THE CENTRAL MONITORING SYSTEM AND PRIVACY: ANALYSING WHAT WE KNOW SO FAR

Jaideep Reddy*

ABSTRACT

State-run surveillance is as old as the ages, but the wired state of our lives has put it in the spotlight more now than perhaps ever before. Our communication and data can often be veritable repositories of all that we are, and many governments today have the technological means to give them relatively easy access to most of our private data. Civil society around the world has therefore naturally expressed concern over the increasing scope of State surveillance.

The Central Monitoring System (hereafter, "CMS") is a new technology for State surveillance in India, and is in the nascent stages of implementation. It was in 2009, amidst the first hints of information from government sources about this new technology that concern began to arise in civil society in India about the impact of the new form of surveillance on private data and communication.

This paper, based on an analysis of the little and scattered official information available on the CMS, discusses, from a privacy viewpoint, the extent to which the CMS is likely to change the landscape of State surveillance in India from what it is today. A tentative evaluation is also made of whether the CMS looks likely to achieve the security-privacy balance, followed by certain suggestions that may help in achieving such a balance.

INTRODUCTION

Official information on the CMS is scarce, and the little material that is available has tended to give the public and sections of the media the impression that the CMS will facilitate threateningly direct and sweeping surveillance.[1] Activists are also worried that the CMS is being designed without public

*Associate, Samvād: Partners. B.A. LL.B. (Hons.), West Bengal National University of Juridical Sciences, 2013. The author would like to thank Mr. Bhairav Acharya, Advocate, Supreme Court of India, for his comments to the author on the Central Monitoring System, and Dr. Vinod Vaikuntanathan, Assistant Professor, Massachusetts Institute of Technology, for his comments on a draft of this paper.

[1] *See, e.g.,* Rohin Dharmakumar, *Is CMS a Compromise of Your Security?*, FORBES INDIA, July 9, 2013, available at http://forbesindia.com/article/real-issue/is-cms-a-compromise-of-national-security/35543/1, last accessed January 26, 2014; Anurag Kotoky, *India sets up elaborate system to tap phone calls, e-mail*, REUTERS, June 20, 2013, available at http://www.reuters.com/article/2013/06/20/us-india-surveillance-idUSBRE95J05G20130620, last accessed January 26, 2014; Maria Xynou, *India's 'Big Brother': The Central Monitoring System (CMS)*, CENTRE FOR INTERNET AND SOCIETY, April 8, 2013, available at http://cis-india.org/internet-

debate, and will work in a non-transparent manner, thereby facilitating arbitrary access to, and misuse of, private data and communication.[2]

This paper explores the various known and proposed features of the CMS, with a view to analyse the extent to which the CMS, as such, may warrant the above and other privacy concerns. This paper analyses the CMS as a surveillance tool as such, and does not separately discuss the concerns about the manner in which State surveillance in general is conducted in India.[3] This analysis is made, first, by looking at the changes that the CMS makes to the existing surveillance system, and, next, by tentatively assessing the CMS ('tentatively', because of the fledgling stage the CMS is at today) against various standards seeking to protect privacy in the conduct of State surveillance. Preceding the analysis of the CMS is a brief statement of the law governing privacy and surveillance in India.

In analysing the CMS, I rely as such on official sources for information, and to a supplementary extent, on official sources as reported in the media.

PRIVACY AND SURVEILLANCE IN INDIA

In India, the right to privacy is a judicially evolved right. It derives its authority from interpretations of Article 21 of the Constitution, which guards against the deprivation of a person's "*life or personal liberty except according to procedure established by law*." The features of the right to privacy in India are currently as follows:

1. It is the right to be let alone.[4]

---

governance/blog/indias-big-brother-the-central-monitoring-system, last accessed January 26, 2014. *See also infra* nn. 24-29 and accompanying text.

[2]*Ibid.*

[3]*See, e.g.,* Bhairav Acharya, *Turning India into a Surveillance State - II*, THE HOOT, November 20, 2013 (observing, "*[i]n India, the laws that allow communications interceptions are minimal, they do not conform to global best practices and they do not accord the protections afforded by the laws of many other liberal democracies.*"), available at http://www.thehoot.org/web/Turning-India-into-a-surveillance-state-----II/7150-1-1-12-true.html, last accessed January 26, 2014; Elonnai Hickok, *Why India needs a Snowden of its own*, YAHOO! NEWS INDIA, October 23, 2013 (stating, "*[t]he gaps in the Indian surveillance regime are many and begin with a lack of enforcement and harmonization of existing safeguards and protocols.*"), available at http://in.news.yahoo.com/why-india-needs-a-snowden-of-its-own-054956734.html, last accessed January 26, 2014.

[4]R. *Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.

2. It can only be infringed by a more powerful countervailing interest, including a compelling State interest of paramount importance.[5]

3. It is a fundamental right, under Article 21 of the Constitution.[6]

4. One's privacy right extends to oneself, one's family, marriage, procreation, motherhood, child bearing and education "among many other matters".[7]

5. The dictum under Article 17 of the International Covenant on Civil and Political Rights, 1966 that "*[n]o one shall be subject to arbitrary or unlawful interference with his privacy, family, human or correspondence, nor to lawful attacks on his honour and reputation*" is relevant to the right to privacy in India.[8]

Also to note, discussions are currently rife about a *sui generis* privacy law. A draft Privacy Bill prepared by the Department of Personnel and Training[9] was leaked to the public in 2011, and the said Bill is reportedly undergoing revision.[10] In October, 2012, a Group of Experts on Privacy constituted by the Planning Commission, Government of India, and chaired by Justice A.P. Shah, submitted its report formulating a set of 'national privacy principles'. The report analysed existing laws, and recommended certain points for consideration in the drafting of a new Privacy Act.[11]

On the interface between State surveillance and privacy, there is a pivotal judgment of the Supreme Court of India in *People's Union for Civil Liberties v. Union of India*.[12] In the judgment, the Court found

---

[5]*Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.

[6]*R. Rajagopal*, *supra* n. 4; *People's Union for Civil Liberties v. Union of India*, *infra* n. 12.

[7]*R. Rajagopal*, *ibid.*

[8]*People's Union for Civil Liberties*, *infra* n. 12.

[9]The Department of Personnel and Training is an agency under the administrative control of the Ministry of Human Resource Development, Government of India.

[10]Bhairav Acharya, *India: Privacy in Peril*, FRONTLINE, July 12, 2013, available at http://www.frontline.in/cover-story/india-privacy-in-peril/article4849211.ece, last accessed January 26, 2014.

[11] PLANNING COMMISSION, GOVERNMENT OF INDIA, REPORT OF THE GROUP OF EXPERTS ON PRIVACY (CHAIRED BY JUSTICE A P SHAH, FORMER CHIEF JUSTICE, DELHI HIGH COURT) (16th October, 2012).

[12]*People's Union for Civil Liberties*, (1997) 1 SCC 301.

that the tapping of telephones by the State, which is done under the Indian Telegraph Act, 1885 (*hereafter*, "Telegraph Act"), was being carried out without adequate safeguards.[13] The Court thereby laid down certain procedural safeguards to protect individuals' privacy rights.[14] These safeguards were subsequently legislatively incorporated in the Indian Telegraph Rules, 1951 (*hereafter*, "Telegraph Rules"). While the Court in *People's Union for Civil Liberties* did not explicitly mandate such safeguards for monitoring and surveillance in forms other than telephone tapping, the substance of the Court's guidelines in the case were incorporated in relation to the surveillance of "*information through any computer resource*" in the form of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (*hereafter*, "IT Monitoring Rules"), made under the Information Technology Act, 2000 (*hereafter*, "IT Act").

Presently, the procedure for monitoring under the Telegraph Act, the IT Act, and the rules framed thereunder, is briefly as follows:

1. To initiate interception, a written order, with reasons recorded, directing interception is to be made by the Central or State Government, acting through the Secretary in the Ministry of Home Affairs or Secretary in charge of the Home Department, respectively.[15]

2. The statutory thresholds for interception are (any of): "*the interest of the sovereignty or integrity of India*", "*defence of India*", "*security of the State*", "*friendly relations with foreign States*", "*public order*", "*preventing incitement to the commission of any offence*", and "*investigation of any offence*".[16]

---

[13] *People's Union for Civil Liberties*, *ibid*, ¶¶ 42, 46.

[14] *People's Union for Civil Liberties*, *ibid*, ¶¶ 47-55.

[15] Rule 419-A(1), Telegraph Rules, and Rule 2(d), IT Monitoring Rules. In unavoidable circumstances, the order may be issued by an officer not below the rank of Joint Secretary of the Government of India. In emergencies, where obtaining prior directions for interception from the above mentioned officers is not feasible, the most senior or second most senior officer of the concerned law enforcement agency is required to approve the interception; confirmation from the Home Secretary or Joint Secretary, as the case may be, would then be required within a period of seven days. *See* Rule 419-A(1), Telegraph Rules, and Rule 3, IT Monitoring Rules.

[16] *See* Section 5(2), Telegraph Act, and Section 69(1), IT Act.

3. The officer directing interception is to "*consider the possibility of acquiring the information by other means and [such direction of interception] shall be issued only when it is not possible to acquire the information by any other reasonable means.*"[17]

4. The written order directing interception is to be forwarded to a Review Committee which is to be constituted by the Central and State Governments, separately.[18] The Review Committees consist of three high-ranking officers of the executive wing of government.[19]

5. The directions for interception are to be conveyed to telecommunications service providers (*hereafter*, "TSPs") by law enforcement agencies and the requested data is to be granted by the TSPs upon receipt of such directions.[20]

6. The concerned Review Committee is to meet at least once in two months and assess whether the directions of interception are in accordance with the Telegraph Act and the IT Act, and if it finds that such directions are not so, it may set aside the order for interception, and order for destruction of copies of the intercepted material.[21]

CONCERNS OF THE PUBLIC

Since the news of the government's plans for the CMS became public - and more so in the wake of the revelations by Edward Snowden on surveillance by the United States' National Security Agency - the Indian public and media have expressed concern on the apparently sweeping powers of monitoring that are to be facilitated by the CMS.[22] The CMS has also received international

---

[17] Rule 419A(3), Telegraph Rules, and Rule 8, IT Monitoring Rules.

[18] Rule 419A(2), Telegraph Rules, and Rule 7, IT Monitoring Rules.

[19]Rule 419A(16), Telegraph Rules.For the Central Government, the Review Committee is to consist: Cabinet Secretary as Chairman; Secretary to the Government of India in charge of Legal Affairs, as Member; and, Secretary to the Department of Telecommunications, Government of India, as Member. For State Governments, the Review Committees are to consist: Chief Secretary as Chairman; Secretary Law / Legal Remembrancer In-charge, Legal Affairs, as Member; and, Secretary to the State Government (other than the Home Secretary), as Member.

[20] Section 5(2), Telegraph Act; Rule 419A(7) and (9), Telegraph Rules; and, Section 69(3), IT Act.

[21] Rule 419A(17), Telegraph Rules, and Rule 22, IT Monitoring Rules.

[22]*See,e.g.*, *India to set up a central monitoring system*, LOSS OF PRIVACY, November 30, 2009 (demonstrating concern freshly in the wake of the first government announcements on the CMS), available at

attention; Human Rights Watch, the well-known international human rights advocacy organisation, expressed its view that the CMS appears to threaten the human rights of privacy and free speech.[23]

Various sections of the media and the public have expressed the main reasons why the CMS poses a threat to privacy as follows:

1. The lack of public documentation to explain the scope, functions, and technical architecture of the CMS betrays a lack of transparency, and transparency is necessary in the conduct of surveillance in democratic societies.[24]

2. There is a lack of adequate legal safeguards governing the use of a powerful surveillance tool such as the CMS,[25] and adequate legal safeguards include:

---

http://www.lossofprivacy.com/index.php/2009/11/india-to-set-up-a-central-monitoring-system/, last accessed January 26, 2014. After the Snowden leaks, more extensive opinions have been made, expressing anxiety over the potential sweep of the CMS;*see infra* nn. 24-29, and accompanying text.

[23]*India: New Monitoring System Threatens Rights: Safeguards Needed to Protect Privacy, Free Speech*, HUMAN RIGHTS WATCH, JUNE 7, 2013, available at http://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights, last accessed January 26, 2014. *See also*, Jillian C. York, *NSA Leaks Prompt Surveillance Dialogue in India*, ELECTRONIC FRONTIER FOUNDATION, July 10, 2013, available at https://www.eff.org/deeplinks/2013/07/nsa-leaks-prompt-surveillance-dialogue-india, last accessed January 26, 2014; Pranesh Prakash, *How Surveillance Works in India*, NEW YORK TIMES (INTERNATIONAL EDITION: INDIA), July 10, 2013, available at http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/, last accessed January 26, 2014.

[24]Bhairav Acharya, *The Central Monitoring System: Some Questions to be Raised in Parliament*, CENTRE FOR INTERNET AND SOCIETY, September 19, 2013, available at http://cis-india.org/internet-governance/blog/central-monitoring-system-questions-to-be-asked-in-parliament, last accessed January 26, 2014; Anurag Kotoky, *India sets up elaborate system to tap phone calls, e-mail*, *supra* n. 1; Danish Raza, *India's Central Monitoring System: Security can't come at cost of privacy*, FIRSTPOSTINDIA, available at http://www.firstpost.com/india/indias-central-monitoring-system-security-cant-come-at-cost-of-privacy-944475.html, last accessed January 26, 2014; Human Rights Watch, *India: New Monitoring System Threatens Rights: Safeguards Needed to Protect Privacy, Free Speech, supra* n. 23; Shalini Singh, *Lethal surveillance versus privacy*, THE HINDU, June 22, 2013, available at http://www.thehindu.com/opinion/lead/lethal-surveillance-versus-privacy/article4837932.ece, last accessed January 26, 2014; Rohan Joshi, *India's Central Monitoring System*, THE TAKSHASHILA INSTITUTION, July, 2013, available at http://takshashila.org.in/wp-content/uploads/2013/07/India%E2%80%99s-Central-Monitoring-System-Rohan-Joshi.pdf, last accessed January 26, 2014.

[25]Jillian C. York, *NSA Leaks Prompt Surveillance Dialogue in India*, *supra* n. 23; Rohan Joshi, *India's Central Monitoring System, ibid*; Danish Raza, *India's Central Monitoring System: Security can't come at cost of privacy*, *ibid.*

- A procedure for judicial authorisation of surveillance,
- Checks on the rights and duties of the functionaries carrying out surveillance, and
- Checks on the use and disclosure of the information gathered through surveillance.[26]

3. Since the nature of surveillance under the CMS is mass-based and direct, as opposed to the extant target-based mechanism which is routed through requests to TSPs, existing legal safeguards pertaining to surveillance will not suffice for the CMS.[27]

4. In the absence of proper safeguards, the CMS may cause widespread and unwarranted infractions of privacy rights.[28]

5. The CMS appears to require the aggregation of the nation's communications data in a single, centralised location, and such aggregation would make the data highly susceptible to security breaches.[29]

---

[26]Pranesh Prakash, *How Surveillance Works in India*, *supra* n. 23; Rohin Dharmakumar, *Is CMS a Compromise of Your Security?, supra* n. 1; Bhairav Acharya, *India: Privacy in Peril, supra* n. 10; Karishma D'Souza, *The Central Monitoring System (CMS) and the International Principles on the Application of Human Rights to Communications Surveillance*, CENTRE FOR LAW AND POLICY RESEARCH, September 23, 2013, available at http://clpr.org.in/the-central-monitoring-system-cms-and-the-international-principles-on-the-application-of-human-rights-to-communications-surveillance/, last accessed January 26, 2014; Shalini Singh, *Lethal surveillance versus privacy*, *supra* n. 24.

[27] Elonnai Hickok, *Why India needs a Snowden of its own*, *supra* n. 3, (observing, "*[e]ven if the Central Monitoring System were to adhere to the legal safeguards and procedures defined under the Indian Telegraph Act and Information Technology Act, the system can only do so partially, as both provisions create a clear chain of custody that the government and service providers must follow – that is, the service provider was included as an integral component of the interception process*"). *See also* Bhairav Acharya, *The Central Monitoring System: Some Questions to be Raised in Parliament, supra* n. 24; Rohan Joshi, *India's Central Monitoring System, supra* n. 24; Bhairav Acharya, *India: Privacy in Peril, supra* n. 10.

[28]Bhairav Acharya, *India: Privacy in Peril, ibid*; Shalini Singh, *Lethal surveillance versus privacy*, *supra* n. 24.

[29] Opinion of Bhairav Acharya, expressed in conversation with the author on December 9, 2013. Notes of the conversation are on file with the author.

ANALYSING THE CMS

As mentioned previously, there is limited official information on the CMS available in the public domain. The resources that are publicly available on the subject are the following: statements in Parliament; recent amendments to the wordings of TSPs' licenses, granted under the Telegraph Act; annual reports of the Department of Telecommunications (a department of the Ministry of Communications and Information Technology, Government of India (*hereafter*, "DoT"));publicly available documents of the Centre for Department of Telematics (*hereafter*, "C-DoT"); a response to the author's application under the Right to Information Act, 2005(*hereafter*, "RTI Act"); and statements by government officials and agencies reported in the media. This article bases its analysis on these various resources. As is apparent, few of these resources are sources of binding law. They are, in the most part, expressions of governmental intent. However, as of the date of writing, they are the best that we can use to paint a true and fair picture of the scheme of the CMS and to analyse its features.

A BRIEF BACKGROUND

In the DoT's annual report for the year 2007-08, it was stated that "*[t]he requirements for the Project on Central Monitoring System [were] finalized by TEC after detailed deliberations with various Security Agencies.*"[30] (The 'TEC' is the Telecommunication Engineering Centre, an agency of the DoT).[31]

In the above statement, it is not clear what these requirements were, what these deliberations were about, or which security agencies were involved in the deliberations. However, we may surmise that requirements for the CMS were finalised based on the needs expressed by the security agencies for effective monitoring from the point of view of security.

---

[30]DEPARTMENT OF TELECOMMUNICATIONS, MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY, ANNUAL REPORT (*hereafter*, "DOT ANNUAL REPORT") 2007-2008 43, available at http://www.dot.gov.in/sites/default/files/English%20annual%20report%202007-08_0.pdf, last accessed January 26, 2014.

[31]DOT ANNUAL REPORT 2012-2013 43 ("*Telecommunications Engineering Centre (TEC) is the technical wing of the Department of Telecommunications*"), available at http://www.dot.gov.in/sites/default/files/Telecom%20Annual%20Report-2012-13%20%28English%29%20_For%20web%20%281%29.pdf, last accessed January 26, 2014.

The annual reports of the DoT for the years 2007-08 to 2009-10 stated that the "*architecture and dimensioning*" of the CMS was finalised by C-DoT, and the research and development for the CMS project was on-going.[32] The annual report for the year 2009-10 further stated, "*The lab Data Centre has been made operational. The dimensioning of the CMS Data Centre has been completed and the process initiated for setting-up the required infrastructure for connecting to the TSPs and conducting trials and later, services.*"[33] On a broader note, it is confirmed that C-DoT is the government agency entrusted with the execution of the CMS project,[34] while the operation of the CMS (which stage we have not yet reached) is to be carried out by the various regional Telecom Enforcement Resource and Monitoring (TERM) cells which work under the administrative authority of the DoT.[35]

In 2011, the Cabinet Committee on Security (CCS) approved the CMS project.[36] In the same year, a pilot run of the CMS was initiated in New Delhi, whereby two TSPs were connected with the CMS infrastructure and access to communications facilitated by them was given to two law enforcement agencies.[37]The latest official news on the status of the CMS is that the pilot implementation of the CMS is continuing, and that the installation of a key component of the CMS, the 'Intercept, Store and Forward' (ISF) server,[38] has begun on the premises of TSPs in seven different licensed service

---

[32]DOT ANNUAL REPORT 2007-2008 43, *supra* n. 30; DOT ANNUAL REPORT 2008-2009 49,available at http://www.dot.gov.in/sites/default/files/AR_English_2008-09_0.pdf, last accessed January 26, 2014; DOT ANNUAL REPORT 2009-2010 53, available at http://www.dot.gov.in/sites/default/files/final_0.pdf, last accessed January 26, 2014.

[33]DOT ANNUAL REPORT 2009-2010 80, *ibid.*

[34]Answer by Mr. Milind Deora dated February 19, 2014, to unstarred question number 4181 asked by Dr. Dilesh Narayan Rane, in the 15th Session of the 15th Lok Sabha, available at http://164.100.47.132/LssNew/psearch/QResult15.aspx?qref=150407, last accessed April 13, 2014; response of the DoT dated January 6, 2014, to the author's RTI application bearing Application Registration No. DOTEL/R/2013/60886, and dated December 9, 2013 (both the application and response are on file with the author).

[35]DOT ANNUAL REPORT 2012-2013 60, *supra* n. 31.

[36] Answer to unstarred question number 1598 asked by Rajeev Chandrasekhar the 229th Session of the Rajya Sabha, available at http://rajyasabha.nic.in/, last accessed January 26, 2014 (direct link not available).

[37]DOT ANNUAL REPORT 2011-2012 86, available at http://www.dot.gov.in/sites/default/files/AR%20Englsih%2011-12_0.pdf, last accessed January 26, 2014.

[38]*Infra* n. 44;DOT ANNUAL REPORT 2012-2013 84, *supra* n.31.

areas of the DoT.[39]A February 2014 statement of Mr. Milind Deora declared that the CMS "*has been planned to be implemented in phased manner in about 3 years.*"[40]

ANALYSING THE FEATURES OF THE CMS

In our analysis of the CMS, it may be best to closely read quotations of government statements about the system, so that we can have a clear picture of the government's intent. Discussed below are the features of the CMS that result from various government statements.

Central and direct

At its heart, the CMS is a "*centralized system to monitor communications on mobile phones, landlines and the internet in the country.*"[41] Through it, "*[d]irect [e]lectronic [p]rovisioning of target numbers by Government agencies without any manual intervention from Telecom Service Providers"* is proposed, with the expectation that *"[i]nterception through CMS will be instant as compared to the existing system*".[42]

What does it mean that the CMS is a 'centralized system'? There is a plan for the setting up of a Central Monitoring Centre (CMC) which will aggregate all of the nation's communications, upon forwarding by various Regional Monitoring Centres (RMCs) that are to be located in the several licensed service areas of the DoT.[43]'Intercept, Store and Forward' (ISF) servers installed on the premises of TSPs, will as the name suggests, intercept, store and forward data passing through the TSPs' channels to the RMCs.[44] Graphically, we can understand this scheme as in the following page:

---

[39] The seven licensed service areas in which the installation of ISF servers has commenced are New Delhi, Haryana, Kolkata, Karnataka, Mumbai, Rajasthan, and Tamil Nadu. *See* DOT ANNUAL REPORT 2012-2013 84, *supra* n. 31.

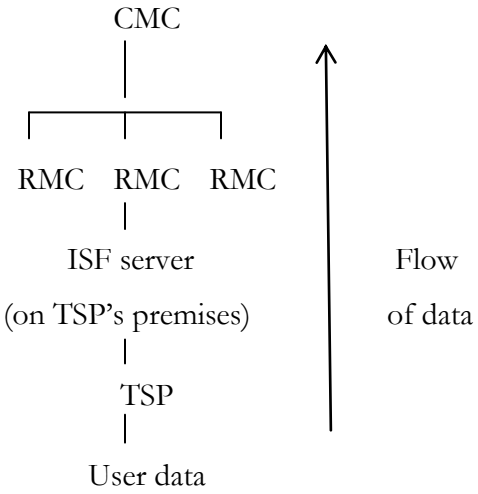
[40]Answer by Mr. Milind Deora dated February 19, 2014, to unstarred question number 4181, *supra* n. 34.

[41]*Centralised System to Monitor Communicaitons [sic]*, Press Information Bureau, Government of India, November 26, 2009, available at http://pib.nic.in/newsite/erelease.aspx?relid=54679, last accessed January 26, 2014. In the actual proceedings in Parliament, the Minister was asked, "*whether Government proposes to set up a centralized system to monitor communications on mobile phones, landlines and the internet in the country*", to which he replied in the affirmative. *See* Answer to unstarred question number 772 asked by Nand Kumar Sai the 218th Session of the Rajya Sabha, available at http://rajyasabha.nic.in/, last accessed January 26, 2014 (direct link not available).

[42]*See* Answer to unstarred question number 772 asked by Nand Kumar Sai, *ibid.*

[43]*See*DOT ANNUAL REPORT 2012-2013 84, *supra* n. 31; DOT ANNUAL REPORT 2011-2012 86, *supra* n. 37.

[44]Amendments to the Unified License agreement, Unified Access Services (UAS) License agreement, Unified License (Access Services) agreement, CMTS License agreement, each *vide* letters from the Access Service Cell



The CMS is 'direct' in the sense that, contrary to the present system under which the law enforcement agencies make their requests to TSPs, surveillance under the CMS will no longer involve any parties other than government agencies.

The CMS Authority

The proposal of the CMS to be 'central and direct' does not give the law enforcement authorities automatic and unrestricted access to all private data. The current mode of operation, based on requests for data to TSPs, is to be replaced by a scheme wherein law enforcement agencies would be making their requests to a new authority that has been referred to as the 'provisioning authority' and the 'CMS authority'. It has been officially stated that, "*Law Enforcement Agencies (LEAs) are not able to provision the target themselves and the provisioning authority is not able to see the content of the intercepted communication* (emphasis added)."[45]Also, an internal note of the DoT is reported to mention a 'CMS authority' in the context of the same role, stating, "*[t]he law enforcement agency (LEA) cannot provision for*

---

of the DoT to the respective licensees, dated October 11, 2013, bearing File No. 800-12/2013-AS.II, and available at http://www.dot.gov.in/sites/default/files/DOC231013.pdf, http://www.dot.gov.in/sites/default/files/DOC231013-004.pdf, http://www.dot.gov.in/sites/default/files/DOC231013-005.pdf, and http://www.dot.gov.in/sites/default/files/DOC231013-006.pdf, respectively; last accessed January 26, 2014. *See alsoibid.*

[45]*See* Answer to unstarred question number 1598 asked by Rajeev Chandrasekhar, *supra* n. 36.

interception and monitoring and the CMS authority cannot see the content but would be able to provision the request from the LEA."[46]

This CMS authority or provisioning authority is therefore an authority that is distinct from a law enforcement agency, and appears to be contemplated to have charge of the operation of the monitoring system. The scheme appears to be that the CMS authority is to carry out the monitoring and interception of data, upon a duly made request by an authorised law enforcement agency.

Facilitation of law enforcement concerns

Since the purpose of the CMS is to "*strengthen the security environment in the country*",[47] and since monitoring is done based on the requirements of the law enforcement agencies,[48] the CMS creates certain new tools to facilitate the work of these law enforcement agencies.

There is proposed to be a "*[c]entral and regional database which will help Central and State level Law Enforcement Agencies in Interception and Monitoring*".[49] It is not clear what this database will consist of. The possibilities are, data intercepted; data sought to be intercepted; targets; and/or, potential targets. There are also to be "*[f]ilters and Alert creation on the target numbers*".[50] This presumably means that filters will be used to mine desired data from the mass of data available, and alert creation will keep law enforcement agencies updated on the activities of their targets. Also, meta-data is available: an envisaged salient feature of the CMS is mentioned as, "*Call Data Records (CDR) analysis and data mining on CDRs to identify call details, location details etc. of the target numbers*".[51]

---

[46] Joji Thomas Philip, Leslie D'Monte, and Shauvik Ghosh, *Your telco could help spy on you*, LIVEMINT, July 30, 2013, available at http://www.livemint.com/Politics/rpWFiDJroLgpLQ6yKdR3pJ/Telcos-to-soon-link-with-government-monitoring-system.html, last accessed January 26, 2014.*See also* Danish Raza, *India's Central Monitoring System: Security can't come at cost of privacy*, *supra* n. 24 (referring to an internal note of the DoT to the same effect).

[47] Answer to unstarred question number 772 asked by Nand Kumar Sai, *supra* n. 41.

[48] We can infer this from the statement, "*provisioning of the targets as required by Law Enforcement Agencies (LEAs)*", as mentioned in DOT ANNUAL REPORT 2011-2012 58, *supra* n. 37, and DOT ANNUAL REPORT 2012-2013 60, *supra* n. 31.

[49] Answer to unstarred question number 772 asked by Nand Kumar Sai, supra n. 41.

[50] *Ibid.*

[51] *Ibid.*

Security of intercepted data; safeguards over monitoring

The government envisages that "*functions will be performed on secured electronic link and there will be minimum manual intervention*",[52] and that this will enhance the secrecy of interception, as well as protect individuals' privacy rights.[53] Since TSPs will no longer to be in the picture for monitoring, the two relevant parties are the law enforcement agency and the CMS authority. To govern this relationship, the former Minister of State for Communications and IT, Milind Deora, has told us, "*CMS has an inbuilt mechanism of check and balance, wherein the Law Enforcement Agencies (LEAs) are not able to provision the target themselves and the provisioning authority is not able to see the content of the intercepted communication*".[54]

Another mechanism being put forth as a safeguard by the government is the "*auto generation of audit trail of command logs related to interception and monitoring, which works as a deterrent to any unauthorized provisioning*".[55] Such logs are said to be non-erasable records, and the DoT is reported to have stated that the logs can be "*examined anytime for misuse*".[56]

At this point, it is not clear precisely what these logs will contain, and whether they will be comprehensive enough to hold errant authorities accountable for misuse of the surveillance systems. While certain logs are maintained under the Telegraph Rules and the IT Monitoring Rules, there is no defined mechanism for their inspection by any authority.[57]

---

[52] *Ibid.*

[53] *Ibid* and Answer to unstarred question number 1598 asked by Rajeev Chandrasekhar, supra n. 36 (where enhanced secrecy as a feature of the CMS is noted); *Milind Deora on Central Monitoring System,* available at http://www.youtube.com/watch?v=rwTsek5WUfE, last accessed January 26, 2014, 3:13 minutes to 3:27 minutes (where the Minister states, "*[the Central Monitoring System] is precisely being set up to safeguard your privacy and … protect our national security*"). *See also* Joji Thomas Philip, Leslie D'Monte, and Shauvik Ghosh, *Your telco could help spy on you*, *supra* n. 46 (where an internal note of the DoT is reported to state that the CMS "*will rather enhance the privacy of the citizens*").

[54] See Answer to unstarred question number 1598 asked by Rajeev Chandrasekhar, *supra* n. 36.

[55] *Ibid.*

[56] Joji Thomas Philip, Leslie D'Monte, and Shauvik Ghosh, *Your telco could help spy on you*, *supra* n. 46 (reporting that an email reply by the DoT to a questionnaire and an internal note of the DoT, both, state, "*[f]urther, a non-erasable command log will be maintained by the system, which can be examined anytime for misuse, thus having an additional safeguard*").

[57] The provisions on the maintenance of records of monitoring are Rule 419-A(8), Telegraph Rules and Rule 16, IT Monitoring Rules. Rule 419-A(8) of the Telegraph Rules states, "*The officer authorized to intercept any*

Compliance with law

The former Minister for Communications and Information Technology, Milind Deora, in his statement of August, 2013, was at pains to state that surveillance under the CMS is subject to the safeguards for monitoring contained in the Telegraph Act, including the requirement for authorisation of interceptions, destruction of intercepted records periodically, sharing of intercepted data, and checks against unlawful interception and monitoring.[58] While Mr. Deora did not explicitly state that the IT Act and the IT Monitoring Rules are intended to be complied with, we may surmise such intention, since the IT Act and the IT Monitoring Rules prescribe norms similar to those under the Telegraph Act and the Telegraph Rules.

CHANGES TO THE PRESENT SCHEME OF SURVEILLANCE

The chief changes that the CMS will make to the present scheme of surveillance are discussed below.

1. TECHNOLOGICAL CHANGES, BRINGING DATA AT THE GOVERNMENT'S FINGERTIPS

In contrast with the current targeted, request-based system of surveillance, the CMS contemplates a system where the government (through the CMS authority) would sit at the helm of the wired and wireless data passing through the nation's communication channels. The removal of the request-based system may be a double-edged sword. While TSPs did act as a third party to private data, and therefore another source of leaks and potential breaches of privacy rights, they may have kept an

---

message or class of message shall maintain proper records mentioning therein, the intercepted message or class of messages, the particulars of persons whose message has been intercepted, the name and other particulars of the officer or the authority to whom the intercepted message or class of messages has been disclosed, the number of copies of the intercepted message or class of messages made and the mode or the method by which such copies are made, the date of destruction of the copies and the duration within which the directions remain in force." Rule 16 of the IT Monitoring Rules states, "*Maintenance of records by designated officer.— The designated officer of intermediary or person in-charge of computer resource authorised to intercept or monitor or decrypt any information shall maintain proper records mentioning therein, the intercepted or monitored or decrypted information, the particulars of persons, computer resource, e-mail account, website address, etc. whose information has been intercepted or monitored or decrypted, the name and other particulars of the officer or the authority to whom the intercepted or monitored or decrypted information has been disclosed, the number of copies, including corresponding electronic records of the intercepted or monitored or decrypted information made and the mode of the method by which such copies, including corresponding electronic records are made, the date of destruction of the copies, including corresponding electronic record and the duration within which the directions remain in force.*"

[58] *See* Answer to unstarred question number 1598 asked by Rajeev Chandrasekhar, *supra* n. 36.

unofficial check on arbitrary surveillance powers to an extent, as they were privy to the monitoring system.[59] With requests not having to be made to TSPs, the operation of surveillance now solely rests with the government.

2. A NEW OFFICE

Essential to the proposed working of the CMS is the new office of the 'CMS authority', also referred to as the "provisioning authority". The CMS authority is at the centre of much power, and there has so far been no mention of the exact contours of its role and its rights and duties, or whether such role, rights and duties have been definitively finalised by the government, even internally. Significantly, the government does not appear to contemplate any regulation to especially govern the CMS authority's functioning.[60]

Also, it is not completely clear how this new office will play out in relation to the TERM cells of the DoT. While it is clear that the government contemplates that the CMS authority is responsible for interception of communications and forwarding of these communications to law enforcement agencies, annual reports of the DoT suggest that TERM cells will also be involved in implementing the CMS once it is functional.[61]

---

[59] *See e.g.*, Bhairav Acharya, *India: Privacy in Peril, supra* n. 10 (opining, "*[n]o doubt, trusting private persons with the power to intercept and store the private data of citizens is flawed. The leaking of the Niira Radia tapes, which contain the private communications of Niira Radia taped on the orders of the Income Tax Department, testifies to this flaw. However, bypassing private players to enable direct state access to private communications will preclude leaks and, thereby, remove from public knowledge the fact of surveillance.*"); Shalini Singh, *Lethal surveillance versus privacy*, *supra* n. 24 (opining, "*[h]owever, this means that the checks-and-balance system provided by the nodal officers in mobile networks — which discovered the illegal request for BJP leader Arun Jaitley's CDRs, leading to the arrest of three persons including a Delhi police constable — will no longer exist.*")

[60] Answer to unstarred question number 1598 asked by Rajeev Chandrasekhar, *supra* n. 36 (mentioning only the Telegraph Act and Telegraph Rules as the legal framework surrounding the CMS); response of the DoT dated January 6, 2014, to the author's RTI application, *supra* n. 34 (stating, "*[l]awful interception and monitoring under CMS is governed by Section 5 (2) of Indian Telegraph Act 1885 read with Rule 419A of Indian Telegraph (Amendment) Rules, 2007*."). None of the above sources contemplated any regulation which would take into account the particular role of the CMS authority.

[61] DOT ANNUAL REPORT 2012-2013 60, *supra* n. 31.

3. AUTOMATICALLY GENERATED AND NON-ERASABLE LOGS

While there exists in the Telegraph Rules a provision requiring the intercepting officer to maintain certain records relating to the monitoring,[62] the government appears to contemplate different types of records when it speaks of an "*auto generation of audit trail of command logs related to interception and monitoring*" as mentioned previously. Unlike the keeping of records under the Telegraph Rules presently, this audit trail of command logs is automatically generated each time surveillance is carried out. While it is not clear exactly what the logs will record, the fact that they are not manually generated, and that they are represented to be non-erasable is different - and if developed carefully, a step forward - from the current scheme of surveillance.

TENTATIVELY EVALUATING THE CMS AGAINST STANDARDS FOR PRIVACY IN SURVEILLANCE

In the evaluation of a system of State surveillance of communications, we may assume the ultimate end to be an appropriate balance between State surveillance and individuals' privacy.[63] Therefore, in our tentative evaluation of the CMS, we must assess how much the CMS helps or hurts India's chances of achieving this balance.

In making the evaluation, we will discuss only the CMS and the law that is or may be relevant to it as such. We will not critique the scheme of surveillance law in India as a whole.

We can use the various authorities listed below to arrive at standards for privacy safeguards in State surveillance, all of which express views on the boundaries of such surveillance:

1. The United Nations General Assembly resolution on the right to privacy in the digital age, passed on December 18, 2013.[64]

---

[62] *Supra* n. 57.

[63] *See,e.g.*, the observations of the unanimous opinion in *People's Union for Civil Liberties, supra* n. 12 (stating "*[i]t is no doubt correct that every Government, howsoever democratic, exercises some degree of subrosa operation as a part of its intelligence outfit but at the same time citizen's right to privacy has to be protected from being abused by the authorities of the day.*")

[64] General Assembly, United Nations, *The right to privacy in the digital age*, A/RES/68/167 (68th session, December 18, 2013)(*hereafter*, "G.A. Resolution"). *See* United Nations Research Guides and Resources, *Resolutions adopted by the General Assembly at its 68th session* (mentioning the document number and date of

2. The International Principles on the Application of Human Rights to Communications Surveillance, formulated by a consensus of various civil society organisations (including Privacy International and the Electronic Frontier Foundation), and privacy and technology experts, and launched on July 31, 2013.[65]

3. The Report of the Special Rapporteur, Frank La Rue, on the promotion and protection of the right to freedom of opinion and expression, made to the United Nations Human Rights Council, and dated April 17, 2013.[66]

4. The General Comment of the United Nations Human Rights Committee on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation, under the International Covenant on Civil and Political Rights (ICCPR), expressed in 1988.[67]

---

adoption of the resolution; an adopted copy of the resolution was not available at the time of writing), available at http://www.un.org/depts/dhl/resguide/r68_en.shtml, last accessed January 26, 2014. The draft resolution of the above-mentioned General Assembly resolution is available at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N13/544/07/PDF/N1354407.pdf?OpenElement, last accessed January 26, 2014. The draft resolution was approved by the General Assembly without a vote. *See* Department of Public Information, News and Media Division, United Nations, *General Assembly Adopts 68 Resolutions, 7 Decisions as It Takes Action on Reports of Its Third Committee, available at* http://www.un.org/News/Press/docs//2013/ga11475.doc.htm, last accessed January 26, 2014.

[65]*See International Principles on the Application of Human Rights to Communications Surveillance*, July 10, 2013 (*hereafter*, "International Principles"), available at https://en.necessaryandproportionate.org/text, last accessed January 26, 2014; Carly Nyst, *Introducing the International Principles on the Application of Human Rights to Communications Surveillance*, PRIVACY INTERNATIONAL, July 31, 2013, available at https://www.privacyinternational.org/blog/introducing-the-international-principles-on-the-application-of-human-rights-to-communications last accessed January 26, 2014.

[66] Human Rights Council, United Nations, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/23/40 (23rd Session, April 17, 2013) (*hereafter*, "Special Rapporteur's Report"), available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf, last accessed January 26, 2014.

[67] Human Rights Committee, *General Comment No. 16 on Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation)*, (32nd session, April 8, 1988) (*hereafter*, "General Comment No. 16"), as reproduced in International Human Rights Instruments, United Nations, *Compilation of General Comments and General Recommendations adopted by Human Rights Treaty Bodies*191, HRI/GEN/1/Rev.9 (Vol. I)

While the precise views of each of the above are separate and not identical, there is mutual focus on the fact that in order to be considered legitimate, and for the security-privacy balance to have a chance of being achieved, State surveillance must function with *legality* and *transparency*. Each of the above authorities demand that the working of State surveillance be subject to legality through clear and precise law, which law itself must look to safeguard the right to privacy.[68]The above authorities also recommend transparency in the use of State surveillance techniques and powers.[69] Three of the four authorities listed above further suggest that transparency would be strengthened by having

---

(May 27, 2008), available at www.ohchr.org/Documents/HRBodies/TB/HRI-GEN-1-REV-9-VOL-I_en.doc, last accessed January 26, 2014.

[68]G.A. Resolution, *supra* n. 64, ¶4(c) ("*[t]he General Assembly calls upon all States … [t]o review their procedures, practices and legislation regarding the surveillance of communications, their interception and collection of personal data, including massive surveillance, interception and collection, with a view to upholding the right to privacy and ensuring the full and effective implementation of all their obligations under international human rights law*".); International Principles, *supra* n. 65 ("*[a]ny limitation to the right to privacy must be prescribed by law. The State must not adopt or implement a measure that interferes with the right to privacy in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application.*"); Special Rapporteur's Report, *supra* n. 66, ¶50 ("*[w]ithout explicit laws authorizing [surveillance] technologies and techniques, and defining the scope of their use, individuals are not able to foresee – or even know about – their application.*"); General Comment No. 16, *ibid*, ¶3 ("*[i]nterference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the [International Covenant on Civil and Political Rights]*").

[69]G.A. Resolution, *ibid*, ¶4(d) ("*[t]he General Assembly calls upon all States] [t]o establish independent national oversight mechanisms capable of ensuring transparency and accountability of State surveillance of communications, their interception and collection of personal data*"); International Principles, *ibid* ("*States should be transparent about the use and scope of communications surveillance techniques and powers. They should publish, at a minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation type and purpose. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance.*"); Special Rapporteur's Report, *ibid*, ¶¶ 91, 92 (recommending transparency in almost exactly the same words as the above quoted text of the International Principles); General Comment No. 16, *ibid*, ¶10 ("*[i]n order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorises or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.*")

oversight mechanisms to supervise the functioning of the surveillance authorities and be an interface to the public, so that surveillance authorities can be held accountable where necessary.[70]

Pitting these values against the CMS, the following position emerges:

1. TRANSPARENCY IN SURVEILLANCE

There has been no public debate on the CMS either at its conception or at its current stage. Information on the CMS has not been made clearly and publicly available. Further, in response to the author's application under the RTI Act, despite a detailed enquiry on all aspects surrounding the CMS, the DoT's response was not forthcoming. It did not provide any but the most basic and already publicly available information, citing the national security exception under the RTI Act, and relying on a narrow definition of the word "information" under that Act.[71]

Regarding transparency through oversight mechanisms in the CMS, while some level of such mechanisms seem to be contemplated (since the DoT is reported to have stated that the logs maintained under the CMS can be "*examined anytime for misuse*"),[72] we can only speculate as to the actual fact and extent of such oversight mechanisms. Moreover, there is nothing to suggest that oversight would be conducted by a judicial authority, or even a functionary other than those government agencies responsible for surveillance.

---

[70]G.A. Resolution, *ibid;* International Principles, *ibid* ("*States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. Oversight mechanisms should have the authority to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been transparently and accurately publishing information about the use and scope of communications surveillance techniques and powers; and to publish periodic reports and other information relevant to communications surveillance*."); Special Rapporteur's Report, *ibid*, ¶ 86 ("*[t]he provision of communications data to the State should be monitored by an independent authority, such as a court or oversight mechanism*.").

[71] Response of the DoT dated January 6, 2014, to the author's RTI application, *supra* n. 34.The only information given was: (a) "*Centralized Monitoring System is a Security Project of Govt. of India for lawful interception and monitoring. This project is being executed by C-DOT across the country including Bengaluru.*" (b) "*Cabinet Committee on Security (CCS) has approved this project on 16.06.2011*".; (c) "*Lawful interception and monitoring under CMS is governed by Section 5 (2) of Indian Telegraph Act 1885 read with Rule 419A of Indian Telegraph (Amendment) Rules, 2007*." Answers to 5 queries were wholly or partially withheld stating that the "*information sought is related to security of nation hence exempt under Section 8 (1) (a) of RTI Act 2005*", while answers to two other queries stated, "*[t]his is a question and does not fall under the definition of information under RTI Act*".

[72]*Supra* n. 56 and accompanying text.

2. LEGALITY SURROUNDING SURVEILLANCE

As mentioned above, the CMS brings into play a new office viz. the 'CMS authority', also called the 'provisioning authority', and is meant to have a system of comprehensive maintenance of logs. The maintenance of logs requires regulation to enhance the privacy safeguards in surveillance, while the CMS authority requires regulation to ensure the most minimum level of privacy in the conduct of surveillance. We can say this because of the enormous scope of misuse of the power held by the CMS authority's office, absent sufficient regulation.[73]After all, a pilot run is underway at this moment, and even to this limited extent, regulation over a surveillance functionary as important as the CMS authority and the use and storage of the data collected by the CMS is called for.

Moreover, with requests not having to be made to TSPs, surveillance is now operated solely by the executive wing of government. The safeguards of the CMS, discussed previously, are meant to quell the power associated with this. Nonetheless, none of these safeguards take away from the centralisation of power at the executive wing of government.

Therefore, without discussing the shortcomings of the existing jurisprudence surrounding surveillance in India,[74] it still appears that there is a fair development of regulation required to say that there is legality surrounding the working of the CMS. What is of concern is that government sources appear to be under the impression that the Telegraph Act and Telegraph Rules alone, as they stand today, would act as sufficient regulation for the CMS.[75]

The inbuilt safeguards of the CMS, namely, the fact that access to data is mediated through a CMS authority who will not be able to access the content of the data monitored, and that logs will be maintained about all interceptions, appear to hold promise, but they hold no water absent sufficient legality and transparency in the entire mechanism of the CMS.

---

[73] The only caveat to this statement is that if there are failsafe technical safeguards preventing the CMS authority's misuse of its power, we may not need regulation over such power. There is nothing to suggest so far that such failsafe technology is in place or is in the pipeline.

[74] *Supra* n. 3.

[75] *Supra* n. 60.

TENTATIVE SUGGESTIONS FOR IMPROVEMENT

1. PUBLIC COMMENTS

Before implementation of the CMS (beyond the current pilot runs), the scheme of the CMS as developed so far ought to be made public as far as practicable, along with calls for objections and/or suggestions.

2. UPDATED LAW

New law governing the CMS should be considered, to govern the rights and duties of functionaries, especially the CMS authority; specifications of logs to be maintained, and other legally relevant technical details; and to create an *ombudsman* authority to supervise the CMS authority.

The substantive rights under the CMS may be incorporated as part of the Telegraph Act, IT Act, and proposed Privacy Act.

3. SECURITY OF DATA; DETAILED LOGS

Data collected by the CMS is proposed to be aggregated on a large scale in one location (the CMC). It is suggested that in the interest of securing such data against malicious activity, the data be subject to strong encryption at a minimum of a 128-bit level.[76] The encryption key ought to be securely stored with the CMS authority using cryptography technology that prevents the key from being subject to any single point of security breach.[77]

With respect to the surveillance logs proposed to be maintained, in order to be useful tools for accountability, such logs should contain the name and designation of the officer carrying out the interception, and all content about the monitored data including any meta-data, such as the IP addresses (for online data), IMEI numbers (for data originating from mobile devices), and/or PSTN numbers (for data originating from landline devices), as applicable, of all parties to the data.[78]

---

[76]Opinion of Vinod Vaikuntanathan, expressed in comment to a draft of this paper, on January 5, 2014.

[77]*Ibid* ("*There are cryptographic tools for distributed storage of (encrypted) data and distributed computation over them, without ever transferring all the data to a single location and without ever creating a single point of failure. This is made possible by tools such as "secret sharing" and "threshold encryption" that were developed in the cryptography community in the 1980s. The fundamental idea is to distribute the data in a few, say ten, locations so that an adversary that compromises, say, four out of ten locations does not learn anything about the data.*")

[78] Opinion of Bhairav Acharya, *supra* n. 29.

CONCLUDING REMARKS

The CMS is in one sense merely a new technology for surveillance, and in that sense, it may be asked why any legal analysis is relevant to it, as distinct from the law surrounding surveillance in general. The answer is that, as detailed above, the CMS creates new legal powers and responsibilities, and alters existing legal relationships. This merits legal analysis specific to the CMS.

Regarding the new legal powers, responsibilities, and relationships created by the CMS, I have suggested that the values of legality and transparency - which are essential to a security-privacy balance - may go a-begging if public authorities do not soon hasten to consciously uphold these values in the implementation of the CMS. One way that public authorities may begin to do this is to consider implementing the suggestions discussed in the preceding Section of this paper.