

# Trusted Design Global Case Study: India

Titiksha Vashist

---

<b>Focus Area Rationale</b>	<b>2</b>
<b>Landscape Assessment</b>	<b>2</b>
Issue Areas	2
1. Fake loan apps shark borrowers through deceptive data practices	2
2. Crypto apps mislead users by non-disclosure of risks	3
3. Did Google Pay violate the interoperability of public infrastructure?	3
4. The Competition Commission of India fines Google for pre-installation on Android phones, and calls it an abuse of dominance	3
5. Amazon's search algorithms rig search results to favour its product lines	3
6. WhatsApp forces privacy policy updates on Indian users	4
7. Language, economic status, and digital literacy hinder access	4
Perceptions	4
Relevant Infrastructure & Relevant Initiatives	4
Relevant regional regulatory frameworks, policies, or guidelines and standards	4
Stakeholders	6
Stakeholders and resources relevant to the region	6
Government bodies	6
Civil society/ volunteer groups	6
Traders associations	6
Industry associations	6
Others (government schemes and programmes to build awareness and empowerment)	6
<b>Recommendations</b>	<b>7</b>
Opportunities	7
Policy Guidance	7
Key Stakeholders	8
Next Steps	8
<b>References</b>	<b>8</b>

## Trusted Design Global Case Study: India

About the author: Titiksha Vashist

Titiksha Vashist is Co-founder and Lead Researcher at The Pranava Institute. Her work focuses on emerging tech regulation and the socio-political implications of technology in India. She drives research projects at Pranava, focussing on technology, ethics, design, and policy. She holds a Masters's in Political Science and International Affairs from Jawaharlal Nehru University. She has worked with organisations like Konrad Adenauer Stiftung and Tactical Tech, as well as universities like the National Law University, Delhi, on various projects. She served as Visiting Faculty at the Daksha Fellowship, India's first law and technology fellowship program. She's a 2022 awardee of the University of Notre Dame-IBM's Tech Ethics Lab, wherein she works on technology ethics in design. She can be reached at [titiksha@pranavainstitute.com](mailto:titiksha@pranavainstitute.com).

*The following is a region-specific discussion of Trusted and Deceptive Design, including exploring relevant issues and recommendations. The perspectives and conclusions presented represent those of the author.*

### Focus Area Rationale

India is one of the fastest-growing digital markets in the world. With [44% per cent of its population online](#) and increasing internet penetration, global tech giants see Indian users as the *next billion* who will shape the internet. However, issues of the [digital divide](#) exist across lines of divisions of rural-urban contexts, gender, literacy, and income levels. India's approach to building digital public infrastructure has also led to increased digital adoption and enabled development goals such as social services and financial inclusion. This has resulted in a fast uptake of digitisation of public and private services in sectors such as finance, education, and health, as well as rapidly changing the interfaces between digital natives, the state, and the digital economy.

However, India's digital sector remains highly unregulated. India is yet to formulate a data protection law and other legislation to protect the interests of its citizens online. With one of the [largest startup ecosystems in the world](#), India will need to address the challenges of deceptive design practices prevalent across sectors. Policy and regulation around deceptive practices will enable India to push innovation and entrepreneurship and create a safe cyberspace for all. This study analyses the issues around deceptive design relevant in the Indian context. The landscape assessment begins with analysing issue areas in deceptive design in India which have found space in public media or have attracted regulatory attention. It goes on to explain how some of these concerns are discursively being raised in the Indian technology policy landscape and are finding space through rules, policies and industry practices. Apart from a review of secondary literature on policy and digital rights, the assessment included informal interviews with academics in the field of Human-Computer Interaction and User Researchers working with both public and private entities. This study rests heavily on the various policies and draft reports currently existing in the Indian technology policy landscape and constitutes its 'regulation', albeit in various stages of development. It also draws from work done by researchers in digital rights, accessibility, financial security and public interest technology.

### Landscape Assessment

#### Issue Areas

*Relevant issues related to Deceptive Design affecting the region, and common perceptions*

##### 1. Fake loan apps shark borrowers through deceptive data practices.

India's technology policy landscape is fairly new and rapidly evolving. India's attempts at creating a data protection law have been ongoing since 2018, and [efforts are underway to change](#) its competition laws to accommodate digital markets. While the term *deceptive design* is relatively new to the policy and regulatory discourse, several issues linked to deceptive design have been affecting India. The foremost among these have been concerns with illegal [loan sharking apps which trap borrowers](#), including vulnerable groups as well as startups. [Suicides](#) in several

states have been attributed to harassment by loan operators who threaten customers with social harm, naming and shaming, as well as sharing sensitive data which is collected by stealth. Such loan apps attracted the attention of India's financial regulator, the Reserve Bank of India (RBI), which has tried to curb the issue by raising awareness and increasing protection measures.

The harms described here are the result of Deceptive Design practices such as excessive data collection (e.g., collecting sensitive personal data, contacts on the device, etc.), as well as lack of full disclosure of terms of a loan. [Users are nudged to sign up for instant loans](#) through ad pop-up advertisements for loans equalling a few thousand rupees, mainly intended to target lower-income groups. Once a person downloads the app, it asks for the user's permission to access contacts and photo galleries on their smartphones before extending the loan. Once the loan amount is transferred to the user's account, barely a week passes before the recipient begins receiving calls requesting repayment. The catch is that the repayment amount demanded is typically 70–80% higher than the principal amount borrowed. These apps prey on customers in tier-2 and tier-3 towns (with populations between 50,000 and 99,999 and 20,000 and 49,999, respectively), where digital literacy levels are low. According to sources, more than 1000 such apps exist in India, and the Reserve Bank of India banned 300 instant loan apps to protect consumers.

## 2. Crypto apps mislead users by non-disclosure of risks.

A similar challenge arose with cryptocurrency apps, for which experts stated that crypto platforms were creating [hype and misrepresenting information](#) about the security and returns associated with investments in cryptocurrency. Critics stated that some of these ads could lure Indians into investing in an asset class notorious for wild price swings and without any knowledge of the risks involved. As a regulatory measure, the Advertising Standards Council of India (ASCI) [issued guidelines](#) for crypto ads, stating clearly that "Crypto products and NFTs are unregulated and can be highly risky. There may be no regulatory recourse for any loss from such transactions." Use of financial language associated with secure investment products, as well as advertising using [influences](#) who do not disclose risks, has emerged as issues which mislead users.

## 3. Did Google Pay violate the interoperability of public infrastructure?

India's fintech economy has seen a massive boom in the last few years. India is expected to clock the fastest growth in the digital payments sector between 2019 and 2023, with a compounded annual growth of 20.2 per cent. India's [Unified Payments Interface \(UPI\)](#) is a real-time payments system that allows users to transfer funds between bank accounts through a mobile application instantly. With 200 banks live on a single platform and multiple private service providers, it has fostered a diverse and innovative fintech ecosystem. The UPI can be seen as a case of a GovTech innovation that puts the user at the centre, designs for safety in transactions, and allows multiple private players to build on top of a public, regulated platform. The UPI is a part of the larger *India Stack*, a family of APIs, open standards, and infrastructure components. The central tenet of the *public* nature of the UPI is *interoperability* which has been ensured by the platform's design. In 2020, a [plea was filed in the Delhi High Court against Google](#) stating that its GPay app was flouting rules of interoperability on the UPI by barring users from making transactions if they did not have a GooglePay UPI ID. This opened up the issue of competition in digital markets, making India's anti-trust regulator, the Competition Commission of India, take notice of such flouting of rules.

## 4. The Competition Commission of India fines Google for pre-installation on Android phones and calls it an abuse of dominance.

Google's Android operating system powers 97 per cent of India's 600 million smartphones, according to [Counterpoint Research](#). On October 20, 2022, the Competition Commission of India (CCI) [fined Google \\$162 million for abuse of dominance](#) and anti-competitive practices on its android platform. India ordered Google not to restrict smartphone users from uninstalling its pre-installed apps like Google Maps and Gmail. The commission said it imposed the fine as Google allegedly abused its dominant position in five markets — the market for licensable OS for smart mobile devices; the app store for Android smart mobile OS; the market for general web search services; the market for non-OS specific mobile web browsers; and, the one for online video hosting platform (OVHP). [On October 25, 2022, the CCI fined Google another \\$113 million for denying access in-app billing/payments ecosystem.](#) The CCI instructed Google not to restrict app developers from using third-party billing or payment processing services. Such dominance is often operationalised by making design choices where pre-installed apps cannot be uninstalled, as well as preventing users from installing competitor apps through the

Google Play Store. Such defaults, which force manufacturers as well as users to stick to the Google suite, are anti-competitive, as well as deny user agency.

#### 5. Amazon's search algorithms rig search results to favour its product lines

An [investigation by Reuters in 2021](#) demonstrated that Amazon ran a systematic campaign in India, which included creating knockoff goods and manipulating search results to boost its product lines in the country. The documents reveal how Amazon's private brands team in India secretly exploited internal data from amazon.in to copy products sold by other companies and then offer them on its platform. The e-commerce giant's algorithm then pushed these products to the first three search results when customers search for products.

From a deceptive design standpoint, Amazon not only violated consumer trust by sharing shopping data to increase its own sales, but it also violated competition by showing search results which favour its brands. Practices such as search listing manipulation violate platform neutrality and fairness practices and put millions of small retailers on Amazon at a disadvantage by design.

#### 6. WhatsApp forces privacy policy updates on Indian users

In early 2021, WhatsApp changed its privacy policy for all Indian users, forcing them to accept sharing of business chats with WhatsApp's parent company Meta. This coercive update was designed to appear as a consent request—a simple 'I Agree' button to share all personal and contact information or opt-out of using WhatsApp altogether. Per [estimates](#), there are over 500 million WhatsApp users in India. The Competition Commission [found a prima facie case of abuse of dominance](#) against WhatsApp as WhatsApp was found to be a dominant player in the relevant market (messaging services), and the user would be forced to accept these terms. The Indian government intervened and called this move "discriminatory" towards Indians- since no such updates were made in the US or Europe.

#### 7. Language, economic status, and digital literacy hinder access.

Research conducted by HCI scholars in India has shown that ethical design means that an overwhelmingly English internet created for the English-speaking minority in India excludes and harms the population majority in the country. User researchers interviewed for this study shared that owing to the highly text-first design of apps, users often confused purposes (mistaking an investment app for a loan app, for example). This is also accompanied by the issue of low digital literacy in India, as well as the gendered nature of access to technology. HCI researchers I spoke to stated that vulnerable groups in India lie at the intersection of being linguistic minorities, with often low digital literacy and economic backwardness. These three intersections create issues of access as well as increase the potential for harm for such users. Research on HCI and designing for the vulnerable nudges towards adopting more culturally sensitive design practices.

A [study](#) by the Center for Internet and Society showed that website inaccessibility is the largest and most common barrier to implementing effective e-governance. In a country like India, where a very large percentage of the population is disabled, elderly, illiterate, rural, has limited bandwidth, speaks only a vernacular language, or uses alternative platforms like mobile phones, having accessible websites becomes all the more important to ensure that government information and services which are available online are accessible and usable by these groups. The study showed that nearly 75 per cent of surveyed government websites had accessibility errors on their home pages.

### Perceptions

Commonly found deceptive design practices such as forced data sharing, meaningless consent, and deceptive data practices, among others, lead to loss of consumer trust online in the long run. This has been a worry for regulators in the financial sector, who believe that such practices will harm India's journey from a predominantly cash economy towards a digitalised economy. India's regulators, such as the RBI, are motivated to safeguard consumer trust and build consumer confidence, making regulations stringent in India's burgeoning fintech sector. For deceptive design in e-commerce and social media, a broader understanding within the public which sees Indian platforms being dominated by large American technology companies, has emerged. A mix of

anti-competitive practices, nationalistic comments from political leaders, and a lack of laws governing cyberspace may also feed into users perceiving a loss of control over data, as well as the perception of the internet being dominated or colonised by big tech companies.

## Relevant Infrastructure & Relevant Initiatives

*Relevant regional regulatory frameworks, policies, or guidelines and standards*

India's current digital regulatory architecture focuses on issues of data protection and privacy, competition, and e-commerce regulation. These three pillars are aided by the government's heavy focus on launching public digital infrastructures for different sectors: fintech, e-commerce, health, and digital lending.

India passed a [National Policy on Universal Electronic Accessibility](#) in August 2009, which was aimed at eliminating discrimination based on disabilities as well as facilitating equal access to electronics and Information and Communication Technologies. It brought together several organisations from civil society, industry, and the public sector to draft a policy. The key players were the government through the Department of Information Technology (DIT), the National Informatics Center, and other organisations like the National Centre for Promotion of Employment for Disabled People (NCPEDP), Barrier Break Technologies, Center for Internet and Society, Microsoft Corporation, Maharaja Agrasen Institute Of Technology (MAIT), Enet, National Association of Software and Service Companies (NASSCOM) and several other organisations. The policy requires that all government websites comply with WCAG 2.0 and internationally accepted accessibility standards in all areas of electronic information, products, and service delivery. It also provides for research and development and awareness and training to promote universal electronic accessibility.

**The Insurance and Regulatory Development Authority of India (IRDAI)** has [prohibited](#) travel portals in India from using them for selling travel insurance. IRDAI has directed travel insurance companies to ensure that any portal or app providing travel insurance coverage shall not pre-select the option of buying the travel cover as a default option.

India's draft [Personal Data Protection Bill](#) (now withdrawn and replaced with a new bill) included privacy-by-design as a paradigm to make data protection meaningful and operational. According to the bill, the policy would contain the managerial, organisational, and business practices and technical systems designed to anticipate, identify, and avoid harm to the data principal.

While India has legal requirements in place to ensure **easy readability of privacy policies**, the final form rests with private companies which currently need to carry out such compliance.

India's recent **Parliamentary Committees on Finance, as well as Commerce**, have [raised issues](#) of **market dominance and gatekeeping norms**, which will be central to how social media and e-commerce companies operate. These norms will include clauses relating to **aggregating user data, data collection, purpose limitation, and compliance for companies with a large user base**. The recent hype around cryptocurrency and loan apps has also led to [new guidelines](#) around **influencer-based advertising**, as well as guidelines for unregulated financial products. Each of these initiatives will change company design practices once enforced. India's Competition Commission is setting up an independent [Digital Markets Unit](#) to check big tech companies for anti-competitive practices.

While India's Data Protection bill stands revoked, [recent efforts to create a Digital India Act](#) will likely include provisions focusing on making the web safer for children. The DSA and the DMA in Europe will influence the Act.



---

Legislation around non-personal data protection seeks to promote safe data-sharing mechanisms which promote fair use.

## Stakeholders

*Stakeholders and resources relevant to the region*

### Government bodies

- The Ministry of Electronics and Information Technology (<https://www.meity.gov.in/>)
- The Ministry of Commerce (<https://commerce.gov.in/>)
- The Reserve Bank of India (<https://www.rbi.org.in/>)
- The Competition Commission of India (<https://www.cci.gov.in/>)
- Department of Information Technology (state-wise/regional bodies)
- Ministry of Education (<https://www.education.gov.in/en>)
- NITI Aayog(<http://www.niti.gov.in/>)
- Insurance and Regulatory Development Authority of India (IRDAI) (<https://www.irdai.gov.in/>)
- Central Consumer Protection Authority (CCPA) (<https://consumeraffairs.nic.in/en/slider/ccpa>)

### Civil society, volunteer groups and relevant institutions

- Center for Internet and Society (<https://cis-india.org/>)
- Dvara Research (<https://www.dvara.com/research/>)
- BarrierBreak (<https://www.barrierbreak.com/>)
- iSPIRT (<https://ispirt.in/>)
- ICAR-Indian Agricultural Research Institute (<https://icar.org.in/>)
- MIT Institute of Design (<https://www.mitid.edu/>)
- National Institute of Design (<https://www.nid.edu/>)
- Microsoft Research Labs (<https://www.microsoft.com/en-us/research/lab/microsoft-research-india/>)
- The Pranava Institute (<https://pranavainstitute.com/>)
- Independent researchers in UI-UX and HCI
- Dalberg in India (<https://dalberg.com/>)

### Trade and industry

- NASSCOM (<https://nasscom.in/>)
- Confederation of All India Traders (<https://www.cait.in/>)
- National Restaurant Association of India (<https://nrai.org/>)
- Microsoft Research Lab (<https://www.microsoft.com/en-us/research/lab/microsoft-research-india/>)
- Meta (<https://about.meta.com/>)
- India Tech (<https://www.indiatech.org/>)
- U.S.-India Business Council (<https://www.uschamber.com/program/international-affairs/south-asia-program/us-india-business-council>)

### Others (government schemes and programmes to build awareness and empowerment across issues)

- Digital India Mission (<https://www.digitalindia.gov.in/>)
- Skill India Mission (<https://www.msde.gov.in/>)
- MyGov (<https://www.mygov.in/>)
- National Mission on Education using ICT (<https://digitalindia.gov.in/content/national-mission-education-using-ict#:~:text=The%20National%20Mission%20on%20Education,any%20time%20any%20where%20mode.>)
- OpenForge (<https://openforge.gov.in/>)

## Recommendations

### Opportunities

*Opportunities and recommendations related to regional policy, regulation, and enforcement*

- India's attempts at creating a data protection bill led to the creation of the 2019 draft Personal Data Protection Bill (PDPB), which included clauses relating to privacy-by-design as an important concept. According to the Bill, the policy would contain the managerial, organizational, and business practices and technical systems designed to anticipate, identify, and avoid harm to the data principal. However, these were not elucidated in detail (like in the EU). Following failure of the PDPB effort, as India prepares a new data protection bill, incorporating PbD has a serious approach for implementation, especially in an economy of its size, which will protect consumer data as well as reduce implementation challenges.
- As one of the fastest-growing markets, India has the opportunity to incorporate digital rights and safeguards early, as opposed to addressing them as post-facto challenges. New bills interrogating competition, dominance in digital markets, and gatekeeping norms can include recommendations on design and its impact on different sectors of the digital economy.
- However, a constructive move towards regulating deceptive design will require researching and understanding deceptive design and its impact in India. Deceptive design and its harms are not a monolith but change according to contexts. Understanding the nature and needs that arise from deceptive design in India will be necessary before regulation and strategising steps towards trusted design can be taken.
- India's novel approach to building public digital infrastructures like the [UPI](#) which decentralizes online payments, or the [ONDC](#) which de-segregates e-commerce are architectures which can pave the way for a public, accountable, decentralized web. Such opportunities also provide playgrounds for designing more responsibly, for all.

### Policy Guidance

*A suggested policy guideline contextualized to your region*

- Data Protection laws which include design guidelines in different sectors of the digital economy. (Such as [this](#)).
- Competition laws which address [the commonest dark patterns identified on e-commerce websites](#) and clarify the core principles of competition- tying up with practices which harm these.
- Stronger implementation of existing accessibility guidelines for online interfaces and creating bodies and institutions which implement these guidelines.
- Stronger focus on consumer protection laws which link online harms to pre-existing offline laws. Such an approach may help bridge the gap between currently unregulated harms and existing legal practices.

## Key Stakeholders

*Suggestions for key stakeholders and roles to involve in a Trusted Design coalition/task force.*

The Center for Internet and Society in Bangalore has been working on data protection from a design standpoint in their [project on analyzing India's PDP from a privacy-by-design](#) perspective. Their work around accessibility of the web also resulted in the [Making Voices heard](#) project, which focuses on creating inclusive voice interfaces in India.

The Pranava Institute's [Ethical Design Project](#) is working towards creating a hands-on manual for ethical design for practitioners. The project is also curating a blog series inviting scholars (focused on the global south) to concretely study the harms which result from deceptive design in various sectors, as well as on specific groups.

[Dvara Research](#)'s Beni Chugh and others working on financial inclusion have looked at dark patterns in the financial sector. Their report on dark patterns and their implications for consumer protection in the digital economy can be found [here](#).

Other organizations working on digital rights in India are the [Internet Freedom Foundation \(IFF\)](#) which is working on legal advocacy for safeguarding digital rights, the [Observer Research Foundation](#) which works on core policy aspects of technology in India, and engages diplomatically with regulatory bodies across the world (eg. it is crucially involved in shaping India's G20 agenda around technology).

The [DesignUp Conference](#) is an annual event where designers across Asia come together. Its 2022 edition included sessions on Privacy by Design by Rahul Matthan, Partner at legal firm Trilegal and author of the book Privacy 3.0. The conference brings together designers from across the region as well as working professionals in product teams, user research roles, technology and startup companies, and education, etc.

## Next Steps

*What are the next steps for key stakeholders? What are the opportunities for further investigation?*

- As regulators look at digital markets from a consumer protection and competition lens, learning from other jurisdictions which are creating new laws regulating harmful design practices (such as California) can be helpful.
- Researchers and universities will play a pivotal role in understanding the nature of harm created by deceptive design in various contexts in India. This is crucial since India is a highly diverse linguistic, social, cultural, and ethnic society. Multiple intersections will create harm unlike those we understand from research conducted in the global north countries.
- Civil society organizations can play a pivotal role in bridging the research and application end of the spectrum. Research in fields of HCI, human-centered design, user research, social sciences, etc. need to engage with communities of technologists and designers who ultimately practice design which impacts users.
- Including deceptive design in education curriculums in national design schools in India can go a long way to prevent the perpetuation of currently commonplace deceptive design practices. To this end, working with researchers, educators, government bodies, and designers can create holistic curricula.
- Engage stakeholders in creating new ethical practices in creating digital experiences for *the next billion* users who are vastly different from their counterparts in the global north. Since trust is vastly different for different people, the needs, realities, and challenges of different communities on the web are different and need to be co-developed. Creating new participatory processes based on ethics and trust is crucial to advance the conversation on trusted design in India.