CENTER *for*
FINANCIAL
INCLUSION
ACCION

The Privacy as Product Playbook

How to Practice Privacy by Design When Building Inclusive Finance Products

Acknowledgments

The Center for Financial Inclusion (CFI) is grateful to the lead author, Dr. Maritza Johnson, for her leadership and incredible contributions to this publication. CFI managed this project, led by Alex Rizzi, with support from Colin Rice, Tanwi Kumari, and Henry Bruce. Special thanks to the team at GRID Impact (Alexandra Fiorillo, Adam Little, Matthew Morales, and Greta Rasmus) for their invaluable facilitation and design expertise and to Stella Dawson and Elizabeth Miller for their editorial guidance. We are particularly grateful to Aria Widyanto, Ana Nurhasanah, and their colleagues at Amartha for providing meaningful feedback through a live workshop. The authors would also like to give extensive thanks to the range of experts who provided insight and feedback across this project: Edoardo Totolo, Dan Cassara, Nitin Kohli, Jasiel Martin-Odoom, John Launchbury, Amelia Greenberg, Camilo Téllez-Merchan, Caitlin Sanford, and Nishanth Kumar.

This playbook is a result of CFI's partnership with PayPal's Global Privacy Team. The CFI team is especially grateful to Shikha Kamboj and Tenneale Smith for generously sharing their technical expertise and feedback and to Ilana Mayid for overall project support. The team is also appreciative of Rosita Najmi for initiating the partnership.

Table of Contents

Introduction to Privacy for Inclusive Finance

Introduction

A decade ago, discussions about consumer privacy in inclusive finance centered on paper files and their physical storage. Front-line financial services staff collected data in person from potential consumers using paper forms, clipboards, and pens. The best practice for data storage was a limited-access room that could be locked with a key.

Today, inclusive financial products are fueled by ever-growing volumes of digital consumer data, primarily collected by mobile phones. Coupled with advances in analytics and innovations in data sharing, the face of privacy has changed radically.

At the same time, data-driven digital finance has led to new privacy harms for low-income consumers. From accusations that an Indian educational technology company misused biometric information to lock parents into loans to East African digital lenders using borrowers' contact information to harass friends and family, the risks are real and have caused financial and emotional damage. Privacy harms can also damage consumer trust, sometimes irreparably. For inclusive finance to achieve its promise, consumers must not only gain access to financial services but also have the confidence that they can use the products and services without harm. The design of products is integral to building or breaking that trust.

> **Consumers must not only gain access to financial services but also have the confidence that they can use the products and services without harm. The design of products is integral to building or breaking that trust.**

Data protection regulations lay a strong foundation. For example, the European Union's General Data Protection Regulation (GDPR) redefines what companies can and cannot do with personal data. The GDPR also emphasizes the importance of informed consent and promotes new digital rights, such as the Right to be Forgotten. Unfortunately, product teams typically do not allocate much attention to privacy during the product lifecycle. Instead of being a central driver of design, privacy is often an afterthought.

Additionally, companies rarely write corporate privacy notices with the end user in mind, particularly users with digital or financial literacy constraints. Deceptive design — a collection of design practices encouraging users to choose a path that may not be in their best interest — can confuse user expectations, manipulate their choices, and conceal potential privacy risks. Providers must consider how onboarding to digital finance can replicate offline privacy risks or create new ones — particularly for vulnerable groups.

The privacy needs in inclusive finance go far beyond compliance, and designers of digital financial services must bring privacy needs front and center.

> **This playbook aims to empower product teams to rethink how they integrate privacy into their work.**

Privacy by Design

Where to begin? First, it's essential to incorporate the privacy needs and expectations of end users at the center of product design. This is a key precept of Privacy by Design (PbD), a systems-engineering approach initially developed by Dr. Ann Cavoukian in 2009. PbD calls for companies to consider privacy throughout the engineering process, while remaining mindful of human values and behavior. Pbd also aims to reframe privacy as a business enhancement rather than a compliance-driven cost. This playbook aims to empower fintech product teams to rethink how to integrate privacy into their work.

Buy-in for implementing Privacy by Design within digital financial products and services processes must begin with a fintech company's senior leadership. Without support from leadership, product teams may not have the space to prioritize PbD against competing interests, deadlines, and key performance indicators.

Despite the growing interest in Privacy by Design, current approaches overlook the growing importance of product managers in digital and software product development. This playbook aims to fill that gap and demonstrate a comprehensive way to integrate responsible data practices into the design process. The playbook is based on the central tenets and emerging practices in Privacy by Design but is animated by additional unique considerations for product teams in the inclusive finance space. The core foundational principles of this playbook are:

- PbD must be adapted to work for resource-constrained companies and emerging markets.
- PbD should incorporate low-income and vulnerable consumers' offline privacy needs and privacy for their digital data.
- PbD should be positioned as business-enhancing.
- PbD must balance consumer privacy preferences with companies' needs.
- PbD must articulate privacy responsibilities across disaggregated value chains and partnerships.

How Is This Playbook Organized?

Creating a Responsible Data Strategy

The playbook first explores how teams can develop a responsible data strategy that is unique and appropriate to their work. This section outlines privacy principles and acts as the guidepost for product design and execution decisions.

Incorporating Privacy into Your Product Development Lifecycle

The playbook then goes step by step through the product development lifecycle. It helps fintech companies integrate their responsible data strategy into the design of a new product by placing the end user's privacy needs and concerns at the forefront of all decisions. The goal of the playbook is to help teams incorporate the Privacy by Design approach into the flow of their existing work without the need to develop new systems or processes. This section also includes worksheets to help teams implement PbD.

Explore Further

Throughout the playbook, many sections include an 'Explore Further' page featuring resources from a wide range of privacy and inclusive finance experts, academics, and industry leaders. The resources referenced also offer examples of successful and unsuccessful practices, in-depth explorations of various concepts, and valuable analyses to provide context.

Advocating for Privacy by Design

This section provides practical tips on championing privacy by design within a company. It also offers advice on effectively introducing a new vision to the company and articulating the business case for prioritizing privacy as a profitable endeavor.

Common Traps to Avoid

The final section addresses common traps to digital privacy — problems that product teams might encounter when implementing PbD — and outlines ways to avoid them.

Explore Further

"Worst Decision of My Life"

An article about the predatory practices of Byju's

Read article

A Startup's Guide to New Product Development

Accion's guide for startups in inclusive finance

Read the guide

Privacy's Blueprint

A book about privacy risks

Get the book

Embedding Trust: The Potential of Privacy by Design for Inclusive Finance

An introduction to Privacy by Design for inclusive finance practitioners

Read the report

Privacy as Product

Consider the case for treating privacy as a product issue

Read article

Product Development Lifecycle (PDLC): Complete Guide

A deeper dive into the product development lifecycle

Read the guide

Creating a Responsible Data Strategy

What Is a Responsible Data Strategy?

Many companies intend to be transparent and accountable in their dealings with data. They articulate a data strategy that includes how the company thinks about, collects, manages, stores, and uses data. But not all data strategies consider consumers' needs. By applying the guidance in this playbook, your team can develop and commit to a data privacy strategy that meets the needs and expectations of individuals.

The Data Board at the Massachusetts Institute for Technology's Center for Information Systems Research defines a data strategy as: "A central, integrated concept that articulates how data will enable and inspire business strategy."

If your company already has a data strategy, use it as a guidepost. The privacy commitments might be broad, such as "We are committed to transparency." Or they may be more specific, such as, "We will collect the minimum amount of data necessary." Regardless, your company's existing data strategy can be your team's starting point and reference.

If your company does not yet have a data strategy, the product team can design a responsible data strategy for a new product. This requires your product team to identify the various decision points about privacy and to document how your team will approach them — a process that makes privacy concerns visible and enables your team to develop a plan consistent with your company's goals, the user's goals, and the goals for the new product.

A responsible data strategy addresses the following key questions:

Inventory
What's the role of data in this product?

Objectives
What privacy commitments are relevant to the users of this product? Consider how you would operationalize those commitments differently for end users with literacy or digital capability constraints.

Plan
What steps will you take to ensure you handle the data as described?

Maintain
Is the data strategy accurate and effective?

When you approach data from the user's perspective in this way, you may find gaps or open questions about the data strategy, which presents an excellent opportunity to strengthen your company's position.

Explore the questions in the worksheet on pages 12-18. A responsible data strategy is an important step in the process, even for Business-to-Business (B2B) and Business-to-Business-to-Customer (B2B2C) products.

> **Privacy is about people. When a product uses, stores, or processes data about people, clearly documenting how you handle the data upfront is essential.**

Worksheet

Responsbile Data Strategy

Objective: Collect the relevant information needed to develop and refine your data strategy.

Duration: Approximately 90 minutes.

Note that the time required will vary, depending on how data-intensive the product is, the sensitivity of the data utilized, the data source, the amount of time dedicated to discussing these issues, and your team's experience with user privacy, data protection, and data security.

Facilitator Notes

Tactics to Complete This Worksheet

There are two general approaches you can take for this worksheet; decide what works best for your team:

1. **Product manager-led effort:** In this approach, the product manager completes the worksheet to the best of their ability. They may have prior knowledge from past discussions or want to propose a draft for the design team to review and discuss.

2. **Team-driven effort:** In this approach, your team collaborates on the worksheet. The output is a shared document reflecting your team's collective ideas. Team members may find it useful to work individually on certain sections before discussing them together. If you take this approach, remember to allocate time for reaching a consensus and documenting your responses.

Other Notes

Practitioners often aim to follow best practices. As you work through this worksheet, you may wonder if your responses align with best practices. Due to the highly contextual nature of data privacy, the answer is "it depends." As you may know, the state of data privacy can be highly contextual, which is why the worksheet asks you to document your responses in stages. This exercise intends to pull the relevant context into a document so your team can decide, "Is this good enough based on what we know today?" That said, there are some established best practices and standards, and we encourage you to seek them out or find a team member or consultant with the relevant expertise.

Your responses to the worksheet may vary depending on the type of product being developed and the stage of your company. There are two typical categories:

1. **A new company that is designing its first product:** Here, your team is making decisions for the first time. You're debating what data to collect and how to use and store the data. While team members may bring their past experiences and recommendations from previous jobs, your team determines its approach from the outset.

2. **An existing company that is designing a new product:** Here, your team is making decisions based on existing policies, roles, technical infrastructure, and products. Sometimes, your team may consider using data that your company collected for another purpose.

Note: The worksheet is written as though the team is in the first category (a new company working on its first product). If you feel the second category more accurately describes your situation, you can adjust the worksheet accordingly.

Worksheet: Responsible Data Strategy

Step 1 of 4: Make a Data Inventory

What data are you using?	→	How do you acquire this data?	→	How will you use this data?
Contact information, personal identifiers, device identifiers, usage metrics, location, demographics, health information, personal habits, trends for marketing, etc.		From the primary user: through direct use of the product or approved access to a data archive? Through a party that has a direct relationship with the user? Through a third party without a relationship with the user?		On behalf of the primary user? On behalf of the company? On behalf of people similar to the primary user?
Example:				
Phone number	→	The user enters their phone number during the account sign-up flow	→	To comply with local KYC regulation, account security(two-factor authentication), and to contact the customer
	→		→	
	→		→	
	→		→	
	→		→	
	→		→	
	→		→	

Step 2 of 4: List Your Objectives

List your privacy commitments to your end users. What commitments are you willing to make about handling their data and protecting their privacy?

Example Commitment: We only use your phone number to comply with local regulations and, with your permission, for account security and communications.

Privacy Commitment 1:

Privacy Commitment 2:

Privacy Commitment 3:

Privacy Commitment 4:

Privacy Commitment 5:

Check your company's policy on data rights and privacy principles.
What has your company already committed to?

What needs to be implemented?

What local laws and regulations govern data rights?
e.g., Right to Informed Consent, Right to Access, Right to Delete, Right to Correct, etc.

Step 3 of 4: Create a Plan

Decide how you might achieve the privacy commitments and data rights you identified in the previous sections. In the spaces below, select how you plan to address the commitment — by policy, process, product feature, or infrastructure. Then, expand on each item and describe how your team approaches the work.

Example Commitment

First, check how you will address this commmitment:

☒ A POLICY ☒ A PROCESS □ A PRODUCT FEATURE □ INFRASTRUCTURE

Now, document how the team plans to approach the work:

Policy: Write a data use policy that documents the data collected and how your company uses it. Distinguish which uses are required and which uses are optional.

Process: Create a review process to ensure that employees follow the policy.

If a team proposes a new product requiring additional permission from the user to use the data in a new way, design a clear and consistent consent experience and update the database.

Privacy Commitment 1

First, check how you will address this commmitment:

□ A POLICY □ A PROCESS □ A PRODUCT FEATURE □ INFRASTRUCTURE

Now, document how the team plans to approach the work:

Privacy Commitment 2

First, check how you will address this commmitment:

□ A POLICY □ A PROCESS □ A PRODUCT FEATURE □ INFRASTRUCTURE

Now, document how the team plans to approach the work:

Privacy Commitment 3

First, check how you will address this commmitment:

□ **A POLICY** □ **A PROCESS** □ **A PRODUCT FEATURE** □ **INFRASTRUCTURE**

Now, document how the team plans to approach the work:

Privacy Commitment 4

First, check how you will address this commmitment:

□ **A POLICY** □ **A PROCESS** □ **A PRODUCT FEATURE** □ **INFRASTRUCTURE**

Now, document how the team plans to approach the work:

Privacy Commitment 5

First, check how you will address this commmitment:

□ **A POLICY** □ **A PROCESS** □ **A PRODUCT FEATURE** □ **INFRASTRUCTURE**

Now, document how the team plans to approach the work:

Step 4 of 4: Maintain

What processes are in place to ensure the data inventory (from Step 1) is accurate?

Example: A cross-functional team of product, legal, data security, data protection, and policy employees regularly meets to review how data is collected, stored, used, and maintained.

The team documents responses to the responsible data strategy worksheet where team members can easily reference it.

What processes are in place to ensure the plan (from Step 3) is effective?

Example: A Cross-functional team regularly reviews the data strategy, and a third party conducts an audit every two years to ensure the policies, people, and mechanisms are working as intended.

Explore Further

How to Build a Data Strategy

More ideas for developing your data strategy

Read the guide

Why Privacy is Generative and Constantly Moving

On the evolving privacy landscape

Read article

8 Data Subject Rights According to the GDPR

Information on and definitions of data rights

Learn about GDPR

Privacy and Confidentiality

The ethics of making privacy about people

Read article

MIT CISR Data Research

Research highlighting how companies generate value through data

View the data

Incorporating Privacy Into Your Product Development Lifecycle

This section is a step-by-step guide for product management teams at fintech companies to integrate their responsible data strategy into the design of a new product by placing the end user's privacy needs and concerns at the forefront of all decisions.

PHASE 1

Ideate & Explore

This phase of the Product Development Lifecycle is about exploring potential cornerstones of the product: Who are the users? What are their needs? What can you build that addresses user needs? What are potential business models? What have you tried? Are there opportunities to innovate?

Typical Tasks

- Identify target customers and user groups
- Understand users’ needs, context, and constraints
- Generate product ideas to alleviate users’ problems and help them achieve a goal
- Assess the feasibility of evaluating and validating your assumptions: Is your team ready to move through the next stage? Have you scoped this enough to validate an idea or two?

Ideating and Exploring with Privacy by Design

As soon as your team starts thinking about working with data about people, it's time to start thinking about privacy.

While your exploratory conversations may naturally lean toward exciting features for the new product and creative things you can do with data, integrating Privacy by Design can and should begin at this stage. The degree to which you consider privacy depends on what data is used, collected, stored, and shared, and having a responsible data strategy to guide you from the outset is key.

In this early stage, the head of your product team leads team members through initial conversations about potential data sources. These conversations surface potential concerns for end users. The team lead can also use this time to explore your team's commitment to ensuring the product strategy includes robust privacy protections.

Which approach will your team take?

✗ **Tired:** Teams use any available data source they can collect because it's possible from a technical standpoint.

✓ **Wired:** Teams commit to ensuring users understand the purpose and procedures of how to handle their data. Users can make informed choices about their data, and any collected or utilized data is directly linked to providing the service.

Draft Your Responsible Data Strategy

Using the worksheet on page 26, write down your team's vision and goals for working with data and supporting user privacy. Then, consider which principles and tactics you'd like to deploy. And finally, commit to acting on your ideas.

Using the worksheet on page 27, hold a team discussion about privacy sensibilities. You can begin by writing down your personal views and assumptions about privacy and how you bring those into your work. Then, invite everyone to share their ideas and discuss them as a team.

As soon as the team starts working with data about people, it's time to start thinking about privacy.

What Are the Dangers of Omitting Privacy by Design?

While it may be tempting to skip the discussions about designing with privacy in mind, there are consequences for omitting this step. Consider these outcomes:

Second-Rate Product

Your team delays privacy considerations until it is time to address the pre-launch checklist. You notice it calls for a data compliance review. You get feedback from compliance reviewers on issues that would have been easy to address early in the process but now require significant resources to fix. The timing creates another challenge: it's right before the launch, so the product team feels frustrated and unfairly blocked, and reviewers avoid scrutiny of the product for fear of postponing the launch. The result is a second-rate product.

Reputational Damage

Users are unhappy with how data is collected, stored, used, or treated. They post poor product reviews and alert the media. Your company is caught flat-footed, and users question your company's trustworthiness. Under pressure to answer detailed questions, your company finds it difficult to respond because it either did not do data privacy work or did not document it adequately. The fumbled response heightens public scrutiny, causing lost sales and possible legal action (e.g., consent decrees in the U.S. or fines in the E.U. for violating the GDPR).

If you aim to promote users' well-being by respectfully handling and protecting their data, delaying privacy considerations risks subpar results.

Worksheet

Opening Up About Privacy

Objective: Deepen your privacy sensibilities and document your findings.

Duration: 10 minutes on your own and 20 minutes as a team.

In this activity, team members examine their opinions and assumptions and explore how they bring their views into your company's work. Team members may have instinctual responses based on personal experiences with data. Write these down and explore these perspectives with the team. If it is difficult to begin the discussion, use the Common Traps section, beginning on page 51, to prompt a conversation. Remember, the purpose is to generate ideas, not to be overly prescriptive.

Worksheet: Opening Up About Privacy

01

On Your Own

Complete this worksheet, then review your answers and decide what you want to share with your team.

10 MINUTES

1. What types of data are typically used by fintechs like yours?

2. To what extent do you think fintech end users know about what data is collected and used by fintechs (e.g., types of data, how their data is protected, etc.)? Does your answer to this question depend on different user types (e.g., rural vs. urban, young vs. old, literate vs. illiterate)?

3. When and how would a first-time user of digital finance learn about data practices?

4. If an app requires sensitive data, how can a company mitigate the risks of using this data in unintended or harmful ways?

Worksheet: Opening Up About Privacy

5. Considering your interactions with digital apps and services, think of a time when you wondered what personal data a company collected or used. Describe the situation — what stoked your curiosity, and what did you do next?

6. What does data privacy mean to you?

7. What would it look like to be transparent with users about how their data is collected or used?

8. What would it look like to give users options for managing how their data is collected, used, stored, or deleted?

02

Team Discussion

First, choose someone to be a notetaker. Then, go around the room and discuss the questions above.

Prompts: Where is your team aligned? Where are you not aligned? In what aspects might the team need to develop its understanding of these issues?

20 MINUTES

Explore Further

What is Data Privacy?

Revisit common terminology as explained by an engineer

Read the article

Pedantic About Privacy

An explanation of concepts related to privacy as told by a "translator from geek to human"

Read the article

Firefox's Privacy Philosophy

A good example of how to center privacy rights

Learn how they did it

Smashing Magazine's Privacy Policy

Another good example of how to center privacy rights

Learn how they didi it

Your Company's Privacy Policy

Reread your company's privacy policy in the context of this playbook

Your Competitors' Privacy Policies

Read your competitor's privacy policy and compare it to your own. What do they do better? Where do they need to improve?

PHASE 2

Validate

This phase of the Product Development Lifecycle aims to refine and evaluate the possibilities your team generated during the Ideate & Explore phase. A key objective is to de-risk the product strategy as early and thoroughly as possible. In addition, the tasks will uncover additional insights to inform the product design.

Typical Tasks

- Refine user stories, personas, and use cases
- Identify potential business models
- Identify objectives and success metrics
- Understand potential risks
- Understand the competitive landscape

Validating with Privacy by Design

As your product and responsible data strategy begin to take shape, validate whether your team can use data in the ways identified in the Ideate & Explore stage.

This process may include the following:

- ✓ Understanding relevant laws and regulations according to local jurisdictions
- ✓ Understanding users' attitudes, preferences, and concerns about the data that may be used or created by the new product
- ✓ Exploring potential harms introduced by creating new data sources or combining existing ones

Acting now positions your team to identify opportunities to address concerns before entering the Design & Develop stage. This approach optimizes the likelihood that your product will meet users' needs and expectations while also reducing unanticipated harm.

Add Data Privacy to User Experience (UX) Research Plans

Identify opportunities to include research questions about users' attitudes, preferences, and concerns about data collection, use, storage, and sharing. Find ways to explore these topics in primary and secondary UX research initiatives in order to gain a clear and realistic understanding of your users' expectations and needs. Two additional pointers:

01 **Avoid solely focusing on your first wave of users.** In inclusive finance, many digital providers initially serve urban, young, and employed consumers. With higher and more predictable income streams and greater digital savviness, this swath of customers represents low-hanging fruit. However, as fintechs expand their customer bases, they reach demographics and user groups with different attitudes, preferences, capabilities, and concerns regarding data and data privacy. Therefore, customers in your second and third waves of expansion may think differently about your products and data practices, and they may not have the same digital capabilities.

02 **Consider how your product might exacerbate offline privacy risks for vulnerable groups.** Explore how the onboarding process for your digital product might heighten data privacy risks for any potential user group. For example, for low-

income women, the digital world poses numerous risks – ranging from a higher potential for fraud, surveillance, and identity theft, to targeted violence, misuse of personal images and data, and sharing inappropriate content or behavior. While some companies assume digital financial services are solely a channel to economic empowerment for women, it can also lead to adverse impacts (such as domestic violence) if companies do not take sufficient time to understand the potential risks from overlooking privacy needs.

Learn From the Bad News

Following industry news is a great way to stay up-to-date on emerging trends and learn about the successes and failures of other tech companies. We recommend:

Adding data privacy and data-related consumer protection issues to the topics you follow. Even if news coverage seems sensational or unfair to new tech, reading it is worthwhile.

Searching for the value in the bad news and asking yourself, "How could the product team have better managed the data issues?"

Looking for situations where people feel they were wrongly informed or taken advantage of regarding their data. Users might also read about data problems and wonder if your product presents similar challenges.

By following the news, you can learn from criticism and differentiate your product by using better data practices.

Options for conducting UX research include:

User Surveys - Add questions that assess users' comprehension of the data collected during transactions and identify which data rights are most important to them.

Interviews or Focus Groups - Include questions about users' past experiences with data and their concerns about potential harm or adverse effects.

Prototypes - When getting feedback on low-fidelity prototypes, include mockups of the consent flow and screens with settings relevant to data collection or data-centric features.

Desk Research - Look for findings to inform the team's understanding of acceptable data practices, necessary safeguards, and features a user might expect to see on data collection and its usage.

Understand Privacy from a User's Point of View

Product teams sometimes complain that privacy is too subjective. Using the concept of 'contextual integrity' may help teams better understand privacy from a user's point of view.

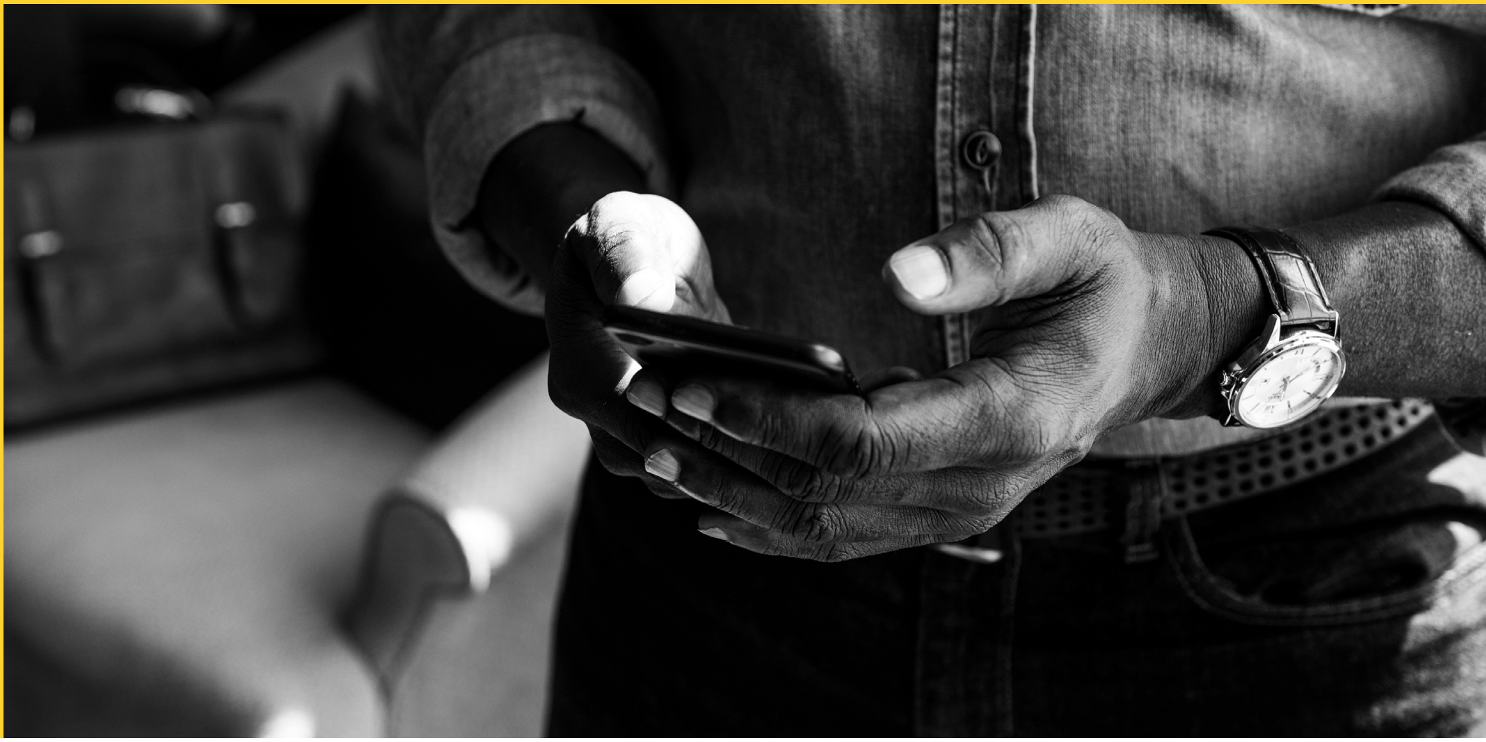
Contextual integrity prompts a change from thinking about types of data toward a mindful approach, one related to the flow of information (i.e., the use of information).

> **Contextual integrity is highly relevant to your work because the user should know if the product will use data unexpectedly or in a new way. Do not assume that a secondary use is acceptable.**

Rather than expending time and effort marking pieces of information as private or sensitive, contextual integrity acknowledges that information may be disclosed willingly in specific contexts to achieve a particular goal, even if the information would be considered highly sensitive in another context.

For example, when patients seek medical care, they are willing to share sensitive information with their doctors, expecting them to use it solely to treat their condition. However, when the care team needs to use the sensitive information for other purposes, they typically ask for informed consent, allowing patients to accept or decline. Understandably, patients may be upset and consider it a privacy violation if their doctors, without their permission, share that information with third parties or use it to attempt to sell them nonmedical items. That would be a violation of contextual integrity.

> **"They should not care about where I get money for my airtime. Being a good borrower is repaying your lenders well. Trying to know how much airtime you use daily is like trying to know how you eat daily."**
>
> **Response from a 29-year-old Rwandan man when asked about the fairness of different data sources that digital lenders could use to assess creditworthiness, as part of CFI research in Rwanda in 2021**



What Are the Dangers of Omitting Privacy by Design?

You can expect user backlash if you conflate the ability to collect the data with permission to use the data.

In 2010, Google learned this lesson the hard way when it launched a new social networking, microblogging, and messaging tool called Buzz. At the time, social networking websites were quickly gaining popularity, and Google mined Gmail usage patterns to auto-populate follower lists in Buzz. This unexpected secondary use of customers' data was easy to spot because the new social network publicly displayed the top five most frequent contacts for each user. Gmail users pushed back, and Google had to make rapid changes (see the 'Explore Further' section for the full story).

By applying contextual integrity and following the advice in this playbook, you can explore more effective pathways for launching a new product.

Explore Further

Fintech & Data Privacy: Keeping Customer Data Safe

Read more about typical security and privacy concerns related to fintech adoption

Read the article

Desk Research

How to use desk research to kick-start your design process

Read the guide

Contextual Integrity

Explore the academic background and other applications of contextual integrity

Read the article

Privacy, Security, and Surveillance in the Global South

Explore the research findings and consider the implications of the cultural context in key markets

See the findings

Data and the Global South

A look at key issues with implications on inclusive digital development in less developed countries

Read the report

Google Buzz Privacy Issues Have Real Life Implications

Learn about the implications of product design choices

Read the article

A New Buzz Start-Up Experience Based on Your Feedback

Read about the product changes made after the initial release of Buzz

Read the article

PHASE 3

Design & Develop

In this phase of the Product Development Lifecycle, the product team begins to turn an idea into a reality.

Typical Tasks

- Deciding which features are critical to satisfy user needs
- Creating prototypes for further validation
- Prioritizing features and functionality
- Documenting a product plan and adapting product development processes to match the team's goals and constraints

Designing and Developing with Privacy by Design

Here are three things you can do at this stage:

01 Put your data strategy into the product roadmap

02 Ensure that the UX matches the back-end implementation

03 Design usable notice and consent

Put Your Responsible Data Strategy Into the Product Roadmap

As you determine your product roadmap and your team prioritizes which features to implement first, use the Responsible Data Strategy Worksheet on page 12 to guide decision-making and incorporate updates when needed. For example, in the 'List Your Objectives' section of the worksheet, you spelled out the data rights that users might expect. Now, you can translate those objectives into user stories and user interface (UI) flows that support the intended goals. This is also the time to specify how you hold your team accountable for implementing your responsible data strategy.

At this stage, confirm that the product roadmap includes a plan for implementing your data objectives. It's also helpful to consider any design decisions that might impede your team's ability to add these features in a future release. For example, if your team decides a Right to Access is relevant to the product, plan to build corresponding features for the initial product launch. If your team feels it could delay the Right to Access functionality until a future product update, seek appropriate legal counsel to understand the risks.

From a product perspective, consider whether the product can still satisfy the objectives from your responsible data strategy in the initial release or future releases. Sometimes early product decisions can make it difficult, time-consuming, or nearly impossible to make changes later.

Design Usable Notice and Consent

Whenever possible, consumers should be empowered to choose how companies use their data. However, for people to be able to make that choice, they must first understand what data is used, how it is used and the possible implications, their options, how to express their choices, and where to seek additional information.

Consent is a critical concept because the nature of privacy decisions is personal, contextual, and circumstantial. Therefore, companies must ask users for permission to process or use their data for the intended purposes. Unfortunately, there are many examples of poorly designed consent experiences. For example, instead of notices presented in clear, simple-to-understand terms, it's common for services to rely on legalese which often includes jargon that is complex and difficult for users to understand.

Most users understand how companies use their data from personal experience, advertising, a product's user interface, and related apps and services. Usually, users do not review the privacy policy. Therefore, the product team must use other points of engagement for users to build and maintain an accurate understanding of how the product uses and protects their data. The goal is to communicate clearly and concisely so users can determine how and if they want to proceed.

Consent is a critical concept because the nature of privacy decisions is personal, contextual, and circumstantial. Therefore, companies need to ask users for permission to process or use their data for the intended purposes.

Design Tips

Find the Seams and Points of Integration

Your team should integrate and design screens for privacy choices to be a critical part of a product's primary functionality rather than an afterthought. For example, if you're building a mobile app, the user may see standard dialogs and terminology during installation, especially if the product requests permissions. While there may be limited options to customize the visual design or the timing of these screens, the product should present a coherent experience for the user. Where possible, add context to explain how and when your company uses the permissions. You may also direct users to the UI to revisit decisions within the app or the operating system.

Avoid Using Deceptive Design Practices

Deceptive design, also known as dark patterns, is a common practice that can show up when users make privacy decisions. Unfortunately, it can result in users making decisions against their best interests. An audit of digital lenders and insurers in India found that many apps used deceptive design patterns to force the disclosure of excessive information, including SMS data, social media accounts, photo galleries, location data, or certain health conditions, without explanation or clear linkage to the financial product. Lenders also combined multiple consent requirements and hyperlinks into one checkbox and a pre-selected checkbox representing the more privacy-intrusive option.

These design patterns can be a way for companies to meet product growth goals. However, even if they work in the short term, they are counterproductive in building long-term, trusted relationships with users over the long term.

Ensure That the UX Matches the Back-End Implementation

Before deploying the product, confirm that the information presented to users on the front end matches what happens on the back end. Consider the following examples:

The Sign-Up

If the sign-up flow requires the user to enter a phone number, and the accompanying text says, “We only use your phone number for account security purposes,” then the product, database, and related code should reflect that commitment consistently. Achieving this requires carefully designing internal systems and configuring databases to ensure that you store phone numbers with appropriate access control mechanisms.

The Privacy Promise

If the UI text says, “Your calls are secure; we use end-to-end encryption,” confirm that the appropriate security measures are in place. Here, your team should have correctly configured and implemented end-to-end encryption, which a user might reasonably expect based on the accompanying text.

The Data Promise

If the sign-up flow promises that only anonymized data is stored, confirm this is true throughout the code and in any integrated third-party libraries or services. Properly anonymizing data can be complex, so proceed with caution when committing to work with anonymized data.

Sometimes, there’s an indirect relationship between the commitment and the mechanisms to satisfy that commitment. For example, a company may claim that it does not share personal information about its users with third parties. However, it plans to work with a third party on ad measurement. In that case, the company can utilize privacy-enhancing technology (PET) to achieve its objective while also maintaining its privacy promise. Work with relevant experts to ensure your team validates its claims. When communicating privacy commitments, it’s better to under promise and over deliver.

Explore Further

What is Consentful Tech?

Expand your understanding of the elements of consent

Read the article

Nobody Reads Privacy Policies: Here's how to fix that

Read about why it's important to think about notice as bigger than the Privacy Policy

Read the article

Ruined by Design: How Designers Destroyed the World, and What We Can Do to Fix It

A design ethics and activism book

Get the book

Mozilla Study on Data Privacy Labels

Explore many examples where an app's data practices do not match the Privacy Policy

See the study

Basic Principles for Requesting Permissions in Android Apps

Review high-level guidance for designing the permission flow in an app

View the guidance

Good and Bad Examples of Privacy Notices

Learn the difference between a good and bad privacy notice

Download the PDF

Explore Further

Privacy in the Product Design Lifecycle by the UK's ICO

Explore this resource for additional guidance on operationalizing privacy in products

See the guidance

Privacy Enhancing Technologies

Browse this report on the state of privacy-enhancing technologies to seek ideas for potential solutions and also areas in need of development

View the report

Privacy Enhancing Technologies Decision Tree

Explore the decision tree to understand the uses and drawbacks of existing PETs

Read the article

Tricked by Design: Deceptive Patterns in Indian Fintech Apps

An overview of deceptive designs in the Indian fintech market

Read the article

Deidentification vs. Anonymization

A brief explanation of why anonymization is harder to achieve than you might expect

Read the article

PHASE 4

Deploy & Maintain

This phase of the product development lifecycle covers everything between launching the initial product and transitioning into the Retire phase. The details differ by company and product. In some cases, this phase focuses on growing the user base, product features, and offerings; in other cases, the emphasis is on responding to external changes in the marketplace, social culture, or regulatory environment.

Typical Tasks

- Release the product
- Monitor metrics
- Connect with users
- Stay abreast of changes

Deploying and Maintaining with Privacy by Design

Whatever product changes may occur when deploying your product, your team must focus on maintaining your commitment to user privacy. Your goal is to stay true to your original responsible data strategy or to adapt the strategy if needed. If product updates are required, proactively communicate any changes with current and future users.

> **Whatever product changes may occur when deploying your product, your team must focus on maintaining your commitment to user privacy.**

Product changes can stem from various sources, including internal changes within your company, changes prompted by new laws or regulations, or changes influenced by social or public policy pressure. Below are a few product changes that may impact your responsible data strategy.

Internal Changes

Internally motivated changes are generally straightforward. Depending on their size or scope, return to the relevant portion of the responsible data strategy and design new features that are consistent with the original plan and messaging. If adaptations to your responsible data strategy are needed, ensure that the product marketing, UX copy, sales material, and legal disclosures match the new features.

Sometimes a change relates to entering a new market or pursuing a new customer segment. In this case, even if your team assumes that the product will stay the same, you'll still want to revisit your responsible data strategy. Assess the objectives for their suitability in the new market and repeat the work from the earlier phases to uncover relevant data-related harms or concerns specific to new user groups.

Laws and Policy Changes

New laws or regulations may require changes to how a company uses data. If companies lack a responsible data strategy, distinguishing between what the company implemented and what it needs to add to a product can become a lengthy and challenging task. However, with a responsible data strategy, your product team has clear documentation about collecting, storing, using, and deleting data. As a result, it can be simpler to identify when a new law is relevant and what your company needs to do to accommodate the new law or policy. Continue to update the strategy as lawmakers enact new changes.

External Events (But Not New Laws)

Technology usually moves faster than applicable laws and regulations. However, the widespread use of technology and devices means that seemingly unrelated issues can suddenly prompt tough questions about data and require product changes.

For example, the Cambridge Analytica scandal raised many questions about how the company accessed the dataset. When it became public that researchers exploited Facebook's Graph API to gain access to data through a personality quiz, it raised concerns about other app developers having access to sensitive permissions on Facebook. The Facebook product team was caught flat-footed, unable to quickly answer basic questions, such as, "Which apps had requested access to specific permissions? Which users were affected by the survey app? How much data did apps request through the API?" The situation motivated Facebook to redesign old features, retire some features, and design new ones.

Similarly, when the U.S. Supreme Court overturned the ruling in the abortion case, Roe vs. Wade, it raised questions about apps collecting reproductive health data from users. The concern was that law officials could accuse individuals of crimes using personal and sensitive information, which led to public inquiries about the data practices of health apps.

When the spotlight is focused on how a company uses data, a team should be ready to respond in at least two ways:

01 Give clear answers about whether an emerging situation raises a relevant concern.

02 Determine if the user can report feedback, ask questions, turn off a feature, or take any other meaningful action.

PHASE 5

Retire

The objective at this stage is to ensure that customers and partners experience a smooth offboarding once the product is no longer available or if it changes substantially differs from the start of the relationship.

Typical Tasks

- Consider options for discontinuing the product
- Decide how to handle existing user data
- Decide how to communicate changes to customers and partners

Retiring with Privacy by Design

Users should have autonomy over their data if the product becomes unavailable, undergoes significant changes, or stewardship is transferred to another entity.

As early as possible, your product team should devise a plan for retiring the product that is consistent with your responsible data strategy. When it's time to execute the plan, discuss how to stay as true to the data strategy as possible, knowing that resources may be limited or circumstances may have changed.

Sometimes, your team may need to develop new software features. For example, if the responsible data strategy emphasizes a Right to Access, be sure users can download a copy of their data. Even better, allow users to export the data in a form compatible with similar services. If the responsible data strategy emphasizes a Right to Control, be sure users can opt out of a data transfer or can delete their data if another entity takes ownership of the product.

Guiding Questions

In the initial phases of any Product Development Lifecycle, adopt a proactive approach toward retiring a product. These considerations should also extend consistently throughout a product's lifecycle. Here are some key questions to bear in mind:

- □ What factors should you consider when developing a new product to determine when and how it should be retired?
- □ What privacy commitments did you make to users during the life of the product, and how can you continue to meet these commitments as you phase out the product?
- □ How (and when) will you communicate to users that you plan to retire a product?
- □ Who in the company should lead the retirement of a product? Are the people with the most knowledge about the product, data structure, and privacy commitments actively involved?
- □ What is the most productive use of the resources (staff time, data storage, etc.) that become available when you discontinue a product?

Explore Further

Checklist For the End-of-Life of Your Product

Understand the broader concept of the Retire phase for products

Read the article

Google Buzz Has Gone Away

Read this example of a lasting note from Google about retiring the Buzz product

See the example

Reaping the Product End of Life: A Product Management Research Agenda

Read an optimistic take on the opportunity presented by the Retire phase

Read the article

Advocating for Privacy by Design

For privacy as product to take hold within your company, it is important for all team members to strongly advocate for the principles of Privacy by Design and the value it provides to the company and the end users. A company that is privately and publicly committed to the foundational principles in this playbook reduces its operational and reputational risk, builds trust with new and existing customers, and upholds the commitments it makes to the low-income customers it serves. Treating privacy as product is not only good for the bottom line, but it is the right thing to do for your customers.

While you and your team should promote the PbD principles internally, it is also important to work with your company's marketing team who can communicate your company's privacy commitments to customers, investors, and other key stakeholders.

Inspire Your Team

If the concepts of Privacy by Design are new for your team members, you should emphasize the value of the work and take the time to help show your team why privacy as product is so important. In the Common Traps section, you'll find several examples of the attitudes you may encounter within your team and tactics to overcome or avoid the traps. Work with your team to review the playbook carefully, create space for new conversations, and clarify how the guidance supports the team's goals.

Manage Up

As early as possible, begin planning conversations with your leadership and partner teams about the most effective ways to apply the concepts within this playbook. Hold regular planning conversations throughout the process, share the findings from desk and UX research, and manage expectations about what's realistic to achieve.

When speaking with management, emphasize the business case for privacy. Senior executives may take a more active interest in the topic if you frame the benefits in terms of increased customer retention, establishing a trustworthy brand in the market, and reducing the risk of fraud or costly data breaches.

Collaborate with Partner Teams

Privacy and data protection approaches span many teams and roles. Look for partners who work on data protection, data security, customer success, marketing, and user experience. Then, speak with them about your plans for collecting, storing, using, and deleting data according to user needs and preferences. Remember that this playbook is about building a product and seek additional legal guidance to ensure the team knows relevant laws or regulations.

Transition with Consistency

If another entity is taking on new ownership of the product or the data, share your responsible data strategy and clarify your commitments to users regarding how your team collected, stored, used, deleted, and shared the data.

Build Institutional Knowledge

Be sure to document your work on PbD and the valuable insights gained to share with internal teams and the broader community. Document what your team decided to do, and not do, and what led to those choices. Record what you implemented and how you arrived at those solutions and evaluated them.

Stay Up to Date on Current Events

You'll want to observe how users receive your product and watch for external events that may impact the design or reception of the product. Stay in touch with your stakeholders to determine when your company needs to take action.

Communicate Clearly to Users

Be prepared to communicate with users and stakeholders about how you use, store, delete, or share their data. Explain the processes you take to handle the data and articulate your rationale; customers typically are more comfortable sharing their data if they understand why you want to use it. These efforts demonstrate that your company values privacy and sets you apart from competitors who do not share the same commitment.

The effort to incorporate Privacy by Design is worthwhile, regardless of the audience. Vocally expressing your values and commitments – both internally and externally – will cultivate a loyal customer base and create a powerful opportunity to grow your business. Keep your marketing team well-informed of the work so they clearly understand the value and know how to communicate these changes to customers.

Common Traps to Avoid

This section is based on Ari Waldman’s work in *Industry Unbound*

As you apply the guidance within this playbook and incorporate privacy as product, you may encounter one or more common traps. In reviewing them, pay close attention to clues that your team is at risk of falling into a trap. Do the signs seem familiar? Have you encountered them in your work? If the answer is ‘yes,’ closely review the recommended tactics and share them with your team.

The Technology Trap

This trap represents the false belief that implementing a specific technical mechanism is sufficient to address broader concerns about the appropriate use of information.

Signs

> "Okay, we'll just use _____."
>
> Reaching for the latest advances in privacy enhancing technologies (PETs) or encryption without the expertise to respect the limitations

> "Well, we encrypt the data; that's enough protection."
>
> Conflating user privacy concerns about the use of data with confidentiality/secrecy.

Tactics to Overcome

□ Take time to research and understand the strengths and tradeoffs of applying encryption or PETs. Cryptographic methods for protecting information are notoriously sensitive to correct implementation and use. Each technique makes assumptions about how the data is processed and how the encryption keys are managed. Not all methods are equal. Remember the familiar refrain, "Don't roll your own," which means you should leave the design of cryptographic protocols to cryptographers and stick to using reputable methods.

□ Learn about this 'Lightweight approach to privacy threat modeling.'

□ Read relevant industry research reports on consumer attitudes toward data, privacy, and data protection. Some resources include:

- The Persona Behind the Data
- Data Transparency's Essential Role in Building Customer Trust
- Americans and Privacy
- Share of FinTech application users who feel comfortable sharing data on the financial information and history in the United States in 2018

□ Revisit the callout in the Validate section on contextual integrity (see page 32).

□ Revisit the section called "Add Data Privacy to UX Research Plans" in the Validate section (see page 30).

□ The Choice Trap

Team members forgo responsible design practices and instead rely on presenting the user with more choices.

Signs

> "Let's enable it by default, and we'll put an opt-out on the settings page."

> "I'm not sure if people will go for it, but if they despise it, they'll be motivated to find the off switch in settings."

> "We don't have time for more UXR, so let's make it an option."

Tactics to Overcome

□ Spend time as a team to understand user needs and design a product that matches.

□ Carefully consider every decision behind enabling a feature by default. Many users will not take the time to learn the defaults or make changes, but you shouldn't use this against them.

□ Read about the limits of relying too heavily on individual notice and consent. Some references to begin with include:

- Rethinking notice and consent – A chat with Jen King
- How "Notice and Consent" Fails to Protect Our Privacy
- Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency

□ The Nihilism Trap

Team members believe that protecting user privacy and building privacy features is a wasted effort.

Signs

"But other services are collecting so much data; why should we do it differently?"

"Data breaches happen constantly, and privacy and security practices are imperfect; why bother?"

"Privacy is dead."

"No one cares about privacy anymore anyway."

"If we don't build it, a competitor will."

Tactics to Overcome

□ Return to the Responsible Data Strategy worksheet (see page 12) and remember what your team and company set out to achieve.

□ Read existing research on users' attitudes and behaviors regarding their data.

□ Pay attention to how companies are held responsible for their inattention to data privacy and look for headlines about privacy-related issues.

□ The Codability Trap

This trap represents the false belief that a team cannot implement privacy measures unless it can fully address the issue by code.

Signs

A team claims it would be glad to implement privacy measures, but someone else must deliver precise requirements.

A team dismisses users' privacy concerns as too subjective or difficult to capture in code.

Tactics to Overcome

□ Product teams make difficult and subjective design decisions at many points throughout the Product Development Lifecycle. So, developing suitable designs to support users' privacy concerns should be no different. Use the Responsible Data Strategy worksheet (see page 12) to guide the process of translating user needs to requirements and identify places where you may need additional people or processes.

The Efficiency Trap

Teams become fixated on near-term goals in the name of efficiency.

Signs

The team is hyper-focused on deploying a product as quickly as possible and chooses to postpone working on other qualities like usability, privacy, or security.

A company prioritizes shipping quickly. This can include configuring the internal development environment to put ease of access to data ahead of implementing appropriate access control mechanisms.

Tactics to Overcome

- □ Pay attention when the instinct to move quickly emerges and revisit the Responsible Data Strategy worksheet.
- □ Learn about the first mover advantage myth.

The Bystander Trap

Team members fail to take personal responsibility for privacy.

Signs

The team delays consideration of data privacy concerns until a security, privacy, or compliance review.

The team assumes that someone else handles pertinent issues.

Team members assume that any data that's accessible internally is available for use in their product.

Tactics to Overcome

- □ Ensure all team members understand that privacy is their responsibility. Especially if you work with data, it's vital to take personal responsibility for the people represented by the data you have.
- □ Apply the guidance in this playbook and seek additional resources like "Privacy in the Design Cycle."

□ The Myopia Trap

Team members design the product to meet the needs of users like themselves and fail to account for diverse user groups.

Signs

Leaders on the product team create a product to satisfy users' needs that match their own needs.

A predominantly male team fails to consider the gender-specific concerns that might arise.

Tactics to Overcome

□ Apply user experience research methods to ensure your team accurately understands the desired users' needs and concerns.

□ Stay aware of developing privacy concerns that marginalized demographics may experience.

□ The Goodness Trap

Team members feel their 'goodness' staves off potential problems.

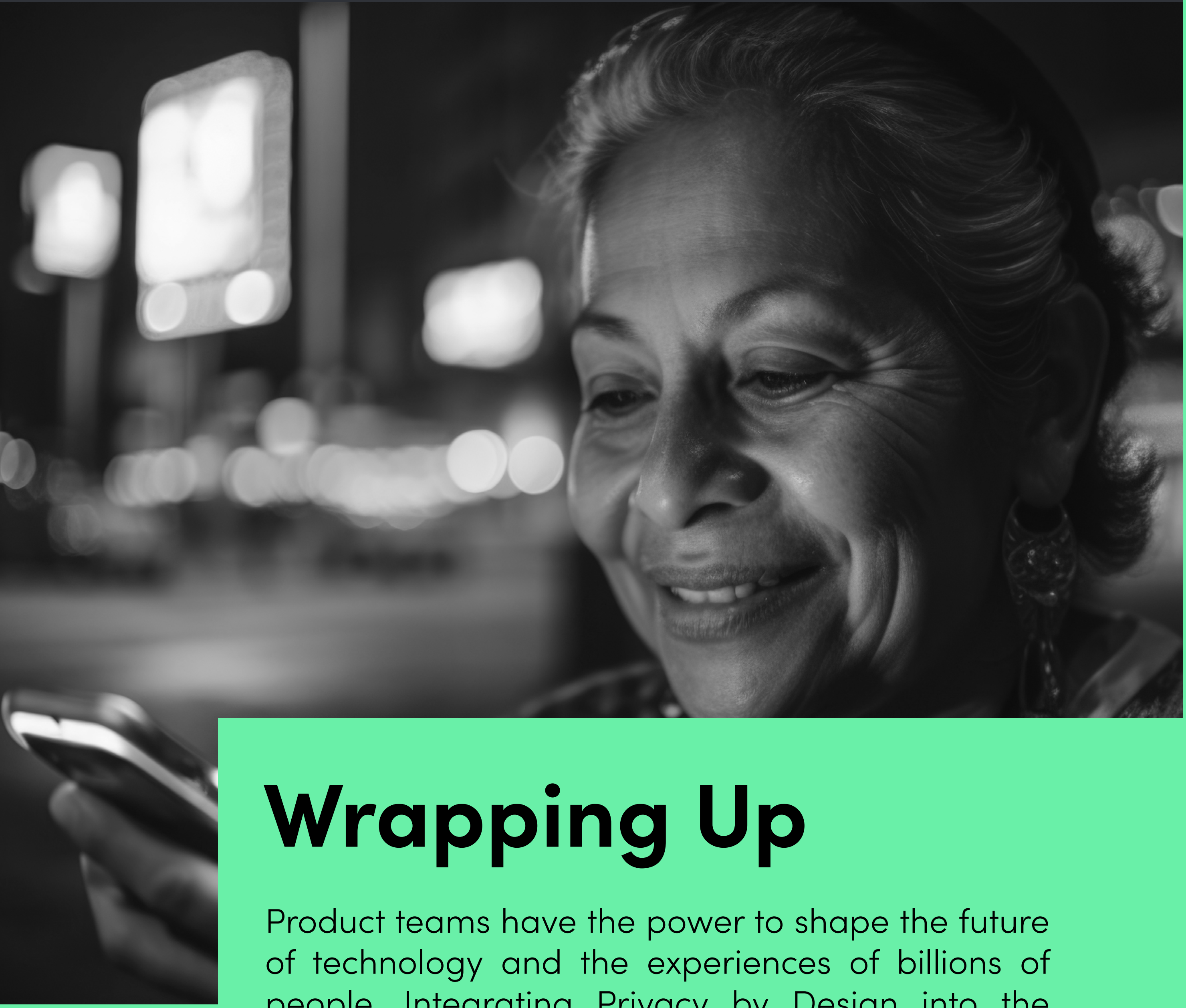
Signs

Team members claim they care deeply about user safety and privacy concerns, but they take no action.

Tactics to Overcome

□ Do the work. Good intentions, without meaningful action, are insufficient.

□ Stay aware of developing privacy concerns that marginalized demographics may experience.



Wrapping Up

Product teams have the power to shape the future of technology and the experiences of billions of people. Integrating Privacy by Design into the product development process creates a safer, more transparent digital ecosystem that ultimately helps low-income users realize the full benefits of digital finance.

This playbook should serve as a stepping stone, rather than a final destination. While the ideas, practices, and resources provided here give you a foundation to build upon, practicing Privacy by Design requires consistency. It is not enough to tick off compliance checkboxes; true privacy leadership demands a proactive and ongoing commitment.

References

INTRODUCTION

Accion Venture Lab, "A Startup's Guide to New Product Development," accessed Jun. 2023. https://content.accion.org/wp-content/uploads/2020/09/accion-venture-lab-startup-guide-to-new-product-development.pdf

Banerji, Annie. "'Worst decision of my life': Byju's accused of driving parents into debt with predatory practices." Scroll.in, Dec. 2022. https://scroll.in/article/1039797/worst-decision-of-my-life-byjus-accused-of-driving-parents-into-debt-with-predatory-practices

Berjon, Robin. "Privacy as Product." Personal website/blog, accessed. Jun. 2023. https://berjon.com/privacy-as-product/

Cerise+SPTF, "Universal Standards for Social and Environmental Performance Management," Feb. 2022. https://cerise-sptf.org/download-the-manual/

Duflos, Eric and Juan Carlos Izaguirre. "Reading Findex With A Consumer Protection Lens." CGAP, Oct. 2022. https://www.cgap.org/blog/reading-findex-with-consumer-protection-lens

Hartzog, Woodrow. "Privacy's Blueprint: The Battle to Control the Design of New Technologies." Harvard University Press, Apr. 2018. https://www.hup.harvard.edu/catalog.php?isbn=9780674976009

Mamadov, Elmar. "Product Development Lifecycle (PDLC): Complete Guide." CS Careerline, Jan. 2023. https://cscareerline.com/product-development-lifecycle-pdlc/

Rizzi, Alexandra. "Embedding Trust: The Potential of Privacy by Design for Inclusive Finance." Center for Financial Inclusion, Dec. 2022. https://www.centerforfinancialinclusion.org/embedding-trust-the-potential-of-privacy-by-design-for-inclusive-finance

Waldman, Ari. "Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power." Cambridge University Press, Sep. 2021. https://doi.org/10.1017/9781108591386

CREATING A RESPONSIBLE DATA STRATEGY

Data Privacy Manager, "What are 8 Data Subject rights according to the GDPR," accessed Jun. 2023. https://dataprivacymanager.net/what-are-data-subject-rights-according-to-the-gdpr/

Dennedy, Michelle. "Why Privacy Is Generative and Constantly Moving." BankInfoSecurity.com, May 2023. https://www.bankinfosecurity.com/privacy-generative-constantly-moving-a-21924

Lotame, "How to Build a Data Strategy," May 2019; Last modified Jan. 2023. https://www.lotame.com/how-to-build-a-data-strategy/

Olsen, Nicole. "The Eight User Rights Under the GDPR." PrivacyPolicies.com, Jul. 2022. https://www.privacypolicies.com/blog/gdpr-eight-user-rights/#Summary

MIT Center for Information Systems Research, "Classic Topics: Data," accessed Jun. 2023. https://cisr.mit.edu/content/classic-topics-data

UCI Office of Research, "Privacy and Confidentiality," accessed Jun. 2023. https://research.uci.edu/human-research-protections/research-subjects/privacy-and-confidentiality/

IDEATE & EXPLORE

Flanagan, Heather. "Pedantic about Privacy." Spherical Cow Consulting, Jan. 2023. https://sphericalcowconsulting.com/2023/01/08/pedantic-about-privacy/

Kelly, M.J. "Here's what we think about your privacy at Mozilla." Mozilla, Aug. 2018. https://blog.mozilla.org/en/privacy-security/firefox-privacy-philosophy/

Smashing Magazine, "Privacy Notice," May 2018. https://www.smashingmagazine.com/privacy-policy/

Wilde, Jonathan. "What is Data Privacy?" Personal website/blog, Jan. 2023. https://jwilde.me/blog/2023/01/21/what-is-data-privacy/

VALIDATE

Ahmed, Syed I., Md. Romael Haque, Shion Guha, Md. Rashidujjaman Rifat, and Nicola Dell. "Privacy, Security, and Surveillance in the Global South: A Study of Biometric Mobile SIM Registration in Bangladesh." Research article from proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, May 2017. https://doi.org/10.1145/3025453.3025961

De Bastion, Geraldine and Sreekanth Mukku. "Data and the Global South: Key Issues for Inclusive Digital Development." Heinrich-Böll-Stiftung, Oct. 2020. https://us.boell.org/en/2020/10/20/data-and-global-south-key-issues-inclusive-digital-development

Official Gmail Blog, "A new Buzz start-up experience based on your feedback," Feb. 2010. https://gmail.googleblog.com/2010/02/new-buzz-start-up-experience-based-on.html

TechCrunch, "Google Buzz Privacy Issues Have Real Life Implications," Feb. 2010. https://techcrunch.com/2010/02/12/google-buzz-privacy

Tudor, Teisanu. "How to use desk research to kick-start your design process." UX Collective, May 2020. https://uxdesign.cc/how-to-use-desk-research-to-kick-start-your-design-process-aab6e67fd7a4

Valdellon, Lionel. "Fintech & Data Privacy: Keeping Customer Data Safe." CleverTap, Jun. 2021. https://clevertap.com/blog/fintech-data-privacy/

Wikipedia contributors, "Contextual integrity," Wikipedia, The Free Encyclopedia, accessed Jun. 2023. https://en.wikipedia.org/w/index.php?title=Contextual_integrity&oldid=1153002358

DESIGN & DEVELOP

Android, "Guides: Request runtime permissions," accessed Jun. 2023. https://developer.android.com/training/permissions/requesting#principles

References

Dasgupta, Monami, Vinith Kurian, and Rajashree Gopalakrishnan. "Tricked by Design: Deceptive Patterns in Indian Fintech Apps." Tales of Bharat Substack, May 2023. https://d91labs.substack.com/p/tricked-by-design-deceptive-patterns

Deceptive Patterns, accessed Jun. 2023. https://www.deceptive.design/

ICO, "Privacy notices, transparency and control," accessed Jun. 2023. https://ico.org.uk/media/for-organisations/documents/1625136/good-and-bad-examples-of-privacy-notices.pdf

Information Commissioner's Office (ICO), "Privacy in the product design lifecycle: Design," accessed Jun. 2023. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/designing-products-that-protect-privacy/privacy-in-the-product-design-lifecycle/design/

Jarovsky, Luiza. "Dark Patterns (Deceptive Design) in Data Protection." UX Planet, May 2022. https://uxplanet.org/dark-patterns-deceptive-design-in-data-protection-5dc79a045030

Kissner, Lea. "Deidentification versus anonymization." IAPP, Jun. 2019. https://iapp.org/news/a/de-identification-vs-anonymization/

Monteriro, Mike. "Ruined by Design: How Designers Destroyed the World, and What We Can Do to Fix It." Mule Books, Apr. 2019. https://www.ruinedby.design/

Mozilla, "Mozilla Study: Data Privacy Labels for Most Top Apps in Google Play Store are False or Misleading," Feb. 2023. https://foundation.mozilla.org/en/blog/mozilla-study-data-privacy-labels-for-most-top-apps-in-google-play-store-are-false-or-misleading/

Thaine, Patricia. "Privacy Enhancing Technologies Decision Tree." Private AI, Oct. 2020. https://www.private-ai.com/2020/10/18/privacy-enhancing-technologies-decision-tree-v2/

The Consentful Tech Project, accessed Jun. 2023. https://www.consentfultech.io/

The Conversation, "Nobody reads privacy policies – here's how to fix that," Oct. 2017. https://theconversation.com/nobody-reads-privacy-policies-heres-how-to-fix-that-81932

The Royal Society, "Privacy Enhancing Technologies," Jan. 2023. https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/

The Royal Society, "Protecting privacy in practice: The current use, development, and limits of Privacy Enhancing Technologies in data analysis," Mar. 2019. https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/Protecting-privacy-in-practice.pdf

RETIRE

Gmail Help Center, "Google Buzz has gone away," accessed Jun. 2023. https://support.google.com/mail/answer/1698228?hl=en&ctx=mail

ProductPlan, "A 10-Step Checklist for the End-of-Life of Your Product," accessed Jun. 2023. https://www.productplan.com/learn/how-to-end-of-life-product/

Wolff, Phil. "Reaping the Product End of Life: A Product Management Research Agenda." Product Hospice, Oct. 2017. https://medium.com/product-hospice/reapingresearchtopics-25aa8fc07029

COMMON TRAPS

Adjerid, Idris, Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. "Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency." Carnegie Mellon University, Jul. 2013. https://dl.acm.org/doi/10.1145/2501604.2501613

Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information." Pew Research Center, Nov. 2019. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

CISCO, "Data Transparency's Essential Role in Building Consumer Trust: CISCO 2022 Consumer Privacy Survey," Oct. 2022. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-survey-2022.pdf

IAPP, "Rethinking notice and consent -- A chat with Jen King," Podcast episode: The Privacy Advisor Podcast, Jun. 2021. https://iapp.org/news/a/rethinking-notice-and-consent-a-chat-with-jen-king/

Information Commissioner's Office (ICO), "Privacy in the product design lifecycle: Design," accessed Jun. 2023. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/designing-products-that-protect-privacy/privacy-in-the-product-design-lifecycle/design

LINDDUN, "Getting Started with GO," accessed Jun. 2023. https://linddun.org/go-getting-started/

MAGNA, "The Person Behind the Data: Consumer perspectives on data privacy -- US Edition," accessed Jun. 2023. https://content.ketch.com/consumer-privacy-perspectives-study

Park, Claire. "How 'Notice and Consent' Fails to Protect Our Privacy." New America, Mar. 2020. https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/

Statista, "Share of FinTech application users who feel comfortable sharing data on the financial information and history in the United States in 2018," Oct. 2018. https://www.statista.com/statistics/1093382/fintech-users-data-sharing-financial-information-history/

Tullman, Howard. "The Myth of the First Mover Advantage." Inc., Oct. 2019. https://www.inc.com/howard-tulllman/the-myth-of-the-first-mover-advantage.html

Waldman, Ari. "Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power." Cambridge University Press, Sep. 2021. https://doi.org/10.1017/9781108591386

CENTER *for*
FINANCIAL
INCLUSION | ACCION

The Center for Financial Inclusion (CFI) works to advance inclusive financial services for the billions of people who currently lack the financial tools needed to improve their lives and prosper. We leverage partnerships to conduct rigorous research and test promising solutions, and then advocate for evidence based change. CFI was founded by Accion in 2008 to serve as an independent think tank on inclusive finance.

www.centerforfinancialinclusion.org
@CFI_Accion