The Missing Link in Privacy Risk Assessments

Jared Maslin

September 12, 2023

About the Speaker: Jared Maslin

Warning: The following story may sound familiar.

Your company is expanding quickly and you're processing more personal information than ever before.

New privacy laws require privacy reviews and cross-functional assessments. So, what do you do?

Quick! Someone google "privacy risk assessments"!

Common Approach to Privacy Risk: Leverage Industry Frameworks

Industry risk for privacy and security frameworks today tend to fall into one of three buckets:

1. A prescribed list of controls to apply, then align to your own risks (e.g., ISO).
2. A prescribed list of risks to assess, then design your own controls (e.g., SOC 2).
3. A prescribed list of functional areas or processes to consider, and then define your own risks and your own controls (e.g., NIST).

One problem is common to most frameworks:

- Prescribed risks and controls don't reflect your business or how you operate.

Shining light on (more) missing links

Common complaints from organizations that have attempted to apply frameworks directly to their unique business:

1. *How do I know which framework to choose? What's right for me?*
2. *Identify the risks? Where do I start?!?*
3. *How do I know when I'm done? Have I covered everything?*
4. *Okay, I'm done… what now?*

Typical Result: Budget consumed, resources allocated, team members frustrated, and time lost that could be better spent.

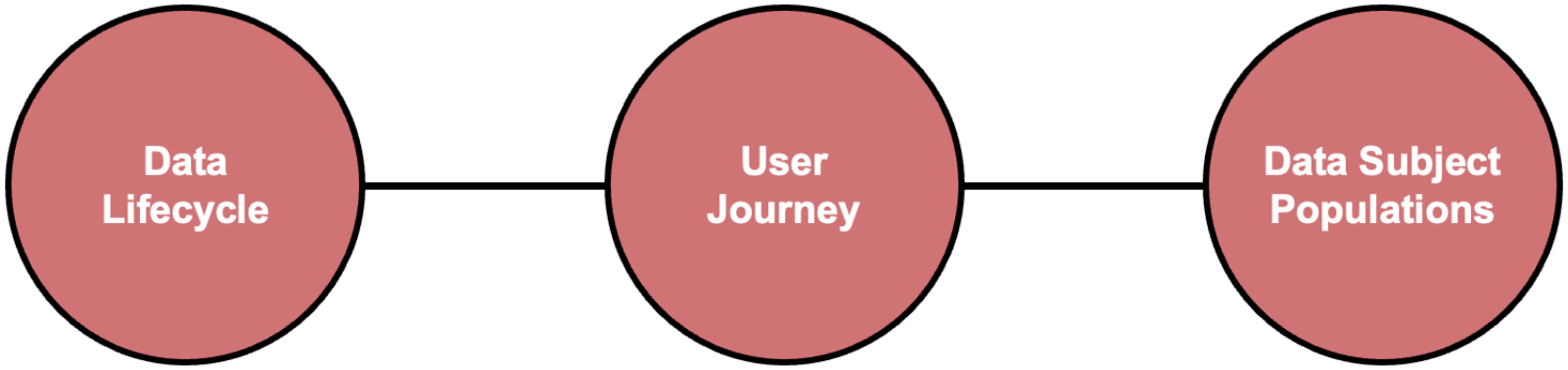
Our Solution

A new, comprehensive approach to privacy risk identification:

- Leverage a persona-based approach.
  - Risk identification can be overwhelming, but using personas to more directly fit your privacy risk needs can make it less daunting.
- We have field-tested such an approach, which utilizes a three-prong model to curate a custom, fit-for-purpose risk profile that reflects your business, how you operate, and how you view the risks before you.

Defining Risk Profiles

Persona-based assessments with flexible, comprehensive risk profiles that grow from cross-functional collaboration and increase visibility.

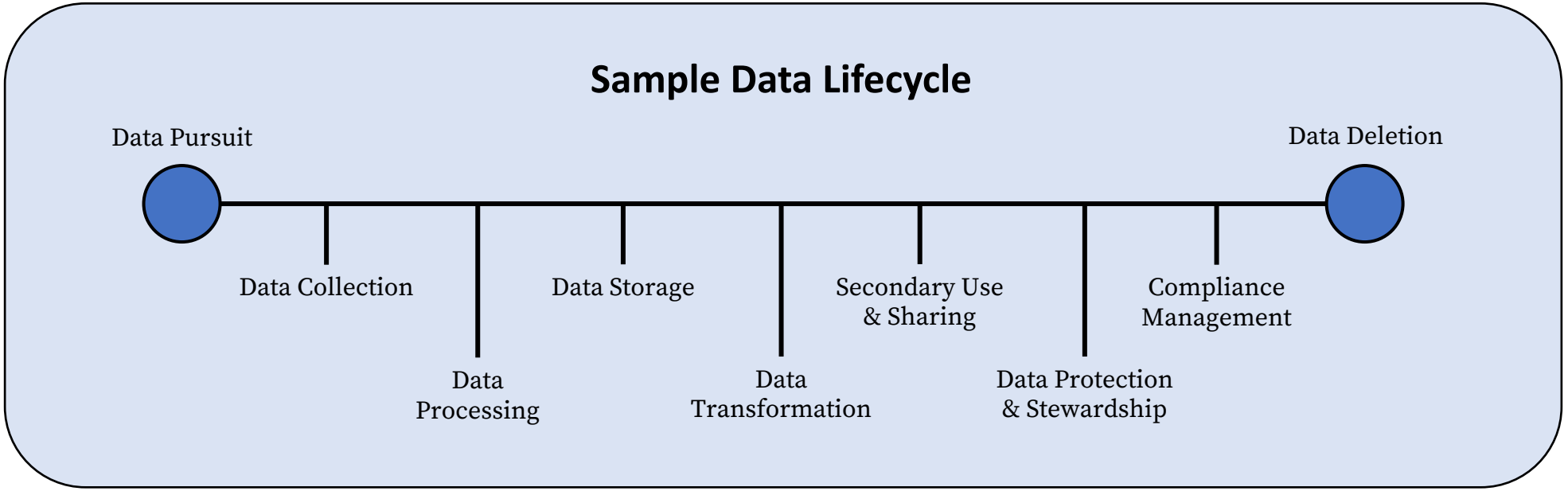


Each profile component is customizable and will support stewardship over time.

Risk Profile: Data Lifecycle

Assess the phases of personal data handling from the moment of pursuit to the moment the data no longer exists in your ecosystem.

Risk Profile: Data Lifecycle

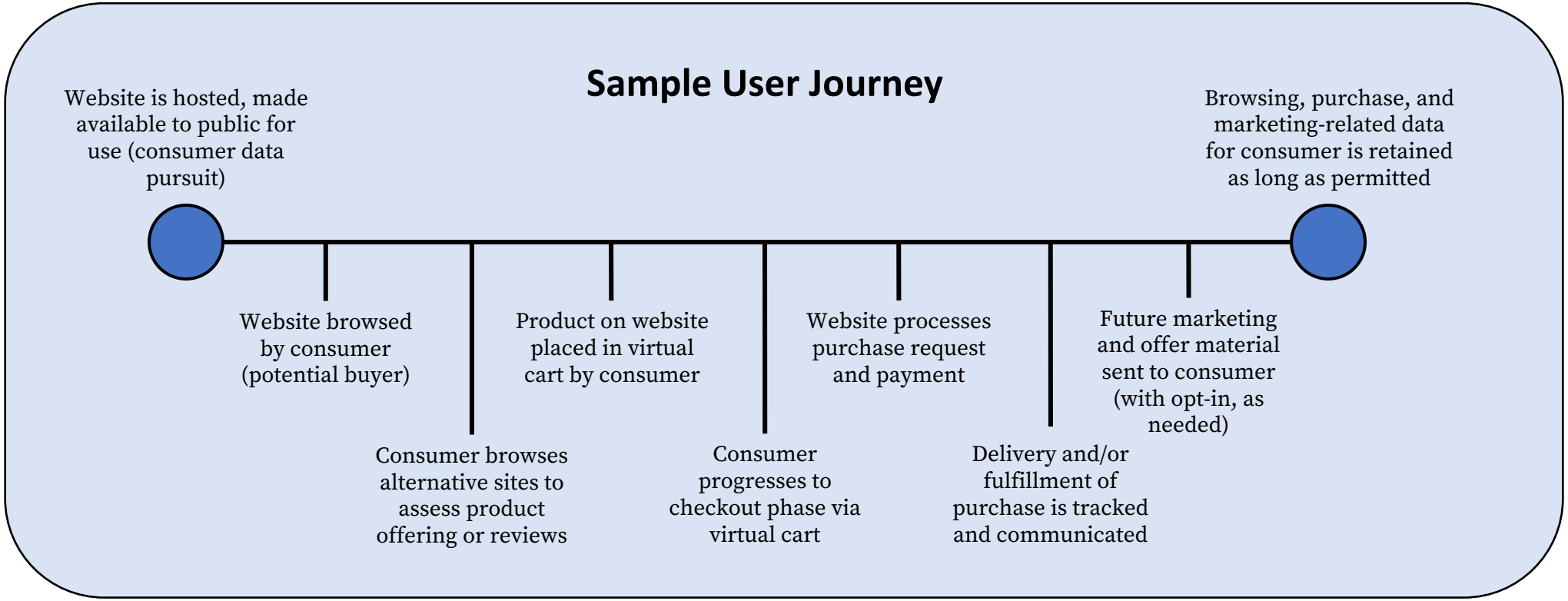


Assess the phases of personal data handling from the moment of pursuit to the moment the data no longer exists in your ecosystem.

Risk Profile: User Journey

Map out and assess the different paths that data subjects can experience and how that impacts data collection and processing.

Risk Profile: User Journey



Map out and assess the different paths that data subjects can experience and how that impacts data collection and processing.

Risk Profile: Data Subject Populations

Categorize distinct data subject groupings that could result in distinct processes, systems, and corresponding compliance obligations.

Risk Profile: Data Subject Populations

Data Subject Classification

Data subject category (or type), such as consumer, patient, business contact, job applicant, or employee).

Data Sensitivity Classification

The nature of personal information processed according to degree of sensitivity such as public, private, confidential, and sensitive/restricted.

Data Subject Geolocation

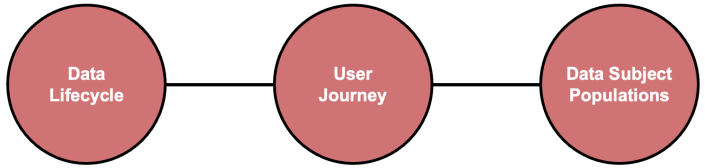
The distinct geographies or residencies of data subjects (and thus, applicable regulatory jurisdictions).

Data Processing Business Purpose

The purpose(s) aligned to notice or informed consent of data subjects for processing such as product delivery, marketing, or UX personalization.

Categorize distinct data subject groupings that could result in distinct processes, systems, and corresponding compliance obligations.

Case Study: Bring it all together



A global technology company sought a better way to identify privacy risk:

- Leveraged several industry frameworks in prior attempts, but not all risks were addressed, and risk/control prescription created confusion and resistance.

Results from use of our model:

1. Produced a risk inventory that is tailored to their organization, their infrastructure, and their ways of working.
2. Uncovered instances of risk acceptance that can be hard to see and are often missed – this is a BIG deal.
3. Prioritized an investment plan in privacy risk remediation according to need – both in risk remediation and in supporting functions like internal audit.

Would this help with emerging challenges?

Use Case: New and Emerging AI Regulation

1. **Data Lifecycle:** Identify the tooling and data infrastructure flows responsible for training, deploying, and stewarding AI functionality and related predictive models.
2. **User Journey:** Identify the phases of each distinct user journey in which user data may be subject to AI or in which AI contributes to experience and decisions regarding users.
3. **Data Subject Populations:** Classify the data subject types exposed to AI, the sensitivity of data processed, the contextual and geographic footprint of data subjects (and processing), and the business purposes for which AI is being applied to personal data.

Getting Started

- **No matter your industry and no matter your maturity in privacy, this can help your organization.**
  - It's a change in mindset – not a change in technology, and it does not negate your hard work to date.
  - This does not preclude certification maintenance – in fact, it can help consolidate your efforts for greater consistency and efficiency.
- **What you can do today to get started:**
  - Read more about this approach here.
  - Contact me – I want to help you!

Thank you so much for your time, and to PEPR for the opportunity to speak with you all today!

Contact the Speaker

Email: jfmyq9@berkeley.edu, jared.maslin@goodresearch.com

LinkedIn Profile: https://www.linkedin.com/in/jared-maslin-6315934b/

Link to our Supporting Paper

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4545137