The Internet Democracy Project [https://internetdemocracy.in] seeks to promote an Internet that supports free speech, democracy and social justice, in India and beyond. Through in-depth, quality research, we shed light on the challenges that the Internet poses for us all. Through advocacy and debate, we promote empowering solutions among policymakers and Internet users alike.

We have been engaging in research, government-led consultations and advocacy around the right to privacy in India, including from a gender perspective [https://genderingsurveillance.in].

Our submission to the United Nations High Commissioner for Human Rights on the report 'Right to Privacy in the Digital Age' are as follows:

I. Recent developments in national or regional legislation, case law, and practice concerning the right to privacy in the digital age.

Aadhaar, biometric identity database

Among recent developments, one of the most prominent are the developments around the biometric identity program, called 'Aadhaar'. Proudly touted as the largest identity project in the world, it combines a massive digital identity infrastructure that has not been designed with privacy in mind, with an unaccountable institution at the helm, making the project problematic at several levels. The Aadhaar database consists of demographic and biometric information of residents, linked to a unique twelve digit number, which is stored in a centralised manner.

This program is the tip of the spear when it comes to datafication of people's lives without consent and control. The program is governed by a legislation, Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016, that was brought into effect more than five years after the program was rolled out. The Act was tabled and passed as a 'money bill', circumventing proper parliamentary procedure for passing legislation.[1] The law allows for sharing of personal information and authentication records with intelligence agencies with no oversight, has an expandable definition of 'biometrics' that can include other invasive types of information and does not provide a recourse for misuse of data collected under the program.

The scope of the program has been expanding - the UIDAI now plans to implement facial recognition as an additional biometric authentication, starting from July 1 2018. This development is alarming in a country without a data protection framework.

Despite the sensitivity of the data, reports by journalists and security researchers, of government and private agencies flouting the Act by publishing a large number of persons'

[1] https://thewire.in/economy/the-aadhaar-act-is-not-a-money-bill

Aadhaar information, has been met with denials and persecution by the Unique Identity Authority of India.[2]

As a consequence of bad design and absent privacy safeguards, parallel databases of residents are being built by State authorities, using information collected at the stage of enrolment.[3] There is no law regulating the collection and use of this data at this time, and the Aadhaar Act does not apply to such extraneous use.

Data protection consultations

The other major development is a consultation for a data protection framework for India. At the moment, India does not have a data protection framework under which legitimate uses of data are identified and effective remedies for misuse are provided. In January 2018, a committee consisting of members, some of whom drafted the Aadhaar Act, concluded consultations on a data protection framework for India. According to news reports, a bill is expected to be filed in the Parliament by May 15.

Right to privacy a fundamental right under the Indian Constitution

The Supreme Court of India unanimously declared the right to privacy as a fundamental right under the Indian constitution in the Puttaswamy case. This positive development emerged from the challenge to the Aadhaar program on grounds of violation of privacy. However, the question of whether the Aadhaar project violates this right or not, is still under litigation. It should be noted that beyond privacy, there are other challenges to the Aadhaar program in the Supreme Court.[4]

While this judgment recognising the right to privacy comes as a relief, much depends on how it will be applied to decide about whether the Aadhar program's intrusion on the right to privacy has a legitimate State aim and is proportionate.

II. Surveillance and communications interception: Government surveillance, including, for example, communications interception and bulk data collection and processing, targeted intrusions in ICT systems and issues relating to cross-border surveillance and access to personal data.

There is a profound lack of transparency in the way that State surveillance is conducted in India. There are multiple mass surveillance programs that have been operational like the Central Monitoring System, NATGRID and CCTNS but there is barely any information about the workings of the program, the technology used, the institutions responsible for them and their operations or their budgetary allocations.

---

[2] https://in.reuters.com/article/india-aadhaar-breach/critics-of-aadhaar-project-say-they-have-been-harassed-put-under-surveillance-idINKCN1FX1SS

[3] https://medium.com/karana/the-360-degree-database-17a0f91e6a33

[4] https://thewire.in/government/aadhaar-privacy-government-supreme-court

At the moment, intelligence agencies are only subject to executive oversight, without any legal framework limiting their scope for surveillance. Further, the Aadhaar Act allows for sharing of information, including identity information and authentication records for the purpose of 'national security', an undefined term in the Act.

In its report submitted to the United Nations Human Rights Council for the Universal Periodic Review, the Ministry for External Affairs admits the mass surveillance system and defends it in the name of national security, safeguarding the law etc.:

> *55. India believes that its surveillance programme furthers its national security interests, and that safeguards in the law, including safe transmission of content, requirement for authorization from senior officials, and the existence of a Review Committee to oversee such authorizations, are sufficient to address concerns regarding privacy and freedom of speech. However, in recognition of the potential of such a system to impinge on the freedom of speech, the Government is in the process of legislating on right to privacy.*

Given the lack of transparency and burgeoning surveillance programs, it is crucial that the upcoming data protection framework apply to government agencies also, apart from private parties.

III. Encryption and anonymity as enablers for the enjoyment of human rights, including the right to freedom of expression and of opinion; challenges raised by encryption and anonymity and ways to address these challenges.

Encryption and anonymity are rightly recognised as important enablers of the right to freedom of expression. The right to anonymity is most important for persons who are vulnerable to reveal their identities for reasons of persecution. This includes persons of marginalised gender and sexualities.

The right to not be identified at all times is under heavy attack, due to the Aadhaar program. The relative anonymity afforded by unlinked databases has come under attack due to the networked identification of Aadhaar. For example, in a forthcoming study on the chilling effects of Aadhaar, our interviews confirmed that several persons are unable to avail of ART (anti-retroviral) treatment for HIV because an Aadhaar number is required.

Beyond the corrosion of anonymity by the government, the right comes under attack from corporate surveillance as well. The "authentic name" policy of Facebook requires users of the platform to identify oneself with their 'legal' names. This has enabled harassment not only of persons using pseudonyms, but also others using their legal names. Despite pushback from activists for many years, Facebook has retained this policy.

IV. National legislative and regulatory frameworks concerning the collection, processing, retention or use of personal data by Governments and other actors, in particular business enterprises, related human rights protection gaps and ways to bridge those gaps.

1. **Growing reliance on data-driven technology and biometric data:**
    1. **How can new technologies help promote and protect the right to privacy?**
    2. **What are the main challenges regarding the impact on the right to privacy and other human rights?**
    3. **What are the avenues for adequate protection of the right to privacy against threats created by those technologies? How can the international community, including the UN, address human rights challenges arising in the context of new and emerging digital technology?**

At the outset, important to note that there is no legislative or regulatory framework. There are numerous programs, both by central and state Governments that amass and process data, without regulation or retention limitation.

For example, there is a move to create a 'National Health Information Network', by linking Aadhaar to health information records.[5] These are troubling developments being undertaken even as multiple challenges to the Aadhar program are being contested in the Supreme Court.

A strong move from the government towards use of "Artificial Intelligence" (AI) is another occasion for pause. The report of the AI task force, constituted by the Ministry of Industry and Commerce, signals a continuation of the trend of the government in pushing for increased datafication. The report's national security agenda includes 'autonomous surveillance and combat systems' and outlines plans to use AI along with 'Aadhaar-enabled systems'.

V. Undue interferences with the right to privacy in the digital age that may have particular effects for women, as well as children and persons in vulnerable situations or marginalized groups, and approaches to protect those individuals.

Violation of privacy has different impacts on different persons, and affects some disproportionately. The impact of a denial of privacy is felt more heavily by persons with marginalised identities.

Although the Supreme Court declared the right to privacy a fundamental right, and placed primacy on autonomy and decision-making of an individual, only a few months later, it failed to strike down a challenge to the marriage of an adult woman with a man of her choice. In the case that came to be known as the 'Hadiya case', the marriage was eventually upheld. However,

[5] https://www.medianama.com/2018/03/223-disha-electronic-health-records/

the case showed that the right to make these personal choices for certain people can be in jeopardy from the State even when autonomy is considered a core aspect of the right to privacy.

Serious issues arise when it comes to the right to privacy in the digital age for women and sexual minorities. Instances of rape videos being sold, databases being created by sim card sellers of women buyers are reported. While there are protections in place where images are concerned [Section 66 E of the Information Technology Act, 2000], control over data is not provided for in the current laws.

In our research project 'Gendering Surveillance'[6], we undertook an inquiry into the uneven ways in which surveillance impacts people, on the basis of their gender. This of course, is one axis of differential impact, and there are many other axes that intersect with gender. In one of the case studies, we examined the phenomenon of mobile phone bans for young and unmarried women imposed by local self-governing bodies called *Khap* panchayats. In the study, we found that mobile phones create a space for privacy that did not heretofore exist, and this has left a ripple of anxiety in many areas where there is a high degree of control over women.[7]

VI. Procedural and institutional safeguards, oversight mechanisms and remedies available to individuals exposed to domestic or extraterritorial surveillance, the interception of digital communications or other forms of processing of personal data by governments, business enterprises or private organisations.

As already mentioned in answer 2, the Aadhaar Act is woefully inadequate for data protection, and ineffective where there are provisions imposing penalties for leaking Aadhaar data. While the Act prohibits an authenticating agency from collecting or using their information without their consent, many entities including government agencies have published Aadhaar details of several millions of persons.[8]

Even beyond Aadhaar, India lacks effective institutional safeguards and oversight mechanisms for domestic surveillance. The limited protections that are available in the Telegraph Act for targeted surveillance are effectively overridden because of infrastructure of mass surveillance programs.

Going forward, a framework for data protection cannot rely on consent of data subjects alone. We have argued in our submission[9] to the consultations on a data protection framework for

---

[6] https://genderingsurveillance.in

[7] https://genderingsurveillance.internetdemocracy.in/phone_ban/

[8] https://tech.economictimes.indiatimes.com/news/corporate/210-govt-websites-made-public-aadhaar-details-uidai/61719345

[9] https://internetdemocracy.in/reports/submission-in-response-to-the-white-paper-of-the-committee-of-experts-on-data-protection-framework-for-india/

India that there should be other mitigating mechanisms in the law (for example, allowing data collection for legitimate purpose only, as in the GDPR). Over the course of the last decade, many new articulations of the right to privacy are evolving in response to new technologies. It is important that many of these are incorporated in any new framework introduced. The right to explanation, introduced in the EU General Data Protection Regulation (GDPR), a right against profiling are other examples.