

Received: 4 February Revised: 9 February Accepted: 19 February

Unfolding the Global Spread of State Surveillance

Dr. Bhushan Arekar

Assistant Professor,
Department of Political Science,
Ramniranjan Jhunjhunwala College of Arts, Science and Commerce,
Ghatkopar, Mumbai: 4000086

Abstract

The study aims to explore the history of state surveillance in modern times. The research paper will argue that surveillance mechanisms have been perfected in the crucibles of the nation state system. The nation state system originated from the Treaty of Westphalia and by 20th century it has spread on a planetary scale. In the age of globalisation surveillance practices have also transcended the borders of the nation state. One distinguishing feature of modern surveillance is the use of cyber technology for global monitoring. The paper will use the ideas of Michel Foucault, especially his concept of disciplinary and biopolitical power to explain the functioning of modern surveillance modalities.

Terms: Biopolitics, discipline, dispositif, apparatus of Security, governmentality.

Introduction

We live in the age of surveillance. Every time we make a telephone call, send an email, surf the Internet, swipe a credit card or walk in public space our actions could be recorded, stored and monitored. Surveillance has permeated several aspects of our public and private life. Yet, due to its surreptitious nature most people are generally unaware about the extent, scale and scope of such practices. Spying and surveillance are as old as civilisation. With the onset of modernity and the emergence of sophisticated technology surveillance proliferated. It has been embedded in various layers of the society and in varied places like factories, industries, corporations, hospitals, asylum, schools, family, community and civil society.

Historical context

Surveillance is not a recent phenomenon; it has existed from time immemorial. Surveillance in ancient times was integral part of *realpolitik*. With the onset of modernity and the emergence of sophisticated technology surveillance proliferated. It has been embedded in various layers of the society and in varied places like factories, industries, corporations, hospitals, asylum, schools, family, community and civil society. The rapid proliferation of surveillance practices over the years is, arguably, due to perceived sense of insecurity. New forms of warfare, terrorism, civil strife, social tensions, refugee crisis, financial malpractices, consumption patterns and economic transactions have spurred growth of surveillance technologies and its practices. We are surrounded by varying types of surveillance technologies.

In modern times surveillance technologies has been perfected in the crucibles of nation state system that emerged in Europe from 15th century and by 19th century expanded on a planetary scale. The Westphalian nation-state system brought epistemic shift in the modalities of surveillance. As territorial state became the building block of political order in Europe, the locus of surveillance shifted to seeking knowledge about the strength of its own territory as well as that of enemy states. during absolutist age modern bureaucratic institutions grew as it was necessary

Received: 4 February Revised: 9 February Accepted: 19 February

for the daily operation of state power. As the monarchical hold on territory strengthened, new administrative structures were created to dispense specialised functions of justice, law, foreign affairs, finance, etc. Bureaucratic surveillance greatly expanded the power of the nation-state.

Rise of Disciplinary and Biopolitical Power

The 18th century witnessed the rise of industrial revolution that was facilitated by mechanised technology. The developments in the 18th century gave rise to a new form of power that the French social thinker Michel Foucault called disciplinary power. According to him the aim of disciplinary power was to create docile bodies from which labour and productivity could be extracted. It was developed and perfected in different locations such as barracks, prisons, factories and workshops. Disciplinary power employed continuous surveillance that involved tactics like hierarchical observation, training, correctional practices, application of norms, written records and profiles. Both nation-state agencies and capitalism used disciplinary surveillance for their own political and economic purposes. The spread of disciplinary surveillance across the society gave rise to new form of power that Foucault termed as biopolitics. According to Foucault biopower or biopolitics emerged in the western society when, '...the basic biological features of the human species became the object of a political strategy, of a general strategy of power...'. Biopolitical surveillance functions at the level of populations and tries to manage, regulate and administer the population. In the 19th century biopolitical surveillance became the datum of politics which brought transformation in the functionality of the modern state. Biological factors became the object of power-knowledge for the nation-state. New scientific discourses like biology, health, hygiene, sanitation and statistics created new forms of biopolitical knowledge about the population. Population was understood in terms of statistical categories like health, education, mortality, morbidity, poverty, etc. The biopolitical technologies that have emerged in the last two centuries made population the target of its application. Though modern state was central in the production of surveillance technologies, some of the political technologies had its origin outside the domains of the states and were later integrated into its surveillance apparatus. Towards the end of 19th century state surveillance crisscross the length and breadth of Europe. The European colonies exported these political technologies to their own colonies for myriad of purpose. In the 20th century many new types of surveillance technologies were developed during the time of World War II.

The onset of Cold war between United States (US) and former United Soviet Socialist Republic (USSR) intensified biopolitical surveillance. New technologies of mass surveillance were legitimised and perfected in the name of national security. Institutional apparatuses were established for monitoring the population and enemy countries. The erstwhile Soviet Union created the formidable Komitet Gosudarstvennoy Bezopasnosti (KGB) and Ministerstvo Vnutrennikh Del (MVD); United States created Central Intelligence Agency (CIA), National Security Agency (NSA) and Federal Bureau of Investigation (FBI); United Kingdom (UK) created Military Intelligence (MI5 and MI6), Government Communication Headquarters (GCHQ); East Germany established the Stasi police. The development of military bases abroad, rise of military industrial complex and nuclear weapons expanded the dragnet of mass surveillance. In the 1950s US, UK, Canada, Australia and New Zealand created 'Echelon' a global project for intercepting electronic communication. Initially focused on military and diplomatic communications, it later began to monitor industrial targets and private individuals. Projects like Echelon remained secret and hidden from public eyes. Some other technologies of mass surveillance are not only known to the public but have gained legitimacy. These include communication, electronic, visual and

Received: 4 February Revised: 9 February Accepted: 19 February

biometric technologies. For instance, the use of census, CCTV, surveillance, fingerprinting, iris scanning and cyber surveillance has become integral part of our lives.

Globalisation of surveillance

The discourse of globalisation described in the language of open borders, free market economy, consumerist behaviour, technological fetishism, global village has not undermined surveillance. On the contrary, the concept of security that was understood in terms of nation-state has become hydra-headed. The rise of transnational crime, money laundering, terrorist network, drugs cartels and illegal arms trade are some of the manifestation of global flows. The September 11, 2001 attacks (hereafter September 11) on the twin towers of New York and the subsequent war on terror conducted on a global scale by the United States was aided by sophisticated technologies of mass surveillance.

The United States enacted stringent laws after the September 11, ostensibly, to fight global terrorism. The legislative measures like *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* of 2001 (USA PATRIOT Act), *Aviation and Transportation Security Act*, and *Homeland Security Act* are some of the Acts that increased manifold the intrusion of state surveillance in the lives of millions of American citizens. *Washington Post*, in its investigative report, exposed that 1,271 government organisations and 1,931 private companies were working on programmes related to counterterrorism, homeland security and intelligence gathering in about 10,000 locations across the United States. Fifty-one federal organisations and military commands, operating in 15 American cities, track the flow of money to and from terrorist networks. By the end of 2001, 24 organisations, including the Office of Homeland Security and the Foreign Terrorist Asset Tracking Task Force, were created. Further, 263 organisations were created or reorganised as a response to September 11 attacks. The surveillance net of the United States spiralled across the globe.

It is not just United State which is engaged in surveillance practices; all nation-states in the name of security have developed surveillance machinery of varying scales. In 2016 United Kingdom passed *Investigatory Powers Act 2016* to allow intelligence agencies to hack into computers, networks, mobile devices and servers of the citizens. The Act mandates communications service providers, which include everything from Internet companies and messenger services to postal services, to store metadata about the communications made through their services. In fact, United Kingdom has one of the most advanced surveillance apparatus to monitor the population. With millions of CCTV cameras and one of the largest DNA databases, the United Kingdom is among the most watched places in the world. As per National DNA Database Strategy Board Annual Report 2015/16, United Kingdom has generated DNA database of 5,860,642 people. Both authoritarian and democratic states have used cyber technology to surveil. China has developed sophisticated cyber surveillance technology known as Golden Shield that filters Internet data before entering China. Censoring technologies flushes out any information that is perceived to be antithetical to the interest of communist regime. Russia's surveillance machinery has stifled dissenting voices by creating laws and policies that gives power to the state to extend its control on the cyberspace. The legal frameworks include regulatory and licensing rules imposed on content providers like news media, both foreign and domestic, to follow national laws related to pornography, hate speech, slander, national security that entails self imposed cyber censorship on the content providers. Such regulations create disincentives for content providers; however, in the age of profit driven economy corporate owned media often accept such stifling regulations. Even democratic India rolled out cyber surveillance programmes like Central Monitoring System, Network Traffic Analysis, National Intelligence Grid and Lawful Interception and Monitoring

Received: 4 February Revised: 9 February Accepted: 19 February

Project to protect national security. In 2010 the Indian state implemented Aadhaar which is a unique identity number (twelve digits) issued by the state to the residents of India. The twelve-digit number is based on biometric and demographic information of the individual. By the end of 2016, the Unique Identification Authority of India (UIDAI) has registered 118,41,21,451 individuals. The entire Aadhaar system sits on the Internet technology platform. It will be easier for the state's cyber surveillance machinery to use Aadhaar number for snooping on the citizen.

In the 1990s Internet was hailed as space of absolute freedom and borders where people would express their thoughts, ideas, creativity and identities without any external barriers imposed by the nation-states and markets. John Barlow well known cyber activist wrote an email in 1997 called 'Declaration of Independence of Cyberspace' which became a manifesto of freedom among the cyber-libertarians. The declaration stated, 'Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather'. The optimism of the cyber-libertarians was belied by the revelation of Edward Snowden in 2013. Snowden a former employee of Booz Allen Hamilton (company hired by National Security Agency) leaked to the media important documents that revealed how United States along with its allies conducted cyber surveillance called PRISM on a global scale. Cyberspace has become frontline terrain of national security because large parts of critical infrastructure of the state like defence, diplomacy, war, transport, communication, energy, commerce and police are strategically linked to it and states have vested interest in monitoring them.

Conclusion

The human race is fated to live in the age of increasing surveillance due to technological advancement in the field of information and communication technologies, big data, deep learning, artificial intelligence, nanotechnology, biotechnology. The longevity and durability of nation state in the context of hyper globalisation will further give impetus to the spread of surveillance. It will be apt to call contemporary surveillance practices as surveillance culture wherein we have become subject and object of surveillance modalities simultaneously. Yet the present age has thrown before us some vexing challenges. The first is the eroding notion of privacy. Is privacy becoming meaningless in the age of surveillance that is making our lives transparent? Second question is about social justice because the accumulation of personal data about the population in the servers of handful of giant corporations will have severe impact on our personal liberties. Third the growing nexus between corporations and intelligence agencies of nation state and the resultant social sorting can gravely undermine democratic institutions. Yet, mankind need not remain pessimistic or optimist about the present age. We have to remain vigilant about the emerging practices in the field of surveillance. Rather than treating everything dystopian, we should learn to recognise the incoming dangers.

Certified as
TRUE COPY

Principal
Ramniranjan Jhunjhunwala College,
Ghatkopar (W), Mumbai-400086.

Received: 4 February Revised: 9 February Accepted: 19 February

References

1. Schwan, A. and Shapiro, S. (2011): Foucault's Discipline and Punish, Pluto Press, p.133.
2. Campbell, P., 'Absolute Monarchy', in Doyle, W. (ed.) (2012), The Oxford Handbook of Ancien Regime, Oxford University Press, Oxford, pp.22-23.
3. Foucault, M. (1995), Discipline and Punishment- The Birth of the Prison, trans. Alan Sheridan, Vintage, New York, p .136.
4. Foucault, M. (2009), Security, Territory, Population - Lectures At The Collège De France, 1977-78, Senellart , M. (ed.), trans. Burchell, G., Palgrave McMillan ,London , p 16.
5. Mattelart, A. (2010), The Globalization of Surveillance, trans. Taponier, S. and Cohen, J., Polity Press, Cambridge, pp. 51-56.
6. Perrone, J. , 'The Echelon Spy Network', The Guardian, May 29, 2001, www.theguardian.com
7. Murakami Wood, D.(ed.) (2006), A Report on the Surveillance Society, Information Commissioner UK, September, pp. 21-22.
8. Priest, D. and Arkin, W. 'A Hidden World, Growing Beyond Control', Washington Post, July 19, 2010, www.projects.washingtonpost.com
9. Investigatory Powers Act 2016, legislation. Gov.uk. www.legislation.gov.uk
10. National DNA Database Strategy Board Annual Report 2015/16, National Police Chiefs' Council Home Office, February 2017, www.gov.uk
11. Randy James, ' Chinese Internet Censorship', Time, March 18, 2009, www.content.time.com
12. Deiber, R. and Rohozinski, R., 'Control and Subversion in Russian Cyberspace' in Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J. and Haraszi, M. (eds.) (2010), Access Controlled : The Shaping of Power, Rights and Rule in Cyberspace, MIT Press, Massachusetts,, p. 24.
13. Balasubramanian, D., 'Privacy in Internet Era: Four Government Surveillance Programs You Must Know About', News 18, August 17, 2017, www.news18.com
14. Dashboard Summary, Unique Identification Authority of India, www.portal.uidai.gov.in
15. Malik, R. and Basu, S. 'India's Doggy Mass Surveillance Project Should Concern us All', Wired, August 25, 2017, www.wired.co.uk
16. Barlow, J., 'Declaration of Independence of Cyberspace (1996)', Electronic Frontier Foundation, www.eff.org

**Certified as
TRUE COPY**
Principal**Ramniranjan Jhunjhunwala College,
Ghatkopar (W), Mumbai-400086.**