Privacy Orchestration

or·ches·tra·tion | \ˌor-kə-strā-shən

noun

1. the planning or coordination of the elements of a situation to produce a desired effect

2. the arrangement or scoring of music for orchestral performance

Ketch

Privacy Orchestration

At Ketch, Privacy Orchestration is the promise to operationalize a company's privacy posture across every touchpoint, every consumer interaction, every jurisdiction. Doing so requires deep capability in data management and control to navigate the complexities of today's privacy landscape.

As laid out in our Privacy Primer, data privacy is a space that's long on rules, but short on tools. First-generation approaches followed a 'paint by numbers' approach: checklists, organizational readiness, quick identification of privacy gaps and compliance risks. They were static, what-you-should-do approaches; necessary, but not sufficient, to actualize privacy across a company's internal and partner systems.

First-generation tools strained and cracked in the face of mounting complexity from:

- The multiple jurisdictions in which new regulations have been enacted, and the shifting nature of existing regulations;
- The challenge of recognizing people's privacy wishes across different digital spaces, devices, and touchpoints; and
- The multiplicity of systems across which privacy must be respected.

Every company that adopted first-generation tools soon knew how much work remains to operationalize their privacy initiatives in a cost-effective, policy-driven manner. The key to conquering complexity in privacy is to embrace new technology for data control.

With granular data control, businesses can build programmatic and scalable privacy programs that collapse the costs of compliance, respect data dignity and responsibly leverage data for growth.

Conquering complexity: a mastery of data control

To realize true privacy–not just the Hollywood façade of privacy–businesses must ensure that this customer's privacy commitments in this jurisdiction are honored not just in this one company's system, but in every system with which its systems interact. If a business collects personal data, it has the responsibility to ensure that its customer's data dignity is respected not just within its four walls, but in the data systems of its service providers and partners as well.

Building capability in data management and control is critical to conquering complexity in today's privacy landscape–across jurisdictions, people, and systems. With the latter, when privacy instructions are required to interface with internal and vendor systems, we face a new challenge: how to communicate with systems that aren't built for privacy.

A flickering policy regime

Addressing jurisdictional complexity–the growing and ever-changing set of rules and regulations emanating from new laws in a growing number of economically significant jurisdictions, each with its own take on data privacy–quickly becomes unscalable and costly.

Just as we have failed to develop coherent, unified regulations regarding climate change, migration, trade, and many other dynamic, cross-border phenomena, it is unlikely privacy regulations will congeal into a unified, global standard. Instead of betting on a single global standard, a more pragmatic path is to create responsive infrastructure that assembles the building blocks of modern privacy and connects them to a *System of Intelligence (SOI)* for permits–to insulate businesses from the slings and arrows of a constantly flickering global privacy regime.

To realize true privacy *—not just the Hollywood façade of privacy*—businesses must ensure that privacy commitments are respected and enforced across the data ecosystem.

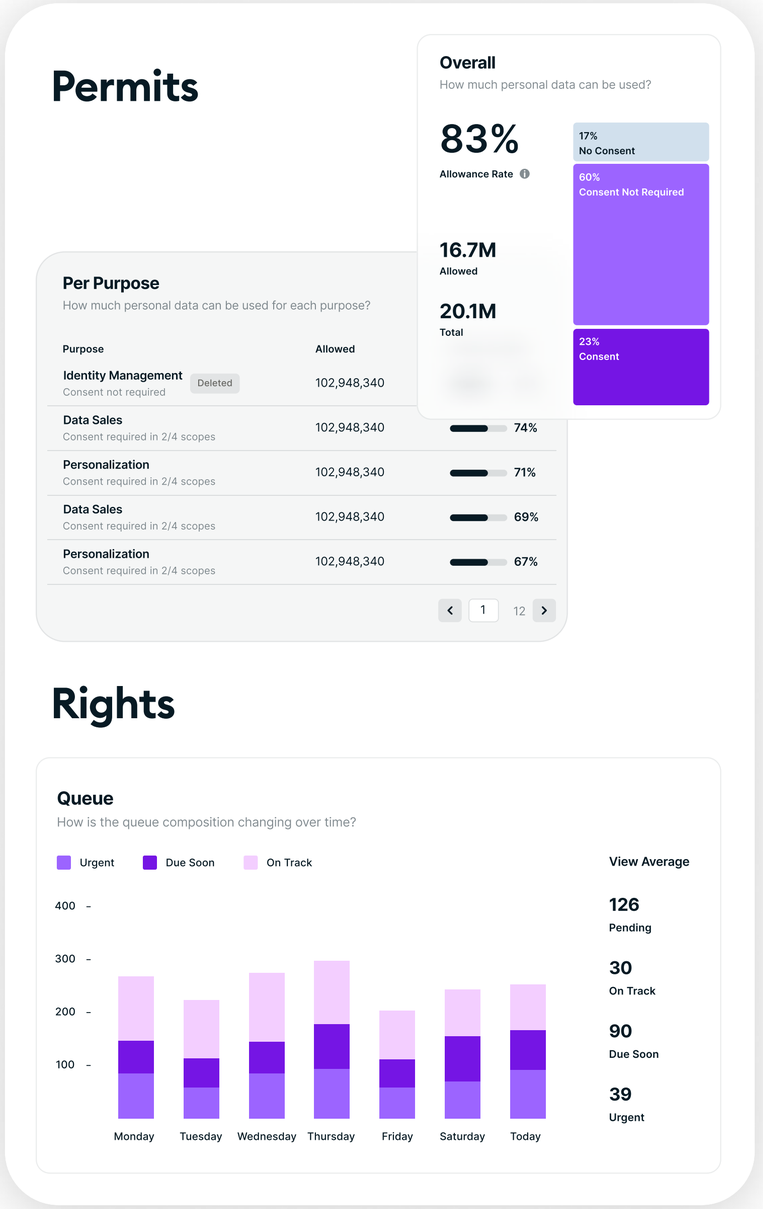
Such a system needs to capture and enact the permissioning of data at the most granular level to ensure flexibility to respond to shifting global regulations:

- Individuals about whom you hold data – **who** is it about
- Categories or attributes of the data – **what** is it
- Uses, or purposes of data processing – **how** can you use it
- Legal basis for processing by jurisdiction – **why** you can use it based on where the individual is located

The SOI for permits communicates with all the data systems that are required to respect those signals, both internal and external (e.g., website infrastructure, internal billing, registration, and shipping systems, external service providers systems).

An effective SOI architecture further enables the **quantification of privacy** for businesses, markets, and regulators. Such a framework allows us to:

- Measure the concentration and compliance of privacy instructions across chains and networks of controllers, processors, and sub-processors;
- Aggregate behaviors and activities (for example, the frequency of deletion or rectification requests in retail vs. media) to measure evolving privacy trends by sector and geography;
- Track and analyze the consent and opt-out levels of customers within different demographic and geographic segments (moms vs. teens, EU vs. North America) so that marketers and product planners can respond to evolving requirements for trust and data stewardship.



Fragmented digital identities

To do all of this in-depth and with partners, businesses must overcome the identity problem: to see people for who they are, recognize them at just the moment in time when their privacy wishes need to be honored and do so across every touchpoint and system.

The challenge is that for most people, their online activity is fragmented across a number of digital identifiers, such as email addresses, mobile advertising IDs and browser IDs. Harmonizing that activity to a 'natural person' (as defined by GDPR) requires a privacy- centric approach to identity resolution.

In the context of privacy, you can run, but you can't hide from the challenge of fragmented digital identities. When a consumer expresses a preference in an email form, a mobile app, a website or a phone, those expressions must be reconciled and mapped to a living, breathing person, not an isolated digital identifier.

For example, consent provided by a consumer on your mobile website or app needs to be associated with the IDs and devices connected to that person, ensuring an efficient and optimized privacy experience.

It's about treating people as people.

This is a task made all the more challenging as the number of digital identifiers proliferates and the Gorillas, like Apple and Facebook, build ever higher walled gardens. The explosion of digital devices has given rise to a proliferation of identity tokens, making it harder for businesses to know whether bob@gmail.com is the same as user K12345 on mobile device IDFA8394, the anonymous user who just downloaded a recipe for hot dogs.

In a context where governments (EU-GDPR, CA-CCPA) and gorillas (Apple, Google, Facebook, Amazon) are rapidly upturning the rules and methods by which consumer data can be captured and shared, there is no God's-eye view from which third-party identity assets can be used to reliably identify every user–which, of course, would be terrifying for privacy in any case. Privacy-centric identity resolution instead focuses on making it as easy as possible for consumers to express their privacy priorities and to leverage all the identity assets a companyhas responsibly gathered, without unduly burdening consumers with too many requests and extra hops and go-do's.

Sprawling data ecosystems

Conquering complexity across multiple systems requires mastery in the coordination, transmission, and enforcement of privacy instructions across multiple systems, both first-party (e.g., subscription, billing, registration) and third-party (e.g., CRM, ecommerce, analytics, personalization, etc). The privacy instructions include the propagation of consent (opt-in, opt-out, disclosure) and data rights requests from individuals in different privacy jurisdictions. Consider how this plays out when someone wishes to invoke their right to have their data deleted under Europe's GDPR or California's CCPA, data that could reside in a multitude of systems. Using Hubspot CRM as an example, here is how the workflow unfolds:

Bob invokes his right to data erasure providing his email address.

Company receives the request and verifies Bob's identity.

Hubspot, with no privacy API1, has no way to receive the instruction programatically;

Company must transmit the erasure instruction to Hubspot, but it has only Bob's email address as an identifier.

Hubspot needs a proprietary ID, the Visitor ID (VID), not an email address, to recognize Bob as the same Bob in its system.

The erasure is executed with an appropriate approval and confirmation workflow

Company sends an email back to Bob confirming the execution.

Company maintains an audit trail and record of the request, while verifying that execution happened within the fulfillment window of the relevant jurisdiction.

Repeat across a network of vendor systems where Bob's data resides and is subject to erasure.

[1] At the center of practically every mature software-enabled market or business process is what's called an API, for Application Programming Interface – an agreed-upon protocol that enables two systems to coordinate their activities in a way that gives each the confidence that the other will do what it said it was going to do.

[2] Company maintains an audit trail and record of the request within one month after receiving the request under Europe's GDPR, and 45 days under California's CCPA., while verifying that execution happened within the fulfillment window of the relevant jurisdiction.

Similarly, for the orchestration of consent: when Bob updates his opt-in (or opt-out) consent in the preference center, businesses are obliged to ensure downstream vendor systems cease data processing for the relevant data purpose. The absence of a common privacy language compounds the challenge for businesses, who likely don't have the tools to programmatically (or even manually) transmit the revised privacy instructions.

With the propagation of consent, a programmatic, automated response is critical. Unlike rights requests, which can be executed in defined fulfillment windows, the updating of consent often creates an immediate expectation in the consumer that their data is no longer being processed. If Bob opted-out of marketing messages, seeing an email from your brand starts to erode trust and build frustration.

Meeting compliance requirements and consumer expectations in this regard requires:

- **Coordinating consent and rights requests** across the network of vendor systems that process Bob's data; and then
- **Managing the transmission of privacy instructions** to vendors who have different methods for receiving the instruction, while requiring specific IDs to make it work; and then
- **Enforcing the execution of the request**, all across a multitude of jurisdictions with different data privacy requirements.

The flow of Bob's data to vendor systems happens via vendor data collection on your website—and this must only happen after Bob has given his consent. It's a common area of non-compliance, where data collection happens before relevant consent is gathered.

A mastery of data control is the only way to address these challenges, and the broad reach of personal data across business and partner systems demands data control that is:

- **Policy Driven:** Centrally controlled, policy-managed processing across data systems governing the collection, storage, access, and use of data across the organization;
- **Transmissible:** It can be communicated across chains of senders and receivers of privacy instructions (or, in the parlance of GDPR, controllers and processors);
- **Enforceable:** It doesn't just broadcast the privacy instruction, it enforces it in connected systems;
- **Programmatic:** It is automated in software, ideally via API's; and,
- **Auditable:** To comply with third-party verification or regulatory requests, past and present privacy instructions (including compliance or non-compliance by user, time, and system) are computable at any moment with instant lookback and total recall.

This interplay of data across business and partners may raise the question of who bears the responsibility for privacy compliance–business or partners.

The buck stops here

Useful data is always moving. It gets transformed, analyzed, combined with new sources, and shared to enhance its utility across a network of stakeholders. All that movement and transformation leads to a foundational data privacy question: who carries the obligation for privacy compliance when data resides outside the four walls of your business?

Drawing upon the principal-agent theory from classical economics, recent privacy laws and regulations have clarified the actors in the data play as:

- **Principals**, identified as *"controllers"* under the European Union's GDPR or as "businesses" under California's CCPA, who are ultimately responsible for the data that has been entrusted to them by data subjects, that is, citizens, customers, employees, etc. and
- **Agents**, known as *"processors"* (GDPR, LGPD) or *"service providers"* (CCPA), who are responsible for supporting the principals in achieving their business objectives, whatever they may be.

Building capability in data management and control is critical for business to achieve compliance and to overcome complexity in today's privacy landscape.

As privacy instructions are transmitted to internal and vendor systems, we come to a new challenge: how to communicate with systems that aren't built for privacy.

Businesses are responsible for protecting the data they collect even if—or perhaps especially *when*—they choose to share it with third-party vendors in service of the business.

The Tower of Babel

Controlling data and operationalizing privacy in third-party systems is hard for businesses because all of the systems, as the various groups spread around the world in the Biblical story of the Tower of Babel, speak different languages. Today, there is no lingua franca for privacy. The absence of a common language for privacy is further compounded by the multiplicity of systems wherein privacy must be respected.

Apples and Freight Trains

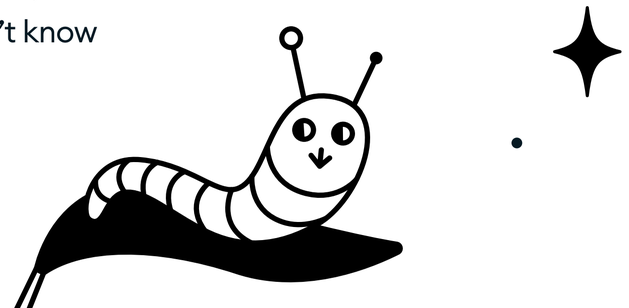
Generally, service provider systems lack the specialized tools and protocols to receive privacy instructions. They fall into three general categories according to their state of maturity:

- **Privacy Infants:** They don't speak privacy: a privacy communication protocol must be created for them from scratch.
- **Colloquial Teens:** They have a privacy language but speak a different dialect from the system sending the privacy instruction: privacy instructions must be translated.
- **Eloquent Poets:** They both speak the same language, and as a result have mastered privacy communication. The processor can easily 'catch' what the controller pit

At Ketch, we've observed that less than 10 percent of service providers can support privacy within their own systems, i.e. they are Privacy Infants, lacking any privacy language, let alone standards for cross-system coordination. As a result, even for well-intentioned businesses it feels as if every day there is a new partner to whom it must deliver a privacy signal it doesn't know how to send, and a new partner pitching a signal it doesn't know how to catch.

To understand the depth of the challenge, consider how personal data processing today is powered by a patchwork of dozens of internal and external systems, each with a specialized contribution to driving business objectives–CRM, marketing automation, site analytics, content management, email marketing, targeted advertising–to name just a few.

Deep compliance requires a quality of data management that enables companies to execute these kinds of privacy signals across a sprawl of disparate systems.



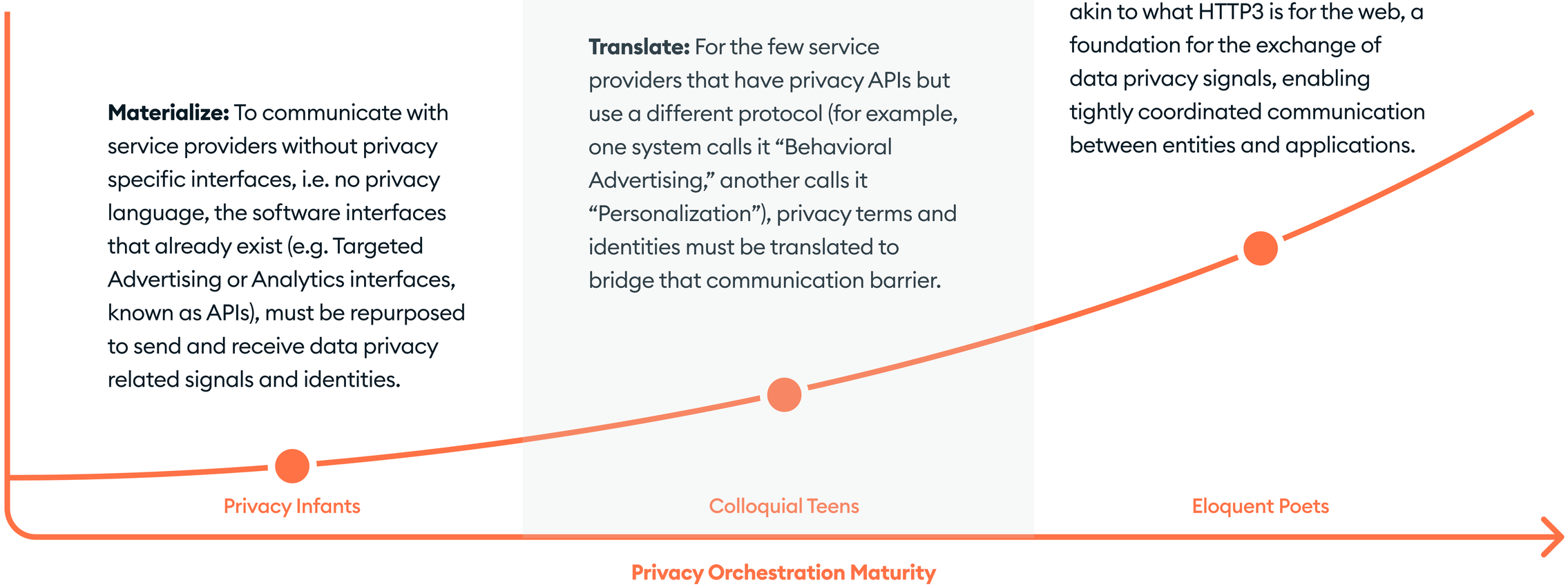
The Rosetta Stone

To fulfill their obligations today, businesses must re-tool to meet their service providers systems wherever they are on the maturity curve:

Materialize: To communicate with service providers without privacy specific interfaces, i.e. no privacy language, the software interfaces that already exist (e.g. Targeted Advertising or Analytics interfaces, known as APIs), must be repurposed to send and receive data privacy related signals and identities.

Translate: For the few service providers that have privacy APIs but use a different protocol (for example, one system calls it “Behavioral Advertising,” another calls it “Personalization”), privacy terms and identities must be translated to bridge that communication barrier.

Overlay: Businesses and service providers will agree on a protocol, akin to what HTTP3 is for the web, a foundation for the exchange of data privacy signals, enabling tightly coordinated communication between entities and applications.



Service providers share the challenge of consumer recognition. To understand who the privacy request refers to, service providers rely on specific and sometimes proprietary digital identifiers. Businesses must parse fragmented digital identifiers and send the one recognized by the service provider for them to honor the request.

All of this needs to unfold in a way that allows a business to stave off developer dependence. Dispatching a privacy engineering team to develop bespoke mappings every time a new system or regulation comes online incurs unsustainable cost.

Companies did this in the early innings of privacy–for example, to respond to GDPR–because they had no other choice but to comply. But every privacy-compliant company recognizes that it can no longer throw more developers at the problem of mapping internal identifiers with external systems every time there's an update. Strategically, they also know that every hour of precious developer time spent on privacy engineering is an hour not spent on building revenue, satisfying customers, or improving core operations.

There has to be a better way.

Ketch-ing up: a common privacy protocol

Whether a business itself has a direct relationship with data subjects, or it helps process personal data for those that do, a privacy *lingua franca* makes it easier to clearly identify **who** across the network of data systems can use personal data; for **what** processing purposes personal data can be used; and **how** systems are supposed to communicate privacy instructions. Building and maintaining trust with customers is the primary benefit of seamlessly communicating privacy instructions.

Brand value is enhanced by respecting your customers' informed and real-time privacy desires and enforcing prescriptions around allowable uses of data–across every touchpoint, every consumer interaction, and every jurisdiction.

Operationally, the benefits of a common privacy protocol are:

- **Scale:** Privacy instructions can be easily and quickly communicated across a multitude of vendor systems, enabling high throughput, on-demand transmission and enforcement
- **Flexibility:** Seamlessly add or replace service providers, without skipping a beat in the security and privacy of your customer's data
- **Productivity:** Fuel growth initiatives by getting a complete set of responsibly sourced data to the right teams: sales and marketing, analytics, data science, HR and finance

At Ketch, through the application of new techniques for data management and control and continuous sense-making of the rapidly evolving global privacy landscape, we are making privacy orchestration a reality.

> **Building and maintaining trust with customers is the primary benefit of seamlessly communicating privacy instructions.**

Privacy Orchestration: the idea in brief

01

Privacy Orchestration is the ability to operationalize a company's privacy posture across every touchpoint, every consumer interaction, and every jurisdiction.

02

Jurisdictional complexity results from the growing and ever-changing set of rules and regulations, each with its own take on data privacy, emanating from new laws in a growing number of economically significant jurisdictions. Responding to it with incremental, legacy approaches is unscalable and costly.

03

Businesses can run, but can't hide, from the challenge of **fragmented digital identities** when it comes to privacy. When a consumer expresses a preference in an email form, a mobile app, a website, or a phone, those expressions must be reconciled and mapped to a living, breathing person, not an isolated digital identifier.

04

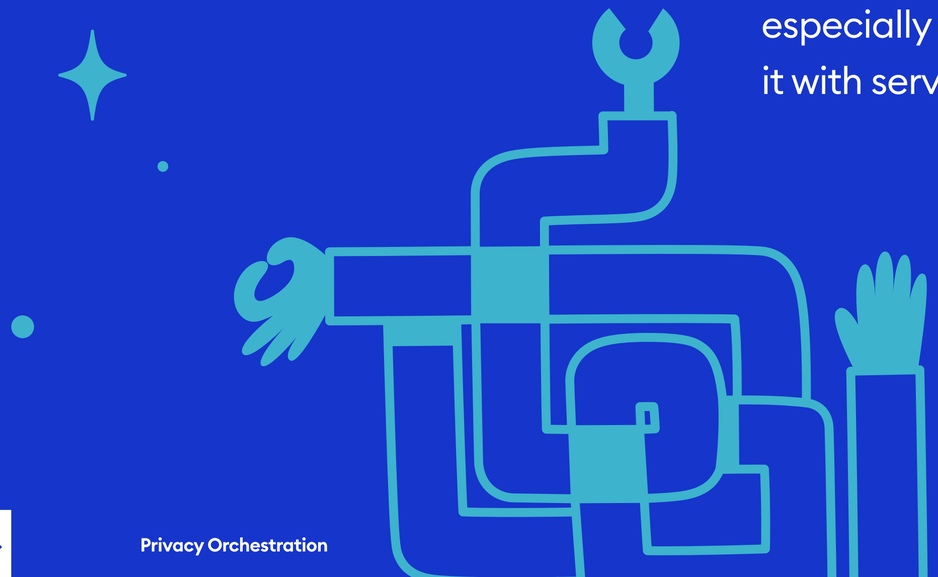
Conquering the complexity of privacy orchestration across a **multiplicity of systems** requires mastery of the coordination, transmission, and enforcement of privacy instructions.

05

Building data control capability is critical for businesses for privacy compliance and to meet consumer expectations because businesses are **responsible** for protecting the data they collect even if–or perhaps especially when–they choose to share it with service providers.

06

Operationalizing privacy requires solving for the absence of a common privacy language i.e. the **Tower of Babel** problem–one compounded by a multiplicity of systems across which privacy must be respected.



07

Businesses must re-tool to meet their service providers systems wherever they are on the maturity curve today:

Privacy Infants who don't speak privacy	**Materialize** privacy interfaces from software interfaces that already exist
Colloquial Teens who speak privacy, but use a different dialect	**Translate** to bridge the communication barrier
Eloquent Poets speak the same language and have mastered privacy communication	**Overlay** using a privacy protocol that enables tightly coordinated communication of privacy instructions

08

Seamless communication of privacy instructions builds and maintains customer trust while ensuring scale, flexibility, and productivity for data-driven initiatives.

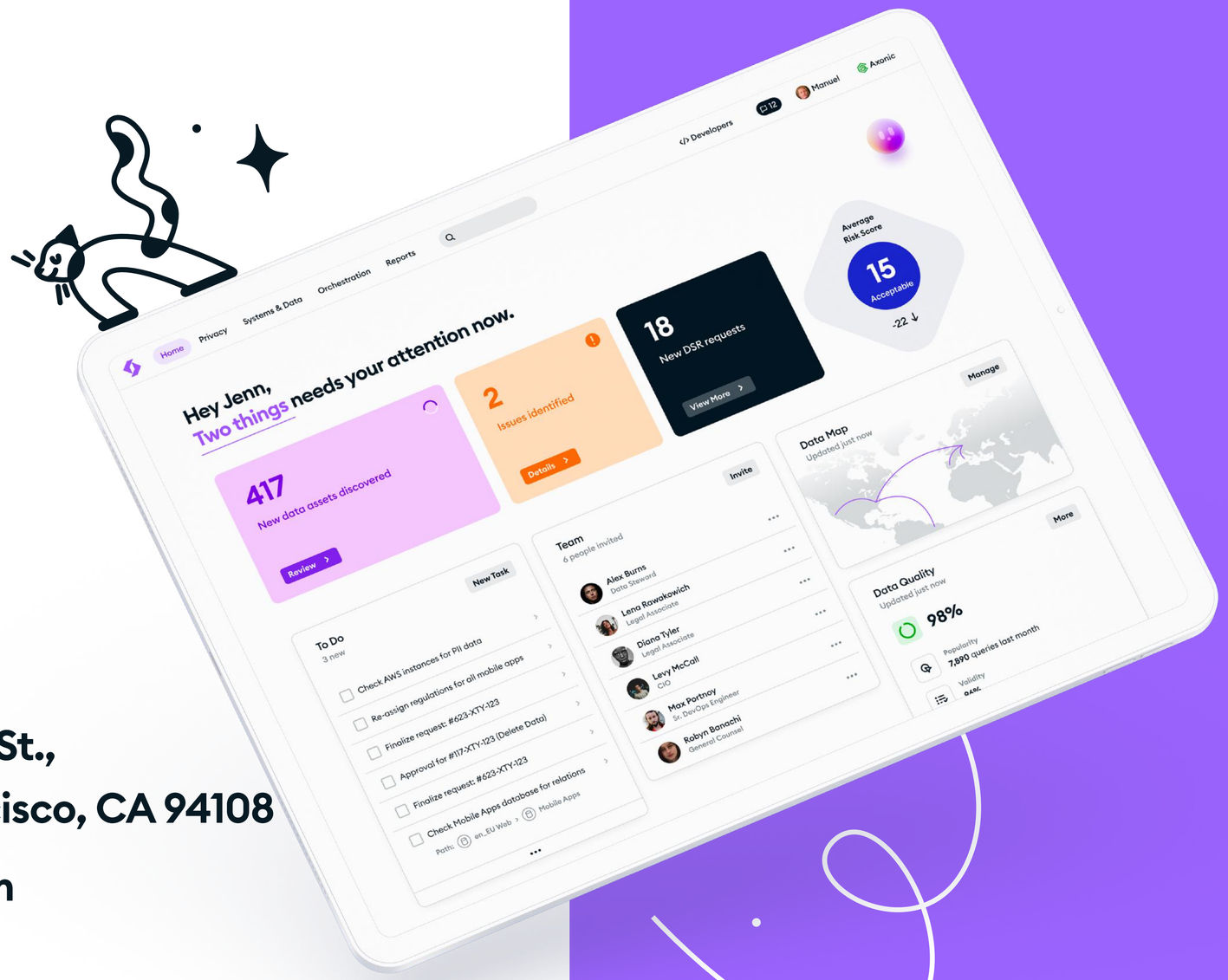
09

The key to conquering complexity in privacy is to embrace new technology for data control.

10

With granular data control, businesses can build programmatic and scalable privacy programs that collapse the costs of compliance, respect data dignity, and responsibly leverage data for growth.

Ketch



Want to learn more?

Get in touch with Ketch for a customized ROI calculator, and to learn more about how programmatic privacy can drive value for your business.

Contact us →

23 Geary St.,
San Francisco, CA 94108

ketch.com