Transcend

A DATA PRIVACY ROSETTA STONE GUIDE
BY TRANSCEND

The Technical Disciplines Involved in Modern Data Privacy Engineering

A collection of “cliff notes” for privacy lawyers and program managers working with engineers.

Contents

A version of this content was
first published in IAPP on September 9, 2020.

INTRODUCTION

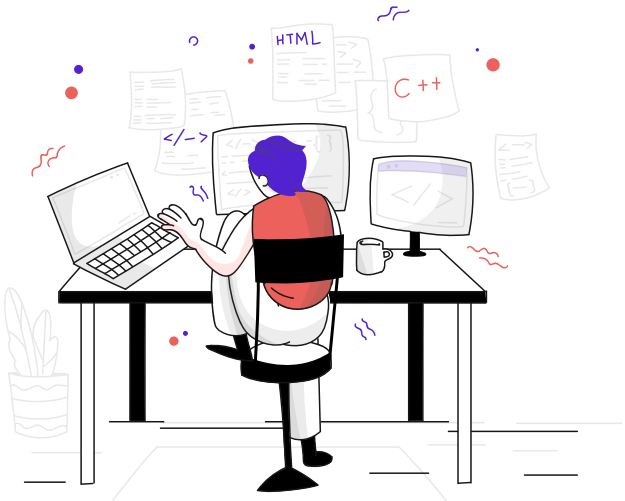
Outside of corporate legal teams, you're unlikely to encounter a team as passionate about privacy as engineering.

From the whistleblowing by Edward Snowden to the aftermath of Cambridge Analytica, data privacy has always been a profoundly philosophical technology topic amongst engineers, and these conversations have only increased with the wave of attention on data privacy.

Whether you're a Fortune 100 company or growing fast, data privacy today is a technology problem as much as a legal one. The problems include the complexity of finding and tracking user data, as well as setting up data privacy-centric consumer features.

Yet the term "engineer" in privacy settings alludes to a one-size-fits-all approach that is not accurate. There are several technical disciplines involved in data privacy today, ranging from UX Designers to Technical Program Managers to Backend Developers and more.

In this guide, we'll unpack the role each person plays in ensuring a compliant and well-functioning privacy program. And while the configurations of technical disciplines inside any one company can look vastly different, you'll leave with an understand of how to best work with each team to drive the most value from your program.



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.**

But what does this mean? Comes down to a few key factors: efficiency, completeness, control and comprehension.

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.

HOW ENGINEERING TEAMS ARE STRUCTURED ON PRIVACY

Let's take a look at a sample privacy project—handling privacy access and erasure requests—to assess the types of teams assembled.

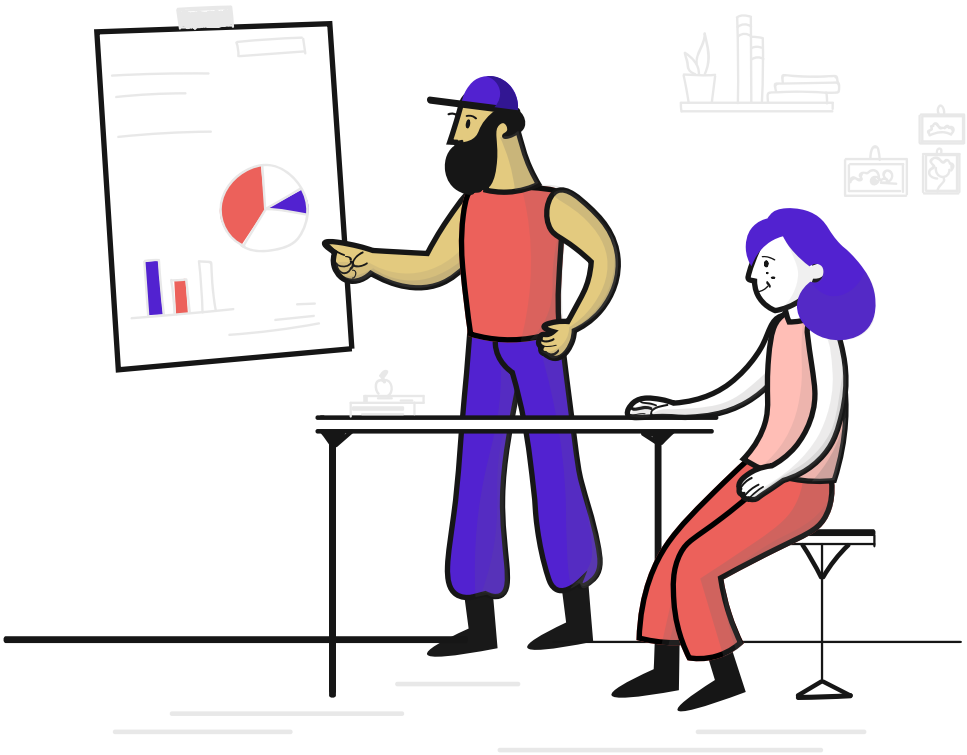
Unfortunately, for small or scrappy business-to-consumer start-ups, the reality is that engineers often don't do much on data privacy today. Even in the hotbed of innovation in Silicon Valley, start-ups are not required by law to comply with data privacy laws if they're sufficiently small.

Additionally, even for those **start-ups** that may be required to comply, given the high-salary costs of engineers and their desire to work on what they perceive as "business-critical," start-ups often make a no-win strategic decision to keep engineers focused on the revenue-driver of the business at the risk of privacy non-compliance.

In **mid-market companies**, let's say between 500–1,000 employees, you might find 6–7 engineers working over the course of a year to put together all of the feature work required for data privacy compliance. The project will depend on whether they're a data controller or data processor but it may include frontend engineers staffed to build consumer-facing tools to manage privacy settings, or having backend engineers set up the workflows needed to siphon user data appropriately.

At a **large company between 1,000 and 10,000 employees**, data privacy can be staffed by up to 100 engineers working on indefinite timelines to wrangle an ever-ballooning amount of user data and a mix of homegrown and vendor data systems and silos. In these scenarios (which may also show up in healthy mid-market companies), frontend and backend engineers are frequently partnered with Technical Program Managers, a specialized role that helps keep complex technical projects on track.

In addition, **at large companies**, privacy projects are often staffed with engineer managers and product managers to help shepherd, shape, and manage the people and the products through various hurdles.



And, of course, at the very top of the world's largest company lists, such as Facebook or Google, it's hard for any engineer to not be affected by or working on some aspect of data privacy. Engineering and Product Vice Presidents oversee large-scale teams working on data privacy. These teams are responsible for shipping their own features and updates and they are also on the hook for asserting influence over far-flung company products that may have an impact on data privacy, even if it's not directly scoped as a privacy-related project.

UNPACKING THE VARIOUS TECHNICAL ROLES

With a topline sense of the structures and groupings of engineering roles in different size companies, let's dive further into the variations of technical professions that may work together to execute a data privacy technical request.

Chief Technology Officer and Chief Information Security Officer

CTO and CISO executives are often the first technology entry-points for privacy officers and general councils. Even when data privacy is a strategic topic at a CEO's cross-functional leadership meetings, it's buried deep below conversations on revenue projections, new product launches and other courses of business. Of course, flashpoints like GDPR-readiness accelerated many executive-level conversations between CTOs, CISOs, and their peers (Chief Marketing Officers, Chief Financial Officers, and Chief Legal Officers).

Additionally, in B2B or Data Processor company environments, data privacy can often land on the CTO or CISO's plate as an output of a customer's requests. For example, a B2B company CTO may suddenly hear from sales or marketing that an influx of prospective customers are asking about data compliance. With increasing frequency, in response, a head of technology will need to scope out and authorize the builds of the technical requirements needed to help ensure deals close.

Backend Engineers >

Backend Engineers

Working on the behind-the-scenes infrastructure that makes up a company's technology stack, backend engineers work on the systems and infrastructure that build the groundwork for data privacy products v ensure they're working as intended. A backend engineer might build the pipelines that pull data from one system into another and ensure that if a user opts out of a feature, that setting is saved and rolled through other parts of the business.

Looking forward, your backend engineering team will continue to help retrofit data privacy into company systems. This need is particularly resonant at hyper-growth companies that often have a mix of patchwork engineering systems that were built quickly to expand with the business. Backend engineers often have one of the following titles: Software Engineer ("SWE"), Infrastructure Engineer ("infra"), or Site Reliability Engineer ("SRE"). Sometimes, they have titles like Linux Engineer to indicate a certain operating system specialization.

THEIR SUPERPOWER:

Designing and operating all the behind-the-scenes business logic, server scripts, and APIs that power everything in your technical stack from corporate systems to product development.

ONE QUESTION TO ASK:

Where does our organization carry the most technical debt?

Frontend Engineers >

Frontend Engineers

Frontend engineers work on the user-facing pieces of your data privacy technology and program.

You might easily recognize their work at B2C companies that are rolling out new features for consumers to navigate and act on their data choices. Behind the scenes, they also build internal tools for employees at all types of companies. Opting out of location data collection or turning off audio and visual recording authorization are just two examples of front-facing privacy features a consumer may encounter. As calls for data privacy become more user-centric, frontend engineers will do more work to ensure that products are intuitive and friendly to their users. Similar to backend engineers, frontend engineers can have different titles, including Software Engineer, Web or Mobile Developer, or Privacy Engineer. They may also have titles indicating a platform specialization such as Android Engineer or iOS Engineer.

THEIR SUPERPOWER:

Building tools and experiences that interact directly with users.

ONE QUESTION TO ASK:

What is the software lifecycle at our organization?

Product Managers >

Product Managers

The management glue of most tech products, Product Managers keep the trains running on time, and are responsible for blending the business needs with the technical details.

Product Managers often work to sketch out the size and impact of a privacy project to guide the backend engineering scope and help decide on the ideal functionality of the experience before it is built by frontend engineers. Increasingly, Product Managers that work on data privacy are also seeing their scope increase to include advising. Specifically, Product Managers may be responsible for giving other teams data privacy guardrails around products. In this case, a product manager may be asked to ship a set of data privacy projects, and also review dozens of company-wide features in order to provide notes in the product requirements document ("PRD") on the technical guardrails on data privacy and data collection.

THEIR SUPERPOWER:

Quickly spotting process inefficiencies and user experience issues, alongside managing the rollout of new privacy features.

ONE QUESTION TO ASK:

How do we integrate privacy into the product experience to avoid surprises for our users?

Technical Program Managers >

Technical Program Managers

In larger companies, Technical Program Managers (or TPMs) receive guidance from their product and engineering managers and handle systems integration and things like data anonymization for integration partners. Additionally, TPMs may also be tasked with running internal assessments across engineering teams, asking what individual teams are doing with user data, and reporting back findings to management.

TPMs are invaluable at working as the additional glue of a large-scale engineering project, such as ensuring that a roll-out of a location-based feature is aligned to all of the technical vendors that feed into the system.

THEIR SUPERPOWER:

Untangling complex technical integrations into workable project tasks.

ONE QUESTION TO ASK:

Where is our technical environment most resistant to change?

Other Engineers >

Other Engineers

Even engineers who are staffed to work on what is considered “core” engineering projects (e.g. product development of your company’s app, for example) will keep bumping into privacy in their day-to-day. While these engineers aren’t held to objectives and key results specific to privacy features or compliance, they may find that data privacy is a factor in the feature they are aiming to ship—such as a new payment collection method that triggers more personal data collection and therefore needs a data privacy review.

Worldwide, there are millions of engineers that fall into this category. More and more, they’re learning new policies for the limits of what they can do with user data, and they are operating in a more restricted environment.

THEIR SUPERPOWER:

Flexibility to quickly onboard to new projects in support of emerging business needs.

ONE QUESTION TO ASK:

Which engineering metrics overlap with privacy needs?

Data Scientists >

Data Scientists

Looking farther out in the technical organization and close partner teams, you'll find Data Scientists who are responsible for reviewing product success and ingesting product-based data into the business in a way that is clear and actionable.

Data privacy impacts data scientists in two common ways: first, there are increasing restrictions on the type of data that data scientists have access to for their analysis based on data privacy laws and company compliance.

Second, it is not uncommon for data scientists to be tasked with the database query writing for data subject access requests in business intelligence tools.

THEIR SUPERPOWER:

Extracting insights from reams of seemingly raw, segregated data.

ONE QUESTION TO ASK:

Who has access to user data at our organization?

Artificial Intelligence and Machine Learning Teams >

Artificial Intelligence (AI) and Machine Learning (ML) Teams

Composed mainly of specialized engineers, this section of the technical organization is also increasingly impacted by data privacy. AI and ML specialists have to think about how to build increasingly private models that may rely on sparser data inputs.

They also are increasingly having to consider how they collect and act on data that is more anonymized than before.

THEIR SUPERPOWER:

Turning once impossible manual computations into instantaneous and adjustable decision-making systems.

ONE QUESTION TO ASK:

How do we account for privacy and related issues, such as fairness and equality, in our training models?

UX Researchers >

User Experience (UX) Researchers

UX Researchers are at the forefront of identifying consumer trends and ensuring that product teams have the information they need to build products that meet user specifications. Everything from notification interfaces, new user screens, and data consent flows are within the remit of their work.

Increasingly, it's not enough for a company to check the product box on offering a data privacy feature. Instead, UX researchers are responsible for letting the business know if the end consumer finds the product experience to be easy to find, intuitive to navigate, and unobtrusive enough to both serve a privacy goal, while not detracting from the core product experience.

THEIR SUPERPOWER:

Helping you see where your privacy program is confusing your users (and where hidden opportunities might exist!)

ONE QUESTION TO ASK:

How intuitive is privacy in the user journey?

THE TAKEAWAY

Leveraging the gamut of technical expertise for great privacy outcomes.

At companies large and small, multiple disciplines are involved in building the future of data privacy projects from data access and erasure to compliance and more. While teams may often wear multiple hats and be responsible for far more than data privacy, you'll be hard-pressed to find a more passionate group of professionals on the topic of data privacy than your technical teams.

Understanding what each member of your technical team can bring to the table when it comes to evolving your privacy program isn't just good for your users, either. The time and 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.

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.