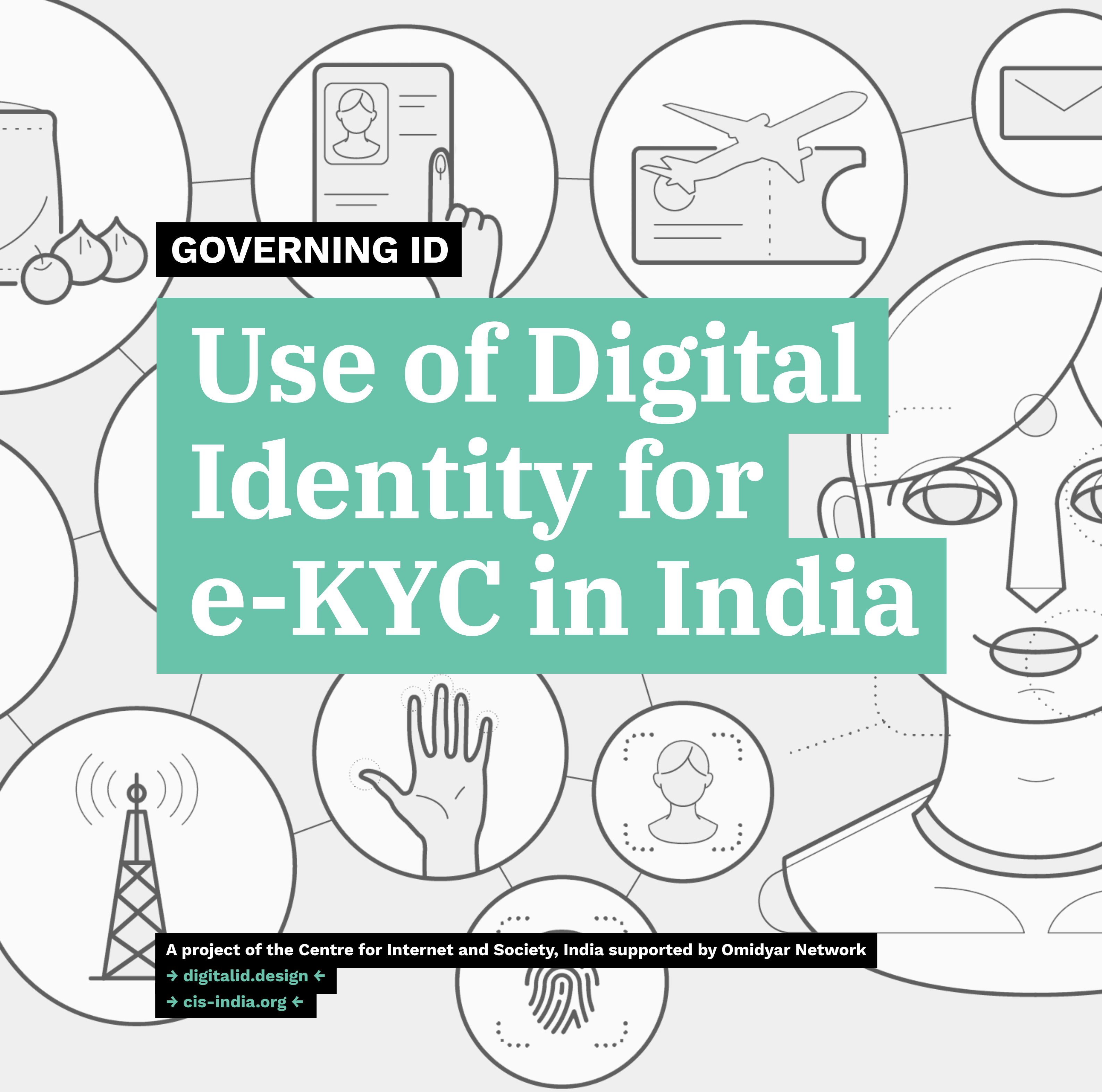

GOVERNING ID

Use of Digital Identity for e-KYC in India

A project of the Centre for Internet and Society, India supported by Omidyar Network

→ digitalid.design ←

→ cis-india.org ←

RESEARCH & WRITING
Yesha Tshering Paul

REVIEW & EDITING
Amber Sinha

DESIGN
Pooja Saxena

COVER ILLUSTRATION
Akash Sheshadri

THE CENTRE FOR internet & society

INTRODUCTION

This is the fifth in a series of case studies, using our evaluation framework for the governance of digital identity systems. These case studies, which analyse identity programmes and their uses, illustrate how our evaluation framework may be adapted to study instances of digital identity across different regions and contexts. This case study looks at the use of digital identity programmes for e-KYC in India.

Financial institutions are required by law to conduct KYC (Know Your Customer) procedures to verify the identity and other details of their clients and crack down on fraudulent transactions. This has traditionally been established by the customer submitting physical copies of their original identity and address proof, and a manual vetting of this information.

Aadhaar-based e-KYC enables the identity and address of a customer to be verified electronically via Aadhaar authentication, making the entire process paperless. The customer provides their explicit consent (by providing biometrics or OTP) for the e-KYC service to instantly generate an electronic, non-repudiable proof of identity and proof of address.

RULE OF LAW TESTS

1.1 LEGISLATIVE MANDATE

Is the use of digital identity system for e-KYC codified in valid law?

When examining the law governing e-KYC in India, it is important to consider whether processes around collection, storage, use, access to and sharing of personally identifiable information ("PII") are regulated by Parliament, or whether they have been delegated to the Executive.

The Prevention of Money Laundering Act, 2002 ("PML Act") mandates that requesting entities must verify the identity of its clients[1], the manner and conditions of which are are to be prescribed as per Rules made by the Central Government[2]. The Aadhaar and Other Laws (Amendment) Act, 2019[3] added a provision enabling e-KYC authentication via Aadhaar by banking entities to the PML Act.[4]

The Aadhaar Act, 2016 is the parent legislation primarily governing the use of Aadhaar in India. However, the Act itself does not codify the use of Aadhaar for e-KYC. The framework governing the use of Aadhaar for e-KYC is instead codified by a number of regulations issued by the Unique Identification Authority of India ("UIDAI", which derives its power as an executive body from the Aadhaar Act), as well as by the Reserve Bank of India ("RBI"), Securities and Exchange Board of India ("SEBI"), and the Ministry of Finance. For instance, the Aadhaar (Authentication) Regulations, 2016 define an "e-KYC authentication facility" as "a type of authentication facility in which the biometric information and/or OTP and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is matched against the data available in the CIDR, and the Authority returns a digitally signed response containing e-KYC data along with other technical details related to

[1] Section 12(1)(c), Prevention of Money Laundering Act, 2002 [”PML Act”].

[2] Section 73, PML Act.

[3] The Aadhaar and Other Laws (Amendment) Ordinance was promulgated in March 2019, and the Aadhaar and Other Laws (Amendment) Act was later passed once Parliament was in session. The constitutional validity of the Ordinance and the Act has been challenged before the Supreme Court of India in *S.G. Vombatkere v. Union of India*.

[4] Section 11A, PML Act.

the authentication transaction".[5] Procedures for identification, authentication, actors, and storage of information are also similarly delegated to the Executive, potentially amounting to excessive delegation.

In a 2013 notification addressed to all recognized stock exchanges, stockbrokers through recognized stock exchanges, depository participants through depositories, Association of Mutual Funds in India, mutual funds through AMFI, Portfolio Managers, KYC Registration Agencies, Alternative Investment Funds, Collective Investment Schemes and Custodians, SEBI originally allowed e-KYC as a valid form of KYC.[6] SEBI exercised its powers under Section 11(1) of the Securities and Exchange Board of India Act, 1992 to protect the interests of investors in securities and to promote the development of, and to regulate the securities markets.[7]

There have been a number of amendments to the executive and legislative framework regulating e-KYC since 2019. The Aadhaar Act was amended via the the Aadhaar and Other Laws (Amendment) Act, 2019 to allow an Aadhaar holder to voluntarily use their Aadhaar number in electronic form for authentication[8], in addition to "an entity" being permitted to perform authentication if it is compliant with standards of privacy and security specified by regulations, or is permitted to offer authentication services by any other law, or seeks authentication for purposes prescribed by the government.[9] A series of amendments to the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 ("PML Rules")[10] and the RBI Master Direction on KYC Norms, added new provisions for authentication via e-KYC.[11] The central government has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (set up under Section 20(1) of the Securitisation and Reconstruction of Financial

[5] Regulation 2(1)(j), Aadhaar (Authentication) Regulations, 2016.

[6] SEBI Circular No. CIR/MIRSD/09/2013.

[7] SEBI Circular No. CIR/MIRSD/09/2013.

[8] Section 4(3), The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 ["Aadhaar Act"].

[9] Section 4(4), Aadhaar Act.

[10] Prevention of Money-laundering (Maintenance of Records) Third Amendment Rules, 2019, Prevention of Money-laundering (Maintenance of Records) Fifth Amendment Rules, 2019.

[11] RBI Master Direction, Know Your Customer (KYC) Direction, 2016 ["RBI Master Direction"].

Assets and Enforcement of Security Interest Act, 2002) to perform the functions of the Central KYC Records Registry.[12]

Thus the framework governing the use of e-KYC in India is primarily made up of delegated legislation.

1.2 LEGITIMATE AIM

Does the law have a legitimate aim?

The use of e-KYC must correspond to a legitimate aim in the law governing it. This legitimate aim should not operate in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. The PML Act aims to "prevent money-laundering and to provide for confiscation of property derived from, or involved in, money-laundering and for matters connected therewith or incidental thereto." In addition, the Aadhaar Act, which governs digital identity in India, states its primary purpose as providing for, "as a good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services".

These objectives qualify as a legitimate aim.

1.3 DEFINING ACTORS AND PURPOSES

Does the law clearly define all the actors and purposes involved in e-KYC?

Section 4(4) of the Aadhaar Act permits "an entity" to perform authentication if it is compliant with standards of privacy and security specified by regulations, or is permitted to offer authentication services by any other law, or seeks authentication for purposes prescribed by the government. The Act does not define who may ask for authentication, and the UIDAI is tasked with determining

[12] Notification 3183(E), Ministry of Finance, November 26, 2015.

who will manage the CIDR.[13] The Aadhaar (Authentication) Regulations define a requesting entity as "an agency or person that submits the Aadhaar number, and demographic information or biometric information, of an individual to the CIDR for authentication".[14] An e-KYC User Agency ("KUA") is defined as a requesting entity which...uses e-KYC authentication facility provided by the UIDAI.[15]

The PML Act defines a reporting entity as "a banking company, financial institution, intermediary or a person carrying on a designated business or profession."[16] Banking companies are the only reporting entities allowed to conduct Aadhaar-based authentication[17], however, the Central Government may allow a reporting entity other than a banking company to perform authentication via Aadhaar if it is satisfied that the company complies with privacy and security standards under the Aadhaar Act, and it is considered necessary and expedient to do so.[18]

The Department of Revenue, Ministry of Finance issued a 2019 circular on the procedure for processing of applications under Section 11A of the PML Act for Aadhaar authentication services by entities other than banking companies. It states that the Central Government may permit a reporting entity to carry out authentication using e-KYC if it is satisfied with the recommendations of the appropriate regulator and the UIDAI, if the reporting entity complies with the privacy and security standards under the Aadhaar Act, and if it is necessary and expedient to do so.[19]

[13] Section 10, Aadhaar Act.

[14] Section 2(1)(o), Aadhaar (Authentication) Regulations, 2016.

[15] Section 2(1)(l), Aadhaar (Authentication) Regulations, 2016.

[16] Section 2(wa), PML Act.

[17] Section 11A(1)(a), PML Act.

[18] Proviso to Section 11A(1)(a), PML Act.

[19] Circular on Procedure for processing of applications under Section 11A of the Prevention of Money-Laundering Act, 2002 for use of Aadhaar authentication services by entities other than Banking companies, Securities and Exchange Board of India, 2019.

The RBI Master Direction on KYC has listed the Regulated Entities that can conduct e-KYC authentication[20]. In addition to these entities, the Master Direction also provides that biometric-based e-KYC authentication can be carried out by bank official/ business correspondents/ business facilitators.[21]

As seen above, the actors and purposes involved in e-KYC have been identified in the regulatory framework with varying degrees of specificity.

1.4 REGULATING PRIVATE ACTORS

Is this use of the ID system by private actors adequately regulated?

The use of e-KYC by private actors is regulated within the governing framework of rules and regulations, and no private entities can mandate the use of Aadhaar.

Private actors were empowered to use Aadhaar under Section 57 of the original Aadhaar Act, 2016. This Section was later read down by the Supreme Court in the *Aadhaar Judgment* to exclude individuals and body corporates from seeking authentication due to concerns that it would "enable commercial exploitation of an individual biometric and demographic information by the private entities".[22] The 2019 amendment[23] to the Aadhaar Act did away with Section 57, but circumvented the spirit of the Judgment by restoring the use of Aadhaar by private actors via other newly added sections. Section 4(4) of the Aadhaar Act now permits "an entity" to perform authentication if it is compliant with standards of privacy and security specified by regulations, or is permitted to offer

[20] As per Direction 3(xiii) of the Master Direction on KYC, Regulated Entities can be: Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licenced under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks', All India Financial Institutions (AIFIs), All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs), All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers), All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

[21] Explanation 2, Direction 16, RBI Master Direction.

[22] *K.S. Puttaswamy v. Union of India*, 1 SCC 1 (2019) ["Aadhaar judgment"].

[23] The Aadhaar (And Other Laws) Amendment Act, 2019 ["Aadhaar Amendment Act"].

authentication services by any other law, or seeks authentication for purposes prescribed by the government.

The 2019 amendment inserted Section 4(3) to the Indian Telegraph Act, 1885, which allows "any person" with a license to identify its customers via authentication or offline verification under the Aadhaar Act, in addition to other modes of identification. The amendment also added Section 11A to the Prevention of Money Laundering Act, 2002 to enable "every reporting entity" to to verify the identity of its clients and beneficial owner by authentication or offline verification under the Aadhaar Act.

The Department of Revenue, Ministry of Finance issued a 2019 circular on the procedure for processing of applications under Section 11A of the PML Act for Aadhaar authentication services by entities other than Banking companies. It states that the Central Government may permit a reporting entity to carry out authentication using e-KYC if it is satisfied with the recommendations of the appropriate regulator and the UIDAI, if the reporting entity complies with the privacy and security standards under the Aadhaar Act, and if it is necessary and expedient to do so.[24] This circular thus enables private entities in the securities market to undertake e-KYC.[25] As per a subsequent circular, these entities will be registered with the UIDAI as KYC user agencies ("KUAs") and shall allow all SEBI registered intermediaries/ mutual fund distributors to undertake e-KYC of their clients through them.[26] The circular also details the the processes by which KUAs and sub-KUAs can adopt e-KYC for resident investors in the securities market.[27]

As seen above, there is regulation of private actors using digital ID for e-KYC.

[24] The circular states that applications by the concerned entities under Section 11A of the PML Act shall be filed before the appropriate regulator, who will scrutinise and recommend certain applications to the UIDAI. The UIDAI shall in turn recommend certain applications to the Department of Revenue for notification under Section 11A of the PML Act. If the Central Government is satisfied with the recommendations and the applicant fulfils all the conditions under Section 11A, it may permit the applicant to perform authentication under Section 11A(1)(a). This notification can be withdrawn at any point after issuing, on the basis of a report by the UIDAI or the regulator that the reporting entity no longer fulfils the requirements for performing authentication.

[25] Circular on Procedure for processing of applications under Section 11A of the Prevention of Money-Laundering Act, 2002 for use of Aadhaar authentication services by entities other than Banking companies, SEBI, 2019.

[26] Circular on e-KYC Authentication facility under section 11A of the Prevention of Money Laundering Act, 2002 by Entities in the securities market for Resident Investors, SEBI, 2019.

[27] Circular on e-KYC Authentication facility under section 11A of the Prevention of Money Laundering Act, 2002 by Entities in the securities market for Resident Investors, SEBI, 2019.

1.5 DATA SPECIFICATION

Does the law clearly define the nature of data that will be collected?

The Aadhaar Act provides a fairly exhaustive list of data that will be collected. Section 3(1) states that a resident shall enroll by submitting their demographic and biometric information. As per the Act, demographic information includes name, date of birth, address and other relevant information as may be specified to issue an Aadhaar number. The Act specifically excludes race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history from this category.[28] Biometric information here includes photograph, fingerprint, iris scan or other biological attributes that may be specified.[29] Core biometric information means fingerprint, iris scan, or other biological attributes as may be specified.[30]

These provisions allow the scope of these categories to be expanded by the executive authority via regulations, which could result in new categories of data being collected without sufficient legislative oversight.

The provision for demographic information guards against this by specifically listing the categories of data that cannot be collected. The Aadhaar (Authentication) Regulations, 2016 define e-KYC data as meaning demographic information and photograph of an Aadhaar number holder. This will include name, address, date of birth, gender, photograph, mobile number, and e-mail ID (if available).

[28] Section 2(k), Aadhaar Act.

[29] Section 2(g), Aadhaar Act.

[30] Section 2(j), Aadhaar Act.

1.6 USER NOTIFICATION

Does the ID system provide adequate user notification mechanisms for this use case?

The law does not explicitly provide for user notification mechanisms for authentication.

However e-KYC requires the explicit consent of the user and is carried out voluntarily.

1.7 USER RIGHTS

Do individuals have rights to access, confirmation, correction and opt out?

Aadhaar holders have the right to access and correct/ update their demographic and biometric information stored in the Central Identities Data Repository ("CIDR").[31] The RBI Master Direction on KYC also allows customers to provide a current address different to that stored in the CIDR, which they may do by submitting a self-declaration to that effect.[32] In addition, e-KYC via Aadhaar is not mandatory, and users can choose to verify their identities through other means.

Most of the user rights are provided to individuals while using e-KYC.

[31] Section 31, Aadhaar Act; Regulation 14 and 16, Aadhaar (Enrollment) Regulations, 2016.

[32] Proviso (i) to Direction 16(a), RBI Master Direction.

1.8 REDRESSAL MECHANISMS

Are there adequate civil and criminal redressal mechanisms in place to deal with violations of their rights arising from the process of e-KYC?

While there are redressal mechanisms under the Aadhaar Act, we did not come across any specific redressals that citizens have access to arising from the failure of e-KYC.

RIGHTS BASED TESTS

2.1 DATA MINIMISATION

Are principles of data minimisation followed in the collection, use, and retention of personal data for this use case?

Data minimisation principles are followed to some extent in the use of e-KYC.

The scope of the data has been clearly defined, and the use of e-KYC has been limited to only KYC purposes.

The PML Act explicitly states that for identification of a client of beneficial owner, authentication or offline verification, neither his core biometric information or Aadhaar number shall be stored [33]. KUAs/ sub-KUAs have been prohibited from storing Aadhaar numbers in their databases for any purposes, and only the full Aadhaar number cannot be stored or displayed anywhere in the system and only the last 4 digits of the Aadhaar number may be displayed wherever required.[34] The Aadhaar (Authentication) Regulations also mandate that a requesting entity cannot store, publish or share core biometric information for any purpose, or keep a copy of this information.[35]

However, the Aadhaar (Authentication) Regulations allow a KUA to store, with consent of the Aadhaar number holder, e-KYC data of an Aadhaar number holder, received upon e-KYC authentication, in encrypted form and subsequently share the e-KYC data with any other agency, for a specified purpose, upon obtaining separate consent for every such sharing from the Aadhaar number holder for that purpose.[36] If the Aadhaar number holder revokes their consent, the KUA shall delete any e-KYC data and not share it further.[37]

[33] Proviso (4) to Section 11A, PML Act.

[34] Circular on e-KYC Authentication facility under section 11A of the Prevention of Money Laundering Act, 2002 by Entities in the securities market for Resident Investors, SEBI, 2019.

[35] Regulation 17(1)(a), Aadhaar (Authentication) Regulations, 2016.

[36] Regulation 16(3), Aadhaar (Authentication) Regulations, 2016.

[37] Regulation 16(5), Aadhaar (Authentication) Regulations, 2016.

KYC records are stored digitally in a Central KYC Records Registry, which is defined under Rule 2(1) of the PML Rules, to receive, store, safeguard and retrieve a customer's KYC records. The PML (Maintenance of Records) Rules mandate that KYC records are to be stored for a period of ten years from the date of cessation of transactions between the client and the reporting entity. However, it is not explicitly mandated that this data must be deleted after ten years.[38]

2.2 ACCESS TO DATA

Does the law specify access that various private and public actors have to personal data in this use case?

KYC records are stored in a Central KYC registry for a period of ten years from the date of cessation of transactions between the client and the reporting entity.[39] The Registry can be accessed by institutions registered/ authorised under the PML Act and other rules.[40]

Under the Indian Telegraph Act, "any person" with a license may use e-KYC for authentication. The PML Act allows "every reporting entity" to verify the identity of its clients and beneficial owner by authentication or offline verification under the Aadhaar Act. As per a 2019 circular issued by the Department of Revenue, Ministry of Finance, entities other than banking companies may also carry out e-KYC if they comply with certain requirements. This notification thus regulates private entities in the securities market to undertake e-KYC.[41] As per a subsequent circular, these entities will be registered with the UIDAI as KUAs and shall allow all SEBI registered intermediaries/ mutual fund distributors to undertake e-KYC of their clients through them.[42] This circular also details the the processes by which KUAs and sub-KUAs can adopt e-KYC for resident investors in the

[38] PML (Maintenance of Records) Rules, 2005.

[39] PML (Maintenance of Records) Rules, 2005.

[40] Guideline IV(a), Central KYC Registry Operating Guidelines, 2016.

[41] Circular on Procedure for processing of applications under Section 11A of the Prevention of Money-Laundering Act, 2002 for use of Aadhaar authentication services by entities other than Banking companies, SEBI, 2019.

[42] Circular on e-KYC Authentication facility under section 11A of the Prevention of Money Laundering Act, 2002 by Entities in the securities market for Resident Investors, SEBI, 2019.

securities market.[43] KUAs shall maintain auditable logs of all such transactions where e-KYC data has been shared with sub-KUA, for a period specified by the Authority.[44]

There is adequate regulation of access to data collected for the purposes of e-KYC using digital ID.

2.3 MANDATORY USE AND EXCLUSIONS

Does the use of digital identity in e-KYC lead to exclusionary impacts?

Since e-KYC is not mandatory and there exist alternative forms of authentication, it does not necessarily lead to exclusionary impacts due to failures.

[43] Circular on e-KYC Authentication facility under section 11A of the Prevention of Money Laundering Act, 2002 by Entities in the securities market for Resident Investors, SEBI, 2019.

[44] Circular on e-KYC Authentication facility under section 11A of the Prevention of Money Laundering Act, 2002 by Entities in the securities market for Resident Investors, SEBI, 2019.

RISK BASED TESTS

3.1 RISK ASSESSMENT

Is this use case regulated taking into account its potential risks?

There is no data protection law in place (and no sufficient judicial oversight) governing the use of personal data for e-KYC.

3.2 RESPONSE TO RISKS

Is there a mitigation strategy in place in case of failure?

There are some mitigation strategies inbuilt in the design for use of e-KYC.

Authentication for e-KYC can be either via OTP or biometrics,[45] and in case of failure of authentication via e-KYC, other authentication alternatives exist. However there does not seem to be any clearly articulated mitigation strategy in case of failure of e-KYC.

[45] Regulation 4(3), Aadhaar (Authentication) Regulations, 2016.