Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**280**
Land:	Indien
Kilde:	Immigration and Refugee Board of Canada
Titel:	India: Communication between police offices across the country, including the use of POLNET; whether police across India can locate an individual, particularly as a result of registration requirements for employment, housing and education, security checks, and surveillance technology
Udgivet:	10. maj 2016
Optaget på baggrundsmaterialet:	15. august 2016

EN | DE

- **Source:**
  IRB - Immigration and Refugee Board of Canada
- **Title:**
  India: Communication between police offices across the country, including the use of POLNET; whether police across India can locate an individual, particularly as a result of registration requirements for employment, housing and education, security checks, and surveillance technology (2013-May 2016) [IND105494.E]
- **Publication date:**
  10 May 2016
- **ecoi.net summary:** Query response on communication between police offices, including use of POLNET, between 2013 and May 2016 (networks and means of communication; surveillance technology) [ID 325089]
- **Countries:**
  India
- Original link http://www.irb.gc.ca/Eng/ResRec/RirRdi/Pages/index.aspx?doc=456507&pls=1

Recommended citation:
IRB - Immigration and Refugee Board of Canada: India: Communication between police offices across the country, including the use of POLNET; whether police across India can locate an individual, particularly as a result of registration requirements for employment, housing and education, security checks, and surveillance technology (2013-May 2016) [IND105494.E], 10 May 2016 (available at ecoi.net) http://www.ecoi.net/local_link/325089/451302_en.html (accessed 16 June 2016)

Immigration and Refugee Board of Canada | Commission de l'immigration et du statut de réfugié du Canada

India: Communication between police offices across the country, including the use of POLNET; whether police across India can locate an individual, particularly as a result of registration requirements for employment, housing and education, security checks, and surveillance technology (2013-May 2016) [IND105494.E]

Research Directorate, Immigration and Refugee Board of Canada, Ottawa

1. Communication Between Police Offices

In correspondence with the Research Directorate, a lawyer with the Delhi High Court stated that police departments typically communicate with one another through the use of wireless messaging, such as text messaging and email, and in "urgent cases, phone or fax is used" (Lawyer 10 Apr. 2016). In correspondence with the Research Directorate, an assistant professor with the Centre for Criminology and Sociolegal Studies at the University of Toronto, who has conducted research on policing in India, stated that communication methods such as fax, phone, email and databases "may be used to varying degrees by various departments," however, to her knowledge, "there is little inter-state police communication except for cases of major crimes like smuggling, terrorism, and some high profile organised crime" (Assistant Professor 14 Apr. 2016).

According to information posted on the website of the Kerala Police Department, police stations across India are "virtually unconnected islands in the case of Crime & Criminal Tracking. There is no system of effective data storage … sharing and accessing data," and there is "no single system" by which a police unit can "talk to another directly" (India n.d.a).

1.1 Communication Mechanisms and Initiatives

1.1.1 Crime and Criminal Tracking Network & Systems (CCTNS)

According to the website of the Kerala Police Department, at the national level, the goal of the Crime and Criminal Tracking Network & Systems (CCTNS) project is to create "an IT enabled system" that will allow police stations to "talk to [one] another directly" (ibid.). In a 2015 article, *India Today*, a news magazine, reported that "CCTNS had its origins" in POLNET [1] (*India Today* 25 Nov. 2015). According to the source, POLNET "never took off," nor did "its successor, the CCTNS" (ibid.). According to the *Indian Express*, a daily newspaper, "over 11,600 police stations countrywide are now using the CCTNS software to register FIRs [First Information

Reports]" (20 Nov. 2015). Without providing further details, the *India Today* article states that "[o]nly six states have so far implemented the CCTNS network in all police stations," which is

> [j]ust the … first stage in getting all police stations to file FIRs online. After this begins the challenge of integrating state databases with central servers and then the second phase with new features such as mobile applications, fingerprint identification systems and an integration with the Integrated Criminal Justice System, a comprehensive database of courts, prisons and forensic evidence. (*India Today* 25 Nov. 2015)

According to the lawyer, "CCTNS is being used, but not to the fullest" (10 Apr. 2016). According to sources, the initial deadline for completing the CCTNS project was 2012, which was then extended to 2015, and has now been extended to March 2017 (*India Express* 20 Nov. 2015; *India Today* 25 Nov. 2015; *Governance Now* 18 Jan. 2016). Further information on the CCTNS project could not be found among the sources consulted by the Research Directorate within the time constraints of this Response.

1.1.2 Zonal Integrated Police Network (ZIPNET)

According to the lawyer, ZIPNET [Zonal Integrated Police Network] is being used to "share information amongst neighboring states" (10 Apr. 2016). According to the ZIPNET website, the project was introduced in 2004 in order to "share crime and criminal information in real-time" and provide "search engines to match information from [the] central repository in [an] online environment" (India n.d.b). The same source states that the project began with the Delhi, Haryana, Uttar Pradesh and Rajasthan police, followed by Punjab, Chandigarh and Uttrakhand police in 2008, and then the Himachal Pradesh police in 2012 (ibid.). According to the site, ZIPNET contains the following information for the public and the police:

1. FIR (Heinous Cases: Murder, Dacoity [gang robbery], Robbery & Snatching)
2. Arrested Persons (Heinous Cases: Murder, Dacoity, Robbery & Snatching)
3. Most Wanted Criminals
4. Missing Children
5. Children Found
6. Missing Person (including action taken module for authenticated Users Only)
7. Un-identified Dead Bodies
8. Un-identified Person Found (Unconscious, Minor, Abandoned, Mentally Disturbed)
9. Stolen Vehicles
10. Unclaimed/Seized Vehicles
11. Missing/Stolen Mobiles
12. Police Alerts
13. Daily Police Bulletin (Authenticated Users Only)
14. Jail Releases (Authenticated Users Only)
15. Bail Out (Authenticated Users Only)
16. Press Releases (Authenticated Users Only)
17. Messaging (Authenticated Users Only). (ibid.)

Information on the use and effectiveness of ZIPNET could not be found among the sources consulted by the Research Directorate within the time constraints of this Response.

1.1.3 National Intelligence Grid (NATGRID)

According to a 2016 article by *Governance Now*, a "fortnightly print magazine" that provides analysis of governance and institutions in India (*Governance Now* n.d.), under the NATGRID program, the "home ministry [Ministry of Home Affairs] wanted to link 81 databases," including those of "10 law enforcement agencies … user agencies, and that of 22 provider agencies, including banks, telecoms and internet service providers, railways, airlines and future databases" (ibid. 18 Jan. 2016). *The Indian Express* similarly reports that the project

> entails combining 21 sensitive databases relating to domains such as banks, credit cards, cellphone usage, immigration records, motor vehicle registrations, Income-Tax records and NCRB [National Crime Records Bureau] into a single database for access by authorised officers from 10 central agencies. (*The Indian Express* 20 Nov. 2015)

According to sources, the implementation of the NATGRID program has been stalled for several years (ibid.; *India Today* 25 Nov. 2015). The 2016 article by *Governance Now* similarly states that the NATGRID project has "not been rolled out" and cites a government official who is associated with the project as stating that the "project exists only on paper" (18 Jan. 2016). Further information on the implementation of the NATGRID program could not be found among the sources consulted by the Research Directorate within the time constraints of this Response.

Information on the ability of police to locate an individual specifically through the use of registration and security checks could not be found among the sources consulted by the Research Directorate within the time constraints of this Response.

2. Use of Surveillance Technology

According to a September 2013 article in the *Hindu*, a daily newspaper, "the Internet activities of India's roughly 160 million users are … subjected to wide-ranging surveillance and monitoring" (8 Sept. 2013). According to a 2014 report co-produced by the Software Freedom Law Centre (SFLC)[2] and the World Wide Web Foundation[3], "Indian citizens are routinely and discreetly subjected to Government surveillance on a … staggering scale" (SFLC and Web Foundation Sept. 2014, 2). According to the same source, an application filed by SFLC "under the Right to Information Act, revealed that on an average, around 7500 - 9000 telephone interception orders are issued by the Central government alone each month" (ibid.).

In 2013, Human Rights Watch reported that "[i]n recent years, authorities have repeatedly used the Information Technology Act to arrest people for posting comments on social media that are critical of the government" (7 June 2013). In March 2014, Reporters Without Borders stated that "[w]ith the CMS [Central Monitoring System] fairly recently established, only a handful of cases have come to light in which web users have been prosecuted based on … surveillance" (Reporters Without Borders 10 Mar. 2014). According to sources, in November 2012 two women were arrested for posts on Facebook critiquing a citywide shutdown due to the death of a prominent politician (ibid.; Human Rights Watch 7 June 2013; BBC 20 Nov. 2012).

2.1 Lawful Interception and Monitoring (LIM) Systems

According to the SFLC and Web Foundation report, LIM systems are "a generic term" used to describe "any surveillance system sanctioned by law" (SFLC and Web Foundation Sept. 2014, 2). The same source states that "a number" of LIM systems have been "installed into India's telephone and Internet networks," which exposes "phone calls, texts, emails and general Internet activity" to government surveillance, in real-time (ibid.). The September 2013 article by the *Hindu* similarly states that LIMs monitor "internet traffic, emails, web-browsing, Skype and any other Internet activity of Indian users" (*The Hindu* 8 Sept. 2013). In June 2013, the same source reported that at the state level, there are approximately 200 LIM systems (ibid. 21 June 2013).

In its June 2013 article, the *Hindu* reports that the following agencies "are authorized to intercept and monitor citizens' calls and emails":

> the Intelligence Bureau (IB) … the Research and Analysis Wing (RAW) … the Central Bureau of Investigation (CBI), the Narcotics Control Bureau, DRI [Directorate of Revenue Intelligence], National Intelligence Agency, CBDT [Central Board of District Taxes], Military Intelligence of Assam and JK and Home Ministry. (ibid.)

2.2 Central Monitoring System (CMS)

According to sources, the CMS program will give centralized access to telecommunications networks and monitor phone calls, text messages and Internet use (Human Rights Watch 7 June 2013; US 13 Apr. 2016; *The Hindu* 21 June 2013) as well as provide capability to identify a user's physical location (ibid.; US 13 Apr. 2016). According to the SFLC and Web Foundation report,

> [a]s of June 2013, the following Government agencies are rumoured to have been authorized to make intercept requests through CMS: Central Board of District Taxes (CBDT), Central Bureau of Investigation (CBI), Defense Intelligence Agency (DIA), Directorate of Revenue Intelligence (DRI), Enforcement Directorate (ED), Intelligence Bureau (IB), Narcotics Control Bureau (NCB), National Investigation Agency (NIA), Research and Analysis Wing (RAW), Military Intelligence of Assam and Jammu and Kashmir, and the Home Ministry. (SFLC and Web Foundation Sept. 2014, 26)

A 2014 article produced by the Centre for Internet & Society (CIS), a non-profit organisation based in Bengaluru and Delhi that conducts research on "internet and digital technologies from policy and academic perspectives" (CIS n.d.), states that

> 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. Now, in the CMS era, all TSPs [telecommunications service providers] in India are required to integrate Interception Store & Forward (ISF) servers with their pre-existing Lawful Interception Systems. Once ISF servers are installed in the premises of TSPs in India and integrated with Lawful Interception Systems, they are then connected to the Regional Monitoring Centres (RMC) of the CMS. Each Regional Monitoring Centre (RMC) in India is connected to the Central Monitoring System (CMS). In short,

> the CMS involves the collection and storage of data intercepted by TSPs in central and regional databases … all data intercepted by TSPs is automatically transmitted to Regional Monitoring Centres, and subsequently automatically transmitted to the Central Monitoring System. This means that not only can the CMS authority have centralized access to all data intercepted by TSPs all over India, but that 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 datacentre, without the involvement of TSPs. (CIS 30 Jan. 2014)

According to the SFLC and Web Foundation report, the CMS is not "a surveillance system *per se*, since the … interception and monitoring of communications will be carried about by the pre-existing framework of LIM systems" (SFLC and Web Foundation Sept. 2014, 25). The same source states that the CMS will automatically access the information that has "already been intercepted by the LIM system" and will have "central and regional databases that will store intercepted data," and provide access to authorized users of the CMS (ibid.). According to the report, users will "no longer need to approach telecom/internet service providers on a case-by-case basis to retrieve intercepted information" (ibid.).

2.2.1 CMS Implementation

In 2013, Human Rights Watch reported that in April of that year, the Indian government began implementing the CMS (Human Rights Watch 7 June 2013). According to the 2013 article in the *Hindu*, "only Delhi and Haryana have tested 'proof of concept' (POC)[4] successfully" and "Kerala, Karnataka and Kolkata are the next three destinations for CMS's implementation" (21 June 2013). Freedom House, in their 2015 *Freedom on the Net* report for India, states that "[n]ews reports indicate that the government is continuing to develop the [CMS], its ambitious nationwide mass surveillance program directed at monitoring individuals' digital communications" (Freedom House 2015, 2). The same source further states that in early 2014, a "minister told parliament … that [CMS] is being phased in over the next three years," and in 2015, "parliament was informed that New Delhi and Karnataka have been chosen for the initial phase" (ibid., 25). According to the US Department of State's *Country Reports on Human Rights Practices for 2015* for India, the CMS program, which "began pilot operations in 2013, continued to allow governmental agencies to monitor electronic communications in real time without informing the subject or a judge" (US 13 Apr. 2016, 23). Further information on the implementation of the CMS program 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] Bharat Electronics Limited (BEL), a company in defence electronics (BEL n.d.a) that has partnered with the Indian Ministry of Home Affairs to establish the Police Communication Network (POLNET), states on its website that POLNET is "a satellite based network that provides voice, video, data and message communication" (BEL n.d.b).

[2] The SLFC is a New Delhi-based "donor supported legal services organisation that brings together lawyers, policy analysts, technoligists, and students to protect freedom in the digital world" (SFLC n.d.).

[3] The World Wide Web foundation (Web Foundation) is an advocacy group that works in "partnership with over 160 organisations" in order to "advance the open Web as a public good and basic right" (Web Foundation n.d.).

[4] According to PC Magazine, a website that provides "independent reviews" of technology products (PC Magazine n.d.a), Proof of Concept (POC) is the "evidence that a product, technology or an information system is viable and capable of solving an organization's particular problem" (PC Magazine n.d.b).

References

Assistant Professor, Centre for Criminology & Sociolegal Studies, University of Toronto. 14 April 2016. Correspondence with the Research Directorate.

Bharat Electronics Limited (BEL). N.d.a. "About Us." <http://www.bel-india.com/?q=vision-mission> [Accessed 10 May 2016]

_____. N.d.b. "Country Network for Police (POLNET)." <http://www.bel-india.com/?q=polnet> [Accessed 10 May 2016]

British Broadcasting Corporation (BBC). 20 November 2012. "India Woman Arrested over Facebook Post in 'Shock.'" <http://www.bbc.com/news/world-asia-india-20405457> [Accessed 22 Apr. 2016]

The Centre for Internet & Society (CIS). 30 January 2014. "India's Central Monitoring System (CMS): Something to Worry About?" <http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about> [Accessed 21 Apr. 2016]

_____. N.d. "About Us." <http://cis-india.org/> [Accessed 22 Apr. 2016]

Freedom House. 2015. "India." *Freedom on the Net 2015*. <https://freedomhouse.org/sites/default/files/resources/FOTN%202015_India.pdf> [Accessed 21 Apr. 2016]

Governance Now. 18 January 2016. Pratap Virkam Singh. "Tracking Slow and Tardy Progress of CCTNS and NATGRID." <http://www.governancenow.com/gov-next/egov/tracking-slow-tardy-progress-cctns-natgrid> [Accessed 21 Apr. 2016]

_____. N.d. "About Us." <http://www.governancenow.com/about-Us> [Accessed 22 Apr. 2016]

The Hindu. 8 September 2013. Shalini Singh. "Govt. Violates Privacy Safeguards to Secretly Monitor Internet Traffic." <http://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece> [Accessed 21 Apr.2016]

_____. 21 June 2013. Shalini Singh. "India's Surveillance Project May Be as Lethal as PRISM." <http://www.thehindu.com/news/national/indias-surveillance-project-may-be-as-lethal-as-prism/article4834619.ece> [Accessed 21 Apr. 2016]

Human Rights Watch. 7 June 2013. "India: New Monitoring System Threatens Rights." <https://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights> [Accessed 20 Apr. 2016]

India. N.d.a. Kerala Police. "About CCTNS - National Level." <http://cctns.keralapolice.gov.in/about-cctns/national-level> [Accessed 20 Apr. 2016]

_____. N.d.b. Zonal Integrated Police Network (ZIPNET). "The ZIPNet Project." <http://zipnet.in/> [Accessed 20 Apr. 2016]

The Indian Express. 20 November 2015. Sagnik Chowdhury. "CCTNS Project to Let Police Stations 'Talk': Where it Stands, and How it Can Help Fight Crime." <http://indianexpress.com/article/explained/cctns-project-to-let-police-stations-talk-where-it-stands-and-how-it-can-help-fight-crime/> [Accessed 20 Apr. 2016]

India Today. 25 November 2015. Sandeep Unnithan. "Anti-Terror Grid in Deep Freeze." <http://indiatoday.intoday.in/story/anti-terror-grid-in-deep-freeze/1/531618.html> [Accessed 20 Apr. 2016]

Lawyer, Delhi High Court. 10 April 2016. Correspondence with the Research Directorate.

PC Magazine. N.d.a. "About." <http://www.ziffdavis.com/#!portfolio-item/pcmag/> [Accessed 10 May 2016]

_____. N.d.b. "Definition of: Proof of Concept." <http://www.pcmag.com/encyclopedia/term/49857/proof-of-concept> [Accessed 26 Apr. 2016]

Reporters Without Borders. 10 March 2014. *Enemies of the Internet.* "India: Big Brother Up and Running." <http://12mars.rsf.org/2014-en/2014/03/10/india-big-brother-up-and-running/> [Accessed 14 Apr. 2016]

The Software Freedom Law Centre (SFLC) and the World Wide Web Foundation (Web Foundation). September 2014. *Communications Surveillance in India*. <http://sflc.in/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf> [Accessed 14 Apr. 2016]

_____. N.d. "About Us." <http://sflc.in/about-us/> [Accessed 22 Apr. 2016]

United States (US). 13 April 2016. Department of State. "India." *Country Reports on Human Rights Practices for 2015*. <http://www.state.gov/documents/organization/253175.pdf> [Accessed 18 Apr. 2016]

World Wide Web Foundation (Web Foundation). N.d. "About Us." <http://webfoundation.org/about/> [Accessed 22 Apr. 2016]

Additional Sources Consulted

Oral sources: Associate Professor, Department of Criminal Justice, Indiana University; India – Directorate of Coordination Police Wireless; Sardar Patel University of Police, Security and Criminal Justice.

Internet sites, including: Amnesty International; ecoi.net; *Economic Times*; Factiva; Transparency International; United Nations – Refworld.