Product Privacy Journey
Towards a Product Centric Privacy Engineering Framework

Igor Trindade Oliveira
igor@work.co
Why a Product centric approach?
Instead of compliance, design, engineering or even user focused
It must be a return to Renaissance
Technology
Design
It is not about compliance, design, technology, or user-centred approach
Everything matters
Product Privacy Principles
Creating Products that respect personal data
Privacy by Design

The 7 Foundational Principles Implementation and Mapping of Fair Information Practices
Ann Cavoukian
Data Ethics

What is data ethics?
Luciano Floridi and Mariarosaria Taddeo
Philosophical Transactions of The Royal Society A Mathematical Physical and Engineering Sciences
Qualitative Experience
<table>
<thead>
<tr>
<th>No choice is forever</th>
<th>Context is Key</th>
<th>Sharing should add value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain language empowers</td>
<td>Tricks erode trust</td>
<td>Personal data belongs to individuals</td>
</tr>
</tbody>
</table>
No choice is forever
We know that people can change their minds. Create data sharing controls that are easy to find and adjust.
No one uses privacy settings

User-centric privacy: designing effective privacy protections
Florian Schaub
2019 USENIX Conference on Privacy Engineering Practice and Respect
Personalize your inspiration
Share your browsing history for more personalized recommendations.

Shop by room

IKEA Mobile APP
Personalize your inspiration
Share your browsing history for more personalized recommendations.

Shop by room
All  Living room  Bedroom  Bath
Context is Key
Pay attention to timing. Ask for permission to share and store data at moments in the experience where the consequences are most relevant and obvious to users
Make sure permission requests occur only when people are using features that clearly need personal data

Human Interface Guidelines: Requesting Permission
Apple
Sharing should add value

Choosing to share the consumer's data can enhance an experience, even though it's not required. We must create experiences that work well whether or not the consumer share personal data.
Your data controls

Private session

Shop the look works with your data

Your recommendations are based on search, favorites, answers to quizzes, and other shopping activity.

See all data controls
Plain language empowers
Favor commonly used terms over jargon. Use straightforward language to help people understand which data they're sharing and with whom
Tricks erode trust
Don't try to manipulate people's decisions around privacy. Avoid leading statements or dark design patterns. Opting out of sharing personal data should be easy
It is possible that users lose trust in the system over time when they realize they are being manipulated into clicking on ads

Dark Patterns: Past, Present, and Future
Arvind Narayanan, Arunesh Mathur, Marshini Chetty, and Mihir Kshirsagar
ACM Queue 18(2):67-92
Personal data belongs to individuals
We let users control what happens.
Show people what data we’re collecting, why we collect it, and give them the option to delete their data
A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

California Consumer Privacy Act
Right to delete
Product Privacy Journey
Applying Privacy in the product Journey
Prioritize privacy issues in every phase of product development
Product Privacy Journey

01 Inspire

02 Acknowledge

03 Conceive

04 Implement

05 Validate
Inspire
Understand how the product and privacy inspires the consumers
Privacy matters

AdWeek: Apple Keeps Beating the Privacy Drum in Relatable, Clever iPhone Ad
Take control of your data

See how sharing personal information can make your experience simpler and smarter.

What data we collect and why

Learn more

I have read and understood IKEA's privacy policy
Acknowledge
Understand what are the consumers and the company expectations, and what are the privacy trade offs
Pay attention to

Consumer Privacy Perspective

Organization Privacy Expectations

Privacy Law Requirements

What to expect to have in the end

Privacy Requirements Mapped in Product Features

Privacy Metrics
Conceive
Design the product with privacy requirements in mind avoiding the privacy dark patterns and the risks of having the data leaked
Pay attention to

Avoid Dark Patterns
Product Privacy Journey Principles

What to expect to have in the end

Data Controls
Visual Components
Implement privacy by pushing boundaries to develop products that are privacy and security ready from the ground up, not only focusing on just adhering to standards.
Pay attention to

Privacy Infrastructure

Information Security Guidelines

Product Privacy Journey Principles

Tech Privacy Considerations

What to expect to have in the end

Improved Privacy Infrastructure

Privacy Components Implemented
Validate

Validate and measure the final solution making sure it is following all privacy and security requirements.
Pay attention to

Usability tests to check clarity of privacy controls

Check if privacy and security measures meet privacy law requirements

What to expect to have in the end

Verify if the measured metrics are aligned with the Privacy KPIs
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Inspire</td>
</tr>
<tr>
<td>02</td>
<td>Acknowledge</td>
</tr>
<tr>
<td>03</td>
<td>Conceive</td>
</tr>
<tr>
<td>04</td>
<td>Implement</td>
</tr>
<tr>
<td>05</td>
<td>Validate</td>
</tr>
</tbody>
</table>

**Privacy Vision**
- Consumer Privacy Perspective
- Organization Privacy Expectations
- Privacy Law Requirements

**Avoid Dark Patterns**
- Product Privacy Journey Principles

**Privacy Infrastructure**
- Information Security
- Product Privacy Journey Principles

**Check that privacy and security measures meet privacy law requirements**
- Run usability tests to check clarity of privacy controls
Thank you