

Digital Revolution The New Culture of Surveillance

Bhushan Arekar

Department of Political Science, Ramniranjan Jhunjhunwala College, Mumbai

Email: arekarbhushan@gmail.com

Citizenship and Identity in the Age of Surveillance

by Pramod Nayar;

Cambridge University Press, New Delhi, 2015;

Pp- 216, Rs 464/-

The book is a timely intervention, especially in the Indian context. The Indian parliament has just passed the AADHAR Bill linking welfare and other public services with fourteen digit numbers assigned to every individual. Digital India initiative is aiming to provide digital services on a massive scale. With the young population increasingly living in the digital world and the resultant socialization process taking place in cyberspace, India will be on the cusp of digital revolution.

The 2014 election fought massively on social media platform along with traditional electoral methods signifies growing penetration of internet in our life world. Surveillance, privacy and data protection debates pertaining to cyber world is gaining traction in India, especially after the Snowden scandal. Surveillance is not a new phenomenon; it is a constitutive element of modernity. The rise of cyber technology has altered the scale and degree of surveillance, as deeper aspects of our lives circulate in the cyber world in the form of data bytes.

The central argument of the book is “Surveillance is an organizing principle of contemporary life like consumption and mobility. Further our subjectivities and practices of citizenship are shaped in the crucibles of surveillance culture on a global scale”. Surveillance is a mode of governance, argues Nayar, used by the state, non-state actors and individuals. The mushrooming of surveillance in our daily lives is the result of risk discourses and the notion of vulnerabilities that circulates around the world emanating from multiple sources. Security is not an attribute or a thing but an ongoing process. Borders are markers of vulnerabilities that surround our lives be it

work place, residential colonies, streets, roads, public transport, social media, e-commerce, e-banking etc. Surveillance scholars perceive surveillance in two phases: Panoptic and Post-Panoptic theories. Panoptic studies are exemplified by Bentham's *Panopticon* prison model which is centralised and hierarchical model of surveillance generally associated with state agencies keeping watch on its own citizens. Foucault used the *Panopticon* diagram to explain the rise and spread of disciplinary power in the western society. Post panoptic scholars argue that in the age of the internet the panoptic model is redundant. Kevin Haggerty calls for demolishing the panopticon model. Unfortunately many post panoptic thinkers attribute *Panopticon* to Foucault's disciplinary power. They prefer Deleuze's Rhizomatic model of surveillance which is lateral and dispersed. Nayar's book uses the Rhizomatic model of surveillance to explain the ubiquitous growth of surveillance. To quote Nayar, "surveillance which was once a narrower and specialised technology of state power has now become ubiquitous, including within its ambit everybody, and extending into domains as diverse as, recreation, leisure, reading habits, consumerism in addition to retaining the older ones of law and order. The routinisation of surveillance is what produces cultures of surveillance... we are surveilled not in a centralized manner but in fragments—as a worker, as a consumer, as an internet user, as a resident in a neighbourhood, as an airline user, at the ATM".

Nayar contends that the surveillance culture is producing biological citizenship by inserting bodies into biometric machines. These machines abstract human bodies from the physical world and reduce them to data. The computers located nearby or at a distance, process the data and throw up the data at other terminals as 'Profiles'. In surveillance culture, there is a continuous dematerialisation and rematerialisation of bodies. This process is not a neutral process, there is politics beneath as to how profiles are generated. Nayar gives an example of Shahrukh Khan's detention at New York airport because computer profiling of his database could have put him in the dangerous or risky category due to his surname, religion, citizenship, etc. The national security discourses embodied in the U.S. computer software automatically targeted Shahrukh Khan not as an *individual* but as a *dividual*. Individuals are not persons but categories, profiles and sorted bodies.

Profiling and Panoptic sorting happen at every moment once we are in the cyber world. Our online behavior is subjected to classification and profiling by Google, Facebook, Yahoo,

Amazon, Flipkart based on our consumption patterns. Even in the physical world our bodies are captured, trapped and mapped by CCTV cameras that hover over our head. In surveillance culture, our unique biological traits act as a key to unlocking digital doors. Finger prints, iris, scan, DNA, etc. have biological uniqueness and they become the proof of our identity. Access to resources depends on validation of our biological identity by the biometric machine. AADHAR is an example of bio-surveillance. Bio-surveillance, according to Nayar, grants cultural legitimacy and corporeal integrity to our bodies and selves.

With the advancement of technology, bio-surveillance is going deeper into areas that were unknown in the past. It ranges from DNA sampling in forensic science, creating nationwide DNA database for policing, storing DNA in genebank for therapeutic purpose, human genome project, organ transplants etc. DNA decoded from human bodies is recoded in the computer and it flows into circuits of capitalism and transnational security. The proliferation of bio-informatics has raised profound questions about privacy, ownership, transfer, commodification, etc. Nayar proposes that a new biological citizenship on a global scale is developing. If globalisation is about flow of goods, services, ideas and bodies then global surveillance is about regulating the flows of bodies by capturing their biological essentials like finger prints, iris, voice, face, DNA etc. Citizenship is not about civic values, ideas, and practices but bringing greater aspects of bio processes within the surveillance machinery. Nayar says biological citizenship is the consequence of 'dispersal of surveillance into our everyday life'.

Global surveillance practices have created a new level of threats that can make life vulnerable to attacks that originate in faraway space-time. Cyber-attacks in the form of phishing, identity theft, virus, worms, stalking have created new vulnerabilities. The notion of the border is reconfigured. Borders are not made of barbed wire in the cyber world; they are created by passwords and encryption. Surveillance culture and neo liberal consumption patterns are redefining security by turning it inwards on the human body. It is about self-responsibility, managing our own safety by means of technical devices like CCTV, safety alarm, codes, software, protocols, and gateways. Consumption and vulnerabilities have developed a reciprocal relationship. Greater consumption means exposing oneself to threats and to overcome it one has to consume more security products. So if more intimate and financial details of your life run on the information superhighways then

you will have to purchase or download powerful privacy protection and anti-virus software. As pointed out by Foucault, in biopolitics there is policing of others and self.

Nayar states that ‘we live in the age of the data gaze and information citizenship’, where data is constantly produced and sorted according to categories and profile. Big data are like massive data guzzlers machines. It is not only the state and the corporate that are engaged in surveillance. It also results from a personal economy where individuals submit themselves voluntarily as consumers of material and cultural products. It can be buying products on Amazon or ticking ‘like’ on Facebook. The informatisation of the economy and culture has raised the issue of privacy and data protection. Nayar calls attention to the lack of privacy laws in India which are necessary to protect ‘data subject’s autonomy of interiority’. However, he highlights the cultural dimension of privacy in the Indian context where millions of people trapped in poverty, surviving on footpaths have no reason to think of privacy the way middle class does. Nayar does not dwell on what happen to people who are outside surveillance culture.

Nayar takes a benign view of new forms of surveillance like multiveillance or participatory surveillance. Big Boss, Moment of Truth, MTV roadies, Facebook, Skype etc. has become forums of self-expression. Nayar gives examples of shows like *Satyamev Jayate*. The show allows victim *self-disclosure* to the audience. Such self-disclosures create a new cultural script that can create moral responsibility among the audience and viewers of the show to respond in various ways to tackle social problems. Self-disclosure in talk shows, “is a surveillance device that mobilises compassion, shame... that results in visible articulation of the same in the proximate one”. Nayar seems to have taken sanitised view of such talk shows which are not about total reality but edited reality. S Anand lambasted (in *Outlook* magazine) *Satyamev Jayate* show on the issue of untouchability, where not a single reference was made to Dr. Ambedkar or reservation policy. S Anand rightly said the references were edited to cater to the sensibilities of middle class (read upper caste) Indians whose aversion for Ambedkar and reservation is well known. In fact, Aamir Khan would never dare to run an episode highlighting the plight of ordinary Muslims in India. His recent self-disclosure on the issue of tolerance invited abusive wrath from many quarters in India.

Nayar explores the potential of surveillance culture in creating *global witness citizenships* wherein witness subjects can post videos, image and visuals about violation of human rights in

any part of the world in order to mobilise compassion. Such dissident culture in the digital sphere creates a social memory that cuts across national borders and brings distant suffering close to our heart. Though it is true to the certain extent that surveillance culture has empowered individuals by turning the gaze on the watchers (state), enabling citizens to speak truth to power.

However, Nayar looks at the whole issue of surveillance from the cultural perspective and hence has ignored the web of power relations that runs the surveillance machinery. Nayar assumes the only the state is a violator of rights and gives a series of examples to highlight how state-led surveillance can be oppressive. He has not analysed power relations operating within various groups in a given society. These relations often get reflected in the media and cyberspace. One can draw from the recent JNU controversy that it was not just government but also some sections of the civil society that haunted the JNU students because of their alleged role in the so-called anti-India sloganeering. The JNU controversy even polarised the mainstream media where abusive language was hurled at one another on the topic of nationalism. In fact, the doctoring of videos of Kanhaiya Kumar reveals the manipulative nature of surveillance technology. Nayar's point about the emancipatory potential of surveillance technology in the form of global witness citizenship is questionable. As Deleuze said, 'every society has a diagram of power' and surveillance is within and not outside the diagram. Overall the book is very informative and analytical providing a certain perspective to Indian readers for whom surveillance is Orwellian.