Responses to Information Requests

Responses to Information Requests (RIR) are research reports on country conditions. They are requested by IRB decision makers.

The database contains a seven-year archive of English and French RIR. Earlier RIR may be found on the UNHCR's Refworld website.

Please note that some RIR have attachments which are not electronically accessible here. To obtain a copy of an attachment, please e-mail us.

Related Links

- Advanced search help

IND106120.E

25 June 2018

India: Surveillance by state authorities; communication between police offices across the country, including use of the Crime and Criminal Tracking Network and Systems (CCTNS); categories of persons that may be included in police databases; tenant verification; whether police authorities across India are able to locate an individual (2016-May 2018)

Research Directorate, Immigration and Refugee Board of Canada, Ottawa

1. Surveillance

According to sources, surveillance schemes have been implemented in India in order to tackle crime and terrorism (openDemocracy 10 Feb. 2014; Privacy International Jan. 2018). Sources indicate that the Central Monitoring System (CMS) is a surveillance programme in India (The Wire 2 Jan. 2018; CIS 14 June 2018).
1.1 CMS

In correspondence with the Research Directorate, a representative of the Centre for Internet and Society (CIS) [1] stated that the CMS is a Central Government project to intercept communications, both voice and data, that is transmitted via telephones and the Internet to, from and within India. … It must be clearly understood that no public documentation exists to explain the scope, functions and technical architecture of the CMS. (CIS 14 June 2018)

According to Human Rights Watch, the Indian government launched the CMS in April 2013 to "monitor all phone and Internet communications in the country," provide "centralized access to [India's] telecommunications network[,] and facilitate direct monitoring of phone calls, text messages, and Internet use by government agencies, bypassing service providers" (Human Rights Watch 7 June 2013). According to the Press Trust of India (PTI), an Indian news agency, regional monitoring centres (RMCs) in New Delhi and Mumbai have been operationalized (PTI 4 May 2016). The same source cites the Minister of Telecommunications as stating in 2016 that "central and regional [monitoring] centres … will help central and state level law enforcement agencies in lawful interception and monitoring in serious desirable cases of national security and allied matters" (PTI 4 May 2016). The CIS representative provided the following information:

From what we understand from publicly available information, prior to the CMS, all service providers in India were required to have Lawful Interception Systems installed at their premises in order to carry out targeted surveillance of individuals by monitoring communications running through their networks. However, in the CMS era, all Telecom Service Providers (TSPs) in India are required to integrate Interception Store and Forward (ISF) servers with their pre-existing Lawful Interception Systems. Once ISF servers are installed on the premises of TSPs in India and integrated with Lawful Interception Systems, they are then connected to the RMCs of the CMS. Each RMC in India is connected to the CMS. In short, the CMS involves the collection and storage of data intercepted by TSPs in central and regional databases.

In other words, all data intercepted by TSPs is automatically transmitted to RMCs, and subsequently automatically transmitted to the CMS. This means that not only [does] the CMS authority have centralized access to all data intercepted by TSPs all
over India, but the authority can also bypass service providers in gaining such access. This is due to the fact that, unlike in the case of so-called "lawful interception" where the nodal officers of TSPs are notified about interception requests, the CMS allows for data to be automatically transmitted to its data centre, without the involvement of TSPs. (CIS 14 June 2018)

2. CCTNS

In a telephone interview with the Research Directorate, a US-based professor of political science, who specializes in the contemporary politics of South Asia and has published on India's national security, stated that "the only police database that exists is the CCTNS" (Professor of political science 15 May 2018). According to the CIS representative, the CCTNS replaces the Common Integrated Police Application (CIPA) (CIS 14 June 2018). The same source explained that the CIPA was a multilingual, non-plan scheme which was initiated in 2004 by the National Crime Records Bureau (NCRB) [2]. It was done to automate the processes at primary sources of data, i.e. police stations, to build a crime and criminal information system … and to provide an efficient way of organizing crime records for generating queries/reports and crime analysis for decision support. (CIS 14 June 2018)

Corroborating information could not be found among the sources consulted by the Research Directorate within the time constraints of this Response.

Sources report that the CCTNS was launched by the Ministry of Home Affairs (MHA) (Razdan 6 Oct. 2017; India n.d.a; MediaNama 22 Aug. 2017) in 2009 (Razdan 6 Oct. 2017; MediaNama 22 Aug. 2017). According to sources, the CCTNS is a database with information on crime and criminals that interconnects police stations across the country (Kanth and Associates 24 Apr. 2018; PTI 26 July 2015; The New Indian Express 1 Oct. 2017). According to the website of the NCRB, the CCTNS "aims at creating … a nationwide networking infrastructure for [the] evolution of [an] IT-enabled-state-of-the-art tracking system around [the] "[i]nvestigation of crime and detection of criminals"" (India n.d.a). In correspondence with the Research Directorate, the Managing Partner of Kanth and Associates, a New Delhi-based law firm whose practice areas include criminal litigation and real estate litigation, stated that the "CCTNS aims to integrate all the data and records of crime … The project involves [the] training of police personnel and setting up of [a] citizen portal to
provide services to citizens” (Kanth and Associates 24 Apr. 2018). Sources indicate that the MHA launched the Digital Police portal under the CCTNS project, which will allow for:

- online passport verification (The Better India 22 Aug. 2017; MediaNama 22 Aug. 2017);
- online registration of First Information Reports (FIRs) (MediaNama 22 Aug. 2017; PTI 12 Feb. 2018); and
- advanced search capabilities for police authorities (MediaNama 22 Aug. 2017; India n.d.b).

The website of the Digital Police portal states that to protect privacy of individuals concerned and for national security reasons, the crime and criminal data and reports can be searched by authorized police officers only. Citizens who seek criminal antecedent verification services will be provided responses through email. (India n.d.b)

According to a press release by the MHA, in March 2018, the NCRB launched the Citizens Services mobile app, which enables citizens to register a police complaint and access an FIR, except those categorized as "[s]ensitive" (India 14 Mar. 2018).

### 2.1 Implementation Status

A press release by the MHA cites the Union Home Minister as stating that "out of 15,398 police stations under the CCTNS project, 14,284 police stations are using CCTNS software. Out of these 14,284 police stations, 100% of FIRs are being generated under this software in 13,775 police stations" (India 21 Aug. 2017). According to the same source, the Union Home Minister said that "the pace of implementation of the CCTNS project is satisfactory in all states" (India 21 Aug. 2017). The minister further indicated that connectivity is enabled at 13,439 out of 15,398 police stations in India, and that 35 of the 36 states and Union Territories (UTs) are sharing the CCTNS database, which contains 70 million records, including 25 million FIRs (India 21 Aug. 2017).

According to an article written by Deepak Razdan [3] that was posted by the Government of India's Press Information Bureau (PIB), "the total number of FIRs registered using CCTNS leapt from less than [150,000] in March 2014 to about [12.5 million] before June" 2017 (Razdan 6 Oct. 2017). According to PTI, "15,023 of the 15,580 police stations covered under the crime and criminal tracking network project
have started using the core software to feed and transmit data relating to crimes and criminals" (PTI 2 Jan. 2018). Without providing further information, PTI cites the Minister of State for Home Affairs as saying that "secured data connectivity, as part of the CCTNS project, was available at 14,363 police stations" (PTI 2 Jan. 2018). According to the website of the CCTNS, the status of the CCTNS, as of 31 January 2018, is that 91 percent of police stations across India are connected to the State Data Centre [4], 94 percent of police stations across India have CCTNS hardware deployed, and 93 percent of police stations across India have "complete [s]oftware" deployed (India 31 Jan. 2018).

According to the Managing Partner of Kanth and Associates, CCTNS "presently spreads across 29 states and 7 UTs of India" (Kanth and Associates 24 Apr. 2018). The CIS representative indicated that "there are varying levels of implementation of the CCTNS project in different states" and that "all states except Bihar and Rajasthan have made substantial progress" in the implementation of the CCTNS (CIS 14 June 2018). Other sources indicate the implementation of CCTNS across various states of India as follows:

- The Hindustan Times, a daily Indian newspaper, reports that the police in Sanjauli [in Himachal Pradesh] were the "first police post" in India to be connected with CCTNS in March 2017 and that the "CCTNS project has linked 114 police stations, 14 control rooms, 13 district headquarters, 26 sub-divisional police officers, three range offices, zone offices, state crime record bureau and police headquarter besides a few other sites" (Hindustan Times 15 Mar. 2017).
- PTI indicates that, according to the Chief Minister of Punjab, Punjab launched the CCTNS in February 2018 (PTI 12 Feb. 2018). The same source cites the Chief Minister of Punjab as stating that the state of Punjab "was among the few states in the country to have launched CCTNS" (PTI 12 Feb. 2018).

However, according to an October 2017 article in The New Indian Express, a daily Indian newspaper, the verification of crime records and criminals is still in its infancy. Sources said the difficulty in interlinking all police stations into a single network and dearth of funds have led to the inordinate delay in implementation.
Though the police sources claim the FIR registration process is being done through CCTNS, a large part of the system is yet to be implemented. *(The New Indian Express 1 Oct. 2017)*

According to a study on the CCTNS by Shivangi Narayan [5], "[p]olice stations in India still work in silos as far as criminal information is concerned" and despite being connected to CCTNS, "police officers on duty still continue with their old ways for registering complaints and FIRs on paper" (Narayan 4 Sept. 2017). According to the same source, "the deadline for the [CCTNS implementation] completion was the year 2012. However, even after its second extended deadline of March 2017, most of its scheduled tasks were incomplete and a new deadline for completion [was] set for March 2018" (Narayan 4 Sept. 2017). In correspondence with the Research Directorate, an associate professor in the Department of Criminal Justice at Indiana University, whose research areas include criminal justice policy issues and the Indian police, and who has worked with India's NCRB, stated that "all FIRs will be recorded into the CCTNS," but that the "CCTNS is yet to become functional across the country" (Associate Professor 16 May 2018). Similarly, the Professor of political science stated that

[i]n principle, the CCTNS is accessible by police authorities across states and UTs; however, in practice, probably not, as the implementation of the CCTNS leaves much to be desired. There are apparently approximately 15,000 police stations using the CCTNS, however, this is probably not the case, as a result of the institutional slackness that exists in India. While some states are complying with the implementation of the CCTNS, others may have a lackadaisical attitude. As such, the government of India cannot be terribly intrusive, because it just does not have the capacity. *(Professor of political science 15 May 2018)*

In a follow-up correspondence with the Research Directorate, the same source provided the following information regarding the recording of FIRs in the CCTNS:

FIRs are supposed to be recorded in the CCTNS. Whether and how they are actually recorded depends on the professionalism of the police station and its capacity, which can vary from state to state. There is great disparity between the efficiency of police stations from state to state, for example, between Maharashtra and Uttar Pradesh – the latter state includes parts that are poorly governed. While all police stations in India are supposed to be equipped with computers, this is not always the case.
There are days when the electricity is gone, which prevents the recording of complaints in the electronic database. As such, across India, FIRs are not entered systematically or uniformly into the CCTNS. (Professor of political science 16 May 2018)

Likewise, in correspondence with the Research Directorate, a US-based professor of sociology, who specializes in criminology and criminal justice and program evaluation and who has written on crime and justice in India, stated that the overall goal of the CCTNS [is for all FIRs across India to be recorded in the CCTNS]. However, it is highly idiosyncratic as to what actually gets done. … [T]he Government of India is investing heavily in implementing this across the country, but it is still far from complete. Thus, there is no systematic way to figure out which crimes are likely to be transferred to the CCTNS and which are not. (Professor of sociology 15 June 2018)

3. Information Included in FIRs

According to the Professor of political science, FIRs are like police reports, which are filed at a local police station (Professor of political science 15 May 2018). The Professor of sociology stated that the FIR is "usually" the "official first record of a criminal complaint made by a victim" and that it "serves to activate a police investigation of the incident" (Professor of sociology 15 June 2018).

According to the Professor of political science, FIRs "specify the nature of a crime, the individuals involved, including the alleged perpetrator, and the location of the incident. It will include the contact information of the complainant, such as their cell phone number and where they live" (Professor of political science 15 May 2018). According to the Professor of Sociology, "[a]ll available information regarding the crime, the alleged perpetrator and related circumstances of the incident (e.g. witnesses) are supposed to be recorded" in the FIR (Professor of sociology 15 June 2018). The CIS representative similarly stated that the following information is "typically" recorded in an FIR:

- Name, Aadhaar number, phone numbers, email addresses and postal address of complainant;
- Date, time and location of the incident reported;
- An account of the incident as it occurred;
- Nature of offence;
• Names and descriptions and any other details of the persons involved in the incident;
• Information about witnesses, if any. (CIS 14 June 2018)

According to the Associate Professor, "FIRs record the information about criminal victimization and the offender's name, if given by the complainant" (Associate Professor 16 May 2018).

For further information on when FIRs are registered and for blank copies of FIRs, see Response to Information Request IND105779 of May 2017.

4. Tenant Verification

According to The Hans India, an English-language newspaper published across Telangana and Andhra Pradesh, "the tenant verification programme is a free service provided by the police department" and "[a]ny citizen can approach the police by filling a form, which is available at all police stations and also on [the] police website" (The Hans India 7 June 2017). According to The Indian Express, an English-language Indian newspaper,

[a] police verification is done whenever a property, commercial or otherwise, is rented out. A form is filled by both the owner and tenant, and has details like name, photograph and residential address of both. It also has copies of proof of identity and residence of both.

The police goes through the documents and checks the background of the tenant. They then sign and declare the property verified. (The Indian Express 11 Dec. 2017)

Sources report on the ability of police verification of tenants across various states of India as follows:

• According to The Hans India, the tenant verification programme exists in Karimnagar, New Delhi, Gurgaon, Kolkata, Mumbai, Pune, Bengaluru, Chennai, Thane, Jammu and Kashmir, and Punjab (The Hans India 7 June 2017).
• According to The Tribune, a daily Indian newspaper, the "Patiala police have started a special tenant verification drive" (The Tribune 23 Aug. 2017). According to the same source, the district police [of Patiala] have conducted surveys of over 200 ... houses" and warned the owners of consequences if they did not register their tenants (The Tribune 23 Aug. 2017). The same source explained that
the Patiala Deputy Commissioner-cum-District Magistrate had passed written orders for verification of tenants from outside the district at the nearest police station within 15 days. However, implementation of the order has remained ineffective. Following this, the police … decided to check all such houses housing tenants without informing the authorities. (The Tribune 23 Aug. 2017)

• According to The Hindu, an Indian daily newspaper, the Cyberabad police have put in place a tenant verification system (The Hindu 21 July 2015).
• The Times of India reports that, according to Kolkata police, all landlords have to "fill up a form giving all the details of their tenants. The form should be submitted to the officer-in-charge of their respective police stations" and "non-compliance of the order might put the landlord behind bar[s]" (Times of India 25 June 2016).
• According to The Hindu, police in Hyderabad have asked "house owners to register their tenants through the Hawk Eye App" (The Hindu 21 July 2015). According to sources, the Hawk Eye App is a mobile app launched by the Hyderabad police (The Hindu 11 Jan. 2017; Hyderabad n.d.) that has approximately 3.5 million users (The Hindu 11 Jan. 2017). According to the website of the Hyderabad police, one of the features of the Hawk Eye App is the registration of tenants with the police (Hyderabad n.d.). According to The Hindu, "[t]he App has [the] facility to upload the photographs and other details of the tenant. Once the details are uploaded[,] they form part of a database of the city police and can be checked at any point of time" (The Hindu 21 July 2015).

According to the Hindustan Times, the CCTNS facilitates police verification of tenants (Hindustan Times 15 Mar. 2017). Further information on the use of the CCTNS during tenant verification procedures could not be found among the sources consulted by the Research Directorate within the time constraints of this Response.

Sources indicate that the Digital Police portal allows for tenant information verification (MediaNama 22 Aug. 2017; India n.d.b). Further information on the use of the Digital Police during tenant verification procedures could not be found among the sources consulted by the Research Directorate within the time constraints of this Response.

The Indian Express cites a Navi Mumbai Police Commissioner as stating that "it is impossible for the police to actually verify the identity of all those who rent property" in Navi Mumbai and that "the police force is not equipped to personally go and check all new tenants" (The Indian Express 11 Dec. 2017). The Indian Express
cites the same Navi Mumbai Police Commissioner as stating that the police does not "have enough men to do thorough checks on each verification form that comes to [them]. [They] can ensure checks against fake documents by asking for multiple documents proof, but that's about it" (The Indian Express 11 Dec. 2017). The Indian Express cites a lawyer as stating that the entire process of tenant verification "has several loopholes" and cites him as stating that police verification, in theory, is meant to ensure that if a criminal or terrorist is seeking tenancy, the police know and keep an eye. It also ensures the safety of the property owner, who can escape … allegations of complicity in a crime, in case a crime is committed, by saying that he had informed the police. However, the cops are often unfamiliar with the rules of the tenancy act. While a stamp duty of … 750 [Indian rupees (INR)] [approximately C$14.45] is minimum for tenancy, sometimes the police accept a stamp paper of … 100 [INR] [approximately C$1.93]. They don't even do spot checks, taking the written document as the final word, which generally leads to discrepancies." (The Indian Express 11 Dec. 2017)

The Indian Express cites the same lawyer as explaining that the "police force is just ill-equipped and short-staffed to actually carry out such verifications when they get over 50 forms daily" (The Indian Express 11 Dec. 2017). According to the Associate Professor, "[i]nformation about tenants is very limited and Delhi/Mumbai and a few other metropolises have intermittently tried to develop a database and verify the information. To the best of [his] knowledge, this is very inadequate and not updated regularly" (Associate Professor 18 Apr. 2018).

5. Categories of Persons That May Be Included in Police Databases and Ability of Police Authorities to Track Persons of Interest

According to the Associate Professor, his "personal impression is that [the CCTNS] is still unfolding. It is yet to become operational in the sense that the police are still not able to trace a person based upon information collected under this project" (Associate Professor 18 Apr. 2018). In another correspondence, the same source also stated that "[i]nformation about persons of interest is not recorded into the CCTNS but in classified databases" (Associate Professor 16 May 2018). According to the same source, "[p]olice surveillance databases are classified and not
shared across states. Concerned officers can seek information through normal official channels" (Associate Professor 16 May 2018). Corroborating information could not be found among the sources consulted by the Research Directorate within the time constraints of this Response.

According to the Professor of sociology,

[s]ome tech-savvy officers and the local agencies they lead [use the CCTNS to record information on persons of interest,] while others may not be familiar with the system or too set in their ways. Rather than using online resources, the latter are likely to contact police in cities and villages where the persons of interest may be suspected of having gone to by phone or by deputing an officer to travel there. (Professor of sociology 15 June 2018)

According to the Associate Professor, the "[t]racking of persons of interest is difficult and police have a mixed record of success" (Associate Professor 16 May 2018).

According to the Professor of political science,

[i]f they put their minds to it, police authorities in India are able to track and locate persons of interest, depending on the heinousness of the crime and the pressure received from political authorities. For example, it is possible [for them] to locate a person of interest in cases of rape, murder or armed robbery. Social class also plays a vital role: the likelihood of prosecution is much greater if a case involves the murder of a politician’s daughter versus the murder of a slum dweller. (Professor of political science 15 May 2018)

In an article published in The Wire, an online Indian news publication, Prashant Reddy T., "an assistant professor at the National Academy for Legal Studies and Research (NALSAR), Hyderabad," indicates that "metadata[,] such as location data or IP [Internet Protocol] addresses[,]" have been used as a form of surveillance by police in India (The Wire 2 Jan. 2018). The same source provided the example that "the police can determine the location of a person by asking the [TSP] to triangulate the location of the mobile phone using cell phone towers or by securing details of the [IP] of an email account" (The Wire 2 Jan. 2018). According to Scroll.in, an Indian online news source, "[c]all data or phone records compris[ing] information held by mobile phone companies with details of the numbers called, the duration of
the calls and their frequency" are accessible to police authorities with the sanction of [Deputy Commissioner Police (DCP)]-level officers for the "purposes of criminal investigation" (Scroll.in 11 Apr. 2018).

Sources indicate that the Aadhaar number can be used as a tool of surveillance (The Wire 2 Jan. 2018; Daily O 9 Jan. 2018). For further information on the Aadhaar number and whether it can be used to track individuals, see Response to Information Request IND106095 of May 2018.

Further information on categories of persons that may be included in police databases and the ability of police authorities to track a person of interest could not be found among the sources consulted by the Research Directorate within the time constraints of this Response.

This Response was prepared after researching publicly accessible information currently available to the Research Directorate within time constraints. This Response is not, and does not purport to be, conclusive as to the merit of any particular claim for refugee protection. Please find below the list of sources consulted in researching this Information Request.

Notes

[1] The CIS is a "non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. The areas of focus include digital accessibility for persons with disabilities, access to knowledge, intellectual property rights, openness (including open data, free and open source software, open standards, open access, open educational resources, and open video), internet governance, telecommunication reform, digital privacy, and cyber-security. The academic research at CIS seeks to understand the reconfiguration of social processes and structures through the internet and digital media technologies, and vice versa" (CIS n.d.). The CIS has offices in Bengaluru and Delhi (CIS n.d.).


[4] The State Data Centre is an "important element of the core infrastructure for supporting [India's] e-Governance initiatives" and helps states to "consolidate services, applications and infrastructure to provide efficient electronic delivery of … services" (India n.d.c).

[5] Shivangi Narayan is a PhD research scholar at the Centre for Study of Social Systems, Jawaharlal Nehru University (JNU), New Delhi, and "[p]rior to joining the research program at JNU, she was the technology correspondent" for GovernanceNow (CIS 31 Oct. 2016), which is a "multi-media initiative for participatory reportage and analyses related to governance of all institutions and processes that are vital to public life in India" (GovernanceNow n.d.).

References

Associate Professor, Indiana University. 16 May 2018. Correspondence with the Research Directorate.

Associate Professor, Indiana University. 18 April 2018. Correspondence with the Research Directorate.


The Centre for Internet and Society (CIS). 14 June 2018. Correspondence from a representative to the Research Directorate.


Professor of Political Science, United States. 16 May 2018. Correspondence with the Research Directorate.

Professor of Political Science, United States. 15 May 2018. Telephone interview with the Research Directorate.

Professor of Sociology, United States. 15 June 2018. Correspondence with the Research Directorate.


Additional Sources Consulted

**Oral sources:** Academics specializing in Indian criminal justice issues; Amnesty International; Centre for Security Studies; Human Rights Watch; India – Digital Police, Directorate of Coordination Police Wireless, embassy in Washington, DC, high commission in Ottawa, Indian Police Service, Ministry of Electronics and Information Technology, Ministry of Home Affairs, National Crime Records Bureau, National Investigation Agency, Police Division; The Indian Law Institute; Indian Police Foundation and Institute; International Crisis Group; lawyers specializing in Indian criminal law; lawyers specializing in Indian real estate law; lawyers specializing in landlord and tenant disputes in India; National Human Rights Commission; National Institute of Advanced Studies – International Strategic and Security Studies Programme; National Law University, Delhi – Centre for Criminology and Victimology; National University of Advanced Legal Studies; Public Affairs Centre; United Federation of Residents Welfare Associations.

**Internet sites, including:** BiometricUpdate; *Business Standard*; ecoi.net; *The Economic Times*; *The Independent*; *India Today*; New Delhi Television; *The New York Times*; Smart Cities Council; UN – Refworld; *Washington University Global Studies Law Review*.

**Date modified:**
2018-06-25