India Digital Freedoms Series

SURVEILLANCE AND DATA PROTECTION: THREATS TO PRIVACY AND DIGITAL SECURITY

BY MIRA SWAMINATHAN AND ARINDRAJIT BASU

PART 5 OF 5

Published October 2020

India Digital Freedoms Series

SURVEILLANCE AND DATA PROTECTION: THREATS TO PRIVACY AND DIGITAL SECURITY

Authors: Mira Swaminathan and Arindrajit Basu

This briefer on surveillance and data protection is part of the Centre for Internet & Society's Report on digital civic space in India, examining the effects of policy and legal frameworks on digital rights for Indian civil society. For more background and to read the rest of the report, click here.

Published in October 2020

In partnership with the International Center for Not-for-Profit Law

TABLE OF CONTENTS

I. INTRODUCTION

In recent times, the Indian state has attempted to design and deploy emerging technologies to capture and aggregate large tracts of data for the purpose of conducting surveillance on its citizens. A large number of objectives - largely driven by the 'trump card' of preserving national security - have been articulated to justify the creation of this dragnet. The expanded surveillance apparatus has a potential chilling effect on dissent and public participation - particularly when conducted in the absence of a clear legal framework restricting the powers of the government.

Interviews with journalists and other civil society activists revealed that over the past few years, there has been increased fear of state surveillance, leading to self-censorship and restraining public participation[1]. Many members of civil society felt that their phones had been tapped or that spyware had been used to track their messages. Journalists who worked on core national security questions - relating to defense, for example - felt especially targeted. Civil society activists felt that their research, particularly output that negatively portrayed the state, had to be altered or compromised due to growing surveillance.

Targeted surveillance of journalists, while receiving greater public attention due to the Pegasus scandal (discussed below), has long existed in India. In March 2016, a detailed report by the Editors Guild of India showed that journalists were unable to function fully in Bastar (a conflict region in south Chhattisgarh) due to, among other reasons, "a general perception that every single journalist is under the government scanner and all their activities are under surveillance"[2]. Journalists have chosen not to discuss anything over the phone, claiming that "the police are listening to every word we speak"[3].

Additionally, it is important to explore the sequence of events that has taken place in the Indian digital sphere concerning the question of information access by governments, and the undermining of privacy of secure communication channels (through 'traceability' or other measures). These issues implicate a particularly unique blend of competing policy interests, making it crucial that any potential regulatory reforms balance the same.

For instance, there is a long-drawn battle around the linking of social media accounts with India's national AADHAAR biometric identity, with civil society activists on both sides of the fence. Animal rights activist Antony Clement Reubin requested this linking via a Public Interest Litigation (PIL) in the Madras High Court filed in response to cyberbullying he faced by anonymous social media entities due to his stances against

1 On the other hand, a couple of journalists said that this did not tangibly impact their work. They admitted that the extent of fear a journalist feels is based on the protection that legacy media houses can provide them. Journalists working for legacy media houses felt much less threatened by surveillance than freelance journalists who do not enjoy the same protections.

2 Full text of report available at https://scroll.in/article/805866/not-a-single-journalist-working-without-fear-or-pressure-editors-guild-on-bastar.

3 Id.

Jalikattu - a traditional practice akin to bull-fighting, criticised for cruelty to animals[4]. Conversely, the Internet Freedom Foundation (IFF), a digital rights group, argued that linking state identity to online accounts would stifle free expression and aid government censorship and surveillance [5]. While the Madras High Court ultimately desisted from ordering such linkage, the question before the court was further expanded to examine whether enabling traceability for secure encrypted communication applications (including WhatsApp) would be possible[6].

For contrast, consider Subodh Gupta's case in the Delhi High Court. In the wake of #MeToo allegations, artist Subodh Gupta was implicated as an abuser by anonymous users, whose experiences were posted through the Instagram account @herdandscene. Subodh Gupta filed a defamation suit against the account; during the proceedings, the Court directed Instagram (through Facebook) to reveal the identities of the users running that particular account. This raised significant alarm, since doing so would successfully dilute the anonymity afforded by the internet to survivors of sexual abuse[7]. Facebook requested the Court to modify this part of the order, since they believed such order would "*[dissuade] not only sexual harassment victims from sharing their experiences in the future, but also whistle-blowers from reporting such unlawful acts*"[8]. In this case, an individual's right to reputation was weighed against the individual right to privacy. Ultimately, however, no clear resolution was reached as the case was settled out-of-court.

Given the nefarious threat that surveillance poses to civil society, public participation, and media, it is necessary to examine the impact of various surveillance technologies being used in India and analyze the legal framework that enables this surveillance.

Our analysis first looks at the various kinds of technology deployed by the state, often in conjunction with private actors to conduct surveillance on citizens and civil society. It moves on to examine the law and policy on surveillance in India, international law and practice in this area, and concludes with some recommendations.

4 Aditi Agrawal," Why Antony Clement Rubin petitioned Madras HC to link Aadhaar to social media accounts," Medianama,July 17,2019, https://www.medianama.com/2019/07/223-why-antony-clement-rubin-petitioned-madras-hc-to-link-aadhaar-to-social-media-accounts/.

5 "IFF files independent expert's submission before Madras HC on PIL relating to encryption and traceability," IFF, August 23, 2019. https://internetfreedom.in/iff-files-independent-expert-submission-before-madras-hc/.

6 "The future of Intermediary liability in India," sflc.in, January 2020, https://sflc.in/sites/default/files/2020-01/SFLC.in%20-%20Intermediary_Liability_Report_%282020%29_1.pdf

7 Mira Swaminathan "Personal Data Protection Bill 2019: A Man's Troll Is A Woman's Allegation," https://feminisminindia.com/2020/01/15/personal-data-protection-bill-2019/.

8 Ophelia Iai, Subodh Gupta Settles Defamation Case Over Instagram #Metoo Allegations, March 03, 2020, http://artasiapacific.com/News/SubodhGuptaSettlesDefamationCaseOverInstagramMeTooAllegations.

II. DESIGN AND IMPACT OF SURVEILLANCE TECHNOLOGY

The design of emerging technologies combined with the aggregation of Big Data (characterised by its three Vs-Volume, Velocity, and Variety enabling the construction of datafied identities of individuals by aggregating disparate strands of data)[9] has the potential to greatly increase the Indian government's ability to conduct surveillance, thereby suppressing dissent and augmenting power asymmetries between the state and the citizen. This ability, combined with an amorphous legal regime on surveillance, creates fear among citizens who believe that they are constantly subjects of the state's gaze. This section examines three case studies on surveillance through the use of emerging technologies.

Automated Facial Recognition Systems (AFRS)

Facial recognition is a biometric-enabled technology using cameras to match stored or live footage of individuals with images or videos collated in a pre-existing database[10]. It increasingly relies on machine learning, a form of artificial intelligence, to sift through still images or video of people's faces, and obtain identity matches[11]. The agency collating this data can use it for conducting sentiment analysis, identifying specific individuals, or generating demographic surveys.

Recently, the Ministry of Home Affairs, through the National Crime Records Bureau (NCRB) put out a tender for a new AFRS, with the declared objective of "acting as a foundation for a national-level searchable platform of facial images"[12]. The AFRS tender aims to pull facial image data from CCTV feeds and compare them with existing records across databases including the Crime and Criminal Tracking Networks and Systems (CCTNS), Inter-operable Criminal Justice System (or ICJS), Immigration Visa Foreigner Registration Tracking (IVFRT), Passport, Prisons, and state police records. Plans are also afoot to integrate this with the yet-to-be-deployed National Automated Fingerprint Identification System (NAFIS), thereby creating a multi-faceted surveillance system. While, as in other parts of the world, the Indian state has often cited national security, suggesting that these technologies have been deployed to protect citizens from various

9 O'Reilly Media, Volume, Velocity, Variety: What You Need to Know About Big Data, January 19, 2012, https://www.forbes.com/sites/oreillymedia/2012/01/19/volume-velocity-variety-what-you-need-to-know-about-big-data/#186d2ac71b6d.

10 Karl Ricanek Jr and Chris Boehnen, 'Facial Analytics: From Big Data to Law Enforcement' (2012) 45(9) Computer 95, 95.

11 Amos Toh, "Rules for a New Surveillance Reality," HRW, November 18, 2019, https://www.hrw.org/news/2019/11/18/rules-new-surveillance-realit.y

12 Available at http://ncrb.gov.in/TENDERS/AFRS/RFP_NAFRS.pdf.

threats, in reality surveillance technology have often been used to target government critics and members of civil society.

Potent use of this technology occurred during the Citizenship Amendment Act protests. Reports suggest that extensive video surveillance was run through facial recognition software to identify protesters, beginning from December 2019 when the protests were still nascent[13]. In March, after the outbreak of targeted violence in New Delhi, India's Home Minister Amit Shah admitted in Parliament that facial recognition technology had been used to identify rioters[14]. Video footage sent by citizens to the police was used to compare data against driver's licenses, voter ID, and "other government data" (it remains unclear what this data might be). Further, the government failed to disclose an accountable, equitable, and transparent process by law enforcement authorities to receive footage and compare it with the existing database.

This is not the first instance of AFRS being used by Indian authorities. Table 1 shows a list of different AFRS techniques used by various state governments, often in conjunction with a private actor.

TABLE 1

STATE	NAME OF APP	PURPOSE	PRIVATE SECTOR PARTNER
Punjab	Punjab Artificial Intelligence System	Tracks the whereabouts of a suspected criminal through digitised criminal records and automated facial recognition	Staqu
Telangana	None	Telangana State Election Commission will be using the app to prevent voter impersonation	None
Delhi	None	To screen "rabble-rousers" and "miscreants," most notably at the recent anti CAA protests	None
Gujarat	None	Vadodara City Police Department is planning to install a network of facial recognition cameras in public places such as railway stations, markets, bus depots, and parks to recognise offenders	Clearview AI

13 Anurag Kotoky, "Police Use Face-Recognition Software as India Protests Intensify", Bloomberg, December 28, 2019, https://www.bloomberg.com/news/articles/2019-12-28/police-use-face-recognition-software-as-india-protests-intensify.

14 Soumyarendra Barik, "Amit Shah: Facial recognition software fed with government data used to identify over 1,100 rioters", MediaNama, March 11, 2020, https://www.medianama.com/2020/03/223-facial-recognition-amit-shah-delhi-riots/.

The use of facial recognition software to identify individuals in public places has a chilling effect on public participation and free expression[15]. While the adverse impact has been felt by the citizenry writ large, the impact on civil society and public participation is particularly pronounced. For one, journalists and activists are increasingly being treated as criminals and being charged with draconian laws such as the Unlawful Activities Prevention Act (UAPA) with little to no evidence[16]. Surveillance technology that seeks to supposedly combat crime or screen "miscreants" abets oppression and aids the culture of suspicion and criminality that is increasingly being associated with any form of dissent.

Case law both in India and abroad has consistently maintained that the right to privacy is contextual and never surrendered just because one is in a public place[17]. However, jurisprudence and legislative or policy endeavours have failed to devise frameworks that protect against surveillance in public spaces through photography or videography[18]. A law that ensures the use of this technology in conformity with the key principles of legality, necessity and proportionality is certainly the need of the hour.

NSO and the Pegasus Spyware

The burgeoning linkages fueled by the global surveillance industry pose a threat to civil society activism and public participation in India as well. In the United States, WhatsApp's suit against the Israeli cyber-intelligence company, NSO Group Technologies (filed in a Northern California court) highlighted the pervasive grasp of global surveillance industries on civil liberties, and in particular, dissent all across the world. In its petition, WhatsApp alleged that the NSO group used the Pegasus spyware to carry out targeted surveillance on the cell phones of over 1400 lawyers and human rights activists

"Case law both in India and abroad has consistently maintained that the right to privacy is contextual and never surrendered just because one is in a public place."

15 Addison Litton, "The State of Surveillance in India: The Central Monitoring System's Chilling E s Chilling Effect on Self-Expr ect on Self-Expression", Washington University Law Review, 2015 https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1556&context=law_globalstudies, at 816.

16 Nikita Khaitan, "New Act UAPA: Absolute power to state," Frontline, October 25, 2019https://frontline.thehindu.com/cover-story/article29618049.ece.

17 AI Policy Exchange, "Automated Facial Recognition Systems and the Mosaic Theory of Privacy: The Way Forward," December 2019, https://aipolicyexchange.org/2019/12/30/automated-facial-recognition-systems-and-the-mosaic-theory-of-privacy-the-way-forward/.

18 Id.

worldwide, including in India[19].

NSO's claim that it only does business with governments has led to widespread suggestions that the Indian government was involved in using the spyware to target activists dissenting against the present government[20]. On November 29, 2019, the IT Minister, Ravi Shankar Prasad did not clearly refute the claim that the Indian government had deployed the spyware to target its own citizens, instead stating that "standard operating procedures ha[d] been followed"[21]. A report by the UN Special Rapporteur on the Freedom of Speech and Expression published even before the suit filed by WhatsApp has highlighted the global reach of the surveillance industry[22]. The global surveillance industry is a dangerous combination of states working with private sector actors that create and deploy surveillance technology to spy on citizens and activists around the world. A UN Special Rapporteur report recommends the use of global export-control arrangements to impose a moratorium on the continued export of technology that could be used for surveillance.

Aggregation of Non-Personal Data

The third surveillance vector is the aggregation of data that the government either holds or can legitimately access. Surveillance by the government is not the only concern here. Aggregated public data which can identify individuals could also threaten individual liberty and security. For example, there were widespread reports suggesting that the names and vehicle numbers of automobile owners on the Ministry of Road and Transportation's Vahaan public data were used by rioters to vandalise vehicles belonging to minorities during the February 2020 communal riots in North East Delhi[23]. Cars belonging to individuals with Muslim first or second names were allegedly targeted specifically for this purpose. While the reports failed to adduce tangible proof that this method was used, the scope for misuse certainly remains. This also opens the possibility for miscreants to acquire the personal information of civil society activists to target and intimidate them.

19 Erik Manukyan, "Summary: WhatsApp Suit Against NSO Group," Lawfare, November 7, 2019, https://www.lawfareblog.com/summary-WhatsApp-suit-against-nso-group.

20 Gurshabad Grover, Tanaya Rajwade, "Pegasus snoopgate, an opportune moment to revisit legal framework governing state surveillance framework," Indian Express, December 25, 2019 https://indianexpress.com/article/opinion/columns/pegasus-WhatsApp-surveillance-data-protection-6183355/.

21 Id.

22 "UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools", https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736.

23 Sreemoyee Mukherjee, "How Poor Data Protection Can Endanger Communities During Communal Riots" The Wire, March 6, 2020, https://thewire.in/rights/vahan-database-protection-riots, https://www.indiatimes.com/news/india/mobile-apps-allegedly-used-to-identify-owner-and-torch-vehicle-this-allegation-is-alarming-507271.html.

Contact Tracing Apps

In response to the ongoing COVID-19 pandemic, India implemented a lockdown on 24 March 2020[24]. Since then, a number of measures have been taken to control the spread of the virus, including contact tracing applications to contain the speed of virus spread[25].

Contact-tracing applications have been implemented by both the Central and state governments[26]. For instance, the state of Karnataka introduced the "Corona Watch" application, which requires an individual's location, media storage and network to show the broad areas in which persons are quarantined and also inform users of the places visited by a person who has tested positive for COVID-19[27]. The Karnataka government also launched an application called "Quarantine Watch," requiring quarantined individuals to send a selfie on an hourly basis, which would then be geo-tagged and reviewed by a specific team[28].

Similarly, the State of Maharashtra launched "Maha Kavach," an application to improve contact tracing and track quarantine compliance. The App provides details regarding all of the public places someone who tested positive for COVID-19 visited, and also enables the selfie attendance and geo fencing features[29]. Meanwhile, the State of Goa launched a GPS-based tracking "Covid-Locator" App, which tracks quarantined persons and identifies their movements[30].

While State governments were introducing their versions of contact tracing apps, the Central government launched Aarogya Setu in April to obtain location details of users and the persons with whom they come in contact[31]. The App seeks to collect personal details such as name, gender, health status, travel history and even obtains the user's contact list to determine the "risk status of users." This information is intended to help

24 Vaishnavi Chandrashekhar, "1.3 billion people. A 21-day lockdown. Can India curb the coronavirus?", Science Magazine, Mar. 31, 2020, https://www.sciencemag.org/news/2020/03/13-billion-people-21-day-lockdown-can-india-curb-coronavirus.

25 Samarth Bansal, "India is pinning hopes on apps in virus fight," Livemint, April 10, 2020, https://www.livemint.com/news/india/india-is-pinning-hopes-on-apps-in-virus-fight-11586447095280.html. Contact tracing applications track individuals who are infected, or who have come in contact with those individuals and ensures that every individual who is a potential carrier can be tested and quarantined before further spread. See Divya Siddarth, "How Can COVID-19 Contact Tracing Techniques be Formulated Without Violating Privacy?", The Wire, April 7, 2020, https://thewire.in/tech/covid-19-contact-tracing-privacy.

26 Abhik Sengupta, "Coronavirus Apps: Every App the Central Government And States Have Deployed to Track COVID-19", Gadget360, April 7, 2020, https://gadgets.ndtv.com/apps/features/central-state-governments-launch-coronavirus-mobile-app-list-2204286.

27 "'Corona Watch' app launched," The Hindu, March 28, 2020, https://www.thehindu.com/news/national/karnataka/corona-watch-app-launched/article31193062.ece

28 Samreen Ahmad,"Quarantine watch: Karnataka uses apps to keep track of people under watch" Business Standard, Apr 3, 2020, https://www.business-standard.com/article/technology/quarantine-watch-karnataka-uses-apps-to-keep-track-of-people-under-watch-120040201641_1.html.

29 Alok Deshpande, "Mahakavach to ease contact tracing load," APRIL 02, 2020 https://www.thehindu.com/news/cities/mumbai/mahakavach-to-ease-contact-tracing-load/article31231782.ece.

30 "Goa govt launches 'COVID-Locator' app to track home quarantine people," HT Science, April 5, 2020, https://tech.hindustantimes.com/tech/news/goa-govt-launches-covid-locator-app-to-track-home-quarantine-people-story-xBJvv1Ssnt5fUaR90oY3HP.html.

31 Abhik Sengupta, "Government Launches Aarogya Setu COVID-19 Tracker App on Android, iOS," April 2, 2020, https://gadgets.ndtv.com/apps/news/aarogya-setu-covid-19-tracker-app-coronavirus-launch-indian-government-android-ios-2204804.

health authorities manage infection outbreaks[32]. With over 75 million downloads[33], Aarogya Setu quickly became one of the fastest downloaded applications[34]. The App was made "mandatory"[35] for certain public sector employees who were forced to download the application, while in some cities people were penalized for not having the application[36].

While a contact tracing app can be viewed as a necessary tool to manage a public health crisis on this scale, it cannot be implemented without ensuring the protection of civil liberties. A rights-respecting legal framework and implementation structure and the realignment of privacy priorities can ensure that the public interest and individual liberties are respected, without a significant tradeoff[37]. Guidelines published by civil society organizations, for example Access Now's "Recommendations on privacy and data protection in the fight against COVID-19"[38], note that contact tracing apps should be voluntary, have clear privacy and security features by design, use open source protocols, develop and implement information user principles, limit data storage and ensure transparency and remedy for any data breaches[39]. Countries that do not adhere to these practices may instead end up using these applications as tools for mass surveillance, further deteriorating civic freedoms[40].

> *"There is an adage that moves in the tech space which is - move fast, break things and then maybe patch them later, launch and iterate - and this can be hugely problematic when it comes to public health space"*[41].

India's introduction to Aarogya Setu has quite clearly followed the pattern stated above. Clarifications around privacy were released a month after the app had already been launched[42], prompted in part by a French hacker's identification of many vulnerabilities

32 Shashank Mohan, "No Covid-19 silver bullet: Aarogya Setu endangers India's privacy – and its usefulness is uncertain," The Scroll, May 12, 2020, https://scroll.in/article/961641/no-covid-19-silver-bullet-aarogya-setu-endangers-indias-privacy-and-its-usefulness-is-uncertain.

33 "75 million people have already downloaded Arogya Setu app," Express Computer, April 27, 2020 https://www.expresscomputer.in/egov-watch/75-million-people-have-already-downloaded-arogya-setu-app/54093/.

34 *Supra* note 36.

35 Ravi Agarwal, "The Pandemic Is Enabling Big Brother," Foreign Policy, May, 5, 2020, https://foreignpolicy.com/2020/05/07/india-coronavirus-pandemic-big-brother-contact-tracing-mobile-app/.

36 Pranav Dixit, "An Entire City Has Been Told To Download A Controversial Contact Tracing App — Or Face Jail," Buzzfeed, May 6, 2020, https://www.buzzfeednews.com/article/pranavdixit/india-coronavirus-aarogya-setu-noida-contact-tracing.

37 "A comprehensive look at Covid Surveillance and Privacy in India #SaveOurPrivacy" https://internetfreedom.in/a-comprehensive-look-at-covid-surveillance-and-privacy-in-india/.

38 "RECOMMENDATIONS ON PRIVACY AND DATA PROTECTION IN THE FIGHT AGAINST COVID-19," accessnow.org, March 2020, https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf.

39 "Privacy and public health: the dos and don'ts for COVID-19 contact tracing apps," accessnow.org, May 4, 2020, https://www.accessnow.org/privacy-and-public-health-the-dos-and-donts-for-covid-19-contact-tracing-apps/.

40 Bhaskar Pant and Amit Lal. "Aarogya Setu App: A Tale of the Complex Challenges of a Rights-Based Regime," The Wire, May 11, 2020 https://thewire.in/tech/aarogya-setu-app-challenges-rights-based-regime.

41 Govindraj Ethiraj, "Interview: Is Aarogya Setu a tool for Covid-19 contact tracing or mass surveillance?," The Scroll, April 30, 2020, https://scroll.in/article/960566/interview-is-aarogya-setu-a-tool-for-covid-19-contact-tracing-or-mass-surveillance.

42 "Govt issues clarification on privacy concerns of Aarogya Setu app," The Telegraph, May 6, 2020, https://www.telegraphindia.com/india/govt-issues-clarification-on-privacy-concerns-of-aarogya-setu-app-after-hacker-flags-issue/cid/1770820.

in the system that could lead to major privacy breaches. One of the concerns is that location data are directly collected by the government from service providers, with a high possibility of the use and abuse of these particular data[43]. Apart from state surveillance, such information could reach markets wherein third parties could use it for anything from advertising to leaking of such information to surveillance actors[44]. One feature of the app "designed to let users check if there are infected people nearby, instead allows users to spoof their GPS location and learn how many people reported themselves as infected within any 500-meter radius"[45]. In sparse areas, any hacker could use a "triangulation attack" and figure out the diagnosis of the users of that area[46]. The intended use of the app has numerous implications for privacy and the potential to lead to mass surveillance by both public and private actors[47]. The lack of a data protection law, the unwillingness of the government to follow transparency practices and other structural problems have contributed to the rise of apps like Aarogya Setu, which are imposed on the general public with little state accountability[48]. India was the first democracy to make a contact tracing app mandatory[49]; though these policies were later relaxed in a protocol released by the Government[50], a surveillance system with long lasting impact has already been created and cannot be undone easily[51].

"The lack of a data protection law, the unwillingness of the government to follow transparency practices and other structural problems have contributed to the rise of apps like Aarogya Setu, which are imposed on the general public with little state accountability."

43 Anurag Mehra, "Contact Tracing, Location Data Markets and the Perils of Being Tracked," The Wire, May, 24, 2020, https://thewire.in/tech/contact-tracing-location-data-markets-and-the-perils-of-being-tracked.

44 Id.

45 Andy Greenberg, "India's Covid-19 Contact Tracing App Could Leak Patient Locations," June 5, 2020, https://www.wired.com/story/india-covid-19-contract-tracing-app-patient-location-privacy/.

46 Id.

47 Id.

48 Patrick Howell O'Neill, "India is forcing people to use its covid app, unlike any other democracy," MIT Tech Review, May 7, 2020, https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/.

49 NILESH CHRISTOPHER, "India made its contact tracing app mandatory. Now people are angry," May 14, 2020, https://www.wired.co.uk/article/india-contact-tracing-app-mandatory-arogya-setu.

50 "Who Is My Aarogya Setu Data Shared With? Govt Group Releases Data Protocol," The Wire, May 11, 2020, https://thewire.in/tech/aargya-setu-share-data-access-protocol.

51 Sidharth Deb, "Privacy prescriptions for technology interventions on Covid-19 in India," Internet Freedom, https://docs.google.com/document/d/1nDoPzygQyTetEguOlzula5O9y5f3f5YJDsA2Pd99O6U/edit.

VICTORY OF CIVIL SOCIETY ORGANIZATIONS IN REDUCING THE SURVEILLANCE IMPACT OF AAROGYA SETU

Many privacy activists and advocates have been fighting against Aarogya Setu's overarching surveillance structure. Given the fact that the country was in lockdown, online convenings, sharing of articles and collaborative documents were used as tools of protest, which underscores our assertion that notwithstanding the threats to digital freedom, online spaces remain a critical forum for the preservation of democratic processes. While the Internet Freedom Foundation is litigating a case in the Kerala High court against the mandatory use of Aarogya Setu[52], the Internet Democracy Project is maintaining a tracker collecting the notifications and frameworks that make the App mandatory[53]. Amongst such persuasive initiatives were over 45 organizations and more than 100 prominent individuals[54] joining together against mandatory use of the Aarogya Setu app. The organizations included trade unions, research centres and gender justice collectives. This joint representation was in response towards a direction given by the Home Ministry demanding "100% coverage" of the app in public offices and a penal provision for any disobedience[55]. In a signed letter sent to the Prime Minister's office on the 1st of May 2020, these organizations detailed the need to follow best international practices while implementing contact tracing apps, as well as the proportionality test established in noted Supreme Court judgement *Justice K. Puttaswamy v Union of India*[56].

As a result of civil society advocacy, the Ministry of Home Affairs released a Protocol on data security practices diluting the mandatory provision of Aarogya Setu to a "best effort basis"[57].

52 "Kerala High Court hears challenges against mandatory imposition of Aarogya Setu," INternet Freedom Foundation, May 112, 2020, https://internetfreedom.in/kerala-hc-hears-challenges-against-mandatory-imposition-of-aarogya-setu/.

53 Tanisha Ranjit, "When and where is Aarogya Setu mandatory? We're keeping track," May 8, 2020, https://internetdemocracy.in/2020/05/aarogya-setu-tracker/.

54 "45 organizations and more than 100 prominent individuals push back against the coercion of Aarogya Setu", May 2, 2020, https://internetfreedom.in/45-organizations-and-105-prominent-individuals-push-back-against-the-coercion-of-aarogya-setu/.

55 Id.

56 https://drive.google.com/file/d/1ELi-Q9FG-eapNFEzVeuJqTROFFrUflT3/view

57 "Aarogya Setu : MHA Dilutes Mandatory Imposition; Says Employers On 'Best Effort Basis' Should Ensure Use Of App By Employees With 'Compatible Mobile Phones" May 17, 2020, https://www.livelaw.in/top-stories/aarogya-setu-mha-dilutes-mandatory-imposition-156921.

III. RELEVANT DOMESTIC LAWS

The legislative framework of India's surveillance laws dates to the colonial era.[58] The specific legislation that authorizes surveillance is as follows:

The Indian Telegraph Act, 1885 and Rules

The interception of post and telegraph/telephone is governed by the provisions of the Telegraph Act. *Section 5(2)* requires a two-fold test that must be satisfied for the Central or State Government to authorise the interception of messages. First, there should be a public emergency or interest of public safety. Second, the interception must be "necessary or expedient" in the interests of the sovereignty and integrity of India, the security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence. Rule 419A of the Indian Telegraph Rules states details regarding the process to be followed before, during, and subsequent to the interception. This includes the relevant sanctioning authority that can issue such an order; the review process; and the total duration of the interception order.

Apart from these laws, certain license agreements issued under the Act such as the Unified Access Service License (UASL), Internet Service License (ISL), and the Unified License (UL) Cellular Mobile Telephony Services (CMTS) License act as an agreement between the Department of Telecommunications and telecommunications service providers. These agreements empower the government to receive assistance from telecommunication service providers in conducting surveillance. For example, Section 41.09 of the CMTS license allows the security agency to acquire call data records of all specified calls for a specified period of time as requested by the agency.

The Information Technology Act, 2000 and Rules

The IT Act provides legal recognition to transactions via electronic exchange of data and other electronic means of communication. Section 69 of the Act permits authorized agencies to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource, without the prerequisites of public emergency or public safety. Section 69(3) imposes an additional obligation on intermediaries and maintainers of computer systems to extend all facilities and technical assistance to the intercepting agency. Section 69B of the Act empowers the Central Government to authorise any government agency to monitor and collect traffic data for cyber security and identification, analysis, and prevention of any intrusion or

58 This session was adapted from an excellent study by NIPFP. See Rishabh Bailey, Vrinda Bhandari, Smriti Parsheera, Faiza Rahman," Use of personal data by intelligence and law enforcement agencies," (August, 2018) https://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf

spread of computer contaminants in the country. Further, the procedural aspects of interception and decryption are laid out in the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009[59], which were issued under section 69(2) of the Act.

Code of Criminal Procedure, 1973

Section 91 of the Code of Criminal Procedure empowers a Court or any officer in charge of a police station to summon any document or any other thing from a person, if it is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under the Code. Section 92 regulates the interception of a document, parcel or thing in the custody of a postal or telegraph authority.

Model Police Manuals[60]

The Model Police Manuals were issued by the Bureau of Police Research and Development to provide specific instructions pertaining to conduct and governance of the Police Force. Rule 6(2) of the Manual states that surveillance and checking of "bad characters" is considered as one of the duties of the police force to maintain peace and security in the community. Further, Rule 1052(1) of this Manual requires a history sheet to be maintained with the names of all persons within the limits of the police station "who are known or are believed to be addicted to or aid or abet the commission of crime," regardless of whether they have been convicted or not.

TABLE 2: SYSTEMS AND AGENCIES FOR CARRYING OUT SURVEILLANCE IN INDIA.[61]

SYSTEMS AND AGENCIES	FUNCTIONS
Central Monitoring System	Centralized telephone interception provisioning system to automate government-approved lawful interception and monitoring of telecommunications
National Intelligence Grid	Integrated master database used for counterterrorism purposes connecting data of core security agencies under GoI
Intelligence Bureau	Internal intelligence agency focusing on executing counter-intelligence and counter-terrorism tasks
Narcotics Control Bureau	Nodal drug law enforcement and intelligence agency of India responsible for fighting drug trafficking and the abuse of illegal substances
Directorate of Enforcement	Law enforcement agency and economic intelligence agency responsible for enforcing economic laws and fighting economic crime in India

59 Available at: https://cis-india.org/internet-governance/resources/it-procedure-and-safeguards-for-interception-monitoring-and-decryption-of-information-rules-2009,

60 Power to do so derived from Article 246(3) of the Constitution of India, read with Entry 2, List II, of the VIIth Schedule.

61 Ibid

Other agencies include: the Directorate of Revenue Intelligence, the Central Bureau of Investigation National Investigation Agency Research & Analysis Wing (R&AW), the Directorate of Signal Intelligence, and the Ministry of Defence - for Jammu & Kashmir, North East & Assam Service Areas only.

Privacy and Surveillance

Increasing levels of surveillance, without adequate protective measures, diminish the privacy rights of individuals. To understand this better we can analyze the various judicial pronouncements in India that developed the jurisprudence of the right to privacy versus surveillance. The first pronouncement came in Kharak Singh v. State of UP[62], which questioned the range of surveillance activities carried out under the UP Police Regulations. While the Hon'ble Court upheld certain provisions (such as the one relating to secret picketing), it struck down provisions that encouraged night-time domiciliary visits. While the Court maintained that such visits are beyond the liberties enshrined under Article 21 (Right to Life), it did not hold privacy to be a fundamental right under the Constitution.

In the case of PUCL v Union of India[63], the Supreme Court issued guidelines to tailor restrictions on privacy in a case challenging Section 5(2) of the Telegraph Act allowing for the wiretapping of phones. The Court, while upholding the provision, outlined a series of guidelines to identify the restrictions on privacy caused by phone wiretapping. In *K Puttaswamy v. Union of India*[64], the Supreme Court affirmed the fundamental right to privacy as an integral part of Article 21 and Part III of the Indian Constitution. Nevertheless, the Court held that the right to privacy is not absolute, and that the State may reasonably restrict privacy for legitimate aims, varying from protecting national security to encouraging innovation in society. Further, it laid down parameters for possible restrictions on the right to privacy through the test of proportionality under Article 21, which includes legality, legitimate goals, proportionality and procedural guarantees.

62 8(1964) 1 SCR 332.

63 AIR 1997 SC 568

64 (2017) 10 SCC 1

IV. INTERNATIONAL STANDARDS

The international law around surveillance technology continues to evolve, as technological advances and new applications - such as contact tracers during the COVID-19 pandemic - develop. That said, much of the relevant law in this area relates to privacy, which is a well-established right under international law.

Numerous human rights treaties establish a fundamental right to privacy. This includes the ICCPR, which states that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation," and furthermore that "[e]veryone has the right to the protection of the law against such interference or attacks"[65].

Such sentiments are reiterated in the Universal Declaration of Human Rights (Article 12), as well as the Convention on the Rights of the Child (Article 16) and the Convention on the Rights of Persons with Disabilities (Article 22), which India has ratified or acceded to (in addition to the ICCPR). The International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families also has a privacy protecting provision (Article 14).

The right to privacy is further guaranteed under various regional instruments, including the Charter of Fundamental Rights of the European Union (Article 7), the Arab Charter on Human Rights (Articles 16 and 21), the American Convention on Human Rights (Article 11), the European Convention of Human Rights (Article 8), and the American Declaration on the Rights and Duties of Man (Article V).

Taken together, "there is little doubt that this [privacy] right applies to a state's domestic collection of data about a person when that collection constitutes 'interference'"; furthermore, "many would agree that correspondence includes a person's online and telephonic communications"[66]. The right to privacy has evolved to include specific rights to access and control of one's personal data[67], and quite clearly applies when a state is conducting domestic surveillance[68].

Soft law and guidelines from regional and international bodies provide additional instruction with respect to the scope of privacy rights. According to European Court of

65 International Covenant on Civil and Political Rights art. 17(1), adopted Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR].

66 Ashley Deeks, An International Legal Framework for Surveillance, 55 Virginia J of Intl L: 291, 305 (2015).

67 Manfred Nowak, U.N. Covenant on Civil and Political Rights: CCPR Commentary at 388 (2005).

68 Deeks, supra note 300, at 311.

Human Rights (ECtHR) case law, any interference with an individual's privacy rights must be necessary in the circumstances of the case and proportional to the end sought, and the surveillance must be conducted under specific and clearly defined laws[69]. The principles of necessity, proportionality, and legality with respect to surveillance have been clearly set forth and defined in a number of other international instruments. This includes the U.N. General Assembly Resolution on the Right to Privacy in the Digital Age 69/166 (2014), which notes "in particular that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and nondiscriminatory and that any interference with the right to privacy must not be arbitrary or unlawful"[70]. A 2017 U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, further recognizes the need to consider "procedural safeguards, effective domestic oversight and remedies, the impact of surveillance on the right to privacy and other human rights, as well as the need to examine the principles of non-arbitrariness, lawfulness, legality, necessity and proportionality in relation to surveillance practices"[71].

With regard to issues of accessibility and secrecy, a report of the Office of the United Nations High Commissioner for Human Rights states that

> *secret rules and secret interpretations …– even secret judicial interpretations – of law do not have the necessary qualities of "law". Neither do laws or rules that give the executive authorities, such as security and intelligence services, excessive discretion… The secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn, demands greater precision in the rule governing the exercise of discretion, and additional oversight*[72].

The report recognizes, as a best practice, states who require that the legal framework for any surveillance be established through primary legislation debated in parliament, rather than simply subsidiary regulations enacted by the executive – "a requirement that helps to ensure that the legal framework is not only accessible to the public concerned after its adoption, but also during its development, in accordance with article 25 of the ICCPR"[73].

With respect to actual data protection, the European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data provides an illustrative example, requiring that any personal data undergoing automatic processing shall be, among other requirements, "obtained and processed fairly and lawfully; stored

69 Marko Milanovic, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, HARV. INT'L L.J. (2015), http://ssrn.com/abstract=2418485.

70 U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (18 December 2014).

71 U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/L.7/Rev.1 (22 March 2017).

72 Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014).

73 Id.

for specified and legitimate purposes and not used in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are stored"[74]. It additionally provides individuals the right to obtain access to personal data relating to them, and to rectify or erase such data as required[75]. The EU's General Data Protection Regulation (GDPR), although weakened by numerous industry and lobbying interests, contains some of these personal data protections.

Additional guidance can be found in the Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980, updated in 2013, which generally calls upon member countries to "demonstrate leadership and commitment to the protection of privacy and free flow of information at the highest levels of government"[76], among other international obligations.

As technologies such as AI and facial recognition software develop, the OECD and the European Union have also formulated relevant ethics-based guidelines around AI. These guidelines call for transparency, privacy and good data governance, and disclosure of a system's internal logic and real-life impact[77].

There are some promising models of laws regulating AI-based technologies like facial recognition software, such as a surveillance oversight law from Oakland, California. Under Oakland's law, government agencies must provide public documentation of what the technologies are, how and where they plan to deploy them, why they are needed and whether there are less intrusive means for accomplishing the agency's objectives[78]. The law also requires safeguards, such as rules for collecting data, and regular audits to monitor and correct misuse. Such information must be submitted for consideration at a public hearing, and approved by the City Council before technology may be acquired[79]. This process institutionalizes public participation and consultation in this type of decision-making, promotes transparency, and insures a broad discussion of whether a technology threatens privacy or might disproportionately affect the rights of marginalized communities. As a result of open consultation processes, governments in certain municipalities in the U.S. have decided to ban facial recognition technology,

74 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.I.1981, art 5.

75 Id. at art 8.

76 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980, updated in 2013, https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

77 See, e.g., Ethics guidelines for trustworthy AI, EC, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

78 Oakland City Council / Rules for Surveillance Use / 4.26.2018, Ordinance Adding Chapter 9.64 to the Oakland Municipal Code Establishing Rules for the City's Acquisition and Use of Surveillance Equipment, https://assets.documentcloud.org/documents/4450176/View-Supplemental-Report-4-26-18.pdf.

79 Id.

V. CONCLUSIONS AND RECOMMENDATIONS

as in Oakland, San Francisco, California, and Somerville, Massachusetts[80].

India's surveillance ecosystem is enabled by multiple policy instruments and various technological innovations, and is often used to hinder civic participation by fostering an atmosphere of uncertainty, or identifying and targeting communities that are triggering movements routed in public participation. Given the significance of privacy and dissent in India's fundamental rights ethos, it is important for the legislature and judiciary to craft policy that prevents excessive state surveillance. These policies need to be rooted in the universally recognised human rights standards of legality, necessity and proportionality. With this in mind, policymakers should pursue surveillance reform that enables the flourishing of India's democratic fibre while still safeguarding national security.

Despite the progressive judgement of the Supreme Court in *Puttaswamy v. Union of India* that sets standards for privacy invasions comparable to those in international human rights law, broad legal reform of state surveillance is still awaited. Rather than reign in state surveillance powers in the Personal Data Protection Bill, the Government is aiming to include a broad exemption for government agencies from complying with data protection provisions as long as the Central government deems it "necessary and expedient." In contrast to a prior draft put forward by the Srikrishna Committee in 2018 that used the term "necessary and proportionate, the new language gives the government unfettered powers to occlude provisions of the Bill which have been designed to protect citizen privacy. Urgent attention is needed to align the state surveillance mechanisms in India to adhere to privacy standards of legality, necessity and proportionality as legal thresholds in international human rights law and Indian constitutional law.

80 Sarah Ravani, Oakland bans use of facial recognition technology, citing bias concerns, San Francisco Chronicle, July 17, 2019, https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php; Dave Lee, San Francisco is first US city to ban facial recognition, BBC News, 15 May 2019, https://www.bbc.com/news/technology-48276660#:~:text=Legislators%20in%20San%20Francisco%20have,transport%20authority%2C%20or%20law%20enforcement; By Sarah Wu,Somerville City Council passes facial recognition ban, Boston Globe, June 27, 2019, https://www.bostonglobe.com/metro/2019/06/27/somerville-city-council-passes-facial-recognition-ban/SfaqQ7mG3DGulXonBHSCYK/story.html.

Additionally, some solutions could be use-case and technology specific. For example, dual use technologies should be restricted due to the uncertainty they cause for lawyers and activists engaging in public participation, while also giving the government entities and private actors access to information that may be used to stifle dissent. Non-personal data needs to be adequately safeguarded to prevent the misuse of aggregated data by state or non-state actors. The report of the Gopalakrishnan Committee on Non-Personal Data marks a first step towards protecting privacy in this context but several questions remain.

At the same time, the state should recognize the continuing validity of constitutional principles for governing technologies, which apply regardless of the use case. A recent draft report by NITI AAYOG emphasizes the significance of these principles in shaping the governance of AI; however, deeper thinking on this issue is needed to identify the precise contours of harm, and how the constitution can guard against it. An ad hoc or incomplete policy framework allows the government of the day to target those who dissent against it, thereby undermining this constitutional fabric.

For civil society, it is clear that the solution lies in continuous advocacy for these reforms. The rollback of the mandate to download Aarogya Setu was a product of concerted civil society activism both in online spaces and litigating the matter in courts. Such concerted attempts have been successful abroad as well. NGOs working on dual use surveillance technology have taken the matter to the UN, with the hope that nation states will harness export control regimes to regulate and constrain these technologies. Similarly, concerted public resistance to algorithmic assessments of the grades of A level students in the UK inadvertently adversely impacting those from lower socio-economic backgrounds caused the government to backtrack. Concerted civil society efforts such as these continue to hold promise and present a way forward.

ICNL

Made possible with the support of the International Center for Not-for-Profit Law
www.icnl.org