Chinese Loan App Legal Dossier

Converted evidence PDF for thenitishkr.in Intelligence archive ? Original source: chinese-loan-app-legal-dossier.docx ? Category: Cross-Border & Loan App Dossiers ? Archive date: 2026-04-06

Summary

Cross-border cyber, loan-app, and jurisdictional evidence record for intelligence review.

Extracted Record Text

CONFIDENTIAL LEGAL DOSSIER

PREPARED UNDER BHARATIYA SAKSHYA ADHINIYAM, 2023 | SECTION 63(4)(c) [erstwhile S.65B IEA]

■ This dossier is structured for use as a primary evidentiary document and affidavit annex before Indian courts. All electronic evidence cited herein requires a valid Section 63(4)(c) certificate (BSA, 2023) from a responsible official of the originating device or platform before it can be admitted. The dossier itself constitutes a compiled research record and is not a substitute for original electronic records.

TABLE OF CONTENTS

PART A — LEGAL FRAMEWORK & EVIDENCE STANDARDS

A.1 Governing Legislation

Bharatiya Sakshya Adhiniyam, 2023 (BSA) — replaces Indian Evidence Act, 1872 effective 1 July 2024

Information Technology Act, 2000 (IT Act) — Sections 43, 66, 66C, 66D, 69, 69A, 72, 72A

Indian Penal Code / Bharatiya Nyaya Sanhita, 2023 (BNS) — Sections 318, 319, 351, 308, 308(2), 308(4)

Prevention of Money Laundering Act, 2002 (PMLA) — Sections 3, 4

Reserve Bank of India Act, 1934 — Sections 45-I, 45-IA (NBFC regulation)

Digital Personal Data Protection Act, 2023 (DPDP) — Sections 4, 8, 16, 25, 33

Consumer Protection Act, 2019 — Sections 2(9), 47

A.2 Electronic Evidence — Section 63(4)(c) BSA [formerly S.65B(4) IEA]

The Bharatiya Sakshya Adhiniyam, 2023 re-enacts the electronic evidence certification requirement under Section 63(4)(c), replacing the erstwhile Section 65B(4) of the Indian Evidence Act, 1872. The requirement is mandatory and not directory.

Mandatory Content of Section 63(4)(c) Certificate:

Identity of the electronic record — describe file name, hash value (SHA-256), date/time of creation

Device particulars — make, model, IMEI/serial, OS version, app version

Manner of production — how the record was generated or captured

Declaration that the device was in proper working condition during the relevant period

Signatory — person in responsible official position (device custodian, forensic examiner, or IT officer)

Statement made to the best of knowledge and belief of the signatory

A.3 Landmark Supreme Court Rulings on Electronic Evidence

PART B — CORPORATE STRUCTURE OF CHINESE LOAN APP ECOSYSTEM

B.1 Entity Architecture

Chinese loan app operators deployed a multi-layer corporate architecture deliberately designed to obscure beneficial ownership and evade regulatory accountability:

Layer 1 — Chinese Parent: Actual beneficial owner and technology controller based in China (Hangzhou, Beijing, Guangzhou). Provides backend technology, SDK integrations, server infrastructure, and AI models.

Layer 2 — Intermediate Entity: Holding company incorporated in Hong Kong, Singapore, or BVI to create jurisdictional separation and enable inter-company fund transfers.

Layer 3 — Indian Shell Company: Registered as Indian NBFC, fintech, or private limited company. Indian nationals listed as nominal directors. RoC registration creates facade of legitimacy.

Layer 4 — App Frontend: Multiple branded loan app identities (CashMaster, RupeeFly, MoneyPlus etc.) sharing identical Chinese backend. Different frontend branding, same data pipeline.

Layer 5 — Recovery Arm: Indian call centres staffed with recovery agents. Operated on commission, receiving contact lists and harassment scripts from Chinese operators remotely.

B.2 Key Entities Identified in ED/CBI Investigations

PART C — TECHNICAL EVIDENCE: SDK SURVEILLANCE CHAIN

C.1 Overview — The Four-SDK Data Pipeline

Chinese loan apps did not write custom surveillance code. Instead, they embedded commercially available Chinese Software Development Kits (SDKs) that performed data exfiltration as a background service. The victim's granted permissions unlocked four concurrent data streams:

PART D — ADTECH LAYER: SILVERPUSH, INMOBI, APUS, BAIDU, ALIBABA

D.1 SilverPush — The Ultrasonic 'Listen' SDK

SilverPush, founded in India (2012), deployed Unique Audio Beacons (UABs) — ultrasonic tones at 18–20 kHz embedded in TV and web advertisements. Any app containing the SilverPush SDK continuously listened via the device microphone for these tones, enabling cross-device tracking and location inference.

Mechanism: App requests RECORD_AUDIO permission → SDK samples microphone at 44.1 kHz in 4,096-sample blocks → detects beacon frequency patterns → reports device IMEI, location, and OS version to

SilverPush servers

Scale: 67 apps by April 2015; 234 identified Android apps by May 2017 (TU Braunschweig study); 18 million devices affected, predominantly in Asia

Companies embedded: McDonald's, Krispy Kreme among apps confirmed by researchers (Infosecurity Magazine, 2017)

Regulatory action: FTC issued warning letters to 12 developers (March 2016); FTC Act violation for undisclosed background listening

SilverPush policy: Company policy was to not disclose which apps used the SDK — making user opt-out impossible

Deanonymization risk: Researchers at UCL/UCSB/PoliMI demonstrated SDK could be used to deanonymize Tor users (BlackHat EU 2016)

D.2 InMobi — The Location Bypass SDK

InMobi (Bengaluru-based, SoftBank-backed) embedded its advertising SDK in thousands of Android and iOS apps. It was caught by the FTC tracking location even when users explicitly denied location permission.

Technical bypass: InMobi SDK collected WiFi SSID and BSSID identifiers, cross-referenced against a proprietary geocoder database to derive precise physical location — bypassing Android's GPS permission denial

Scale: SDK embedded in apps reaching over 1 billion devices worldwide (FTC complaint)

COPPA violation: InMobi collected location data from children's apps despite representing it would not do so

FTC settlement: $950,000 civil penalty (reduced from $4 million); mandatory deletion of all non-consented location data; independent audits for two years

China link: InMobi entered exclusive monetisation partnership with APUS Group (Beijing) in September 2015, granting APUS access to all InMobi Indian users and their behavioral/location data

D.3 APUS Group — The Beijing Data Aggregator

APUS Group (Beijing Qilin Hesheng Network Technology Co., Ltd.) operated Android launcher and utility apps with 1.2 billion users across 200+ countries. 69% of users were in Belt and Road countries. APUS is a self-described 'digital Belt and Road practitioner.'

Data collection: Full installed-app list uploaded to server; all browsing history within APUS Browser sent to Beijing; application usage patterns retained for 30 days on Chinese servers

Privacy policy admission: 'We have purchased a Chinese supplier's traffic monitoring service. The merchant may return the user information to China in order to assist us in analyzing whether there is cheating.'

InMobi deal: Exclusive access to InMobi's India user pool — combining location (InMobi) + app behaviour (APUS) into unified Chinese-held profile of Indian citizens

National security dimension: APUS Nebula Platform described as a 'big data storage and screening' system to 'facilitate accurate prediction of user needs'

D.4 Baidu Push SDK — Device Identity Harvester

Collected: IMSI, IMEI, MAC address — permanent, irrevocable device identifiers — from any app embedding Baidu's push notification SDK

IMSI significance: Unique to each SIM; ties phone identity to mobile subscriber — enables tracking across device changes

Exposed: Palo Alto Networks Unit 42 research, November 2020; Google removed Baidu Maps and Baidu Search Box from Play Store as result

India context: Cashless Consumer analysis (Nov 2020) found 80% of 1,000 Indian loan apps used Alibaba Cloud or Baidu cloud infrastructure

D.5 Alibaba Cloud / ZOLOZ — Facial Biometric Harvester

ZOLOZ is Alibaba Cloud's liveness detection and facial recognition SDK used for KYC

Process: Selfie captured on victim device → immediately uploaded to ZOLOZ server in China → facial feature vectors extracted and stored → compared against retained template on all future logins

Critical finding (Cashless Consumer/Srikanth L, 2021): 600 of 1,050 Indian loan apps analysed used liveness detection with servers in China — collecting 'facial recognition-worthy images along with Aadhaar and personal details'

National security warning: Researcher warned this creates potential to 'build a parallel Aadhaar system — a facial biometric database of Indian citizens on Chinese servers'

All apps confirmed: Storing facial recognition data and personal data on Chinese servers (Cashless Consumer, 2020)

PART E — AI VISION WEAPONISATION: CURRENT & EMERGING THREAT

E.1 What AI Vision Does With Harvested Data — Six Threat Vectors

E.1.1 Real-Time Deepfake Identity Impersonation

A single high-quality KYC selfie (ZOLOZ harvest) combined with call-log voice samples (Igexin harvest) enables generation of a real-time video/audio deepfake of the victim. Operators can place a video call to victim's employer, family, or bank — appearing as the victim — to spread false information, fabricate confessions, or authorize fraudulent transactions. In 2024, a Hong Kong engineering firm (Arup) lost USD 25 million via a deepfake video call impersonating multiple executives.

E.1.2 Contact Graph AI Targeting

The full contact list (extracted by all four SDKs) is processed by AI to map social network structure, weight relationships by call frequency and recency, and identify the most psychologically vulnerable contact — elderly parent, new employer, spouse — for maximum pressure. AI agents then execute automated harassment campaigns against all identified contacts simultaneously, without human operators.

E.1.3 Physical Surveillance via Location AI

GPS data (InMobi WiFi bypass) combined with usage timestamps enables AI to determine: home address (device stationary 10pm–6am), workplace (stationary 9am–6pm weekdays), commute route and timing, and frequented locations. AI can geofence — triggering automated messages precisely when victim arrives at a workplace or bank — creating the appearance of physical surveillance.

E.1.4 Synthetic Identity Fraud

Face biometric + IMSI/IMEI + Aadhaar OCR (collected during KYC) enables creation of a synthetic digital identity that passes standard KYC verification. These fabricated identities can be used to open bank accounts, take new loans, or impersonate the victim in legal/financial proceedings. In 2025, synthetic identities represented 21% of all first-party fraud detected globally (Sumsub).

E.1.5 Autonomous AI Extortion Agents

Modern AI fraud agents combine generative AI, automation frameworks, and reinforcement learning to execute complete harassment campaigns without human intervention. They generate fake IDs/documents on demand,

interact with verification systems, adapt scripts based on victim responses, and attempt multiple harassment vectors simultaneously. Such agents can manage thousands of victims in parallel.

E.1.6 Nation-State Intelligence Infrastructure

The aggregate database — millions of Indian citizens' faces, IMSI identifiers, physical location histories, social graphs, financial stress indicators, and ID documents — stored on Chinese servers constitutes a permanent intelligence asset. With AI Vision, this database can verify any Indian citizen by face, track their movements historically and predictively, map their social connections, and assess financial vulnerabilities. This is functionally equivalent to a parallel Aadhaar system under foreign sovereign control.

E.2 Verified Scale of AI-Enabled Fraud (2024–2025)

PART F — GOVERNMENT OF INDIA RESPONSE: COMPLETE TIMELINE

F.1 Chronological Government Actions

F.2 Identified Gaps in Government Response

No public whitelist of legal apps was actually sent to app stores despite February 2023 parliamentary announcement

S.69A blocking orders issued without transparency — IFF criticized disregard for procedural safeguards and absence of individual bans

Some bans were inadvertently applied to compliant Indian fintechs (LazyPay, Kissht, PayU) — acknowledged by government

RBI governor stated digital lending apps are not under RBI's regulatory purview — creating enforcement gap

No AI-specific regulation for facial recognition or biometric data collected by foreign entities — India has no unified FRT framework as of 2025

DPDP Act 2023 framework for cross-border data transfers remains incompletely implemented

PART G — HARM EVIDENCE & VICTIM TESTIMONY FRAMEWORK

G.1 Documented Harms — Evidenced Cases

Bhumana Prasad, Hyderabad (Nov 2019): Took Rs.3,500 loan from 'My Bank' app. 14 undownloaded apps credited Rs.26,000 to his account and demanded Rs.44,000 repayment. Bank account manipulation documented.

Balaji Vijayaraghavan, Chennai (Oct 2020): Installed Snapit without logging in. Rs.8.49 lakh in unauthorized transactions from Rs.90,000 account. Assisting Telangana & Maharashtra police investigations.

Shivani Rawat, Delhi (June 2023): Rs.4,000 loan from 'Kreditbe' never received. Demanded Rs.9,000. Morphed explicit photographs sent to workplace colleagues. Manager asked her to resign. Case documented by Al Jazeera.

Multiple Suicide Cases, Telangana & AP (2020–2023): Documented suicides caused by loan app harassment, morphed image blackmail, and social shaming. State governments referred cases to Union Home Ministry — triggering the 2023 ban orders.

Suicide note, Bhopal (name withheld): Victim wrote in note that he had visited the Cyber Crime Office in Bhopal but 'received no assistance from the officers.' Documented in Al Jazeera report Dec 2023.

G.2 Harm Categories for FIR / Complaint

Financial fraud: Unauthorized deduction of processing fees before loan disbursement; excess principal claimed over amount received

Data theft: Unauthorized collection of contacts, SMS, photos, location, call logs — without valid consent under DPDP 2023

Criminal intimidation: Threat to publish morphed images — S.506 BNS / S.67A IT Act

Morphed image creation and distribution: S.67 and S.67A IT Act; S.354C BNS

Extortion: S.308(4) BNS (formerly S.386 IPC)

Cheating by personation: S.319 BNS (formerly S.420 IPC)

Identity theft: S.66C IT Act

Money laundering: S.3/S.4 PMLA — routing repayments through mule accounts to Chinese entities

Abetment of suicide: S.108 BNS (formerly S.306 IPC) — where harassment directly caused suicide

Violation of RBI Digital Lending Guidelines (August 2022): Unlicensed lending; interest rate concealment; third-party data sharing

PART H — SECTION 63(4)(C) BSA CERTIFICATE TEMPLATE

(Formerly Section 65B(4) Indian Evidence Act — governing authority: Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1; Chandrabhan Sudam Sanap 2025 INSC 116)

CERTIFICATE UNDER SECTION 63(4)(c) OF THE BHARATIYA SAKSHYA ADHINIYAM, 2023 [Erstwhile Section 65B(4), Indian Evidence Act, 1872] I, _____ [Full Name], aged ____ years, Designation: _____, Organisation: _____, Address: _____, do hereby certify as follows: 1. IDENTIFICATION OF ELECTRONIC RECORD Description of record: _____ File name(s): _____ SHA-256 Hash Value: _____ Date and time of creation / capture: _____ Size of file: _____ 2. DEVICE PARTICULARS Device make and model: _____ IMEI / Serial number: _____ Operating system and version: _____ Application name and version (if applicable): _____ 3. MANNER OF PRODUCTION The electronic record was produced / captured by: _____ Method of capture:

_____ Software tool used (if any): _____ Chain of custody: _____ 4. PROPER FUNCTIONING DECLARATION I certify that during the relevant period from _____ to _____, the device / computer system was operating properly and the electronic record was produced in the course of the ordinary use of the said system. 5. DECLARATION The contents of this certificate are stated to the best of my knowledge and belief. I am the person in a responsible official position in relation to the operation of the relevant device / management of the relevant activities, and am competent to make this certificate. Signed: _____ Name: _____ Date: _____ Place: _____ [Seal / Stamp of Organisation, if applicable] Note: This certificate must be signed BEFORE the electronic record is produced in court. A certificate signed after cross-examination commences may be rejected (Arjun Panditrao Khotkar, para 69).

PART I — AFFIDAVIT TEMPLATE: VICTIM / COMPLAINANT

Instructions: This affidavit is to be sworn before a Notary Public or First Class Judicial Magistrate. All blanks must be filled. Attach supporting documents as Annexures. Electronic annexures must each have a separate

Section 63(4)(c) certificate.

IN THE HON'BLE [COURT NAME] AT [CITY] [Case Number / FIR Number / Complaint Number] AFFIDAVIT OF [NAME OF DEPONENT — VICTIM / COMPLAINANT] I, _____, aged ____ years, [Occupation], resident of _____, do hereby solemnly affirm and declare on oath as follows: 1. That I am the complainant in the above matter and am fully conversant with the facts deposed herein. 2. LOAN APP INTERACTION: a) On or about [Date], I downloaded the application named [App Name] from [Google Play Store / Other] on my mobile device [Model, IMEI]. b) The app demanded the following permissions as a condition of use: [List: Contacts / Camera / Microphone / SMS / Storage / Location / Call Logs / Installed Apps]. c) I granted the above permissions under duress as the loan was urgently needed and the app would not proceed without such permissions. d) I was approved for a loan of Rs. _____ but only received Rs. _____ after deductions of [describe fees], in violation of RBI Digital Lending Guidelines (August 2022). 3. DATA MISUSE AND HARASSMENT: a) From approximately [Date], I began receiving calls / messages from numbers including [list numbers]

demanding repayment of amounts exceeding the loan received. b) On [Date], I received / my contacts received [describe: morphed images / abusive messages / threats / calls identifying as police]. c) My employer / family members [names] were contacted and received [describe content of communication]. d) I have suffered [describe: loss of employment / mental trauma / suicidal ideation / financial loss / damage to reputation]. 4. TECHNICAL EVIDENCE: a) Annexed hereto as ANNEXURE A (with Section 63(4)(c) certificate) are screenshots of the loan app interface, permission requests, and communications received. b) Annexed hereto as ANNEXURE B (with Section 63(4)(c) certificate) are screenshots / call records of harassing communications. c) I have preserved the said app on my device and have not factory reset or deleted any data that may be relevant to forensic examination. 5. That the statements made in this affidavit are true and correct to the best of my knowledge and belief. Nothing material has been concealed. Deponent VERIFICATION: Verified at [City] on [Date] that the contents of paras 1 to 5 of the above affidavit are true and correct to the best of my knowledge and belief, and that

nothing material has been concealed therefrom. Deponent Sworn before me on [Date] Notary Public / 1st Class Judicial Magistrate [Seal & Signature] Registration No.: _____

PART J — AFFIDAVIT TEMPLATE: EXPERT WITNESS (DIGITAL FORENSIC EXAMINER)

IN THE HON'BLE [COURT NAME] AT [CITY] [Case Number] AFFIDAVIT OF EXPERT WITNESS — DIGITAL FORENSIC EXAMINER I, _____, aged ____ years, Designation: [e.g. Cyber Forensic Expert, CERT-In empanelled], Qualifications: [e.g. B.Tech (CS), CHFI, CEH, CISSP], Organisation: _____, Address: _____, do hereby solemnly affirm and declare on oath as follows: 1. EXPERTISE AND EMPANELMENT a) I have [__ years] of experience in digital forensic examination of mobile devices, Android applications, and network traffic analysis. b) I am empanelled with / appointed by [agency] to examine the electronic devices / materials in the present matter. 2. DEVICES / MATERIALS EXAMINED Device: [Make, Model, IMEI], received on [Date] from [Custodian]. Chain of custody maintained as per Exhibit Log, annexed as ANNEXURE A. 3. FORENSIC FINDINGS — SDK EVIDENCE a) The device contained the application [App Name, version, package name]. b) Static analysis of the APK binary revealed embedded SDKs including: [List: Igexin / Baidu Push / ZOLOZ / SilverPush / InMobi — as found]. c) Network traffic capture (PCAP, Annexure B with

S.63(4)(c) certificate) shows data transmissions to the following IP addresses / domains: [List IPs and associated Chinese entities]. d) The following device data was confirmed to have been exfiltrated: [List: contact list / SMS content / GPS coordinates / call logs / selfie images / installed app list / device IMEI/IMSI]. e) The PhoneStateListener was registered by [SDK name], enabling real-time monitoring of call state (idle / ringing / off-hook) and calling number. f) Facial biometric data was transmitted to server: [server address] which resolves to / is hosted by [Alibaba Cloud / Baidu / other] in [location]. 4. SECTION 63(4)(c) CERTIFICATES I hereby certify, pursuant to Section 63(4)(c) of the Bharatiya Sakshya Adhiniyam, 2023, that: a) The electronic records described in paras 3(b)–3(f) and in all Annexures are authentic computer outputs. b) The forensic workstation /

tools used during analysis were in proper working condition and operating correctly. c) The records were produced in the ordinary course of forensic examination. d) The SHA-256 hash values recorded in the examination report match the original evidence items at the time of receipt. [Attach separate S.63(4)(c)

certificates for each distinct electronic exhibit] 5. OPINIONS a) In my expert opinion, the permissions requested by [App Name] exceeded those necessary for its stated loan functionality, and were consistent with systematic data exfiltration. b) The data transmission patterns identified are inconsistent with legitimate lending operations and consistent with unauthorised personal data collection as prohibited under DPDP Act, 2023 and RBI Digital Lending Guidelines, 2022. c) The ultrasonic beacon listener / PhoneStateListener code identified in the SDK constitutes an unauthorised interception mechanism under Section 5 of the Indian Telegraph Act and Section 66 of the IT Act. 6. That this affidavit is made on the basis of my professional examination of the materials produced. The opinions are based on established forensic methodology. Nothing material has been concealed. Expert Deponent VERIFICATION: [Standard verification clause] Sworn before me on [Date] Notary Public / Magistrate

PART K — APPLICABLE STATUTORY PROVISIONS & FIR SECTIONS

K.1 Bharatiya Nyaya Sanhita, 2023 (BNS) [replaces IPC]

S.318 (Cheating): Deceiving borrowers about loan amount, fees, and repayment terms

S.319 (Cheating by personation): Impersonation of police/legal authorities in recovery calls

S.308 (Extortion): Threatening to publish morphed images unless payment made

S.308(4): Extortion by putting person in fear of death or grievous hurt

S.351 (Criminal intimidation): Threatening to harm reputation via contact list notifications

S.108 (Abetment of suicide): Harassment causing victim to take their own life

S.354C (Voyeurism/Image-based abuse): Creating/distributing morphed intimate images without consent

S.503 (Criminal intimidation): Threat via electronic message to cause alarm

K.2 Information Technology Act, 2000

S.43: Unauthorised access to computer / mobile device

S.66: Computer related offence — dishonest or fraudulent access

S.66C: Identity theft — using another's electronic signature, password, or unique identification feature

S.66D: Cheating by personation using computer resource

S.67: Publishing obscene material in electronic form

S.67A: Publishing sexually explicit material in electronic form

S.69: Interception / monitoring / decryption of information (State power — used for app bans)

S.69A: Blocking of public access to information (Government power — used for S.69A app bans)

S.72: Breach of confidentiality and privacy

S.72A: Disclosure of information in breach of lawful contract

K.3 Digital Personal Data Protection Act, 2023 (DPDP)

S.4: Grounds for processing personal data — consent must be freely given, specific, informed, unconditional

S.8: Data fiduciary obligations — accuracy, security, deletion on purpose completion

S.16: Prohibition on processing children's data without verifiable parental consent

S.25: Significant data fiduciaries — enhanced obligations for large-scale processors

S.33: Penalties up to Rs.250 crore per violation for breach of data security obligations

K.4 Prevention of Money Laundering Act, 2002 (PMLA)

S.3: S.3 — Offence of money laundering: routing loan repayments through mule accounts and payment gateways to Chinese entities outside India

S.4: S.4 — Punishment for money laundering: rigorous imprisonment 3–7 years plus fine

S.8: ED jurisdiction to attach and confiscate proceeds of crime including digital assets

K.5 RBI Regulations Violated

RBI Digital Lending Guidelines, August 2022: No fees deducted before disbursement; all transactions through regulated entity account; explicit consent for third-party data sharing

RBI Master Direction — Non-Banking Financial Companies: NBFC must be registered; lending without registration is criminal under S.45-I and S.45-IA RBI Act

RBI Fair Practices Code: Prohibits coercive recovery; mandates disclosure of APR; prohibits harassment of borrower's associates

K.6 Sections 69A IT Act — App Banning Authority

DOCUMENT CERTIFICATION

This dossier was compiled from the following primary sources: Lookout Security Research (2017), Palo Alto Networks Unit 42 (2020), Cashless Consumer / Cashless Consumer Research (2020–2021), CloudSEK Research (2023), Al Jazeera Investigative Report (December 2023), FTC Official Settlement Documents (InMobi, 2016), TU Braunschweig / UCL / UCSB Academic Research (2016–2017), Sumsub Identity Fraud Report 2025, Veriff Identity Fraud Report 2025, World Economic Forum Global Cybersecurity Outlook 2025, Deloitte Center for Financial Services (AI Fraud Projections), deepstrike.io Deepfake Statistics 2025, iProov Study 2025, Enforcement Directorate press releases (2022–2024), MeitY official statements (2020–2025), RBI Digital Lending Guidelines 2022, and Supreme Court judgments: Anvar P.V. (2014), Arjun Panditrao (2020), Chandrabhan Sanap (2025 INSC 116), Kailash v. State of Maharashtra (2025 INSC 1117).

DISCLAIMER: This document is a research and legal reference dossier. It does not constitute legal advice. For use in court proceedings, all electronic evidence must be authenticated with independent Section 63(4)(c) BSA certificates. Consult a qualified advocate admitted to the relevant High Court or the Supreme Court of India for case-specific legal advice.

CHINESE PREDATORY LOAN APP ECOSYSTEM ADTECH SDK SURVEILLANCE | AI VISION WEAPONISATION | GOVERNMENT RESPONSE

Document Type | Legal Research Dossier / Evidentiary Brief

Jurisdiction | Republic of India — Supreme Court & High Courts

Governing Law | Bharatiya Sakshya Adhiniyam, 2023 (BSA) | IT Act, 2000 | DPDP Act, 2023 | RBI Act

Evidence Standard | Section 63(4)(c) BSA [formerly Section 65B(4) IEA] — Electronic Record Certificate

Date of Preparation | 03 April 2026

KEY RULE: Every screenshot, APK network log, server response, CDR, WhatsApp chat, and digital forensic report cited in this dossier must be accompanied by a Section 63(4)(c) certificate to be admissible in court.

Case | Citation | Holding

Anvar P.V. v. P.K. Basheer | (2014) 10 SCC 473 | S.65B forms a complete code for electronic evidence. Oral evidence cannot substitute the certificate.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal | (2020) 7 SCC 1 | 65B(4) certificate is condition precedent. Court may summon custodian if party cannot obtain certificate.

Chandrabhan Sudam Sanap v. State of Maharashtra | 2025 INSC 116 | Certificate is mandatory even in capital cases. Death sentence set aside for failure to produce 65B certificate.

Kailash v. State of Maharashtra | 2025 INSC 1117 (15 Sep 2025) | Video on CD is admissible as document once 65B requirements met. No mandatory transcript required.

State of Rajasthan v. Bhanwar Singh & Ors. | SC Judgment 26 Sep 2025 | CDRs without 65B certificate and produced as handwritten notes — held inadmissible.

Additional extracted text is retained in the archived source record.