indifferent to privacy risks and unlikely to engage deeply with consent decisions regardless of design.

Understanding these personas can help organizations design consent experiences that meet customers where they are.

Harmeling illustrates the contrast with two banking examples. First, Deutsche Bank, whose branding is built on reliability and trust, uses formal, deliberate consent language that aligns directly with what its customer base expects from a legacy financial institution. The second, Revolut, a challenger bank, by contrast, might use lighter, faster language designed to resonate with younger users who prioritize speed and simplicity over institutional formality.



Source: Compiled by MIT Technology Review Insights based on data from Usercentrics, 2026

Realizing that potential depends on getting the data relationship right from the start. The volume and variety of data moments AI introduces then raises the bar for consent communication. Consumers engaging with an AI assistant have different expectations and anxieties than users clicking through a cookie banner. Meeting users where they are requires privacy experiences that are as thoughtfully designed as the AI features they accompany.

In his role as a managing director at DWC Consult, Max Lucas helps enterprise clients implement consent management platforms — the technology that governs how brands ask for and act on user data. At the onset of a new client relationship, he asks about expectations: What consent adoption rate are they anticipating? For U.S. clients, the answer is typically somewhere around 30%. But when the data comes in, many clients are surprised to see higher numbers.

For brands designing these touchpoints and seeking to experiment with privacy-led UX, Lucas outlines a three-pronged approach: "First is transparency, which means you're explaining what you want to do in words that the user can understand. Then there's value — i.e., explaining what your user gets in exchange for their consent. And finally, consistency, which means trying to build the consent model as a natural part of the user journey."

Organizations that establish clear, enforceable privacy practices now, before AI is too heavily ingrained in their customer experiences, will be better positioned to deploy the technology responsibly and at scale. Companies would be prudent to think of privacy-led UX as less a constraint on AI adoption and more of a prerequisite for it — the foundation that makes recommendation and automation both possible and accurate.

The privacy paradox

Harmeling points to a key tension regarding how consumers relate to consent. On one hand, Usercentrics research from 2025 shows that nearly half of users now click "accept all" cookies less frequently than they did three years ago, and opt-in rates are declining in many markets around the globe.[8] On the other hand, the friction and repetition of privacy prompts have led to a kind of numbness — a reflexive click-through that results from the sheer volume of interruptions.

"We tend to see two evolutions. One is consent fatigue: People are tired of seeing consent solutions and cookie banners. But at the same time, we're seeing what I call a 'privacy awakening,'" says Harmeling. "People are clicking on the 'more information' button more frequently to go a little deeper into what's actually being done with their data."

A related dynamic is playing out around AI. Use of AI-powered tools is skyrocketing, even as users express growing discomfort with how their data may be used in training and personalization. This is sometimes called the AI trust gap.

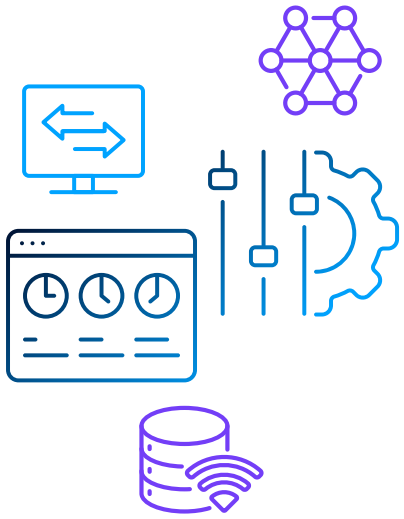
Iannopollo has studied these phenomena closely, and she believes both are less about consumer apathy and more about the conditions under which privacy decisions are made. "If you're going to ask me 25 things in the first two seconds I'm on your website, chances are I'm going to skip through," she says. "This isn't because I don't think privacy is important, but I'm there to accomplish a task, and reading the policy in-depth is not going to help me meet my goal." Cognitive overload, in other words, makes privacy decisions feel like obstacles rather than choices.

That pressure intensifies in AI contexts where urgency around adoption adds layers of rationalization. Peltea points to another psychological element: the fear of being left behind as peers and colleagues adopt the most revolutionary technology of our modern era at breakneck speed. "Individuals and businesses feel a sense of overwhelm, like, 'Oh, if I'm not jumping on AI, I'm falling behind.' And ultimately it's true — it's a very powerful tool." When a technology promises immediate productivity gains, people often prioritize usefulness first and worry about privacy later.

Ultimately, the privacy paradox points to a system under strain rather than a population that does not care. Users who are overwhelmed, rushed, or unaware of what they are agreeing to are more often than not simply responding to poor design.

The bottom line for enterprises: organizations that treat declining consent rates or low engagement as evidence of user apathy are likely misreading the signal. The more accurate diagnosis (and the more actionable one) is that the experience itself is failing them.

03 Privacy-led UX as a catalyst of digital trust



A consent banner is often a user's first interaction with a brand's data practices, and first impressions matter. Still, a lot of organizations miss the mark – sometimes by accident, sometimes by design.

In the TRUST framework, it's no accident that "translate" is the very first pillar. The most common mistake is overwhelming users with text that's difficult to parse. A NordVPN study found that if the average internet user were to read every privacy policy they encountered on the roughly 96 websites they visit in a typical month, it would take a full workweek to accomplish the task.[9]

Some companies lean into that knowledge, deploying dark patterns, or design choices intended to be opaque. These include cognitive overload (overwhelming users with excessive choices or technical jargon), disruptive timing (presenting privacy decisions in high-emotion scenarios), and complexity that makes follow-through impractical (requiring multiple steps or fragmented navigation to adjust preferences).

The short-term conversion gains from these tactics tend to obscure longer-term costs, which can include higher churn, increased data deletion requests, and serious reputational exposure if deceptive design practices become public. This rings particularly true when brands fail to hold up their end of the bargain by taking data without delivering the value users were led to expect. Sauer offers a blunt assessment: "To me, there's always been an unwritten rule of the internet: You're not going to be around very long if you keep on bait and switching people."

> "You can have a very bad or non-compliant consent notice, and your rates might be very high, but it doesn't mean anything. Instead, focus on retaining or winning customers as a verifiable result of privacy design or consent moments. Success is really seen around those metrics."
>
> **Enza Iannopollo**, Vice President and Principal Analyst, Forrester

Other common UX failures are more mundane, such as cookie banners that look visually out of place or privacy messaging written in a generic voice that clashes with a brand's personality everywhere else. These design mismatches subtly signify that privacy is an afterthought, not a considered part of how the company treats its customers.

Peltea notes that the problem is more often rooted in flawed strategy than poor banner design alone. "The

banner is just the tip of the iceberg. The complexity is not in the solution; it's in defining your whole data relationship and the strategy around UX to also incorporate consent and data," she says.

What good privacy-led UX looks like

Effective privacy-led UX ensures that data policies are easily intelligible and that privacy settings are intuitive throughout the entire customer journey.

Circling back to that "Translate" principle of Usercentrics's TRUST framework, the most fundamental best practice is clear, plain-language communication delivered at the right moment. "The idea is to tell consumers what they need to know, when they need to know it, in a way that they don't need a dictionary to understand," says Iannopollo.

"Unify" is another core tenet of TRUST. When a consent experience shares the visual cues and vocabulary of the rest of a company's customer-facing presence, it signals intentionality. Harmeling points to clothing retailer Zalando as an example of well-executed brand consistency: The company uses phrasing like "tailor your privacy settings," aligning the language directly with its fashion identity. Porsche, similarly, frames its privacy experience around "full control," language that nods to putting customers in the driver's seat both literally and figuratively. "This type of on-brand messaging makes users feel welcome," says Harmeling.

The Unify pillar also encompasses internal agreement over brand messaging and governance; privacy-led UX rarely lives entirely within a single team – it touches marketing, legal, product, IT, and data operations. Coordination requires the kind of cross-functional alignment that does not work without deliberate structure.

> "The companies that are most sophisticated avoid sharing identifiable information for two reasons: They respect the privacy of users and get better performance. And that's how companies can shift data consent to their favor."
>
> **Jeff Sauer**, Co-founder and CEO, MeasureU

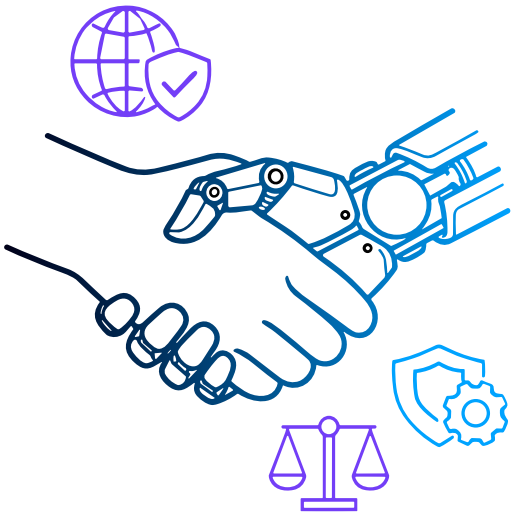
Driving internal alignment

One of the structural challenges to measuring privacy ROI is internal fragmentation. Harmeling has observed a common disconnect in cross-functional conversations about privacy-led UX. "The legal department and the marketing department both want to create a more trusted environment. They have the same goal fundamentally, but how they define trust is entirely different." Establishing shared KPIs that achieve consensus on that definition helps prevent teams from optimizing against each other.

Facilitating that alignment is, increasingly, a CMO-level responsibility. The role's visibility across brand, data, and customer experience puts CMOs in one of the best positions to translate privacy practice into strategy.

The following questions can help surface gaps in strategy and accountability before they become costly downstream:

- What are the five things we should change this quarter, and who owns each of them: marketing or legal?
- How will we know if our strategy is working in 90 days? What are the specific signals we will track?
- What is the revenue upside? What is one credible pathway from privacy investment to measurable business outcome?
- What is the risk if we do nothing? Have we mapped the compliance exposure, the reputational risk, and the data quality cost of the status quo?



> "Even just a few years ago, this space was viewed more as a trade-off between growth and compliance. But as the market has matured, there's been a greater focus on how to tie well-designed privacy experiences to business growth."
>
> **Adelina Peltea**, Chief Marketing Officer, Usercentrics

Timing is where "Reduce" and "Translate" from the TRUST framework come into play. Iannopollo has mapped customer journeys for financial services clients and found that, in the vast majority of cases, privacy communications are presented at the worst possible moments – often during high-friction steps when users are already frustrated, such as when troubleshooting an account error. The fix is architectural: integrating privacy cues contextually, at lower-stakes moments when a user is more likely to engage thoughtfully, such as when first saving a payment method.

Finally, leading organizations are moving away from front-loading all consent requests at once. Peltea advocates for what she calls "contextual consent." "As consumers gain more trust with the company by engaging and subscribing, that's when brands can start to ask for more information," she explains.

Gauging success and measuring what matters

The last pillar of TRUST – "Track" – provides evidence that data transparency efforts are working. Iannopollo is direct about the fact that translating privacy investments into revenue requires measuring more than just consent rates. "You can have a very bad or non-compliant consent notice, and your rates might be very high, but it doesn't mean anything," she says. "Instead, focus on retaining or winning customers as a verifiable result of privacy design or consent moments. Success is really seen around those metrics."

Beyond the headline metrics of customer acquisition and retention, Iannopollo advocates for embedding privacy-related questions directly into customer experience feedback loops: "Ask questions like, 'Do we think we're transparent in the way we explain things? Do you know how we use your data?'"

A/B testing – or split testing, a randomized experimentation method used to compare two versions of a webpage or banner, for example – is another underused tool. Rather than benchmarking against competitors' consent notices, Iannopollo recommends that every organization benchmark against its own prior performance. "I encourage a company to do A/B testing every single time they change any of their privacy messages or pages, because that gives you an idea of what's working," she says. "The metrics should be winning customers, retaining customers, and supporting emerging technology adoption," she reiterates.

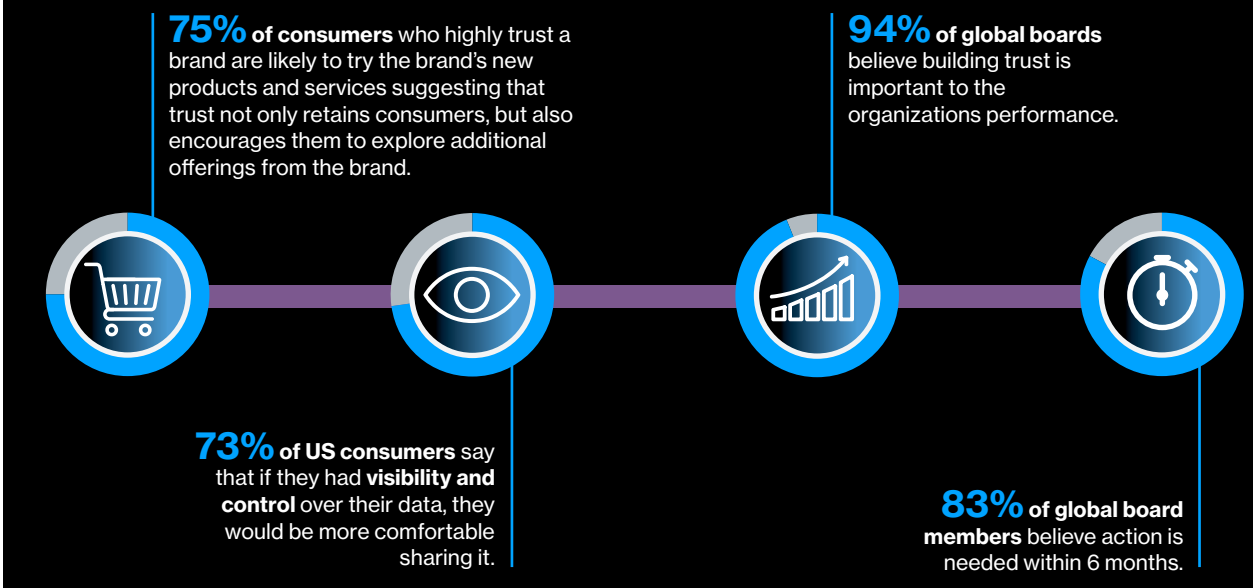
"The companies that are most sophisticated avoid sharing identifiable information for two reasons: They respect the privacy of users and get better performance. And that's how companies can shift data consent to their favor," Sauer adds.

04 The ROI of privacy-led UX

The most direct business case for privacy-led UX relates to first-party data. It can strengthen both the quantity and quality of customer data by encouraging users to engage more deeply with brand ecosystems. "If more businesses would treat things like consent banners as an opportunity instead of as something that only slows them down, I think we could see huge improvements in terms of brand trust," says Lucas.

Iannopollo describes the compounding effect of trust-building: "Consumers feel more comfortable sharing data with a company, and the data itself is the value. We also know that consumers who trust companies tend to buy

Figure 3: Leaders see a strong connection between consumer trust and business performance.



Source: Compiled by MIT Technology Review Insights, based on data from "Navigating Trust," Deloitte, 2026[10]

> "Transparency means explaining what you want to do in words that the user can understand. Then there's value, i.e., explaining what your user gets in exchange for their consent. And finally, consistency, which means trying to build the consent model as a natural part of the user journey."
>
> **Max Lucas**, Senior Consultant and Managing Director, DWC Consult

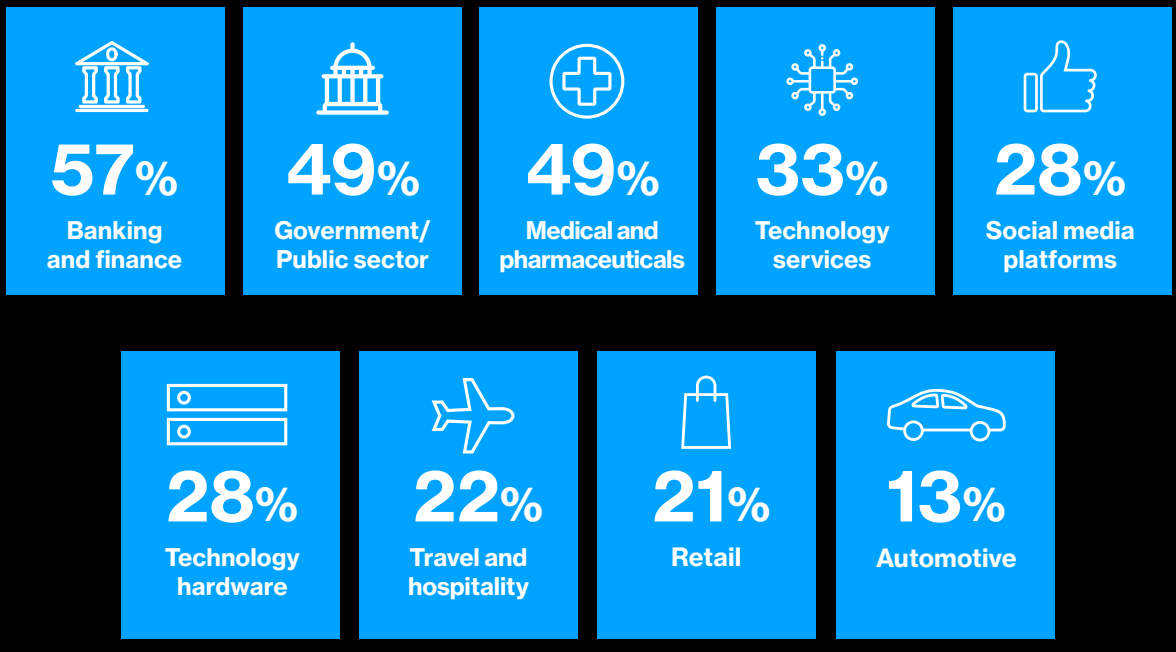
more from them and advocate more for that company. And interestingly, we also know that if a consumer trusts a brand, they're more likely to trust any companies associated with that brand, so there is a third-party effect." For organizations building AI-powered personalization capabilities, consented data is the foundation; You cannot adequately train your models without it.

Conversely, the costs of poor privacy UX often accumulate over time. "When you fail to create a good privacy experience from the beginning, as a company, you've fundamentally lost – you've lost the customer, you've lost the trust, and it will cost you money," says Harmeling.

A regulatory landscape in flux

The business case for privacy-led UX is reinforced by a regulatory environment that's rapidly expanding in scope. In the EU, the General Data Protection Regulation (GDPR) established the baseline, and the EU AI Act is now

Figure 4: Consumers are most likely to share their personal data with highly-regulated sectors like banking, government, and health care.



Source: Compiled by MIT Technology Review Insights based on data from "The State of Digital Trust in 2025," Usercentrics, 2026[12]

layering on additional requirements. In the United States, 20 states have enacted comprehensive privacy laws, and litigation is becoming more common even in the absence of a federal standard.[11]

"...well, it's the U.S. and we don't have federal laws," observes Sauer. "But many states have enacted their own privacy laws, and companies are getting letters threatening lawsuits..."

Notably, beyond being a compliance driver, regulation can also function as a trust signal. "What we are starting to see from the data is that highly regulated companies are the most trusted with AI. There seems to be an idea that if you're highly regulated, you know what you're doing, so consumers immediately have more trust in what these organizations are doing with AI. Less-regulated organizations are farther down in that list," says Iannopollo.

Years of demonstrated compliance have built a reservoir of consumer trust that can be extended to AI initiatives. But Iannopollo caveats that the reservoir is finite, and an AI misstep in a regulated industry likely carries hefty reputational consequences.

Governance as an AI growth lever

Responsible AI deployment runs on governance infrastructure. That includes internal systems for tracking data flows and auditing how privacy commitments are upheld in practice. Without those systems, privacy-led UX remains a surface-level exercise.

Evidence is emerging that AI readiness also draws from the same governance infrastructure. Iannopollo notes that when Forrester surveyed privacy professionals about the return on investment of their privacy programs, the second most common answer last year, after regulatory compliance, was enabling AI adoption. "Much of that work is actually supporting innovation," she says.

Agentic AI highlights the need for proactive governance even further. With generative AI, a governance gap is a disclosure problem – something that can, in principle, be fixed with clearer communication after the fact. With agentic AI, where automated systems can make data-sharing decisions before a user is ever aware, the governance gap becomes structural. There is no moment to go back and correct. The permission architecture must be in place before the agent acts.

> "When you fail to create a good privacy experience from the beginning, as a company, you've fundamentally lost – you've lost the customer, you've lost the trust, and it will cost you money."
>
> **Tilman Harmeling**, Strategy and Market Intelligence, Usercentrics

From disclosure to architecture

Architecture is the operative word in the future-focused conversation about privacy, data transparency, and responsible AI deployment. For much of the internet's history, privacy appeared mainly at the margins of the user experience – present in policies, prompts, and regulatory disclosures. Increasingly, it is becoming part of the product itself. The way companies design those moments of choice and control will play an increasingly important role in how customers evaluate digital services and the organizations behind them.

Put differently: If the past decade forced companies to acknowledge privacy, the next one will require them to design around it.

That transition hinges on a question that no framework or technical standard can fully answer: whether an organization is genuinely committed to earning consumer trust or merely managing the appearance of it. In Iannopollo's view, consumers are better at sensing the difference than most brands assume. "The perception of a brand is the goodwill of the brand. Accountability is the very first dynamic that goes into place for any trust-building exercise," she says. "And your organization needs to remember that accountability helps consumers trust them. I think that is more important now than it has ever been."

Footnotes

1. "The State of Digital Trust in 2025," Usercentrics, July 1, 2025, https://usercentrics.com/resources/state-of-digital-trust-report/.
2. Stephanie Liu and Anna Hoskins, "Consumers are Privacy-Savvy and AI-Wary: Insights from the US Consumer Privacy Segmentation Report," Forrester, October 15, 2025, https://www.forrester.com/blogs/consumers-are-privacy-savvy-and-ai-wary-insights-from-the-us-consumer-privacy-segmentation/.
3. "Cisco 2026 Data and Privacy Benchmark Study," Cisco, https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html.
4. "Global Trust in Digital Services Declines, finds Thales," Thales, March 18, 2025, https://cpl.thalesgroup.com/about-us/newsroom/digital-trust-index-2025.
5. Janice Fernandes, "How Brands Can Rebuild Trust with UK Consumers After Losing It," YouGov, September 19, 2025, https://yougov.com/en-gb/articles/53019-how-brands-can-rebuild-trust-with-uk-consumers-after-losing-it.
6. "The State of Digital Trust in 2025," Usercentrics, July 1, 2025, https://usercentrics.com/resources/state-of-digital-trust-report/.
7. "The State of Digital Trust in 2025," Usercentrics, July 1, 2025, https://usercentrics.com/resources/state-of-digital-trust-report/.
8. "The State of Digital Trust in 2025," Usercentrics, July 1, 2025, https://usercentrics.com/resources/state-of-digital-trust-report/.
9. Irma Šlekyt, "NordVPN Study Shows: Nine Hours to Read the Privacy Policies of the 20 Most Visited Websites in the US," NordVPN, October 23, 2023, https://nordvpn.com/blog/privacy-policy-study-us/.
10. "Navigating Trust: An Advertiser's and Marketer's Guide to Data, Privacy, and Trust," Deloitte, 2024, https://www.deloitte.com/content/dam/assets-zone3/us/en/docs/services/risk-advisory/2024/us-advisory-navigating-trust.pdf.
11. F. Paul Pittman, Hope Anderson, and Abdul M. Hafiz, "US Data Privacy Guide," White & Case, January 20, 2026, https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide.
12. "The State of Digital Trust in 2025," Usercentrics, July 1, 2025, https://usercentrics.com/resources/state-of-digital-trust-report/.

About MIT Technology Review Insights

MIT Technology Review Insights is the custom publishing division of MIT Technology Review, the world's longest-running technology magazine, backed by the world's foremost technology institution – producing live events and research on the leading technology and business challenges of the day. Insights conducts qualitative and quantitative research and analysis in the US and abroad and publishes a wide variety of content, including articles, reports, infographics, videos, and podcasts. This content was researched, designed, and written by human writers, editors, analysts, and illustrators. This includes the writing of surveys and collection of data for surveys. AI tools that may have been used were limited to secondary production processes that passed thorough human review.

About Usercentrics

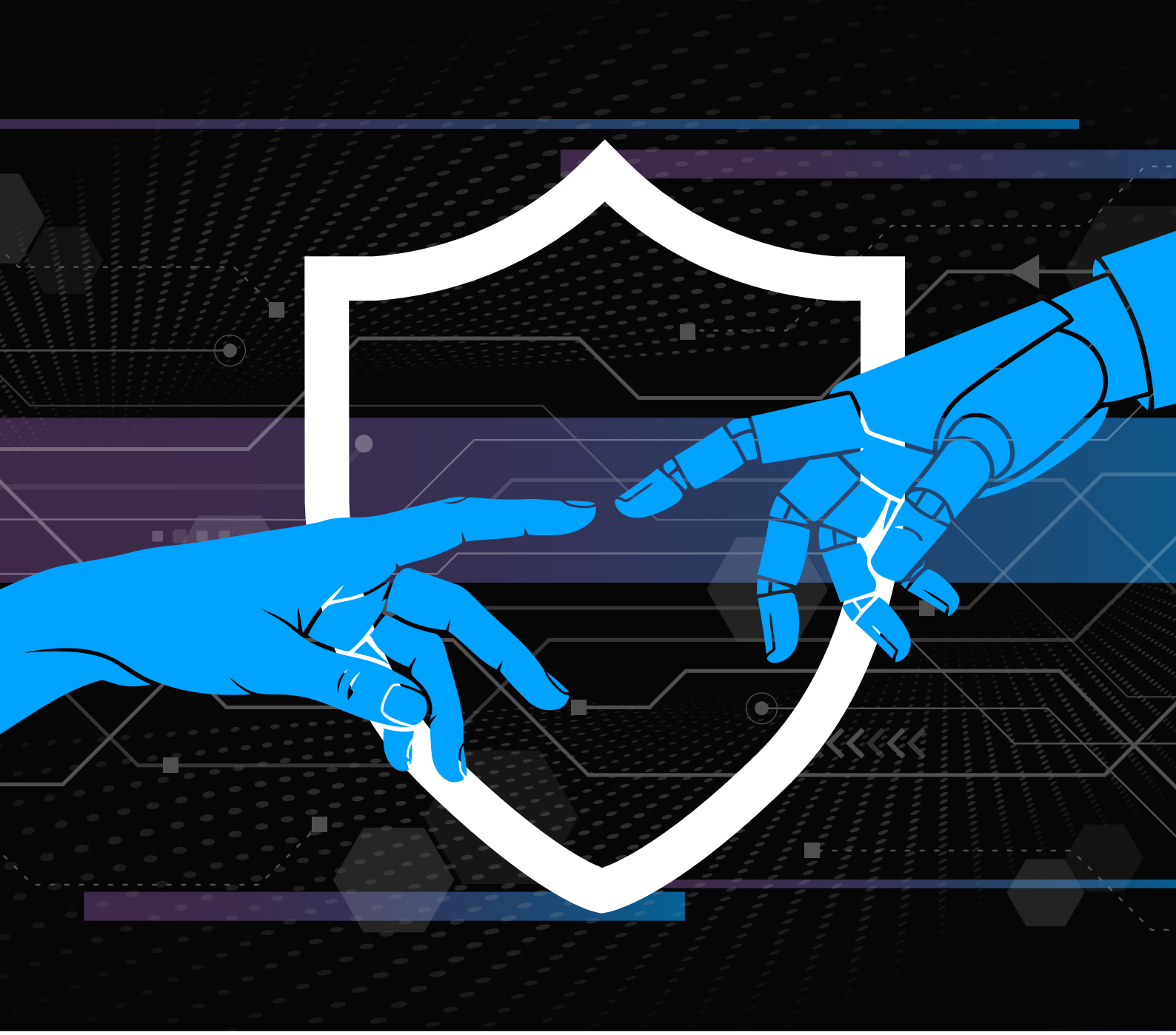
Usercentrics is the global leader in privacy-led marketing, helping turn consented data into business performance. Our suite makes it easy for brands to collect, activate, and measure data across websites, apps, and AI-driven experiences. With privacy built into data flows, we give businesses the infrastructure to run smoothly and grow with confidence. Active in 195 countries and processing over 8.8 billion user consents every month, Usercentrics helps brands do better marketing, grounded in people's choices and built on scalable trust. Learn more at usercentrics.com.

USERCENTRICS

Cookiebot by Usercentrics

Designed by Shultz Design Collaborative, LLC. Illustrations provided by Adobe Stock.

To cite this report, please use: "Building trust in the AI era with privacy-led UX," MIT Technology Review Insights and Usercentrics, April 2026.



MIT Technology Review Insights

www.technologyreview.com

insights@technologyreview.com