publicis
sapient

✦ DBT GPT

Beyond Compliance: What Enterprise Leaders Get Wrong About AI and Privacy

Real insights from our privacy experts who've been in the trenches with Fortune 500 clients

Emma Smith
Lead Data Protection Lawyer, Publicis Groupe
✉

Rachel Trube
Senior Principal Consultant, Data Strategy
✉

Todd Cherkasky
GVP Customer Experience & Innovation Consulting, Publicis Sapient, Chicago, IL
✉ in

Nadiah Bierwerth
Senior Associate, Risk Management
✉

Here's something that might surprise you: The biggest barrier to successful AI implementation isn't technical complexity or budget constraints. It's privacy. But not in the way most C-suite executives think.

We recently convened a roundtable with our privacy experts from across Publicis Sapient—practitioners who work daily with enterprise clients navigating AI transformation. What emerged wasn't the usual "privacy vs. innovation" debate. Instead, our team revealed how the companies winning at AI are the ones that figured out privacy isn't a hurdle to clear, but rather the foundation on which everything else is built. This isn't just about compliance checkboxes; it's about the human element where trust becomes the cornerstone of successful AI adoption.

Their insights challenge almost everything most enterprises think they know about privacy in the AI era.

The Netflix wake-up call: when "compliant" isn't enough

Let's start with a story that should terrify every CTO planning an AI rollout.

Back in 2006, Netflix thought they were being clever. They released viewing data for half a million users to fuel a public algorithm contest, explained Rachel Trube, a senior principal of data strategy in our strategy and consulting practice. "They took all their user profile data and completely anonymized it. So there was nothing personal in there."

Sounds responsible, right? Here's the problem: "A crafty Ph.D. student was still able to cross reference all of the reviews [and] review dates with publicly available IMDb user ratings... [and] successfully identify many of those Netflix users."

The result? A class-action lawsuit and a harsh lesson about the difference between technical compliance and actual privacy protection.

"This proves that you can still make your customers uneasy and erode trust in your brand without violating any technical, legal or compliance guidelines," Trube noted.

The Netflix example hits at something deeper that Emma Smith, our lead data privacy counsel for the United Kingdom and Ireland, emphasized: **"Privacy as a human right is the only right that is recognized in commercial contracts."** Think about that. Out of all human rights, privacy is so fundamental that it shows up in business contracts between companies.

At Publicis Sapient, we see this play out with clients who think they can optimize their way around privacy concerns. It never works in the long run.

Stop feeding the machine: why more data

isn't better data

Here's where most enterprises go wrong with AI: They think success means collecting everything possible. In reality, we've helped clients build AI systems that perform better than their legacy systems while using significantly less customer data.

"There's this sense we have with Gen AI that you just need to feed the machine," Trube observed from her work leading data efforts on our core AI program. "Companies are feeling pressure to differentiate themselves with Gen AI by stockpiling all of their data so that they can feed their machine data no one else has."

But this "data hoarding" approach, as she calls it, "goes completely against a core data privacy principle which is minimization."

The key insight? Companies that practice thoughtful data collection, focusing on quality over quantity, often build better AI systems. They're forced to be more strategic about what they collect, more sophisticated about feature engineering and more focused on genuine business outcomes. This doesn't mean collecting less data necessarily, but collecting the *right* data. After all, AI systems are only as good as the data that powers them, and without sufficient, high-quality data, even the most advanced algorithms will underperform. The goal isn't data minimization for its own sake, but rather purposeful data collection that balances privacy principles with the substantial data requirements that effective AI demands.

Gaurav Goel, our technology lead who works with major financial services clients on digital transformation, sees this firsthand: "We apply principles while we are devising new products for the customers, taking on data security and confidentiality with utmost care. We take considerations in terms of what minimum data to capture, how to store the data, how to synchronize the data."

The result isn't limitation—it's clarity and efficiency.

The five-principle framework that actually works

Most ethics frameworks fail because they're academic exercises that are disconnected from daily decisions. Todd Cherkasky, our CX and innovation consultant who's spent years working with our ethics and responsible use working group, shared an approach that's actively being used in the field with our clients.

"Over the past couple of years, we've built out a framework that has five principles as part of our ethics and responsible use framework," he explained. "One of them is, of course, privacy and security. The others are fairness, transparency, accountability and beneficence."

But here's what makes this different: It's designed to help teams, not constrain them. "When we do all of these things," Cherkasky noted, "we gain trust and our clients gain trust."

He shared a concrete example from our work: "Recently, a team [...] reached out to the working group on Ethics and responsible use, and they were building a chatbot and had some really great ideas for supporting employees who have cancer [...] But as we started talking about privacy, the team realized that they can anticipate a lot of other use cases by thinking through the principles."

The privacy review didn't slow them down—it made their product better. This is the kind of transformation we see when enterprises stop treating privacy as a constraint and start treating it as a design principle.

GDPR isn't the enemy (really)

Here's probably the most counterintuitive insight from our discussion: The General Data Protection Regulation (GDPR) and similar regulations aren't innovation killers. They're innovation directors.

Smith, as lead aata privacy counsel for the U.K. and Ireland, pushed back hard against the common view of GDPR as a blocker: "I very rarely in my professional experience have worked with something where GDPR absolutely forbids you to do it. There may be a different path that's slightly different to what you anticipated, but [...] you'll still be able to achieve the same outcome."

Her advice to our clients? "Think of it more as a resource to go to: Is there another way that

I can do this that sits more comfortably within a legal framework and therefore recognizes people's rights in a more responsible way?"

This reframing is powerful. Instead of asking, "How do we work around privacy rules?" successful companies ask, "How do privacy principles help us build better products?" We've seen this approach lead to breakthrough innovations for our clients.

The consent theater problem

Francis Walton, who heads research and insights in our international practice, highlighted something every enterprise leader should understand: Traditional consent is broken.

"We use a consent form as part of any sort of formal interview, the consent form fields sort of now on about four pages and cover [...] several dozen different options and different levels of complexity around the consent," he said. "I don't think there's any consumer that really genuinely understands fully what they're potentially consenting to."

But here's what's changing: "I think consumers start to understand that their data's got currencies, got value and how that value is expressed to them or can be realized is different," Walton observed from his work with real consumers.

Smart companies are moving beyond consent theater to genuine value exchange. As Trube put it: "Companies need to treat their data collection as part of this two-way relationship they have with their customers [...] you check in and you have to make sure that both parties are getting value out of that relationship."

This is exactly the kind of shift we help our clients navigate—moving from compliance-driven consent to relationship-driven value exchange.

The competitive advantage hidden in plain sight

Here's what became clear from listening to our practitioners: Companies that nail privacy don't just avoid problems—they unlock advantages their competitors can't match.

Smith emphasized this point. "It's really important to protect but also find new ways of innovating this right, implementing this right, creating experiences that uphold this right to privacy."

The companies winning at AI privacy aren't just checking compliance boxes. They're building systems that users actually trust and want to engage with. That trust translates into better data quality, higher user engagement and genuine competitive differentiation.

We see this with our most successful client engagements. The enterprises that treat privacy as a strategic capability—not just a legal requirement—consistently outperform their competitors on user adoption, customer satisfaction and long-term retention.

What this means for your AI strategy

The message from our experts is clear: If you're treating privacy as something to minimize or work around, you're missing the point entirely.

As Cherkasky put its: "Privacy, ethics, responsible use [...] is really core to your work, not just an add-on or something that somebody else is going to help you protect. And not just because it's the right thing to do, which it is. But it creates better outcomes, better design, better practice."

At Publicis Sapient, we've seen this principle validated across hundreds of client engagements. The enterprises that will dominate AI aren't necessarily those with the most data or the fastest algorithms. They're the ones building systems that people actually want to use—systems that feel respectful, valuable and trustworthy.

That's not just good ethics. In an era where AI can feel invasive and impersonal, it's the competitive advantage that separates market leaders from everyone else.

Ready to turn privacy from a constraint into a competitive advantage? Let's talk about how we can help you build AI that people actually trust.

Related Topics

Data Management | AI Ethics