Lead Author
Alexandra Rizzi

Co-Author
Dr. Maritza Johnson

Applying Privacy by Design to Inclusive Finance Product Design

CENTER for FINANCIAL INCLUSION | ACCION

ACKNOWLEDGEMENTS

This brief 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. The authors would also like to thank Edoardo Totolo for overall guidance on the project and Aeriel Emig for editorial guidance.

Introduction 1

Applying Privacy by Design to Inclusive Finance: Rationale and Approach 2

The Case for Privacy by Design 4

Product Managers Are Key Stakeholders in PbD Implementation 5

Implementation Challenges & Playbook Solutions 6

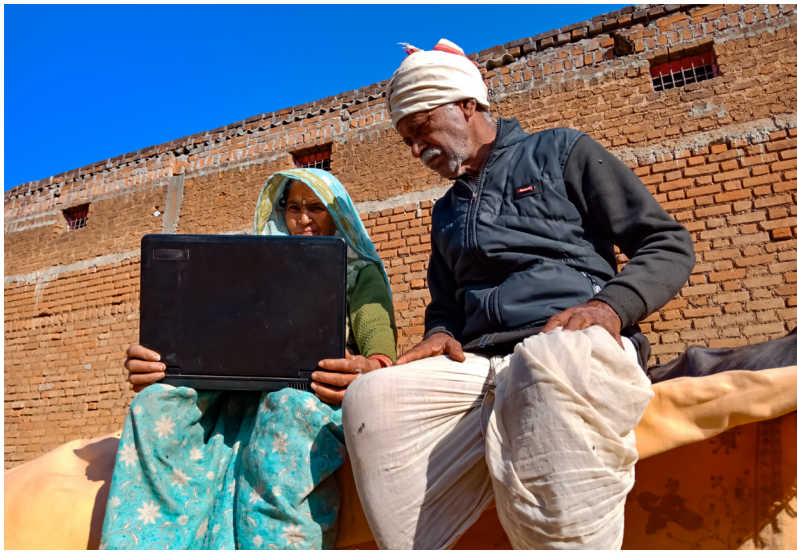
Further Considerations and Frontiers of PbD for Inclusive Finance 9

References 11

Introduction

The arrival of ChatGPT underscores what the Center for Financial Inclusion (CFI) has long found to be true with regards to digital technology and privacy: while consumers value privacy, the rapid and expansive ways that technology has changed no longer afford them the space to properly negotiate their privacy boundaries or choices.[i] [1] This disconnect — between consumer desires and the privacy practices of companies that serve them, including financial service providers — has led to a problematic wedge that can lead to broken trust, tanked user engagement, and lower uptake and usage of digital financial services.[ii] Trust is a key ingredient to achieve the goals of inclusive finance, and there is a need for the sector to develop stronger solutions to better align consumer expectations of privacy and provider practices. While data protection legislation has built a solid foundation, it hinges on informed consent, which has repeatedly proven to be difficult to achieve in practice.

To help bridge the trust gap, CFI has been exploring how the principles of Privacy by Design (PbD) can be applied to inclusive finance and recently launched the Privacy as Product Playbook: How to Practice Privacy by Design When Building Inclusive Finance Products. Privacy by Design is a systems design philosophy to improve how privacy is embedded into systems and offers a counterapproach to the current, compliance-heavy approaches to privacy.[2] By prioritizing privacy within the design of digital products and systems, privacy becomes a defining feature of a system rather than a box-checking exercise.



The Privacy as Product Playbook provides a step-by-step guide for product management teams at digital finance companies to embed a responsible data strategy into the design of new digital financial products while keeping the end user's privacy needs and concerns salient for all major decisions. While the playbook is aimed at product teams, the effort to find solutions that build trust in digital finance for low-income financial consumers is highly relevant for all industry stakeholders.

This brief is intended for all practitioners in the inclusive finance space, shares the rationale and approach for the playbook, and discusses three key challenges for implementation that were uncovered when designing the playbook, how the playbook attempts to address them, and what learning questions remain.

1 For example: Consumers and large corporations alike have been surprised and dismayed to learn that the data they input into the non-enterprise version of ChatGPT does not disappear but rather is used as continuous training data to improve the model. Researchers and red teams have also demonstrated the ease with which training data can be extracted through querying large language models. See Carlini et al. (2021).

2 N.B. It is not the only response. Other frameworks have emerged such as Richards and Hartzog's argument that data-driven companies should be considered fiduciaries of our data and subject to similar obligations as govern our relationships with wealth managers and doctors.

Applying Privacy by Design to Inclusive Finance: Rationale and Approach

First conceived as a framework in 2009 during Dr. Ann Cavoukian's tenure as Canadian Privacy Commissioner, Privacy by Design (PbD) is an approach to IT systems that integrates privacy from the outset. In recent years, PbD has attracted increased attention from regulators, industry experts, and technologists.

In the last year, several regulators have detailed their expectations on PbD, such as Catalonia's Data Protection Authority, which in February 2023 released a guide for developers on Privacy by Design and Privacy by Default.[iii] In March 2023, the California Privacy Protection Agency approved a countermeasure to "Privacy Zuckering" in the form of regulations that require companies to give consumers symmetry in choice, making it as easy for consumers to exercise a more privacy-protective option as it is for them to exercise a less privacy-protective option.[iv] Additionally, the International Standards Organization (ISO) recently published a new standard on PbD which included high-level requirements for organizations as well as specific use cases to help specify their requirements.[v] There have also been rapid improvements and expansions in privacy-enhancing technologies (PETs), such as federated learning and homomorphic encryption, including research agendas for how they could be applied to inclusive finance and in emerging markets.[vi] [3] While the momentum shows progress, for PbD to meet its promise, there is still much to do on the frontiers of inclusive finance.

Recognizing the need for heightened focus on privacy in inclusive finance, CFI set out to understand how PbD could be applied to the sector. To kick off this work, in 2022, CFI published a literature review of approaches to operationalize PbD, most of which stemmed from outside the inclusive finance sector. From this review, CFI found four approaches that consistently emerged: basic compliance, tech-enabled privacy features, user-centered design, and context-dependent approaches (see Table 1).[vii]

While the momentum shows progress, for PbD to meet its promise, there is still much to do on the frontiers of inclusive finance.

3 For more reading on PETs, we suggest Blumenstock and Kohli's Big Data Privacy in Emerging Market Fintech and Financial Services: A Research Agenda, the Royal Society's report on privacy-enhancing technology, or Privacy Enhancing Technologies: What are they and why do they matter? by the Federal Reserve Bank of San Francisco.

TABLE 1: CFI's Categories of Privacy by Design Approaches

Approach	Characteristics and Typical Uses
Basic Compliance	↗ Heavily grounded in regulatory compliance ↗ Uses standardized processes to evaluate privacy risk ↗ Most common among private sector
Tech-Enabled Privacy Features	↗ Deploys an array of technical tools to enable and constrain information flows ↗ Often relies on privacy-enhancing technologies (PETs) for implementation of product changes
User-Centered Design	↗ Organic response to deceptive design from practitioners in ethical design and other human rights-centered design fields
Context-Dependent	↗ Inductive approach that centers the user and context in driving PbD ↗ Largely academic

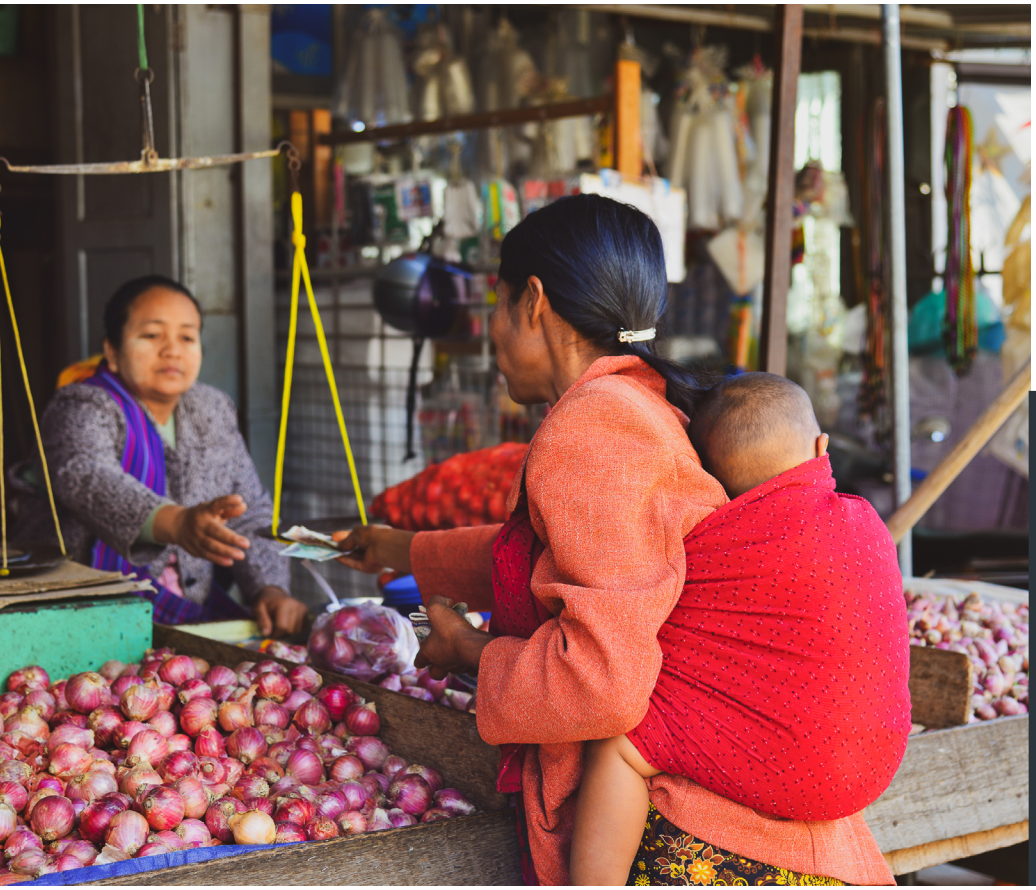
The literature review revealed a dearth of PbD resources available for product teams to support engineers, data scientists, and designers in creating a shared language and approach for embedding privacy.[viii] Further, there is also a lack of tools available to help resource-constrained companies, like fintech startups, working in emerging and developing economies and serving vulnerable consumers who are relatively new to digital products.

Subsequently, CFI worked in close collaboration with privacy and security expert Dr. Maritza Johnson to develop a Privacy by Design playbook tailored specifically for fintech product teams working in emerging and developing economies. This playbook is a first-of-its-kind knowledge product for the inclusive finance sector. The Privacy as Product Playbook recognizes and elevates the integral role that product managers play in shaping the digital financial landscape, and is a concrete tool for building a stronger privacy culture within fintech and digital finance companies. The aim of the playbook is to position privacy as a fundamental value proposition, not just a compliance requirement, for both consumers and businesses.

THE CASE FOR PRIVACY BY DESIGN

Despite overall progress in financial inclusion, lack of trust remains a key barrier — with privacy harms increasingly a cause of mistrust. As noted by a CGAP analysis, for the 1.4 billion people currently outside the formal financial system, lack of trust showed up in the Findex data as a major reason why unbanked adults did not use formal financial services, with almost one in four responding that they did not trust the financial system.[ix] And even for those who already have access, roughly 9 percent of adults in developing economies have accounts but do not use them — with lack of trust being a major driver of these dormant accounts.[x] Privacy- and data-related harms are increasingly a major contributor to mistrust and disengagement from digital financial services, stymieing industry efforts to reach the last mile of consumers.[xi]

Privacy by Design offers providers an opportunity to proactively foster trust, leading to improved reputation and increased customer engagement and retention. For example, in 2021, Apple launched a new privacy feature called App Tracking Transparency. App Tracking Transparency allows users to see more privacy prompts as they navigate their regular apps, and lets users adjust their data sharing preferences more easily through the iOS Tracking menu.[xii] One year after its launch, analysis suggests that the privacy feature was well received by consumers and helped to grow Apple's share of search ad business to better compete with Facebook and Google.[xiii]



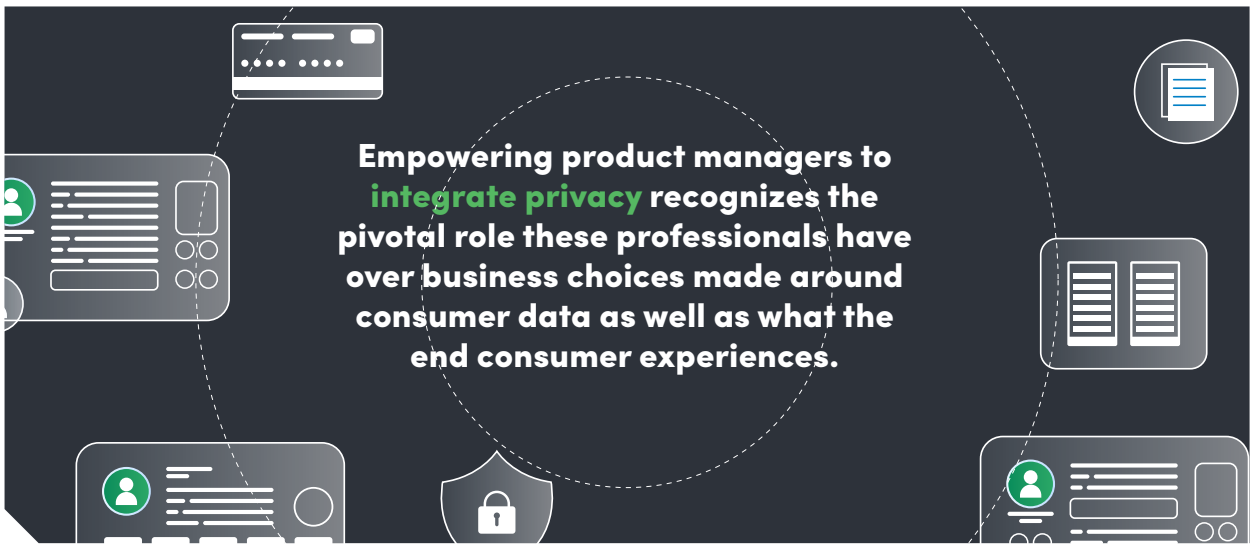
For the 1.4 billion people currently outside the formal financial system, lack of trust showed up in the Findex data as a major reason why unbanked adults did not use formal financial services.

PRODUCT MANAGERS ARE KEY STAKEHOLDERS IN PRIVACY BY DESIGN IMPLEMENTATION

In designing the playbook, CFI made a deliberate choice to specifically target product managers at fintechs and digital finance companies. Product managers are primarily responsible for the end-to-end design, development, launch, and maintenance of a digital financial product.[xiv] Empowering product managers to integrate privacy recognizes the pivotal role these professionals have over business choices made around consumer data as well as what the end consumer experiences.

Because product managers have the responsibility to create value for both the customer and the business, they must balance the development of a product that meets users' needs along with one that has a viable path to commercialization.[xv] They also often oversee the work of technologists — data architects, engineers, UX/UI teams, data scientists, and others — who design and implement the front end and back end of any digital financial product and coordinate with other functions within a company such as legal, marketing, security, and public policy.

It is worth noting that while the playbook's target audience is product managers, this should not discount or diminish the mission-critical work of privacy professionals in compliance and legal. Rather, the goal of the playbook is to facilitate a partnership between the functions by developing a more nuanced understanding of how to consider privacy concerns and risks as a product team.



Implementation Challenges & Playbook Solutions

While constructing and gathering feedback on the playbook, CFI identified three challenges in applying Privacy by Design approaches to the inclusive finance sector. These include:

1. Product teams often do not view privacy as part of their purview or do not have the time to address privacy and, as such, do not make the space to focus on it.
2. There is a dearth of compelling positive examples of PbD's use within the inclusive finance field, which is slowing the pace of adoption.
3. It is difficult to get cross-departmental and C-suite buy-in, which are crucial for PbD to succeed.

While the playbook provides solutions that aim to meet these challenges, more work and research are needed.

CHALLENGE 1: Product teams often do not view privacy as part of their purview or do not have the time to address privacy and, as such, do not make the space to focus on it

Digital product teams are focused on meeting high-stakes launches and deadlines, and typically are not incentivized to prioritize privacy or do not view it as part of their job. Product teams at startups — fintechs included — are infamous for their relentless pace. They work quickly to bring their offerings to market, stay competitive, and capture customer attention. Within the fintech space, startups aim to disrupt traditional financial services and offer innovative and new solutions. Often, product managers are "locked into" launch deadlines that are scheduled months in advance. Therefore, if a team does not understand the relevance of privacy to their end users, they will not be incentivized to prioritize designing for privacy concerns amid a host of other competing goals.

Further, product teams often see privacy as a cost and an impediment to innovation, rather than an enhancement.[xvi] There may even be competing incentives — for example, when the commercial incentives to maximize data collection outweigh the privacy principle of data minimization. There is also a privacy "codability" trap that treats only the codable aspects of privacy as feasible, with non-codable dimensions — like user expectations, diverse privacy concerns, and third-party data use — seeming to be too abstract.

In building the playbook, CFI developed an approach that allows product teams to break away from their previous beliefs about how privacy should be practiced and embrace a new way of thinking. The playbook aims to help shift product teams' views about privacy from it being costly, compliance-driven, and too abstract, to instead be thought of as a generative problem in need of a creative solution.

Playbook Solution 1: Problem-Solving Space for PbD: Product Development Lifecycle

The playbook is oriented around the product development lifecycle, which is a product design framework that outlines the stages a product team goes through from first having an idea to market launch and beyond: Ideation, Validation, Design and Deploy, Maintenance, and Retire. CFI's PbD playbook is organized in line with the product development lifecycle for two reasons:

1. PbD calls for privacy to be considered from the very outset of any conversation around a product that uses personal data. By using the product development lifecycle as a prompt for privacy discussions, privacy becomes part of the ideation stage — the very first step. By following the playbook, a product team can create a responsible data strategy that supports the broader product goals. Deliberating and documenting the data strategy early in the product lifecycle positions the team to handle the work as needed throughout the later stages.

2. The product development lifecycle is an existing "problem space" that helps establish a shared vision for the product team and allows for creative and collaborative problem-solving as well as risk management. The playbook offers privacy guidelines and prompts for every stage of the product development lifecycle so that product managers can easily introduce privacy considerations into their existing workflows.

Playbook Solution 2: Pragmatic Approach With Opportunities for Deep Dives

The playbook is designed for time-strapped product managers and their teams. Product managers, engineers, UX/UI teams, and data architects already know how to execute the technical responsibilities of their jobs. Rather than try to redefine their role, the playbook provides an additional lens through which team members can view their existing tasks and decisions. This approach posits that users do not need to become experts in PbD to meaningfully uphold privacy as a fundamental company value.

The playbook is also designed for different levels of engagement, with copious resources referenced and listed for readers who want to do deeper dives into different subject areas. Additionally, the playbook has a section called "Common Traps to Avoid" that present common challenges that product teams may face when working on embedded privacy; examples include the "Codability Trap," the "Nihilism Trap," and the "Efficiency Trap." Each example suggests signs that signal the trap and recommends tactics for overcoming them.

CHALLENGE 2: There is a dearth of compelling positive examples of PbD's use within the inclusive finance field, which is slowing the pace of adoption

While the concept of Privacy by Design has been around since 2009, there are very few examples of good practices in inclusive fintech. This may be due to several factors. For one, despite first being introduced over a decade ago, PbD does not have a single, standardized definition beyond the Seven Foundational Principles (see Box 1). This lack of standardization can hinder the development of best practices. Additionally, given that regulation on PbD is relatively amorphous, organizations may worry that highlighting their best practices could potentially reveal any noncompliance issues or vulnerabilities in their practices. Certain privacy-enhancing technologies or techniques may also be considered proprietary and inappropriate to share publicly.

The scarcity of inclusive finance examples showing PbD has slowed the curve of adoption. Without tangible case studies or success stories,

BOX 1: CAVOUKIAN´S SEVEN FOUNDATIONAL PRINCIPLES OF PRIVACY BY DESIGN

1. Proactive not reactive: preventive not remedial
2. Privacy as the default
3. Privacy embedded into design
4. Full functionality - positive-sum, not zero-sum
5. End-to-end security - full lifecycle protection
6. Visibility and transparency - keep it open
7. Respect for user privacy - keep it user-centric

providers have struggled to envision the feasibility of integrating PbD or to make the case for its practical benefits.

Playbook Solution: Leveraging Good Examples From Outside Inclusive Fintech

Ideally, there are examples from successful fintechs to make a case that applying PbD leads to better outcomes for consumers and companies. However, because there is a lack of exemplars in inclusive finance, CFI leverages notable instances in other industries where PbD has been applied, while also noting mishaps where advice was not followed. For example, Mozilla's web browser Firefox and Smashing Magazine show how companies can prioritize user rights in a business (see Box 2). While these examples might not align perfectly with the intended context, the examples offer inspiration that the work can be done and provide valuable insights about how to do it. The goal is for readers to learn from examples and cultivate an understanding of PbD that could be applied to their own product team at their fintech.

CHALLENGE 3: It is difficult to get cross-departmental and C-suite buy-in, which are crucial for PbD to succeed

While the playbook is aimed at product managers, PbD practices necessitate close collaboration with other functions within a fintech, including marketing and legal. Marketing teams and product teams must coordinate to ensure that any promises made in marketing materials are aligned with the product's actual privacy practices. In addition, for PbD to be a true differentiator to customers, the user-centric privacy practices must be communicated proactively to them through marketing to help inform their choices. Additionally, the legal or compliance function is responsible for navigating emerging data protection regulation, as well as drafting privacy policies and terms of service. Unfortunately, product teams often engage with the legal team only to ask for approval of a near-finished product, rather than engaging them at earlier stages of ideation and design.[xvii] The playbook encourages these conversations to happen sooner in the product development lifecycle.

BOX 2: MOZILLA FIREFOX'S PRIVACY PHILOSOPHY

1. **No surprises:** This means we´re up-front and obvious about how and when we´re collecting and using sensitive information.
2. **User control:** This means we develop products and advocate for best practices that put users in control of their data and online experiences.
3. **Limited data:** We only collect what we need; we de-identify data whenever possible; we delete data when it´s no longer necessary.
4. **Sensible settings:** This design principle helps us strike a thoughtful balance between safety and user experience. We build our products so that it´s easy for people to be in control of their settings rather than making it hard and confusing.
5. **Defense in depth:** This means we build in security. We´ve put multiple layers of security controls in place, within the products we produce and our day-to-day business practices.

Excerpts from Firefox Privacy Philosophy. Accessed September 2023.

Finally, organizational structure can impede privacy considerations. Examples abound from large tech companies where chief privacy officers' strong user-centric perspectives on privacy do not trickle down to product teams.[xviii] Often, leadership might also have a predisposition to see privacy as a cost source rather than a revenue generator.

Playbook Solution: Empower Product Managers in Cross-Departmental Interactions

The playbook is a resource not only for product managers to successfully implement PbD into their work, but it also offers practical guidance, tips, and language to effectively advocate for PbD within other departments. It equips readers with ideas and examples to bridge gaps between product teams and departments like marketing, legal and compliance, and leadership. In short, the playbook aims to empower product managers to reframe the value of privacy as a business asset rather than a compliance burden or cost center.

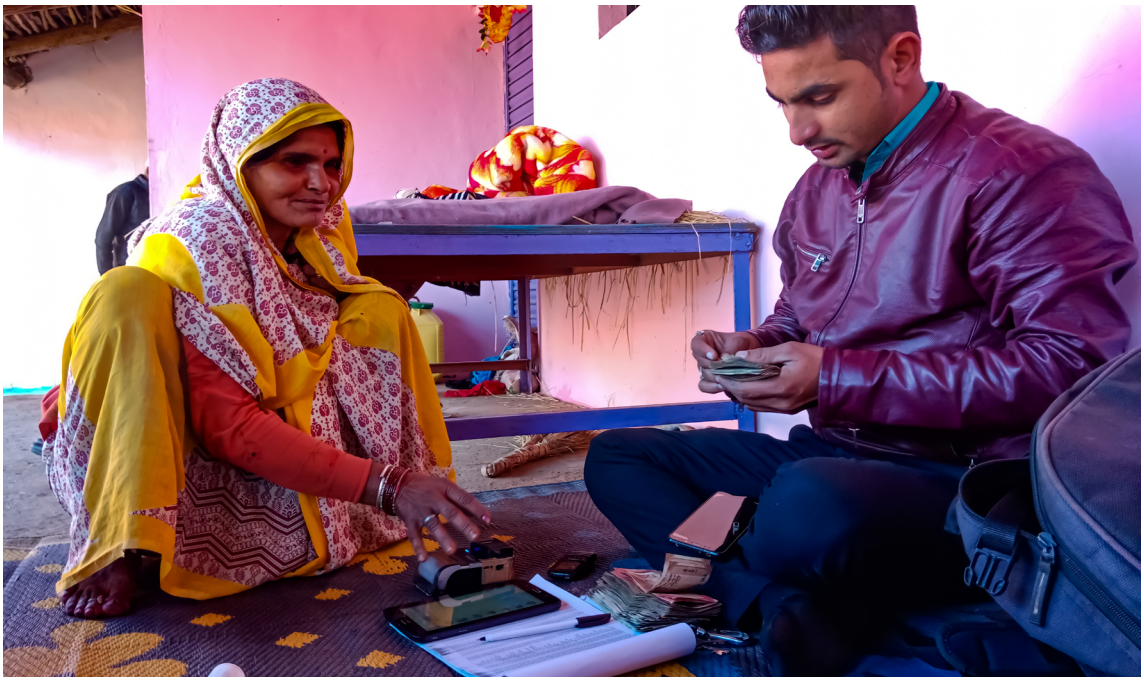
Further Considerations and Frontiers of PbD for Inclusive Finance

While the playbook is a helpful tool, it is one of many steps that the inclusive finance sector must take to truly embed privacy by design. In addition, inclusive finance players should also should consider the following:

↗ Understand PbD's Potential in an Increasingly Complex Data Ecosystem

The data ecosystem that supports inclusive finance grows more complex by the day. In sectors like agriculture, health, or ecommerce, embedded finance business models rely on a closer integration between fintech companies and non-finance firms to add financial services through APIs. For example, many fintechs are partnering with platforms, such as Uber or Flipkart, to offer digital financial services for gig workers and consumers. Additionally, buy now, pay later (BNPL) providers are often embedded into online retailers' experience at the point of payment.

At a policy level, initiatives in the financial sector — such as open banking, open finance, and digital public infrastructure — have established transformative infrastructure and allowed for new sources of data to be used and shared. Open banking and finance regimes also give consumers the ability to authorize the transfer of their data from one financial service provider to another, or even to a third-party provider. To practice PbD in this complex ecosystem, fintechs must have a solid privacy foundation to engage with a multitude of partners, customer bases, and data value chains. There is much more research to do in this area to illuminate good practices, particularly in offerings that involve multiple entities, multiple data sources, and multiple product teams.



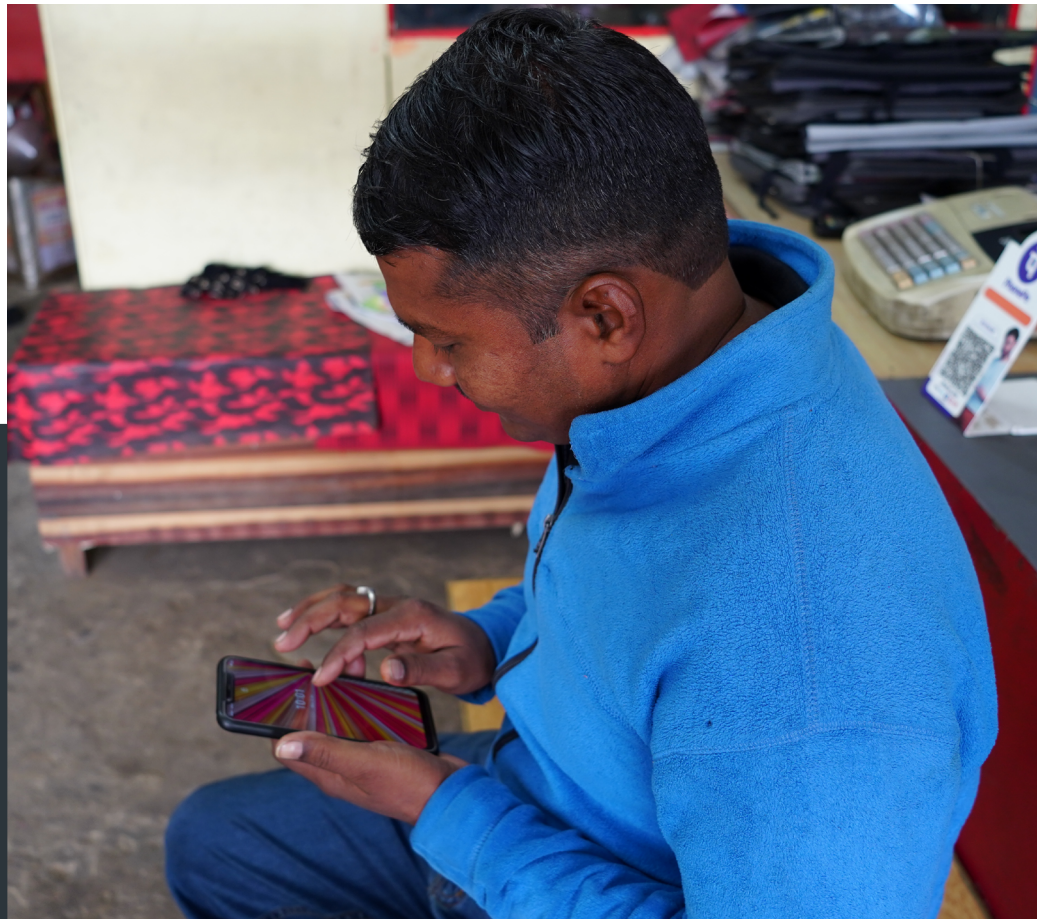
↗ Enhance PbD Through Stronger Understanding of Consumers' Privacy Paradigms and Expectations

Deidre Mulligan, one of the privacy field's preeminent thinkers, noted that it is essential that product teams consider the possibility that privacy may be thought of differently by different parties.[xix] In other words, users and designers approach privacy very differently, and we must take this into account when developing products. There is scant research on consumer privacy expectations and attitudes in emerging markets and developing economies. While CFI's playbook asks for UX/UI teams to conduct user engagement analysis, it is not expected that a single fintech provider should bear the financial burden of large-scale qualitative surveys.

Thus, as CFI has long argued, there is a pressing need for consumer research that draws from fields including psychology, economics, computer science, and law. This research is essential to gain a deeper comprehension of how consumers interact within the data ecosystem — and how to design privacy policies and practices that align with user expectations. It is also crucial for assessing the various policy interventions that can aid consumers in making informed decisions about privacy, and ultimately, creating a more trusted digital financial ecosystem.[xx]

Consumer trust plays a pivotal role in enabling digital finance to drive financial inclusion, particularly as the next billion users come online from underserved and excluded populations.[xxi] By embedding privacy into digital financial products, fintechs that practice Privacy by Design can build trustworthy products that inspire usage and loyalty from consumers.

By embedding privacy into digital financial products, fintechs that practice Privacy by Design can build trustworthy products that inspire usage and loyalty from consumers.



References

i Rizzi, A. (2022). Embedding Trust: The Potential of Privacy by Design for Inclusive Finance. Center for Financial Inclusion. https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/2022/12/Potential-of-Privacy-by-Design-in-Inclusive-Finance-3.pdf; Best Media Info. (2022, August 29). 99% of Consumers Say Privacy is Important When Browsing Online: Integral Ad Science Report. https://bestmediainfo.com/2022/08/99-of-consumers-say-privacy-is-important-when-browsing-online-integral-ad-science-report; Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/; Carlini, N., Tramèr, F., Wallace, E., Jagielski, M., Herbert-Voss, A., Lee, K., Roberts, A., Brown, T., Song, D., Erlingsson, U., Oprea, A., & Raffel, C. (2021). Extracting Training Data from Large Language Models. Proceedings of the 30th USENIX Security Symposium. https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting; O'Connell, B. (2023, April 7). This Tech Giant Accidentally Just Leaked Sensitive Info to ChatGPT. The Street. https://www.thestreet.com/technology/this-tech-giant-accidentally-just-leaked-sensitive-info-to-chatgpt

ii Spencer, S., Nakhai, M., & Weinstock, J. (2018). The Role of Trust in Increasing Women's Access to Finance Through Digital Technologies. USAID and NetHope.

iii Catalan Data Protection Authority. (2023, February). Privacy by design and privacy by default: A guide for developers. https://apdcat.gencat.cat/web/.content/03-documentacio/documents/guiaDesenvolupadors/GUIA-PDDD_EN.pdf

iv California Privacy Protection Agency. (2023, January). California Consumer Privacy Act Regulations. State of California. https://cppa.ca.gov/regulations/pdf/20230329_final_regs_text.pdf

v International Organization for Standardization. (2023, January). Consumer Protection: Privacy by design for consumer goods and services. https://www.iso.org/standard/84977.html

vi Blumenstock, J., & Kohli, N. (2023, August). Big Data Privacy in Emerging Market Fintech and Financial Services: A Research Agenda. Center for Effective Global Action. https://escholarship.org/uc/item/9nw1w6nd

vii Rizzi (2022)

viii Waldman, A. (2021). Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power. Cambridge University Press.

ix Duflos, E., & Izaguirre, J. (2022, October 19). Reading Findex With a Consumer Protection Lens. CGAP. https://www.cgap.org/blog/reading-findex-with-consumer-protection-lens

x Duflos & Izaguirre (2022)

xi Medine, D. (2020, May 5). Financial Scams Rise as Coronavirus Hits Developing Countries. Inter Press Service. http://www.ipsnews.net/2020/05/financial-scams-rise-coronavirus-hits-developing-countries/; Bird, M. (2020, November 25). Complaints

Data as a Tool for Consumer Protection: Lessons from Uganda. Innovations for Poverty Action. https://poverty-action.org/sites/default/files/presentation/IPA%20Uganda%20Complaints%20Data%20Analysis%20Webinar%20-%20Bird%20-%2020201125.pdf

xii Ha, A. (2021, April 26). Apple's App Tracking Transparency feature has arrived — here's what you need to know. TechCrunch. https://techcrunch.com/2021/04/26/apples-app-tracking-transparency-feature-has-arrived-heres-what-you-need-to-know/

xiii Perez, S. (2022, September 6). One year later, Apple's privacy changes helped boost its own ads business, report finds. TechCrunch. https://techcrunch.com/2022/09/06/one-year-later-apples-privacy-changes-helped-boost-its-own-ads-business-report-finds/?guccounter=1

xiv Clark, H. Product Management: Roles and Responsibilities Through the Career Timeline. The Product Manager. https://theproductmanager.com/topics/product-management-roles-and-responsibilities/

xv Mansour, S. Product Manager: The role and best practices for beginners. Atlassian.

xvi Waldman (2021)

xvii Waldman (2021)

xviii Waldman (2021)

xix Mulligan, D., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. 2016. Philosophical Transactions of the Royal Society A, 374(2083). https://royalsocietypublishing.org/doi/10.1098/rsta.2016.0118

xx Chakraborty, A. (2022). Privacy Perceptions, Attitudes, and Behaviors: Perspectives from Indonesian Smartphone Users. Center for Financial Inclusion. https://www.centerforfinancialinclusion.org/privacy-perceptions-attitudes-and-behaviors-perspectives-from-indonesian-smartphone-users

xxi Better Than Cash Alliance. (2021). UN Principles for Responsible Digital Payments. https://responsiblepayments.org/

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

CENTER *for* FINANCIAL INCLUSION | ACCION