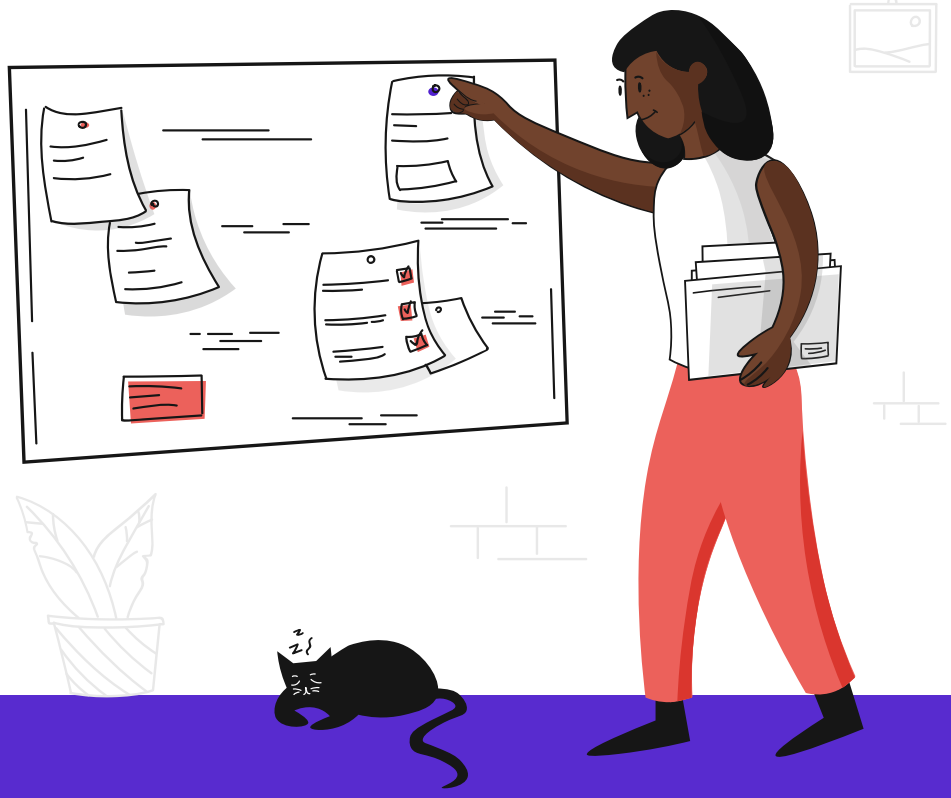
Transcend



A DATA PRIVACY ROSETTA STONE GUIDE
BY TRANSCEND

Building a Best-in-Class Privacy Program Without Breaking the Budget

Strategic learnings to help build user-centric data privacy experiences without burning out your engineering team, or blowing your budget.

transcend.io

Contents

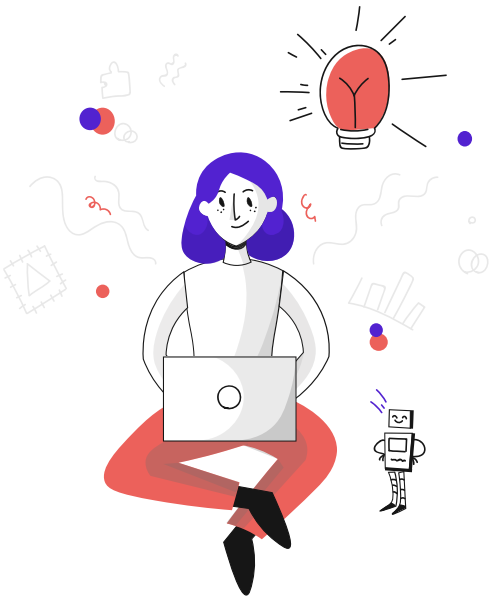
INTRODUCTION

At the world's largest technology companies, data privacy is often treated like a product line—staffed with hundreds of backend and frontend engineers, product managers, and technical program managers who are all tasked with building privacy features and scalable infrastructure.

However, if you're an engineering leader at any other company, resourcing data privacy is likely a far more daunting and sometimes miserable task. Between driving cross-functional alignment, creating scalable solutions, and managing engineering staffing preferences, there's a lot to consider in an area that is only increasing in complexity and importance.

But is it possible to build a strong corporate privacy program and tech stack without dedicated teams, a budget with more than a few zeroes, and a board-level prioritization mandate?

Based on our work helping companies like Robinhood, Indiegogo, and Patreon future-proof their data privacy programs, **we believe the answer is yes**, and that any company can make smart data privacy investments based on four core principles that unlock not only competitive leadership on privacy, but bring down costs and scaling challenges in the long run.



BACKGROUNDER: DEFINING CONSUMER-CENTRIC PRIVACY

Before diving into the specifics of each role of your privacy engineering team, it's useful to stop and understand the end goal — what makes a great data privacy program.

At Transcend, we believe that these programs—often exemplified by giants like Apple and other enterprise leaders—start with one simple mission of **going beyond compliance to deliver great user experiences when it comes to privacy**.

Best-in-class privacy programs:

- Establish data privacy operations that occur automatically at speed for both internal parties (such as legal) and the end consumer.
- Ensure privacy requests are completed across all data stores—homegrown and vendor—so that no user data is left behind or missing in action.
- Give consumers control over their personal data and the ability to exercise their right to access (and erase) their personal data if they so choose.
- Structure consumer-facing touchpoints to ensure that data practices are crystal clear, and show how you collect consumer data, and what you do with it.

Even if some of these factors feel out of reach today, based on ever-growing tech debt, or limited headcount, know that your engineering program is going to only increase in importance over time and these principles can help today and in the future.

WHY YOUR PRIVACY ENGINEERING PROGRAM MATTERS MORE THAN EVER

The reality: Whether you're Apple or a Series A startup, data privacy's impact on your overall company's regulatory compliance, technical security, and consumer brand is only growing.

First up, **compliance**. As an engineering leader, it's likely you're being asked more and more to help your legal colleagues comply with a ballooning set of privacy regulations that only continues to expand—from the EU to California, Brazil, and more. As the inevitable variables from fragmented legislation grows, so does the list of engineering requests from legal to help manage and scale this compliance.

Security-wise, if you can't quickly identify and respond to data access or erasure requests, it becomes harder to believe that your company has adequate mastery over the technical systems that protect data from unauthorized access or corruption. In many ways, data privacy is a way of demonstrating healthy stewardship and reliability over the personal data in your company's possession.

On the **reputation front**, consumer awareness of privacy is growing, and so is the standard that consumers expect. Our survey of over 1,000 Americans found that nearly all Americans (98%) agree that data privacy is important and that it will be even more critical 5 years into the future (94%). And good experiences translate into positive perceptions—62% of Americans also rate companies that provide instant access to a user's data as trustworthy, 58% say transparent, and 55% deem them to be helpful.

It's no secret that the largest tech companies (Facebook, Apple, Amazon, Netflix, and Google) are prioritizing these vectors daily. Apple continues to run a multimillion dollar advertising campaign on their privacy-centric values, and Facebook is now pushing for greater data portability.

THE BUILDING BLOCKS OF A PRIVACY-FORWARD, COST-SENSITIVE PROGRAM

One Chief Security Officer we work with described the new engineering challenge of data privacy as the "triangle to death," referring to anytime engineering, legal and growth need to get in a room to discuss the topic.

Here's how to help avoid that scenario and emerge with a stronger and more scalable data privacy program:

1 Alignment over antagonism

Privacy is a place for cross-organizational alignment. Study after study shows that data privacy prioritization will only continue to increase for technical leaders, and the investments made to align engineering, legal, and growth on the topic now will likely only continue to set your organization up for success in the next two to five years.

Another way to think about it—your privacy debt is the new technical debt; by ignoring it, you're growing an internal problem. Instead, gain alignment by effectively and proactively communicating the realities of current data infrastructures to your colleagues.

For example, ensuring that privacy programs support the metrics tracked in performance reviews can help. "The ultimate goal is to build a reputation for engaging with your privacy program as a must-have experience for

employees seeking career advancement," this International Association of Privacy Professionals article notes.

Another strong way to build alignment is to set up a cross-functional privacy working group. This internal working group, consisting of employees from legal, engineering, marketing, and product, can provide an opportunity for cross-functional discussion and motivates companies to stay on top of privacy best practices.

It can also give your technical teams the opportunity to lean into cost-effective privacy by design instead of relying on potentially costly responsive infrastructure every time new legislation is passed.

2. User Experience over Compliance >

2 User Experience over Compliance

As an engineering and product leader, you're not in the day-to-day business of compliance (that's legal's place to shine). What's both good and bad is that your team feels the same way.

"We don't want to build and maintain compliance code" is a common refrain we've heard from engineering executives.

Companies that are willing to shift from a compliance mindset to a user experience mindset stand to win financially. In fact, 93% of Americans would switch to a company that prioritizes data privacy if given the option.

So, what does the typical user experience look like today? In a word: slow. Two-thirds of respondents to a 2019 Gartner Security and Risk Survey reported that fulfilling a single consumer data request takes two or more weeks.

Our 2020 Data Privacy Feedback Loop found that more than half of Americans (56%) want immediate access to their personal data, but only a quarter (26%) think they would actually get their data instantly if they were to ask for it.

And speed is just one angle to explore on user experience. As we flagged at the outset, completeness is an important factor of user-centric privacy programs—are you mapping and returning all user data, from all SaaS vendorsand internal systems? And on the scale front, does your user experience deliver the same result for 500 privacy requests as well as it does for 5,000?

Reviewing your data privacy experience through the lens of user experience can help to improve operational planning and performance for both internal partners and end consumers.

3. Real automation over workflow >

3 Real automation over workflow

Data privacy programs today are by and large managed in one of two ways. There is option one, a manual, labor-intensive series of "shoulder taps" to gather personal data from an ever-growing list of in-house and SaaS-based data silos. Or option two, where management is done via legacy data subject request software that might automate some parts of the process, but in reality still leaves your engineers, and teams across the company, chasing down each piece of the puzzle or being asked to build more patchworks to accommodate it.

The hard reality is that while the costs of these two pathways might not be immediately apparent, especially if your request volume is still low, the hidden costs can be high—from manual labor, to incomplete data gathering, insecure data trails, inability to scale, and more.

Instead, true consumer-centric programs prioritize real "set-and-forget" automation—secure, system-agnostic infrastructure that can be connected once to wherever personal data lives, and allow for automatic fulfillment of personal data requests.

Like constant refinement of a codebase, the goal of your program should always be trim fat, reduce redundancies, and automate, automate, automate wherever you can.

4. Pressure test build versus buy >

4 Pressure test build versus buy

Building software can cost from two to twenty times more than an off-the-shelf solution if you hire an external team, according to Atomic Object. Yet, since technical infrastructure can be specific to each company's growth patterns and needs, building can seem like an attractive first alternative. But you should critically reflect on the resource drain of this approach, not only in the initial resourcing phase, but in continuing to support rapidly evolving privacy legislation nationally and globally, versus outsourcing to a trusted SaaS partner with deep bench expertise.

Additionally, using your internal team comes at the cost of pulling engineers away from shipping on your core business product, and comes with the underscoped investment of significant downstream maintenance costs to keep up with every vendor change made by growth or operations teams.

A NOTE ON MAINTENANCE:

Maintenance and upkeep is an often overlooked component of data privacy infrastructure, and is worth interrogating deeply when considering the build vs. buy argument. What is the process every time marketing changes a vendor or data begins to flow into another data store? For rapidly growing companies that are scaling fast, data flows move quickly into new systems. Even for more stagnant companies, there's often changes in product and vendors to gain a better competitive advantage. Managing the upkeep of this infrastructure requires significant investment that can quickly skew the equation against tooling entirely in house.

When done right, investing in partner solutions provides savings in the long run due to lower headcount, quick implementation, and the most minimal amount of upkeep required.

One last tip when evaluating data privacy infrastructure. If you're a California or EU-based engineering leader, you can easily have someone on your team submit a privacy request at a customer of the solution you are evaluating. You'll be able to be the end user of the entire system and try before you buy.

CONCLUSION

While a FAANG-size budget might be nice, it isn't necessary to create user-centric data privacy programs. By following the core principles above, and focusing on a North Star of respectful privacy experiences for your users, you can make a big impact on a limited budget.

ABOUT TRANSCEND

This Data Privacy Rosetta Stone Guide was brought to you by Transcend.

At Transcend, we're big believers in fostering cross-team alignment in the service of better data privacy for you and your end users.

We provide a full-stack solution to receive, manage, and automatically fulfill privacy requests from your users—trusted by leading brands including Masterclass, Indiegogo, Robinhood, and more.

Free up engineering resources, meet—exceed—regulatory obligations with auditable automation, and build brand trust through respectful data and consent transparency and control.

Speak to our solutions team or learn more at transcend.io.