TerraTrue | Lyft

How **Lyft** does privacy at scale

In terms of ratios, Lyft's privacy team was greatly outnumbered even before some recent downsizing. Now, it's a team of two conducting somewhere around 200 reviews per year on various products and features.

"We really need to keep pace with the demands of the business. And our plan for accomplishing this, at the beginning, was really just prioritizing operational workload over project work, since we had more flexibility on certain projects and less on the consumer-facing areas with those reviews," Rhyne said. "We also saw this as a sign to start prioritizing within these reviews and highlight the need to quickly differentiate, at the onset, whether this launch posed a level of risk warranting a review in the first place."

In this case study, learn how Lyft achieves privacy at scale.

Brittany Rhyne
Privacy Analyst at Lyft

When Brittany Rhyne started at Lyft about four years ago, she walked into a program that had buy-in from the top but needed some improvements. The privacy team was doing hundreds of reviews a year but its size was outnumbered by the rest of the business. It needed to move away from manual work in Google Docs and implement some automation to help the privacy team keep pace with the business as it prepared to go public. It also sought to deepen the relationship between product and privacy. In this case study, learn how Lyft approached finding a tool that could help it reach its strategic initiatives, as well as how the privacy team implemented that tool seamlessly to meet product & engineering where they already worked.

> *"We didn't really have the opportunity to build that deep knowledge on a particular product or feature because we were rotating reviews, and we were still working on building those relationships across the teams. It was a little difficult to do. We needed to get the word out about our process and streamline how we performed reviews."*

The **operational problems** Lyft aimed to triage

1

Privacy reviews were manual:

Conducted in Google Docs, lacking consistency.

In the beginning, reviews at Lyft varied from analyst to analyst, and they worked like a round-robin. Once a review came in, the appropriate "next step" analyst would take it. One person might write a novel of sorts, while another might jot notes. That resulted in recommendations that varied.

2

Product and privacy lacked deep relationships

Collaboration happened through reviews, mainly.

While the company had recently introduced public Slack channels and "privacy consults" where the team could answer one-off questions, the teams didn't yet have deep relationships. "People just didn't necessarily know how to get to us," Rhyne said.

3

Privacy needed to scale quickly to keep up with the biz

Lyft aimed to go public in the near-term

With an eye toward going public soon (keep in mind this was four years ago), Lyft needed to launch new products and features as quickly as possible, so there was a strong emphasis on speed and velocity.

"This really presented a unique opportunity for the privacy program," Rhyne said. "We wanted to show that we shared that core tenant, and that by coming through our process, teams would not only be guided through an efficient review, but they'd also be saving a lot of time in the long run. If we were going to scale we needed to introduce some automation into our process to take the burden off of the team and focus our attention on the highest levels of risk."

Lyft identified 3 focus areas any SaaS tool would have to address

To keep pace with the business, the Lyft team decided it would need to put some automation in place, and it identified three areas it needing tooling to help.

Visibility

The privacy team needed more visibility outside of the company-wide tech spec template. It needed advocates and awareness. to help the company embody the message that "privacy is everyone's responsibility"

Scaling

The team needed to produce reviews that were more consistent and focused on areas of high risk.

Metrics

The team needed to demonstrate its outputs, which was difficult to do with reviews that weren't quaryable. "We needed to figure out what measurements provided the clearest picture of what we do," Rhyne said.

> *If we were going to scale, we needed to introduce some automation into our process to take the burden off of the team and focus our attention on the highest levels of risk.*
>
> *Brittany Rhyne, Privacy Analyst at Lyft.*

How Lyft evaluated for the right tool

Once Lyft's privacy team identified areas for improvement, it started evaluating privacy operations management tools to help it close those gaps. It needed a tool that:

- Could fit seamlessly into its existing process, which started and ended in Jira.
- Wouldn't add additional time for stakeholders awaiting a review.
- Mirrored how stakeholders operated, met them where they worked.
- Would be compatible with existing systems and processes.
- Would allow the team to generate custom reports quickly to demonstrate the team's outputs.

"We did not have the bandwidth to sign on for high maintenance costs, so this ruled out other solutions that operated more like customizable workflow builders," Rhyne said. "The feature to create custom reports was important to us, because we were still honing in on the best way to represent our team's outputs.

In seeking budget approval for a tool, Rhyne and her team articulated that performing privacy reviews and maintaining compliance with privacy regulations are some of the basic, keep-the-lights-on operations.

> *"We justified the cost of a privacy operations tool as a core piece of this work," Rhyne said. "if we can scale the fundamentals of our program, that frees up the team to focus on strategic efforts as well."*

After going through an RFP with four different vendors, the team articulated the broad issues Lyft wanted to address (visibility, scaling, and producing metrics) and demonstrated how tooling could solve those problems. Ultimately, the team, the CISO, as well as other leadership decision-makers decided **TerraTrue** would best fit its needs.

Why Lyft chose TerraTrue

Rhyne said the decision came down to taking a realistic look at what the team had bandwidth for, not only regarding initial setup and implementation, but any ongoing maintenance.

> *“We are all very familiar with how frequently new privacy laws and regulations come out,” Rhyne said. “To keep pace with that and make sure that you're capturing all that relevant information in your reviews is really difficult for a small team if you have a tool that constantly needs manual updating, versus something that works out of the box,” Rhyne said. “So that was a key factor for us.”*

In addition, the team valued TerraTrue’s integrations and “being able to not have to change the way people work,” Rhyne said. “That was big, because we wanted it to be complementary to how the product end teams already work. So that's what led us here. We didn't want just a customized workflow builder, because that was just too much manual upkeep.”

Implementation

Change can be hard, so implementation tactics can be key when operationalizing a new tool to stakeholders. As previously mentioned, it was important for the tool to meet stakeholders where they were at: **Jira.**

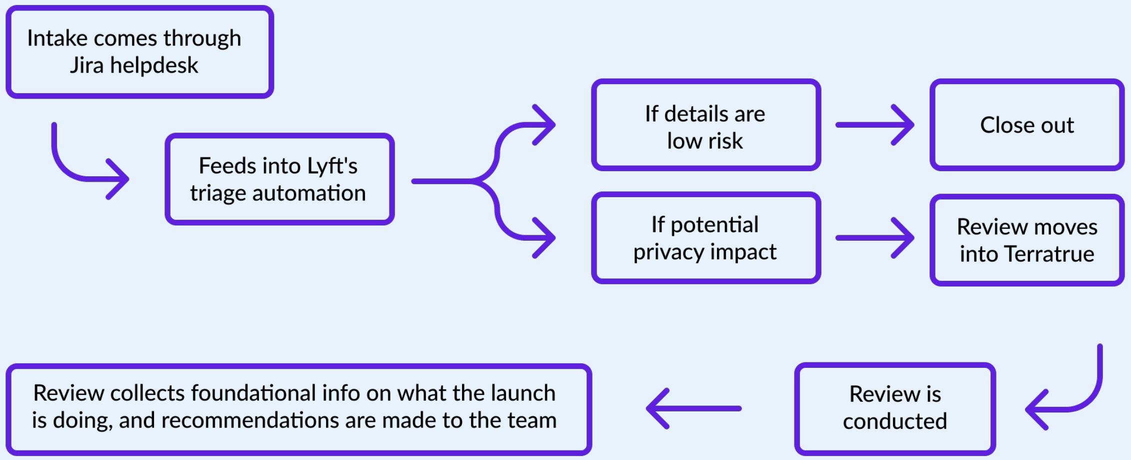
Implementation

"This meant integrating our process in Jira and mirroring the way these partner teams worked," Rhyne said, adding that the team built out its project as a "help desk" in Jira, "even adopting the same SLA metrics that other help desks use, like time-to-acknowledge new tickets and time-to-closure." In addition, they set up an on-call rotation for the analyst team "similar to the eng teams we support," Rhyne said. "So if a question arises in one of our public slack channels, there is a clear point person who can help address."

Next, the privacy team developed automations to allow it to triage launches based on a "feeder question." That question would determine if the launch contained changes that could have significant privacy implications.

To ease implementation, the privacy team reached out to collaborating teams to socialize the process, articulate the benefits, and assure stakeholders they could get through implementation quickly. In debriefs, the team focused on the "where, when, and why" of the review process, including "small things, like an easy-to-remember go link, an accessible landing page from Jira and the corporate home page," as well as "public and conspicuously named Slack channels."

Lyft's end-to-end workflow now


Intake comes through Jira helpdesk
Feeds into Lyft's triage automation
If details are low risk
Close out
If potential privacy impact
Review moves into Terratrue
Review is conducted
Review collects foundational info on what the launch is doing, and recommendations are made to the team

Outcomes

1

Increased visibility early-on

Rhyne said rolling out the process to Lyft's teams "really emphasized relationship building within privacy, encouraging the privacy analysts to form those connections in other organizations, and empowering those individuals with being advocates."

2

An improved relationship between product and privacy

"There is a really positive relationship between our teams," Rhyne said. "Privacy has worked on showing how we enable the business through this proven commitment to reducing the review burden on the product and eng teams, and improving our transparency throughout the process by providing upfront SLAs."

3

Privacy & security reviews achieve economies of scale

Lyft's intake system merges privacy and security, creating identical Jira tickets for both times. In addition, any time a ticket mentions data sharing, the third-party risk team joins in to ensure there's already a review completed on that launch. If not, it automatically becomes one of the recommendations privacy feeds back.

"It's definitely more seamless than when we had separate intake processes altogether, because then we were missing things," Rhyne said. "Or if someone went through a privacy review, they thought they were covered for privacy and security and vice versa."

4

The ability to produce deliverable, meaningful metrics

The two main metrics Lyft's privacy team reports out now relate to any trends among reviews' risk levels and SLAs.

The metrics Lyft uses for risk:

When the team reports up on risk, it looks at how many tickets were identified as “P0,” or the highest level or risk. Then it compares that to how many tickets it identified as high risk the previous quarter.

“That paints a really cool picture of, ‘Oh, are we seeing risk go down? Are we seeing more high risk reviews coming in?’ And then you can kind of talk into the details,” Rhyne said.

Metrics from SLAs:

Lyft uses SLAs to acknowledge tickets and to indicated completed reviews, as well as to track trends on risk designation for each ticket created and closed.

For example, “We can show leadership that over the last 30 days, we have had 5 P0 reviews, which is an increase over the last few months and a signal to drill into the details,” said Rhyne. “Why is this the case? Oh, it’s because there is a large effort underway that involves sensitive processing.”

Using TerraTrue to attack its gaps, Rhyne said ***privacy gained the visibility and awareness it sought and was able to evangelize that privacy is everyone’s responsibility.*** *“We are here to guide, but without the support of the product and eng teams, this is not achievable.”*

"There is a really positive relationship between our teams," Rhyne said. ***"Privacy has worked on showing how we enable the business through this proven commitment to reducing the review burden on the product and eng teams, and improving our transparency throughout the process by providing upfront SLAs."***

For example, in tracking the time to complete a review, the privacy team identified that overdue reviews were often a result of the requesting team's need to track down answers. It wasn't on privacy.

"So calling these reviews 'overdue' was not an accurate reflection of the privacy team's efforts," Rhyne said. As a result, the team employed a "freeze" tag that would pause an SLA timer. "This greatly improved the accuracy of our reporting. Once we had the groundwork laid out, we were able to adjust and fine tune these automations to help scale our work," Rhyne said.

"I measure our success through our impact on the products & features and through upholding our user promise that is the privacy policy. I think that truly enabling the business through privacy does both. Through our SLA's we can prove that we are not slowing down this development, and through the risk tiering of reviews we can demonstrate how we are mitigating these risks to the business and making the necessary changes to stay true to our customers."

Brittany’s tips for success!

1 On avoiding last-minute review ambushes

“We really state to teams, up front, when we want them to come to us. And for us, that's at least three weeks before launch. This allows us to adequately dig in, get the details, and gives them some cushion if we do have a change that needs to be made. This time frame will definitely vary like business to business.”

2 On evaluating risk

“I always feel like you need a little bit of paranoia to be a good privacy analyst. So you're thinking through all the crazy edge cases of what could happen or what a bad actor would do. Also, we like to document very thoroughly whenever there are risk acceptances. Like, if we provide a recommendation, and they don't want to go forward with it. And sometimes that's totally fine, but we do need to just capture the reasons why.”

3 On integrating with Jira

“Jira can be a bit intimidating at first, especially if you are more accustomed to tracking your work through spreadsheets and the like. But once you learn how to use it there are a lot of really powerful tools and automations that can help to streamline your processes.”

About **TerraTrue**

TerraTrue empowers teams to build privacy and security into everything they do through a collaborative, intuitive, and scalable platform. Purpose-built to work with modern product development, TerraTrue seamlessly captures structured data about how teams plan to collect, use, store, and share data. The platform then maps that digital blueprint to the world's privacy laws to automate guidance, risk-flagging, and downstream data maps and reports.

Sitting as a hub between product teams and review teams, TerraTrue also smartly routes rule-based workflows throughout an organization, automatically detects and reports infrastructure changes in cloud environments, and drives vendor management — all from the same single source of truth. With TerraTrue's digital privacy platform, companies run a scalable, fast privacy-by-design program that eliminates spreadsheets, manual ad-hoc processes, and compliance bottlenecks.

Modern brands like Lyft, Robinhood, Roku, and Foursquare are shifting left to get privacy right with TerraTrue.

www.terratrue.com |