December 2022

Author

Alexandra Rizzi

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

CENTER for FINANCIAL INCLUSION | ACCION

## ACKNOWLEDGEMENTS

The author is grateful to Henry Bruce and Tanwi Kumari for their support with this project, and to Edoardo Totolo for his supervision. Special thanks to Caitlin Sanford and Nishanth Kumar for their contributions to the research, and to Mayada El-Zogbhi, Aeriel Emig, Dr. Maritza Johnson, Joanna Ledgerwood, and Loretta Michaels for their editorial guidance. The author is also grateful to the fintechs and privacy experts who graciously took the time to participate in key informant interviews.

# Introduction

Consumer privacy risks have proliferated in the last decade in parallel with the increased adoption of digital technologies and availability of consumer data. High-level incidents at Meta and Equifax,[i] for example, have raised global awareness about the magnitude and diverse nature of the risks involved. Privacy harms are increasingly affecting low-income consumers of digital finance — whether by digital credit lenders in East Africa sharing borrowers' contact lists with collections agencies, or by an ed-tech's manipulative user interface that misused parents' biometric information to lock them into loans. [ii]

In Kenya, for example, digital credit providers scraped users' contact lists from smartphones and reached out to these contacts when borrowers were late in repaying their loans. International media reported the story of borrowers like John, a 42-year-old taxi driver in Nairobi, who received a message that read: "Silence means you don't want to pay your loan which is already due…Take it seriously. Your 50 contacts and emergency contacts will start receiving 20 calls and 15 messages exactly at 6pm. Pay now to avoid embarrassment."[iii]

The great onboarding onto digital finance necessitated by COVID-19 also opened up vulnerable consumers to data misuse through scams in markets like the Philippines, Kenya, and India, among many others.[iv] The impact of these violations can cascade from the financial and economic to the social and emotional.[v] Particularly for those with less financial stability, the interruptions privacy harms can cause can be devastating. [vi]

Privacy violations can also have serious long-term consequences for financial inclusion. The Global Findex 2021 showed that although access to finance had increased, more than 400 million people globally have an open account but have not used it for over a year. [vii] And even as access has improved, trust remains a critical ingredient in translating that progress into sustainable gains for consumers. Evidence shows that when consumers fall prey to privacy-related harms, the loss of trust dissuades them from the opportunities afforded by digital finance.[viii] Privacy implications not only affect consumers, but also impact businesses. Because of this, data privacy and data security are increasingly being considered important ESG (Environmental, Social, Governance) topics by leading regulatory and rating agencies. Businesses are evaluated based on a range of privacy-related metrics, including the amount of personal data they collect and the likelihood of data breaches. [ix]

While compliance with new data protection regulations has brought stronger safeguards, the rapid speed at which consumer data is collected, used, and shared in digital finance has far outpaced consumers' understanding. For low-income digital financial consumers, the limits of informed consent and choice are even starker.[x] In this context, Privacy by Design (PbD) has emerged in the last decade as an approach to embed privacy ex ante into the design of digital products and services.

Originally developed as a framework in 2009 by Dr. Ann Cavoukian, a Canadian privacy commissioner, PbD is a system design philosophy to improve how privacy is embedded into IT systems.[xi] By centering privacy within product and system design, privacy is reframed as a business model differentiator and core value proposition to consumers rather than a matter of regulatory compliance.

This report is intended to be an introduction to Privacy by Design for the inclusive finance sector. The objective is to review the main PbD approaches in literature and wider market practice for their potential applications in the inclusive finance sector. The analysis is based on a literature review and key informant interviews with privacy and inclusive finance experts conducted by the Center for Financial Inclusion (CFI) between May and August 2022.

The paper groups findings into four approaches to PbD, each of which attempts to embed privacy through different means, often by combining various tools, methods, and areas of application. The paper also identifies a series of gaps and barriers that limit the potential of PbD, particularly in emerging markets and developing economies. The report closes with considerations for the adaption of PbD for fintechs working with low-income and vulnerable consumers. CFI aims to build off this initial report to develop practical guidance on PbD for fintech product teams.

**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

# Privacy Concerns in Digital Finance

Evidence shows that while low-income financial consumers care about and value privacy, the rapid deployment and scaling of digital finance has not adequately given them the time or space to negotiate their privacy boundaries or understand their digital rights.[xii] Consumers' digital choices can trigger, unknowingly to the user, intensive data collection, high-stakes algorithmic decisions, or tracking pixels, to name just a few, that work with more stealth and complexity than most can trace. [xiii]

In addition to consumers' digital activities such as mobile money transactions or SMS messages, fintech companies scrape phones for geo-location, battery charging patterns, contact lists, and phone characteristics (e.g., make and model), among other data points.[xiv] Data sharing underpins most fintech offerings, whether facilitated through bilateral agreements, like those between mobile network operators and digital lenders, or more decentralized models, like open banking and account aggregators. Beyond the value of new consumer data for companies' products, companies are monetizing the data itself through sales, data-driven mergers and acquisitions, and booming data brokers.[xv] In addition, companies' proprietary algorithms and artificial intelligence (AI) models have crunched traditional and alternative consumer data to inform product offerings, credit scores, fraud management, and other innovations.[xvi] In a field characterized by increased competition, fintechs can build a competitive edge by having a "data advantage."

The amount of data that digital finance providers collect and use for their services often comes as a surprise to users. CFI research in Rwanda showed that many users of digital financial services are not aware of the data-intensive nature of the products they used daily, such as airtime or other inputs gathered from their phone being used to assess creditworthiness.[xvii] Many consumers are aghast to discover privacy invasions that they may have unwittingly consented to. A 29-year-old male CFI study respondent commented, "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." [xviii]

A lack of awareness among consumers is understandable given that most corporate privacy notices are not written with the end user in mind, particularly those with literacy or other access constraints, and are often long, dense, and littered with legalese and IT jargon.[xix] Additionally, most digital products offer consent

### HIGHER ONLINE RISKS FOR WOMEN

According to the Economist Intelligence Unit, women in countries with long-standing or institutionalized gender inequality tend to experience online violence at higher rates.

For example, a digital lender in India inappropriately used headshots from female IDs used for KYC and falsely morphed them onto nude photos. These fake photos were sent to the borrowers' contacts alongside messaging that they were delayed in repayments.

**Source:** TechCrunch, August 2022

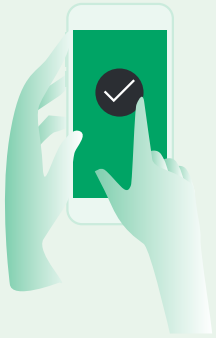
as "take it or leave it," with a rejection of consent typically presented as "leave it."[xx] Beyond privacy notices, there are also mismatches in what corporate privacy and security policies say, and what data providers actually collect. In one analysis of 30 digital finance apps, 72 percent of the apps requested access to users' contacts but did not mention this in their privacy policies. In addition, the apps were accessing users' phone microphones (9.4 percent), device and app history (15.6 percent), and cameras (56.3 percent), but none of this was disclosed in their privacy policies.[xxi]

Even if users did fully comprehend the privacy implications of using digital finance, behavioral scientists have challenged the notion that consumers always behave rationally in privacy-related decisions. Scholars like Alessandro Acquisti have posited that their choices might also be driven by social norms or lack of choice.[xxii]

Finally, onboarding to digital finance can mirror or even inflame offline privacy risks — particularly for vulnerable groups like women and minorities. Social norms and existing discrimination against women can lead them to face higher risks online around surveillance, targeted violence, identity theft, misuse of personal images and data, and sharing of inappropriate content.[xxiii] These groups may have even higher risk aversion and thus require a higher degree of trust before adopting and fully committing to digital finance.[xxiv] Adopting Privacy by Design principles into the design and development of inclusive financial products offers an opportunity to make digital finance more trustworthy, transparent, and user-friendly.

In 30 digital finance apps

**72%**



requested access to users' contacts **but did not mention this in their privacy policies.**

# Implementing Privacy by Design

What might Privacy by Design look like in inclusive finance? In the years since Dr. Cavoukian introduced her framework, PbD has gained traction with many stakeholders, in particular with data protection policymakers through GDPR's Article 25 mandate.[xxv] Yet while the Seven Foundational Principles have been catalytic for raising awareness, they are often seen as too high-level for organizations to operationalize.[xxvi]

Beyond Dr. Cavoukian's initial conceptualization, academics and practitioners have developed new PbD methodologies that draw from human-centered design, engineering, and compliance, among other disciplines. CFI reviewed these methodologies, along with relevant examples where available, to understand both their existing strengths and limits. This review provides an initial foundation from which to draw approaches for inclusive finance.

CFI has grouped the different types of existing methodologies into discrete categories for ease of understanding and presentation. However, in practice, they are not mutually exclusive, and the boundaries can be blurry, especially when applied to large and complex organizations. While each methodology has some applicability for inclusive finance, it is clear there is a need for more holistic approaches and clearer operational guidelines that indicate how the work can be distributed across cross-functional partners inside and beyond an organization's boundaries.

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

| Approach | Characteristics and Typical Uses |
|---|---|
| **Basic Compliance** | ↗ Heavily grounded in regulatory compliance<br>↗ Uses standardized processes to evaluate privacy risk<br>↗ Most common among private sector |
| **Tech-Enabled Privacy Features** | ↗ Deploys an array of technical tools to enable and constrain information flows<br>↗ Often relies on privacy-enhancing technologies (PETs) for implementation of product and system 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<br>↗ Largely academic |

## CATEGORIES OF PRIVACY BY DESIGN METHODOLOGIES

### Basic Compliance

Focusing on basic compliance is arguably the most mature and the most common approach in the private sector.[xxvii] It relies heavily on instruments such as privacy impact assessments and data protection impact assessments (see Box 2) and stems from a time when data privacy was seen primarily as the responsibility of legal or compliance functions.

This approach tends to be reactive rather than proactive, and can at times be disconnected from the implementation of digital products.[xxviii] While these tools are intended to be launched at the ideation stage, in practice they are often conducted by a privacy professional or external vendor only after the product or system has been fully designed.[xxix] They take privacy risks, concerns, and harms to be well defined in advance and the results rarely inspire new ways to frame privacy problems or generate solutions that would address issues. [xxx]

### Tech-Enabled Privacy Features

This approach has attracted increasing interest among both academics and practitioners, particularly in the field of engineering, becoming one of the fastest-growing approaches in PbD. It relies heavily on technical solutions such as coding, mathematical models, and encryption techniques to embed protections into a system, process, or product. These solutions can allow or halt information flows or provide users more control over what companies can collect.

The tech-enabled perspective often requires the use of privacy-enhancing technologies (PETs).[xxxi] PETs use advanced cryptographic protocols and mathematical models to enable and constrain information flows. Some PETs alter data such as pseudonymization or differential privacy, while others shield data using encryption or create new systems for data computation or storage.[xxxii] Table 2 below provides examples of PETs and applications in finance.

**BOX 2: Definition of PIA vs. DPIA**

- **Privacy impact assessment (PIA)** is a process used to identify and mitigate privacy risk associated with a product, service, business process, or other organizational change. They are mandatory for many U.S. government agencies.
- **Data protection impact assessment (DPIA)** is a specific type of PIA required by the GDPR for data processing activities that may pose a high risk to the rights and freedoms of individuals.

**Source:** TrustArc

**TABLE 2: Examples of Privacy-Enhancing Technologies (PETs)**

| Privacy-Enhancing Technology Type | Definition | Finance Example |
|---|---|---|
| **Zero Knowledge Proofs** | Uses encryption to allow one party to prove the truth of a specific claim to another party (verifier) without disclosing or sharing the underlying information. | Allow for customer verification without sharing sensitive information or merchant authentication of a credit card without the card number or card verification value.[xxxiii] |
| **Federated Learning** | Decentralized approach to machine learning where, for instance, multiple mobile phones contribute to creating a new model while keeping the training data on the individuals' phones and sending only the results to a centralized cloud server.[xxxiv] | Development of machine learning models for fraud detection or credit scoring.[xxxv] |
| **Differential Privacy** | Adds additional, random data, or "noise," to a released dataset The objective is to add enough random, additive data so that real information is hidden amidst the noise, essentially creating some level of plausible deniability in terms of what's true about individuals in the dataset. | Allow financial institutions to aggregate and analyze sensitive user data about clients without revealing individual-level data.[xxxvi] |

The tech-enabled approach is a growing field but focuses on product back-end (i.e., data architecture and management of data flows) and leaves out the product's interface with the user. Additionally, the privacy enhancements made by PETs can be reversed or compromised by bad actors and require proper safeguards and oversight.[xxxvii]

## User-Centered Design Approach

The user-centered design approach aims to counter deceptive design — i.e., use interface design and cognitive biases to nudge and even manipulate people into making privacy (and other) decisions that may not be in their best interest.[xxxviii] While some deceptive designs are employed without malicious intent and some may be described merely as nuisances, there are clear examples where deceptive designs do yield an advantage to service providers. In response, design practitioners — UX/UI designers, visual designers, and interaction designers — have taken steps to counter deceptive design and empower users.

Compared to the tech-enabled approach, the contributions of "trusted design patterns" have been less formal, with ideas stemming organically from groups of professional designers organized around ethical design, designing for accessibility, or human rights centered design, to name a few.[xxxix] For example, the co-founders of the Human Rights Centered Design community created a Digital Security

and Privacy Protection UX Checklist on GitHub, an online site for developers to code as a "public good" and work on projects together.[xl] A particular focus of the design community has been to reimagine consent and find a balance between providing overly broad consent versus fatigue from "microconsent" every time consumer data is used.[xli] For instance, the Consentful Tech project creates examples using the FRIES method (freely given, reversible, informed, enthusiastic and specific) while other legal designers are pioneering visual contracts.[xlii]

**BOX 3: Examples of Deceptive Design**

A type of deceptive design, known as "privacy zuckering," uses unnecessarily complex privacy settings to force users to accept a privacy-invasive option. A Norwegian Consumer Advocacy Council found privacy zuckering at Facebook and Google through methods such as "hiding away privacy-friendly choices, take-it-or-leave-it choices, and choice architectures where choosing the privacy-friendly option requires more effort for the users."

Another common tactic is called "address book leeching." Here, providers use the guise of finding friends on a platform but then misuse a user's entire address book to profile and track individuals who do not have provider accounts or to spam them with advertising material. With the arrival of millions of new users to digital financial services over the last two years, and with more to come, there is concern particularly for those with lower levels of education or literacy.

### "Context-Dependent" Approach

Some scholars have called for PbD to be driven by the unique context of the situation.[xliii] The underlying idea behind the context-dependent approach is that the nature and magnitude of privacy risks are not universal, but rather depend on the type of data that consumers share, the type of service they are using, and how the data is analyzed and applied. For example, the privacy risks related to one's health records are different from those related to mobile money call detail records. This is largely because of the different context surrounding the risks — specifically different users, business models, expected use cases, user behaviors and expectations, technologies, applicable laws, and potential harms.[xliv] This line of thinking warns against immediately jumping to tech-enabled solutions and instead advocates for a more inductive approach.

Applying a context-dependent approach would focus on prospective users and their "context-dependent privacy expectations," as well as any "naïveté … uninformed and ill-conceived notions of how technology works … mental models based in prior brick-and-mortar interactions, and their cognitive biases."[xlv] The user and their context form the basis around which interface design patterns, default settings, privacy notices, system architecture, and privacy engineering solutions can be created.[xlvi] To date, there are not many applications of context-dependent approaches in industry settings. While the customer-centric intention of this approach aligns well with the values of inclusive finance, some of the inductive methodologies would be too abstract or too labor-intensive for private businesses.

## ANTICIPATED PRIVACY BY DESIGN CHALLENGES

Privacy by Design offers a wide range of potential strategies to mitigate the challenges that low-income consumers face in digital finance — whether through trusted UX design patterns, tailored consent notices that draw attention to critical aspects of a privacy disclosure, or engineering strategies like data minimization. However, there are also barriers that must be considered in applying PbD, especially in emerging markets.

### Fragmentation of Design Process and Teams

Digital product teams include many different roles — from UX designer to data scientist, from back-end engineer to data architect. These roles work closely together throughout the ideation,

discovery, delivery, and maintenance lifecycle, often overseen by a product manager. Each of these roles makes independent choices that have privacy implications, often without an overall cross-functional plan for handling privacy. As a result, approaches to privacy often are not coherent or unified. Today, PbD approaches tend to be developed around the perspective of only one role in the product team. Current PbD approaches overlook the growing importance and centrality of product managers in digital and software product development, who oversee and are accountable for the design and execution processes.[xlvii]

Digital product teams are oriented around the timely design and deployment of a minimum viable product (MVP). Against a backdrop of production deadlines, privacy is not usually prioritized. Research with technology companies in the United States suggests that even if the chief privacy officer (CPO) has a forward-looking, user-centered vision for privacy, this does not often translate to the product-level teams. Privacy officers may be separated from product teams and see their job as "telling design teams what they're doing is compliant with the law" rather than challenging the design process or being integrated into it.[xlviii] Conversely, product teams may see privacy issues as too abstract, not immediate, not "codable," or not part of their purview.[xlix] Team objectives may even be at odds with privacy goals, such as optimizing user engagement versus data minimization.[l]

## Modularized Digital Services and Agile Production

Cloud computing functions — such as storage, security, etc. — are available at ever-lowering costs for firms. This increases the availability of "everything as a service," where third-party vendors offer modularized services (identity verification, payments, risk profiling, etc.), primed for integration at low, pay-as-you-go prices.[li] As a result, a user sees an app that is offered by a single provider like a fintech but is really a "matryoshka doll concealing dozens of services."[lii] Because of this, privacy risks are often spread across different teams and companies, making accountability and management difficult. Additionally, agile and lean development methodologies have resulted in teams consistently making minor changes to existing products and making major changes every few months, potentially introducing new privacy issues.[liii]

## Limited Application to Emerging Markets and Developing Economies

Privacy by Design scholarship and applied methods have largely been created in developed markets. Because of these origins, the following are implied in PbD approaches to date: a) business environment with (on average) available resources for investing in privacy practices; b) a baseline of data protection legislation, market conduct, and enforcement actions such as the GDPR and Data Protection Commissions; and c) populations with relatively high levels of education and literacy. Inclusive fintech companies working in developing countries usually do not have the luxury of resources or infrastructure for large investments in privacy. Many fintechs operate with low margins and, as such, see privacy as a compliance consideration and not a design differentiator. Additionally, they are operating in markets with weakly enforced or non-existent data protection regulations and are serving consumers with lower educational and literacy levels.

**Inclusive fintech companies working in developing countries usually do not have the luxury of resources or infrastructure for large investments in privacy.**

# Moving Forward: Considerations for Translating Privacy by Design for Inclusive Finance

CFI is leading a portfolio of work on Privacy by Design that will develop practical recommendations for private sector firms like fintechs working with low-income and vulnerable consumers. The recommendations will demonstrate how to incorporate relevant elements from the four PbD approaches described in this report, guided by direct feedback from fintech product managers.

The objective is to: a) reframe privacy work as a generative process where each product team member has a role to play; and b) empower them to integrate relevant practices within their product life cycle and according to their customers' needs and organizational constraints. Of course, any Privacy by Design work should take into account the relevant levels of regulatory obligation in the market(s) of operation.

Moving forward, CFI is prioritizing the following considerations in the context of inclusive finance and fintechs that target un- and underserved customers who may be just beginning their use of digital finance:

### ① PbD should be positioned as business-enhancing.

Because privacy has historically been seen as a compliance-related cost, to encourage private companies and fintechs to employ PbD techniques, PbD needs to be presented as a business-enhancing design benefit. Both external stakeholders like investors as well as internal champions need to encourage companies to consider privacy from the outset when designing products and services.

### ② PbD needs to be adapted to work for resource-constrained companies and emerging markets.

Because PbD has been developed and largely implemented in developed countries, little work has been done to date to make PbD approachable and operational outside of those contexts. The next step will be to translate PbD approaches so they are able to be implemented at resource-constrained companies and in emerging markets.

### ③ PbD should incorporate low-income and vulnerable consumers' offline privacy needs in addition to privacy for their digital data.

In considering the user and their privacy capacities and needs, PbD can bring customer-centricity into the data-intensive aspects of digital financial products. In practice, providers should elicit offline needs, particularly for women and vulnerable groups, and examine whether their digital product inflames or exacerbates existing privacy risks.

### ④ PbD must balance consumer privacy preferences with companies' needs.

When implementing PbD, it will be important to consider both the information that companies must collect to be able to perform their work, as well as the privacy preferences of consumers. A balance must be found to ensure that a product will function without compromising consumer privacy.

### ⑤ PbD must articulate privacy responsibilities across disaggregated value chain and partnerships.

Consumer data can sit and be shared across multiple organizations in today's modularized fintech ecosystem, and not all actors in the value chain have equal power and influence. PbD must consider which actors are accountable for different aspects of consumer privacy as well as their limits.

By positioning privacy as a core value proposition to consumers, fintechs that employ Privacy by Design techniques have the **potential to build trusted products.**

By positioning privacy as a core value proposition to consumers, fintechs that employ Privacy by Design techniques have the potential to build trusted products that resonate with and retain customers. As the "big bang of digitalization" marches onward, with today's underserved or excluded becoming the next billion users, preventing and addressing privacy harms has never been more important.

# References


i Ng, Alfred and Steven Musil. "Equifax data breach may affect nearly half the US population." CNET, Sep. 2017. https://www.cnet.com/news/privacy/equifax-data-leak-hits-nearly-half-of-the-us-population/

ii Njanja, Annie. "Kenya cracks down on digital lenders over data privacy issues." TechCrunch, Oct. 2021. https://techcrunch.com/2021/10/25/kenya-cracks-down-on-digital-lenders-over-data-privacy-issues/; Chugh, Beni and Pranjal Jain. "Unpacking Dark Patterns: Understanding Dark Patterns and Their Implications for Consumer Protection in the Digital Economy." Dvara Research, 2021. https://rsrr.in/wp-content/uploads/2021/04/UNPACKING-DARK-PATTERNS-UNDERSTANDING-DARK.pdf

iii Bhalla, Nita and Dominic Kirui. "'Silicon Savannah' Kenya targets loan apps abusing customer data." Thomson Reuters Foundation, Jan. 2022. https://www.reuters.com/article/kenya-tech-credit/feature-silicon-savannah-kenya-targets-loan-apps-abusing-customer-data-idUSL4N2SM2J6

iv Medine, David. "Financial Scams Rise as Coronavirus Hits Developing Countries." CGAP, Apr. 2020. https://www.cgap.org/blog/financial-scams-rise-coronavirus-hits-developing-countries; Demirgüc-Kunt, Asli, Leora Klapper, Dorothe Singer, and Saniya Ansar. "The Global Findex Database: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19." World Bank, 2022. https://www.worldbank.org/en/publication/globalfindex

v Bansal, Varsha. "Shame, suicide, and the dodgy loan apps plaguing Google's Play Store." Wired, Jan. 2021. https://www.wired.co.uk/article/google-loan-apps-india-deaths

vi Madden, Mary. "The Devastating Consequences of Being Poor in the Digital Age." NY Times, Apr. 25, 2019. https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html

vii Ruiz, Lucciana Alvarez and Edoardo Totolo. "Global Findex 2021: Growth, Stagnation, and (Relative) Decline in Global Financial Inclusion." CFI, Jul. 2022. https://www.centerforfinancialinclusion.org/global-findex-2021-growth-stagnation-and-relative-decline-in-global-financial-inclusion

viii McKee, Kate and Michelle Kaffenberger. "Doing Digital Finance Right." CGAP, Jun. 2015. https://www.cgap.org/research/publication/doing-digital-finance-right; Farbrace, Emily, Loes van der Velde, Medha Sethia, and Alexandra Rizzi. "Client Voices: Rwandans Speak on Digital Financial Services." Laterite, Ltd., Jun. 2019. https://www.rfilc.org/wp-content/uploads/2020/08/CFI54_SMART_rwanda_FINAL-lores.pdf; Garz, Seth, Xavier Giné, Dean Karlan, Rafe Mazer, Caitlin Sanford, and Jonathan Zinman. "Consumer Protection for Financial Inclusion in Low and Middle Income Countries: Bridging Regulator and Academic Perspectives." NBER Working Paper No. 28262, Dec. 2020. https://www.poverty-action.org/sites/default/files/publications/w28262.pdf

ix Alam, Roobi and Carlos Perez Calico. "Connect privacy with ESG to drive broader business success." EY Canada, Feb. 2022. https://www.ey.com/en_ca/sustainability/connect-privacy-with-esg-to-drive-broader-business-success

x Consumers International, "Building Fair Digital Finance: A Vision for Fair Digital Finance," Mar. 2022. https://www.

consumersinternational.org/media/419259/final_vision-for-fair-digital-finance.pdf

xi Cavoukian, Ann. "Privacy by Design: The 7 Foundational Principles." Information and Privacy Commissioner of Ontario, Jan. 2011. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

xii Chakraborty, Anindita. "Privacy Perceptions, Attitudes, and Behaviors: Perspectives from Indonesian Smartphone Users." CFI, May 2022. https://www.centerforfinancialinclusion.org/privacy-perceptions-attitudes-and-behaviors-perspectives-from-indonesian-smartphone-users; Rizzi, Alexandra and Tanwi Kumari. "Trust of Data Usage, Sources, and Decisioning: Perspectives from Rwandan Mobile Money Users." CFI, Oct. 2021. https://www.centerforfinancialinclusion.org/trust-of-data-usage-sources-and-decisioning-perspectives-from-rwandan-mobile-money-users

xiii Spiekermann, Sarah and Lorrie Faith Cranor. "Engineering Privacy." IEEE Transactions on Software Engineering, Vol. 35. No 1., Jan./Feb. 2009. https://ieeexplore.ieee.org/document/4657365

xiv Kemp, Simon. "Digital 2020: 3.8 Billion People Use Social Media." We Are Social, Jan. 2020. https://wearesocial.com/uk/blog/2020/01/digital-2020-3-8-billion-people-use-social-media/; Rizzi, Alexandra, Alexandra Kessler, and Jacobo Menajovsky. "The Stories Algorithms Tell: Bias and Financial Inclusion at the Data Margins." CFI, Mar. 2021. https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/2021/03/The-Stories-Algorithms-Tell-CFI-publication-MAR21.pdf

xv World Bank, "World Development Report 2021: Data for Better Lives," 2021. https://www.worldbank.org/en/publication/wdr2021

xvi Rizzi et al., "The Stories Algorithms Tell."

xvii Rizzi and Kumari, "Trust of Data Usage."

xviii Ibid.

xix Litman-Navarro, Kevin. "We Read 150 Privacy Policies. They Were an Incomprehensible Disaster." NY Times, Jun. 12, 2019. https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html; Auxier, Brooke et al. "Americans' attitudes and experiences with privacy policies and laws." Pew Research Center, Nov. 2019. https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/

xx Flanagan, Anne Josephine, Jen King, and Sheila Warren. "Redesigning Data Privacy: Reimagining Notice & Consent for Human-Technology Interaction." World Economic Forum, Jul. 2020. https://www3.weforum.org/docs/WEF_Redesigning_Data_Privacy_Report_2020.pdf

xxi Traynor, Patrick. "Digital Finance and Data Security." CFI, Sep. 2018. https://www.centerforfinancialinclusion.org/digitalfinance-and-data-security-2

xxii Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. "Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving it in the Digital Age." Journal of Consumer Psychology, Vol. 30, No. 4, 2020. https://www.heinz.cmu.edu/~acquisti/papers/Acquisti_Secrets_Likes_Drive_Privacy_Difficulty_Achieving_Digital_Age_WP.pdf

xxiii Venkatesan, Jayshree and Alexandra Rizzi. "If You See Something, Say Something." CFI, Mar. 2022. https://www.centerforfinancialinclusion.org/if-you-see-something-say-something; Singh, Jagmeet. "Predatory Loan apps in India rake in huge fees, and are driving some users to suicide." TechCrunch, Aug. 2022. https://techcrunch.com/2022/08/26/loan-apps-abuse-harassment-suicide-indian-users-google-apple-india/

xxiv "Nakhai, Mandana, Shelley Spencer, and Jordan Weinstock. "The Role of Trust in Increasing Women's Access to Finance Through Digital Technologies." USAID. May 2018. https://www.usaid.gov/sites/default/files/documents/15396/The_Role_of_Trust.pdf

xxv Gürses, Seda, Carmela Troncoso, and Claudia Diaz. "Engineering Privacy by Design." Computers, Privacy & Data Protection, Vol. 14, No. 3, 2011. https://www.esat.kuleuven.be/cosic/publications/article-1542.pdf

xxvi Raghavan, Malavika and Anubhutie Singh. "Building safe consumer data infrastructure in India: Account Aggregators in the financial sector." Dvara Research, Jan. 2020. https://www.dvara.com/research/blog/2020/01/07/building-safe-consumer-data-infrastructure-in-india-account-aggregators-in-the-financial-sector-part-2/

xxvii Cronk, R. Jason. "Check or Mate: Strategic Privacy by Design." IAPP, Oct. 2017. https://iapp.org/resources/article/check-or-mate-strategic-privacy-by-design/

xxviii Ibid.

xxix Ibid.

xxx Wong, Richmond Y., Dierdre K. Mulligan, Ellen Van Wyk, James Pierce, and John Chuang. "Eliciting Values Reflections by Engaging Privacy Futures Using Design Workbooks." PACM on Human-Computer Interaction, Vol. 1, Nov. 2017. https://dl.acm.org/doi/pdf/10.1145/3134746

xxxi Rubinstein, Ira and Nathan Good. "The Trouble with Article 25 (and How to Fix It): The Future of Data Protection by Design and Default." International Data Privacy Law, Vol. 10., No. 1, Feb. 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3773333; Gürses, Seda, Carmela Troncoso, and Claudia Diaz. "Engineering Privacy by Design Reloaded." Amsterdam Privacy Conference, 2015. http://carmelatroncoso.com/papers/Gurses-APC15.pdf

xxxii Asrow, Kaitlin and Spiro Samonas. "Privacy Enhancing Technologies: Categories, Use Cases, and Considerations." Federal Reserve Bank of San Francisco, Jun. 2021. https://www.frbsf.org/banking/wp-content/uploads/sites/5/Privacy-Enhancing-Technologies_FINAL_V2_TOC-Update.pdf

xxxiii Better Than Cash Alliance, "UN Principles for Responsible Digital Payments: Building trust, mitigating risks & driving inclusive economies," Oct. 2021. https://responsiblepayments.org/pdfs/UN-ResponsiblePayments.pdf

xxxiv Rubinstein and Good, "The Trouble with Article 25."

xxxv Better Than Cash Alliance, "UN Principles for Responsible Digital Payments."

xxxvi Deloitte, "Data sharing in financial services: Five techniques to enhance privacy and confidentiality," 2019. https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/Deloitte_WEF_FS_Executive_summary_Data_sharing_2019.pdf

xxxvii Asrow and Samonas, "Privacy Enhancing Technologies."; Renieris, Elizabeth. "Why PETs (privacy-enhancing technologies) may not always be our friends." Ada Lovelace Institute, Apr. 2021. https://www.adalovelaceinstitute.org/blog/privacy-enhancing-technologies-not-always-our-friends/

xxxviii Chugh and Jain, "Unpacking Dark Patterns."; Bösch, Christoph, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. "Tales From the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns." Proceedings on Privacy Enhancing Technologies, 2016. https://petsymposium.org/2016/files/papers/Tales_from_the_Dark_Side__Privacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf; Deceptive Design, "Hall of Shame," accessed Nov. 2022. https://www.deceptive.design/hall-of-shame/all

xxxix Human Rights Centered Design, accessed Nov. 2022. https://hrcd.pubpub.org/; Raider, Jeremy and Andrea Rabinelli. "A New Tool for Testing Your Design Concepts Ethically." IDEO, Sep. 2019. https://www.ideo.com/blog/a-new-framework-for-testing-your-design-concepts-ethically; Accessibility Lab, "Big Blue Button," March 2021. https://ux.allylab.com/table/bbb

xl GitHub, "Digital Security and Privacy Protection UX Checklist," May 2018. https://github.com/SCheee/DSPPUX-Checklist/; privacypatterns.org, "Patterns," accessed Nov. 2022. https://privacypatterns.org/patterns/; Decentralization Off the Shelf, "Design

patterns for enhanced security," accessed Nov. 2022. https://miro.com/app/board/uXjVOHetu_E=/; Anti-Defamation League Center for Technology & Society, "Social Pattern Library," accessed Nov. 2022. https://socialpatterns.adl.org/

xli Flanagan et al., "Redesigning Data Privacy."

xlii Ibid.; Airtable, "Reimagining Consent Gallery, MozFest 2022," accessed Nov. 2022. https://airtable.com/shrZSumhBM6DSyILb/tblkHBbRqiAaV22gs; Visual Contracts, "Community," accessed Nov. 2022. https://visualcontracts.eu/community/

xliii Nissenbaum, Helen. "Privacy as Contextual Integrity." Washington Law Review, Vol. 79, No. 1, Feb. 2004. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/

xliv Doty, Nicholas, Ann Drobnis, Dierdre Mulligan, and Richmond Wong. "Privacy by Design: State of Research, Workshop 1 Report." Computing Community Consortium, 2015. https://cra.org/ccc/wp-content/uploads/sites/2/2015/02/PbD-Workshop-1-Report-.pdf; Wong, Richard and Deirdre Mulligan. "Bringing Design to the Privacy Table: Broadening 'Design' in 'Privacy by Design' Through the Lens of HCI." CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, May 2019. https://dl.acm.org/doi/fullHtml/10.1145/3290605.3300492

xlv King, Jen. "Privacy by Design and the Uber Settlement." Center for Internet and Society, Oct. 2018. https://cyberlaw.stanford.edu/blog/2018/10/privacy-design-and-uber-settlement

xlvi Mulligan, Deirdre K. and Jennifer King. "Bridging the Gap between Privacy and Design." Journal of Constitutional Law, Vol. 14, No. 4, Mar. 2012. https://scholarship.law.upenn.edu/jcl/vol14/iss4/4/

xlvii Gnanasambandam, Chandra, Martin Harrysson, Shivam Srivastava, and Yun Wu. "Product managers for the digital world." McKinsey, May 2017. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/product-managers-for-the-digital-world

xlviii Waldman, Ari. Industry Unbound. Cambridge University Press, 2021, page 206.

xlix Spiekermann and Cranor, "Engineering Privacy."; Waldman, Industry Unbound, page 167.

l Waldman, Ari Ezra. "Designing without Privacy." New York Law School, 2018. https://digitalcommons.nyls.edu/fac_articles_chapters/1331/

li Gürses, Seda and Joris van Hoboken. "Privacy After the Agile Turn." The Cambridge Handbook of Consumer Privacy, Cambridge University Press, 2017. https://osf.io/preprints/socarxiv/9gy73/

lii Ibid.

liii Ibid.

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