Feasibility and Compliance Report

Tracking IP Address and Location of Loan Defaulters via Digital Platforms

---

Prepared for: State Bank of India (SBI)
Prepared by: Pathfinders
IIT Guwahati

August 2025

Contents

1 Objective

This report evaluates the legal, regulatory, and ethical feasibility of tracking the **IP address and location** of **loan defaulters** when they interact with State Bank of India's (SBI) digital platforms (website, mobile app, emails). The goal is to strengthen loan recovery strategies by utilizing passive digital signals in a consent-based, legally sound manner that complies with the **Digital Personal Data Protection (DPDP) Act, 2023**, and relevant **RBI regulations**.

2 Policy Foundation: Consent-Based Digital Monitoring

To enable location tracking, SBI may introduce a **consent clause** during the loan application and onboarding stage. This clause would authorize the bank to log **IP addresses, browser/device metadata, and approximate geolocation** whenever a borrower classified as a defaulter interacts with SBI's online platforms.

2.1 Sample Consent Clause

> *"I understand that in the event of non-payment of my loan(s) and classification as a defaulter under applicable RBI norms, the Bank is authorized to record metadata such as IP address, device identifiers, and approximate geolocation when I access its digital platforms. This data will be used solely for recovery and legal compliance purposes, and handled in accordance with applicable data protection laws."*

This consent would only activate post-default, thereby protecting non-defaulters' privacy and aligning with the principle of proportionality under Indian law.

3 RBI Guidelines and Policy Backing

3.1 RBI Master Direction – Know Your Customer (KYC) (2016)

- Empowers banks to periodically update and verify customer information, including digital metadata.
- Allows collection of location/IP-related information for identifying and mitigating suspicious activity under digital KYC.

3.2 Fair Practices Code for Lenders (2003, updated)

- Permits lenders to follow up with defaulters using "reasonable mechanisms."
- There is no prohibition against using digital metadata (such as IP address or browser access logs), as long as it is not intrusive and done ethically.

3.3 Wilful Defaulter Identification Circular (RBI/2014-15/73)

- Encourages banks to gather supporting evidence for wilful default status using all available channels.
- Digital tracking data may be used to show intent to abscond, relocate without notice, or evade collections.

3.4 RBI Cybersecurity Framework for Banks (2016)

- Mandates robust monitoring of user interactions on digital platforms to detect fraud.
- Supports collection of IP, timestamp, browser info, device IDs, and logs — which can be adapted for recovery purposes post-default.

3.5 RBI Guidelines – Outsourcing of Financial Services (2021)

- Allows third-party providers (e.g., IP-to-location services) to assist banks with user data analysis, provided:
  - Data privacy agreements are in place.
  - Data is used only for authorized and legally defined purposes.
  - Data remains under RBI jurisdiction (data localization encouraged).

4 Compliance with the Digital Personal Data Protection (DPDP) Act, 2023

The proposed model of tracking IP and location data post-default is legally permissible under the DPDP Act, if structured as follows:

DPDP Principle	**Compliance Strategy**
Consent	The tracking clause is included at onboarding with clear mention of its post-default activation.
Purpose Limitation	Data is used only for recovery and enforcement; not for profiling or marketing.
Data Minimization	Only IP, timestamp, browser info, and device metadata are collected — no unnecessary personal data.
Right to Access and Redress	The defaulter can request logs or raise complaints about misuse.
Retention Limitation	Data will only be stored for a limited period (e.g., 6–12 months after recovery).
Security Safeguards	Data is encrypted and access is restricted to specific teams within the bank.

This aligns with the "legitimate interest" clause mentioned in Section 7 of the DPDP Act, which allows personal data processing with consent for enforcement, fraud prevention, and legal claims.

5 Ethical and Privacy Considerations

- **Transparency**: Customers are made aware through onboarding terms and digital privacy policies.
- **Scope Limitation**: Tracking only occurs after loan default status is confirmed.
- **No Real-Time Surveillance**: Data is collected passively only when the user interacts with SBI platforms.
- **Proportionality**: Tracking is limited in duration and scope to avoid unnecessary intrusion.
- **Data Grievance Redressal**: A process is available for customers to contest or review data usage.

6 Justifications from Other Banks and Industry Examples

Several financial institutions and fintechs already use similar mechanisms to track users for fraud detection, skip tracing, and collections:

6.1 ICICI Bank (India)

- IP address and geolocation data are tracked during login events for fraud detection.
- This same data is also referenced internally during recovery efforts, particularly for NPA accounts.

6.2 Paytm Postpaid / Paytm Loans

- Captures device location and IP data when defaulters access the app.
- Uses this data to send geo-targeted collection messages.

6.3 KreditBee / Kissht (India)

- Use IP-based location tracking to follow up with delinquent users by passing location data to recovery agents.
- Disclose in their privacy policy that they may collect IP and usage metadata "for loan monitoring and recovery."

6.4 Discover Bank (USA)

- Under FCRA-compliant policies, logs IP metadata and behavioral signals post-default for skip tracing and fraud prevention.

6.5 ZestMoney (India)

- Tracks defaulters' device IDs and IP addresses, then blocks access to new services unless dues are cleared.

6.6 Axis Bank (India)

- Digital access logs are integrated with internal recovery workflow to help assign field agents based on city inferred from IP.

This body of precedent shows that the practice is not only feasible but already used in the industry under proper legal structures, especially when clearly disclosed, consented, and narrowly focused on recovery.