3 LEGAL AND GOVERNANCE FRAMEWORK
The legal framework of Aadhaar has evolved significantly since its inception in 2009. The Aadhaar Act 2016 constitutes the current legislative framework governing Aadhaar. Aspects of this Act and the Aadhaar project have been challenged in the Supreme Court and await resolution. These challenges—including the question of a right to privacy—inform important areas of future research.

Aadhaar’s legal and governance framework has been the subject of keen interest throughout the project’s eight-year history. Since Aadhaar’s conception in 2009, its legal framework has undergone significant change. Currently, the Aadhaar Act 2016 and subsequent regulations govern the use of Aadhaar in public and private applications. Together they prescribe procedures for the collection, transfer, maintenance, and sharing of personal information under Aadhaar. In addition, notifications issued by several central and state government ministries also regulate the use of Aadhaar in public service delivery.

Over the years, several aspects of Aadhaar have been contested in court and await final resolution. These challenges may have far-reaching impact, including the determination of whether India’s Constitution affords a right to privacy and what the nature and limitations of such a right may be.

In this Chapter, we trace Aadhaar’s legal evolution, discuss important features of the Aadhaar Act 2016, and outline associated legal challenges. Together with Aadhaar’s technical architecture (discussed in Chapter 2, Aadhaar Architecture), a better understanding of Aadhaar’s governing framework can aid engagement with its use-cases in financial inclusion, social protection, and other emerging areas. The Chapter concludes with suggestions for future research to inform improved policy.
Legal History

Aadhaar was created through an executive order in 2009. Legislation governing Aadhaar was introduced twice—in 2010 and 2016—and passed the second time in the form of the Aadhaar Act 2016. In the interim years, enrolment into Aadhaar continued to grow. The Supreme Court of India has also issued several directives on Aadhaar’s permissible uses. The history of Aadhaar’s conception, passage of supporting legislation, and associated judicial verdicts are discussed below.

Legislative history

The United Progressive Alliance (UPA) government created the Unique Identification Authority of India (UIDAI) through an executive order on 28 January 2009. The creation of the UIDAI capped several years of movement towards a national identity project in India. Housed under the erstwhile Planning Commission, the UIDAI was envisioned as a pan-departmental agency responsible for issuing a unique identifier — Aadhaar — to every Indian resident. The first Aadhaar number was issued on 29 September 2010.

Two months into the enrolment process, on 3 December 2010, the government introduced the National Identification Authority of India Bill in Parliament to provide statutory backing for the Aadhaar project. This bill sought to establish a “National Identification Authority of India” and specified regulations on the collection, storage, use, and disclosure of individuals’ personal information under Aadhaar. The bill was referred by the Lok Sabha (Lower House) to the Standing Committee on Finance (2011-12). The committee raised objections to Aadhaar’s conception, design, implementation, and potential outcomes. It recommended that the government reconsider the scheme and introduce a new bill. It also described the executive’s issuance of Aadhaar numbers, while lawmaking related to Aadhaar was under way, as “unethical” and in violation of Parliament’s prerogatives. A fuller discussion of the concerns expressed in the 2011 Standing Committee report is presented later in this Chapter. Official amendments to the Bill were proposed to be moved in 2013, but were not passed.

The next attempt to formalise the Aadhaar project in law came with the introduction of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Bill 2016 (henceforth referred to as the “Aadhaar Bill” or “Aadhaar Act” as relevant). The bill was introduced in Parliament in March 2016 by the Finance Minister of the National Democratic Alliance (NDA) government. The Act specified that the government could require individuals to possess an Aadhaar number or undergo Aadhaar authentication for the receipt of government benefits financed from the Consolidated Fund of India, in addition to objectives outlined by the previous bill.

The Aadhaar Bill 2016 was introduced as a Money Bill. The Rajya Sabha (Upper House) may suggest amendments to Money Bills, but the Lok Sabha is not bound by them. In this case, the Rajya Sabha suggested five amendments on 16 March 2016. In accordance with the Lok Sabha’s powers, it passed the bill without accepting the amendments. The Act came into effect on 12 September 2016 and constitutes

---

**Figure 3.1: What is a Money Bill?**

According to the Indian Constitution, a bill may be deemed a Money Bill if it contains only provisions dealing with six specific topics, or matters incidental to those topics. The topics include the imposition, alteration, or regulation of taxes, regulations relating to government borrowing, and payments to or from the Consolidated Fund of India. A Money Bill can only be introduced in the Lok Sabha. After it has been passed by the Lok Sabha, it is transmitted to the Rajya Sabha for its recommendations. The Lok Sabha may thereafter accept or reject any or all of the Rajya Sabha’s recommendations. If the Lok Sabha does not accept any of the recommendations of the Rajya Sabha, the Money Bill is deemed to have passed in the form in which it was initially passed by the Lok Sabha.

Source: Constitution of India

---
the current legal framework governing Aadhaar (alongside the regulations and notifications enlisted in Appendix 3.1). Between September 2010 (when the first Aadhaar number was issued) and 2016, the UIDAI continued to issue Aadhaar numbers on the basis of the 2009 executive order.

Other Acts of Parliament can shape the usage of Aadhaar as well. For example, the Finance Act 2017 made Aadhaar a requirement for filing income tax returns, and applying for and retaining a Permanent Account Number (the identification issued by India’s Income Tax Department).\(^{13}\)

The requirement of Aadhaar for tax returns, and the introduction and subsequent passing of the Aadhaar Bill as a Money Bill have been challenged in the Supreme Court. These issues are taken up in the last section of the Chapter.

**Judicial history**

Petitions challenging the legality of the Aadhaar project have been filed before several Indian High Courts and the Supreme Court of India. In this Chapter, we will focus on petitions before the Supreme Court. While these cases await resolution, the Supreme Court issued directives in 2013, 2014, and 2015, emphasising that Aadhaar could not be made a condition for the receipt of government benefits, and that possession of an Aadhaar number must be voluntary.\(^{14,15,16}\)

In an interim order in 2015, the Supreme Court stated that Aadhaar could not be used for any purpose other than for two schemes pertaining to food and cooking fuel subsidies.\(^{17}\) In a later order in the same year, the Supreme Court expanded this list of schemes to include government programmes relating to an employment guarantee, cash transfers to the poor, opening bank accounts, and savings for retirement.\(^{18}\) It further directed that enrolment into Aadhaar is “purely voluntary” and cannot be made mandatory until the matter is decided by the Court.\(^{19}\)

In parallel, several government ministries have issued circulars requiring Aadhaar for the receipt of benefits and allowing its use in schemes other than those specified by the Supreme Court. Both before and after the passage of the 2016 Act, Aadhaar has increasingly been made compulsory for a wide range of government schemes and benefits.\(^{20,21,22,23}\) In addition, it is now required for the filing of income tax returns.\(^{24}\) Meanwhile, the Supreme Court has yet to hear a batch of petitions raising concerns about the legality of the Aadhaar project and Aadhaar’s use in government service delivery.

In Figure 3.2, we illustrate key events in the legislative and judicial evolution of Aadhaar.

---

**Figure 3.2: Timeline of Aadhaar’s evolution**

- **Jan 2009**
  - Creation of the UIDAI

- **Sep 2010**
  - First Aadhaar number issued

- **Dec 2010**
  - Introduction of first Aadhaar Bill

- **Sep 2011**
  - 100 million Aadhaar holders

- **Dec 2011**
  - Standing Committee Report on Aadhaar Bill

- **Dec 2013**
  - 510 million Aadhaar holders

- **Dec 2014**
  - 720 million Aadhaar holders

- **Oct 2015**
  - Supreme Court interim order stating Aadhaar is voluntary

- **Feb 2016**
  - 980 million Aadhaar holders

- **Mar 2016**
  - Re-introduction and passage of Aadhaar legislation

- **Sep 2016**
  - Aadhaar Act comes into effect

- **Mar 2017**
  - 1.14 billion Aadhaar holders
Aadhaar Act 2016: Salient Features

This section discusses some key features of the Aadhaar Act 2016. We also highlight features that interact with the 2011 Standing Committee’s report on the 2010 Bill. Amendments to the 2016 Bill suggested by the Rajya Sabha (but not passed by the Lok Sabha) are also presented.

Eligibility and enrolment

The Aadhaar Act allows for the issuing of Aadhaar numbers to all Indian residents (individuals residing in-country for 182 days or more in the year before application). Aadhaar cannot be proof of citizenship or domicile.

The 2011 Standing Committee report expressed concern that illegal immigrants would be able to obtain an Aadhaar number, posing risks to national security and allowing them access to government benefits. The Committee expressed concerns about the security of the “introducer” system and entrusting the responsibility of verifying Aadhaar applicants’ personal information to Registrars (discussed in Chapter 2, Aadhaar Architecture). It asserted that the complete verification of information of all Aadhaar holders seemed infeasible on a practical basis, and that the possibility of illegal residents possessing Aadhaar numbers through false affidavits or inaccurate introductions could not be ruled out.

Finally, the committee noted that while Aadhaar could provide a proof-of-identity, it could not by itself determine eligibility for receiving government benefits. As things stand, while all residents are eligible for an Aadhaar number, muster rolls (beneficiary lists) are maintained by the relevant government departments implementing a particular scheme or service. Aadhaar can serve as a proof-of-identity or residence while accessing government services, but does not determine eligibility for these services.

Collection of personal information

The Act defines the information that may be collected for the issuance of an Aadhaar number. Currently, this includes biometric (photograph, fingerprint, and iris scan) and demographic (name, date of birth, and address) information. In addition, the UIDAI can specify other biometric and demographic information to be collected through regulations. These regulations have the status of delegated legislation. The Act specifies that information pertaining to “race, religion, caste, tribe, ethnicity, language, records of entitlement, income, or medical history” cannot be collected.

The 2011 Standing Committee report noted that it may be beyond the scope of the Aadhaar legislation to link biometric information with personal information without amending the Citizenship Act 1955 or Citizenship Rules 2003. It recommended this issue be examined in detail by Parliament. In addition, it also identified as concerns the duplication of effort by other government bodies collecting personal information and the continuance of other forms of proof-of-identity and address. No amendments pertaining to Aadhaar have been made to the Citizenship Act 1955 or Citizenship Rules 2003 since the creation of the UIDAI. The impact of Aadhaar on the collection of personal information by different government agencies is a potential area of further research.

Use of Aadhaar

The Act allows for both government and non-government use of the Aadhaar platform.

Government use

The Aadhaar Act specifies that the government can require an individual to have an Aadhaar number for the purpose of receiving a subsidy or service. As noted above, the Supreme Court issued directives in 2013, 2014, and 2015, stating that the lack of Aadhaar identification cannot be grounds for denial of government subsidies and services. The Rajya Sabha passed an amendment allowing for the receipt of government benefits even if an individual chooses not to opt for Aadhaar enrolment. However, this amendment was not passed by the Lok Sabha, and is therefore absent from the current legislation governing
Aadhaar. The Supreme Court is hearing cases that may have implications on the use of Aadhaar for provision of subsidies and other services.

**Private Use**
The Act allows for private sector use of Aadhaar. Any public or private entity may use Aadhaar to establish the identity of an individual. The same data protection and consent provisions (enumerated in the section below) apply to private and public entities alike. The Rajya Sabha passed an amendment to delete the provisions allowing for private and non-governmental applications of Aadhaar, which was not accepted by the Lok Sabha. Today, Aadhaar is being used by several private sector entities for uses ranging from e-KYC for SIM card issuance to background verification of potential employees, as detailed in Chapter 6, *Emerging Uses*.

**Information management**
The Act specifies provisions governing the collection and use of individuals' personal information.

**Data collection and storage**
Enrolling agencies are required to inform individuals about the manner in which their information shall be used, the nature of recipients with whom it will be shared, the right to obtain access to information, and the procedure for this. In addition, the UIDAI is responsible for guaranteeing the security of individuals' Aadhaar data, including authentication records.

The Act delineates several measures that the UIDAI must take to ensure data confidentiality and security. These include implementing technical and organisational security measures, guaranteeing that all entities operating in connection with the Act have adopted equivalent security measures and that these entities act only on the instruction of the UIDAI and are bound by equivalent obligations.

The 2011 Standing Committee report noted that the Aadhaar project allowed the UIDAI to create a large database of personal information, creating the possibility of information misuse. Given this concern, the Committee advocated the enactment of a national data protection law as a prerequisite to any legislation allowing large-scale collection of personal information and linkage across databases. The committee noted that the absence of data protection legislation would make it difficult to deal with issues such as “access and misuse of personal information, surveillance, profiling, linking and matching of databases, and securing confidentiality of information.” Meanwhile, no data protection legislation has been passed by Parliament.

In response to media reports of data misuse by private agencies and individuals, the UIDAI and the Government of India have stated that the Aadhaar database is secure. Instances of government entities publishing residents' Aadhaar numbers have been reported in some states, including Jharkhand. In April 2017, the Aadhaar numbers and bank details of more than a million pension beneficiaries in the state were displayed on a state government website.

While these instances constitute a clear violation of the Aadhaar Act (which forbids the publication of an individual's Aadhaar number), the Government stated that these do not represent a vulnerability in Aadhaar’s framework itself. The UIDAI has directed the Jharkhand state government to identify the individuals responsible for the leak in order for action to be initiated against them.

**Data authentication**
Any entity (public or private) requesting authentication of an Aadhaar number is required to obtain consent of the individual before collecting or verifying her or his identity information. Entities are also required to ensure that identity information of the individual is used only for submission to the Central Identities Data Repository (CIDR) for authentication. In addition, the requesting entity must apprise the individual—whose data is to be authenticated—of the following:

1. The nature of the information that may be shared upon authentication,
2. the uses to which information received by the requesting entity may be put, and,
3. alternatives to submitting personal information to the requesting entity.
The UIDAI shall respond to an authentication query with a positive, negative, or other appropriate response sharing identity information, excluding core biometric information (fingerprints and iris scan). In addition, the UIDAI will maintain authentication records in such manner and for such period as specified by regulations. However, the UIDAI will not collect or maintain data on the purpose of authentication. A detailed discussion of the authentication process is presented in Chapter 2, Aadhaar Architecture.

Data disclosure

No member of the UIDAI nor any of its contracted agencies is entitled to disclose any information contained in the CIDR or authentication record. An individual’s core biometrics (fingerprints and iris scan) may never be disclosed (except under the national security clause discussed below). Authenticating agencies too are forbidden from using individuals’ information in any way other than in the manner specified to Aadhaar holders. They may not disclose individuals’ personal information without their consent.

The Act allows for exceptions wherein the UIDAI may share information about individuals, as specified by regulations. Two specific circumstances have been outlined where information disclosure will be permissible.

First, a district judge or higher court can mandate that identity information, including name, date of birth, address and gender, but not fingerprints or iris scan, be disclosed. Currently, there is no known case of a court requiring that an individual’s personal information—collected under Aadhaar—be disclosed.

Second, a government official of Joint Secretary or higher rank can order the release of an individual’s Aadhaar data, including biometrics, in the interest of national security. This decision would require review by an Oversight Committee before taking effect. The Committee will consist of the Cabinet Secretary (the highest-ranked civil servant in India), as well as the Secretaries of Legal Affairs and Information Technology. Any such decision would be valid for three months, which may be extended further by three months after additional review by the Oversight Committee. The Act does not contain any provisions regarding how the disclosed data (including biometrics) is to be treated after this validity period. Information is not publicly available on whether any release of biometric or demographic information has been mandated by the Oversight Committee so far.

During Parliamentary debate, certain Members argued that citing “national security” as an exception was ambiguous and liable to misuse. The term is not currently defined in either the Indian Penal Code or the National Security Code. Similar but distinct terms such as “public emergency” or “public safety” could be used, it was argued, as they are mentioned in other laws.

Members also discussed a purported lack of specificity in the data-sharing guidelines of the Act, which do not provide clarity on with whom, and in what form, data may be shared when concerning a national security breach. Concern was also raised with regard to lack of opportunities for individuals affected under the national security clause to present their case to, or to appeal the decision of, a court.

For these sections of the Act, the Rajya Sabha passed two amendments. The first amendment sought to replace the term “national security” with “public emergency or in the interest of public safety.” The second amendment proposed the addition of the Central Vigilance Commissioner (CVC) or the Comptroller and Auditor-General (CAG) to the Oversight Committee in charge of reviewing orders pertaining to the release of an individual’s biometric data. Neither of these amendments was accepted by the Lok Sabha.

Role of UIDAI

The Act lays out the governing structure and powers of the UIDAI. Under the Act, the UIDAI consists of a Chairperson, two part-time Members, and a Chief Executive Officer. Members must have at least 10 years of experience in a wide range of matters such as technology, governance, law, finance, or administration. The UIDAI is responsible for specifying the information to be collected under the Act, assigning and authenticating Aadhaar numbers, and specifying the use of Aadhaar numbers for delivery of subsidies and services.
The UIDAI has the power to frame rules governing:

1. The process of information collection and verification,
2. individual access to information,
3. data sharing and disclosure, and the alteration of personal information,
4. data privacy and security processes, and,
5. establishment of grievance redressal mechanisms.

The UIDAI has published detailed regulations governing enrolment, authentication, data security, and disclosure. These are discussed in Appendix 3.1.

User rights and obligations
An Aadhaar holder may request the UIDAI to provide access to her or his identity information, not including the core biometric information. The powers of the UIDAI to accept or deny such requests have not been defined under the Act. In addition, the Act allows Aadhaar holders to request the UIDAI to alter their demographic information in its records. The UIDAI may also require individuals to update their demographic information from time to time. Information is not publicly available about the number of such requests and how many of them were granted.

There exist certain safeguards for the user against misuse of data. The Act imposes a penalty on a data-requesting entity upon non-compliance with the data-storage and data-sharing provisions of the Act. The Act also states that only the UIDAI or its authorised officer can file a complaint before a court for offences defined under the Act. Individual Aadhaar holders cannot independently approach the courts for these offences. The UIDAI has so far filed at least two First Information Reports under the Act for illegal use of biometrics.34,35

The Rajya Sabha passed an amendment inserting a provision empowering individuals to opt out of Aadhaar and to ask for their personal records to be destroyed within 15 days. The Lok Sabha did not accept this amendment. Therefore, there is no provision for a resident to de-enroll from Aadhaar.

### Offences and penalties
Penalties are defined for impersonation and unauthorised conduct with regard to Aadhaar data. Individuals are prohibited from impersonating others to enrol or alter another’s details in the Aadhaar database. Similarly, individuals or bodies pretending to be authorised to collect personal information when not allowed to do so under the Act are also liable to be punished. Penalties for unlawful data storage and disclosure are summarised in Appendix 3.2 of this Chapter. Information is not publicly available about the number and nature of penalties that have been imposed under the Act.

### Legal Challenges

The Supreme Court is currently hearing three key challenges to the Aadhaar Act 2016 and the Aadhaar project more broadly. The judicial outcomes of these challenges hold significant import for the future of Aadhaar.

One challenge constitutes a writ petition filed on 6 April 2016 by Jairam Ramesh, a former Union Minister in the UPA government (2009-2014) and current Member of Parliament. The petition challenges the classification of the Aadhaar Bill as a Money Bill (see Figure 3.1 for a description of Money Bills). It argues that the bill does not fulfill the constitutional provisions for a Money Bill, and that the Speaker’s decision to classify a bill as such may be judicially reviewed in cases of a substantive infraction. There is no historical precedent for the Supreme Court nullifying the Parliament’s classification of a bill as a Money Bill. If the Court were to rule in favour of the petitioners, the Act may be struck down.

A second legal challenge consists of a series of individual petitions combined with a writ petition filed by Justice K.S. Puttaswamy, a retired High Court judge, challenging the Aadhaar project on various grounds. These petitions challenge the legality of collection of personal information on a large scale, the mandatory status of Aadhaar, and most significantly, potential violations of individual privacy engendered by Aadhaar.
No express right to privacy is currently afforded by the text of the Indian Constitution, and varying interpretations of whether such a right may exist have been offered by different court judgements. Various judgements delivered by benches of two or three judges from 1975 onwards have read it to be implicit in the fundamental right to life and liberty enshrined in the Constitution. However, older court judgements dating from 1954 and 1963 (delivered by larger benches) have observed there is no such right afforded under the Constitution.\textsuperscript{36}

The Supreme Court, recognising the divergent judicial verdicts on a right to privacy, has recommended the creation of a bench of at least five judges to settle the matter. The case is pending before the Court. Depending on whether, and how, the Supreme Court reads a right to privacy into the Constitution, this could have varying impact on the legality of the Aadhaar project and whether and how it is used for government service provision.

If a right to privacy were read into the Constitution—in accordance with more recent, but smaller-bench judgements of the Supreme Court—there may be an impact on procedural norms regarding the collection, use, and protection of individual data under Aadhaar. As some petitioners have argued, such a decision may allow individuals to choose to not hold an Aadhaar number, while still availing themselves of government services or interacting with government institutions. However, the implications (if any) of this challenge are unclear until the matter is heard and adjudicated by the Supreme Court.

A third set of petitions challenge Aadhaar’s mandatory linkage to the filing of income tax returns and the holding of a Permanent Account Number (PAN). This link was established by the Finance Act 2017. The petitioners have highlighted that the Aadhaar Act’s provisions do not require every citizen to hold an Aadhaar number (unless seeking to access government benefits), and the UIDAI has maintained that enrolment into Aadhaar is voluntary. According to the petitioners, the voluntary character of Aadhaar enrolment means it cannot be made mandatory for tax returns—which all citizens (above a certain income threshold) are legally bound to submit. In addition, petitioners have raised (1) the right to equality; arguing that the link creates two classes of taxpayers and discriminates against those without Aadhaar, (2) freedom of trade and practice; since the lack of a PAN inhibits individuals from engaging in basic transactions such as opening a bank account, and (3) the right to personal autonomy and self-determination of information disclosure. The Supreme Court is yet to deliver a final judgement on this case. The judgement will determine whether or not the concerned legal provision enforcing Aadhaar’s linkage to tax filing and PAN will stand as is. This will have an impact on the procedure for tax submissions and PAN card documentation for all taxpayers, effective from the current financial year.

The substance of these legal challenges points to important areas for future research.

\textbf{Figure 3.3: Privacy concerns with digital identities}

Digital identities, such as Aadhaar, carry a number of potential risks with regard to identity holders’ privacy. The World Bank highlights four important general concerns: (1) unauthorised access, use or disclosure of information, (2) profiling, through linking databases in illicit ways, including for surveillance objectives, (3) “function creep” whereby data collected for one or more reasons is used for others to which the identity holder has not consented, and (4) inaccuracies in data, leading to mistaken identity or unjust treatment.

Source: Identification for Development Strategic Framework, World Bank Group
Areas for Future Research

Aadhaar’s legal framework has seen significant change over the years. Legal challenges to Aadhaar’s legislative framework and use-cases await resolution, and associated judicial verdicts may reshape the contours of Aadhaar and its uses.

Multi-disciplinary research on Aadhaar’s legal and governance framework can benefit legislators and members of the judiciary as they make decisions on how Aadhaar should be governed, used, and safeguarded. This research may be used to strengthen the legal and regulatory framework for Aadhaar in particular, and digital identity more generally.

We present three important themes of future research:

- Research to improve the implementation of legal safeguards in the Aadhaar Act 2016, and independent and regular assessments of the quality of enforcement of Aadhaar’s legal protections to increase their effectiveness

- Research drawing on international privacy principles, domestic norms, and judicial precedent to inform court judgements and potential legislation on defining and safeguarding individual privacy—including, but not limited to, Aadhaar

- Research focused on informing a modern national data protection framework to strengthen the governance of digital information—including, but not limited to, Aadhaar

To maximise the impact of practitioner-oriented research, we recommend:

- Framing research questions in collaboration with practitioners
- Being responsive to decision-making schedules and other practitioner constraints
- Presenting insights in succinct documents and in-person meetings
- Providing follow-up support to translate research to action on-the-ground
APPENDIX 3.1: Regulations and Notifications on Aadhaar

Following the notification of the Aadhaar Act 2016, the government has introduced various regulations pertaining to the enrolment, authentication, and sharing of information, which have the status of delegated legislation. This Appendix provides a summary of key features of these regulations. The regulations discussed below were notified in September 2016.

Unique Identification Authority of India (Transaction of Business at Meetings of the Authority) Regulations 2016

These regulations provide details on the frequency with which UIDAI meetings shall take place, norms regarding scheduling meetings and notifying members, as well as conduct of meetings. They state that the four members of the Authority should meet at least three times a year. They also detail how the UIDAI will take decisions in these meetings. The UIDAI CEO is empowered to make decisions without the conduct of a meeting in certain urgent scenarios, subject to regulations. All decisions taken in the meeting are to be published online, barring cases in which the Chairperson deems that certain content is confidential.

Aadhaar (Enrolment and Update) Regulations 2016

These regulations set the standard for processes related to Aadhaar enrolment, including provisions on enrolment agencies and registrars, personal information to be collected, and specification of technologies used in the enrolment process. In particular, the regulations detail certain optional information that may be recorded (mobile number and email address) in addition to the biometric and demographic information specified in the Act. Additional information to be collected for children under the age of five, as well as individuals being enrolled through the “introducer” system or using the head of the family’s data, is also noted (see Chapter 2, Aadhaar Architecture, for details). Provisions discuss how to enroll individuals who are unable to provide biometrics.

The regulations also delve into norms regarding the generation of an Aadhaar number and its delivery to residents, updating resident information in the database, omission or deactivation of Aadhaar, and grievance redressal. In particular, Section 32 envisages a contact center to serve as a grievance redressal mechanism for the resolution of queries through calls and emails.

A 2017 amendment to this regulation states that UIDAI may authorise Registrars, Enrolling Agencies, and other service providers to collect a fee for updating demographic and biometric information.

Aadhaar (Authentication) Regulations 2016

These regulations contain rules on the types of authentication provided by UIDAI and provisions on the appointment and actions of authenticating agencies. A detailed discussed of authentication types is presented in Chapter 2, Aadhaar Architecture. The regulations detail the information authenticating agencies must provide to the Aadhaar holder, the procedure for obtaining consent, and capturing biometrics. They also outline certain data security norms for the operations of these agencies. They allow individuals to “lock” their biometrics, and unlock them only when required for authentication. All attempted biometric authentication against locked biometrics shall fail, unless biometrics are temporarily unlocked.

The regulations also state that authentication data shall be maintained for a period of six months and thereafter archived for a period of five years by the UIDAI. Authentication logs will be maintained...
by the requesting entity for a period of two years and archived for a period of five years.

A 2017 amendment expanded the eligibility criteria for appointment as a requesting entity to include airline operators.

**Aadhaar (Data Security) Regulations 2016**

According to these regulations, UIDAI may specify an information security policy setting out technical and organizational measures to be followed by UIDAI and its personnel as well as any and all associated agencies or service providers. The UIDAI shall be responsible for monitoring compliance with the information security policy and will designate a Chief Security Officer for this purpose. Regulations further require all agencies and service providers engaged by UIDAI to undergo audits by recognised entities at specified time periods.

**Aadhaar (Sharing of Information) Regulations 2016**

These rules specify norms regarding the sharing of personal information by UIDAI, authenticating entities, and others. They also specify restrictions on the sharing or circulating of Aadhaar numbers, and the liability for contravention of these regulations. The regulations stipulate that no core biometric information can be shared by UIDAI or stored by requesting entities. Requesting entities have also been directed to not use or share an individual’s Aadhaar number for purposes beyond which consent has been given.
### APPENDIX 3.2:
Offences and Penalties for Unauthorised Data Disclosure in the Aadhaar Act 2016

<table>
<thead>
<tr>
<th>OFFENCES</th>
<th>PENALTIES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DATA DISCLOSURE</strong></td>
<td></td>
</tr>
<tr>
<td>Intentional dissemination of identity information collected in the course of enrolment or authentication in a manner unauthorised by the Act (or ensuing regulations)</td>
<td>Imprisonment of up to three years, and/or a fine up to ₹1,00,000 (for individuals) and ₹1,00,000 (for companies)</td>
</tr>
<tr>
<td><strong>DATA IN THE CENTRAL IDENTITIES DATA REPOSITORY (CIDR)</strong></td>
<td></td>
</tr>
<tr>
<td>Intentional acts corresponding to: • Unauthorised access • Disruption/denial of authorised access • Unauthorised data extraction • Damage or destruction • Unauthorised disclosure • Theft or modification of computer source codes used by UIDAI</td>
<td>Imprisonment of up to three years, and a fine not less than ₹1,00,000</td>
</tr>
<tr>
<td><strong>OTHER</strong></td>
<td></td>
</tr>
<tr>
<td>Use or tampering of data in the CIDR or a removable storage device with the intent of modifying or discovering information related to an Aadhaar holder</td>
<td>Imprisonment of up to three years, and a fine up to ₹10,000</td>
</tr>
<tr>
<td>Use of an individual's identity information by a requesting entity in contravention to the Act</td>
<td>Imprisonment of up to three years, and/or a fine up to ₹10,000 (for individuals) and ₹1,00,000 (for companies)</td>
</tr>
<tr>
<td>Enrolment agencies or requesting entities failing to comply with the requirements of the Act</td>
<td>Imprisonment of up to one year, and/or a fine up to ₹10,000 (for individuals) and ₹1,00,000 (for companies)</td>
</tr>
<tr>
<td>Offences under the Act for which no specific penalties have been provided</td>
<td>Imprisonment of up to one year, and/or a fine up to ₹25,000 (for individuals) and ₹1,00,000 (for companies)</td>
</tr>
</tbody>
</table>
ENDNOTES


3. The evolution (and eventual coalescence) of disparate identity projects that formed the basis for Aadhaar is discussed in Chapter 2, Aadhaar Architecture.


7. Ibid.


9. Individuals to whom an Aadhaar number has not been assigned, must make an application for enrolment. These individuals shall be offered alternate and viable means of identification for the delivery of benefits.

10. The Speaker of the Lok Sabha certified this.


15. These refer to The Public Distribution System (PDS) and the Liquefied Petroleum Gas (LPG) subsidy. Ibid.


17. Ibid.


26. Delegated legislation refers to the rules created by empowered bodies to implement objectives laid out in primary or parent legislation (in this case the Aadhaar Act 2016).
31. Ibid.
32. Ibid.