Shroud of Surveillance and Its Threat to Fundamental Rights and Civil Liberties

Mr. S Freddy Singaraj[i]

Abstract – Technological developments and internet has revolutionised the world we live in. It has enabled scaling down the challenges of distance, borders and time, resulting in corporations and governments comprehensively capitalising on this trend. But as a double edged sword, misuse of these technologies has also led to the birth of cybercrimes and cyber terrorism. Thereby compelling the government to resort to desperate measures of digital surveillance.

With new technologies embedded with digital cameras, biometric scanners and Global Positioning Systems, it is now even more convenient to track, monitor and observe almost all communications and movements. Advancements in technology has contributed largely to the spread of state sponsored mass surveillance. Today governments can collect, monitor and intercept records of several communication data that can be processed at lightning speeds to decrypt location, transactions, habits, preferences, opinions etc. of individuals and groups. This is further used for aggressive ethnic profiling.

Surveillance cannot be restricted and relegated to communist, totalitarian or autocratic governments. In an ever changing digital world, Democratic nations too have adopted mass surveillance as a tool to curb terrorism, fight crimes against national security, prevent financial frauds, and control an ever growing list of cybercrimes. The government articulates its argument for surveillance as a need to protect national security. It is unfair for the state to trade citizen's privacy and liberty for security.

We live in an age of surveillance. It is a growing concern that as a society we fail to grapple with the idea of state surveillance, where at the core it threatens an individual's Fundamental Rights and Civil Liberties. Having perfected the rhetoric that surveillance protects the nation from several threats, the government uses this as a shield to weigh down over privacy and other concerns. Surveillance is a threat not limited to only privacy but extends to other rights and liberties that are now at risk. The erosion of civil rights due to state surveillance is a concern and a threat that needs constitutional safeguards and society's attention.

This papers attempts to analyse the dangers of state sponsored surveillance and its potential to threaten and harm fundamental rights and civil liberties as a façade for national security.

Keywords: Privacy, Surveillance, Fundamental Rights, Civil Liberties

This paper examines surveillance practices across the world and its threat to various fundamental rights and civil liberties. It highlights the problems that have emerged with mass surveillance technologies and practices. The first part threads together information technologies and state sponsored surveillance. Part two deals with several threats to fundamental rights and liberties like right to privacy, discrimination, free speech and expression etc. The concluding part discusses why safeguards are a necessity to protect fundamental rights and civil liberties.

1. INFORMATION TECHNOLOGIES AND STATE SPONSERED SURVEILLANCE

1.1 Information Technology and Surveillance

Originally designed with the purpose of connecting only limited networks, the internet has gradually evolved and expanded its networks, one that now serves everyone. In a globally interconnected world, internet has scaled down the challenges of physical distance, borders and time. This has led to the internet connecting millions of people and information around the world. These developments were followed by increased cybercrimes and cyber threats through cyberspace(Hagen & Lysne, 2016).The same technologies that havetransformedour lives unfortunately has been used to track, monitor, and observe our data and communications. Thanks to newer technologies embedded with cameras, biometrics scanners, web bugs and Global Positioning Systems, the scope of monitoring, tracking and collecting information has surpassed all known forms of reconnaissance. Surveillance practises are not just restricted to autocratic and totalitarian

governments. Democratic governments too have resorted to these practices as measures to fight terrorism, safeguard cyber security, protect intellectual property and an ever growing list of concerns (Richards, Dangers of Surveillance, 2013). These refined technologies have been significantly facilitated by the state to increase government's efficiency at keeping records, identifying and neutralizing frauds and abuses and most importantly investigating law enforcements. This has also increased the risk of inappropriate, unauthorised and unlawful access to government databases(Regan, 1986).Gigantic advancements in sophisticated technology (RFID chips and Semiconductors) has spread the possibilities of gathering information by both state and non-state entities. Masked in the name of efficiency and instantaneous communication, for every benefit technology provides there is a sinister application threatening human rights. In today's scenario the all-seeing state in George Orwell's fiction *1984*represented by a two-way television set has been replaced by the devices we carry in our pockets(Boghosian, 2013).

1.2 State Sponsored Surveillance

Derived from the French words *Sur*(over) and *veiller* (to watch), the term surveillanceroughly translates as 'to watch over'. It dates back to the era of French Revolution where surveillance committees were formed to track and observe suspicious people and political dissenters. Through this context Michel Foucault popularised the term through his seminal work '*Surveiller et punir*' (titled 'Discipline and Punish' in English)(Guzik, 2016).In June 2013, Whistle blower Edward Snowden made some strong revelationson the existence of several state sponsored surveillance programs. These programs designed to monitor millions of private communications on internet and has led to several public debates across the world questioning the need for mass surveillance. Suchpractices by the state violate fundamental rights and weakens the democracy(Morachimo & Rodríguez, 2015). Civil libertarians have sought for the rollback of these surveillance programs but governments imply that they were designed to protect the nation from terrorist attacks or activities in preparation for a terrorist attack. The split precedentcan be noticed in the rulings of the U.S court on*Klayman v. Obama* and *American Civil Liberties Union v. Clapper*. The former case recognises that there is a need to update the laws to protect citizens from unwarranted intrusions by the government. While the judge opined that it was in violation of the Fourth Amendment, surprisingly the judgein the latter one did not find state surveillance violating lawsbutrather justifies the cause of national security(Cramer, 2018).There may be some social benefits as outcomes of these surveillance systems but one cannot ignore the fact that people who have control over these systems tend to have more power and control over those who are surveilled (Wright, Friedewald, & Gellert, 2015). State sponsored surveillance systems like PRISM (American Intelligence), TEMPORA (British Intelligence), CMS, NETRA, NATGRID (Indian bulk surveillance) have 'dubious statutory backing'. These programs with a wide reach and scope are used by the state to monitor, tape, collect and detect information and communications of citizens which clearly invade their fundamental liberties(Bhatia, 2014).Former Home Minister P Chidambaram states that the National Intelligence Grid (NATGRID) will enable intelligence agencies to 'detect patterns, trace sources of monies, track travellers and identify those who must be watched, investigated, disabled and neutralised'. Hamid Ansari, Former Vice President of Indiaquestions the reliability of such secret government gears under democracy. He raises a concern to understand'What will stop them for becoming neither a vehicle for conspiracy nor a suppressor of traditional liberties of democratic self-government' (Ramanathan, 2010).

2. THREATS TO FUNADAMENTAL RIGHTS AND CIVIL LIBERTIES

2.1 Surveillance and threat to Privacy

Privacy can be defined as the impassable individual's space that cannot be invaded or trespassed by any individual or the state. As a right to control one's personal information, Privacy is a fundamental right crucial for democracy and human dignity(Luna & Buzarquis, 2016). With Snowden's revelations of how governments and companies have easier access to private data, much attention has drifted towards the right to privacy in the digital realm. Using intrusion technologies the Azerbaijani government is believed to have arrested, intimidate and at times even sexually harass journalists and activists for unfavourable online activity against the government (Wagner, Bronowicka, Berger, & Behrndt, 2015).

To make opinions on political and social issues people read, think, web surf and communicate with others. Surveillance on these intellectual practices can be extremely dangerous as it will discourage people from experimenting controversial or deviant ideas. Our 'intellectual privacy' needs to be protected from the threat of state surveillance and interference.Privacy therefore is a guardian to the creative and subversive that enables them to develop, exchange and foster ideas and activities (Richards, 2013).

In a widely reported incident involving Target retail stores, shopping patterns and social media posts of a young womenwas collected and promotional coupons for baby care products were sent to her respective contacts when she was potentially calculated to be pregnant(Cramer B. , 2018). It is disturbing that the company learnt about the teenager's pregnancy even before her family did. Such technologies leave privacy safeguards lag far behind, eventually invading privacy (Boghosian, 2013).

2.2 Surveillance and threat to Freedom of Speech

For advocates of free speech, the internet has offered new opportunities for political debates and activism to communicate and raise voices where traditional media is easily controllable. It played a significant role in changing governments in Egypt, Libya, Yemen and Tunisia during the Arab Spring. Unfortunately, repressive governments have developed surveillance technologies to monitor and profile online content for of political oppositions with consequences ranging from arrests to death. In a 2012 survey by Freedom House, Nineteen out of forty seven countries introduced laws restricting online speech and punishing citizens for objectionable and undesirable online content (Brown, 2013). Fearing an uprising very similar to the Arab Spring, former soviet republics like Kazakhstan, Belarus, Ukraine and Uzbekistan have restructured their interception systems, bringing millions of people under surveillance by security agencies(Borogan, 2013).

While internet has provided platforms for people to exercise their right to free speech, the same has been used to restrain free speech thus causing a 'chilling effect' where individuals become more cautious of what they speak and share after realising they are being surveilled. In parts of the world where free speech is risky enough for bloggers to just 'disappear', *Hagen and Lysne* raise serious concerns such as diminishing political discussions and long term impact of hate speech on internet (Hagen & Lysne, 2016).Fear and sophisticated technology have enabled unprecedented surveillance which is used as an invisible and indirect means to silence political disagreements. To avoid the wrath of a watchful and punitive government, people avoid voicing opinions, circulate information or engage in conversations that are likely to displease. Certainly surveillance chills free speech(Kaminer, 2015).

2.3 Surveillance and threat to Freedom from Discrimination

While the Right to Privacy argument has been unsuccessful in the court of law as it lacks the power to overcome the national security rhetoric, we could use the argument of discrimination on the surveillance practices by the state.

In the aftermath of 2001 attacks, a No Fly list was secretly created to prevent suspicious people from boarding airplanes. Surprisingly, 47,000 citizens found their names listed in the 2013 leaked documents. Thanks to data misinterpretation, a large chunk in the list from common man to Congressman Tom McClintock became victims of data driven discrimination. Unfortunately, people caught off guard with their names on the list had no means to get it rectified. American citizens with Middle Eastern names and family origins, people with Islamic names and those who had travelled to countries that gave refuge to terrorist activities were placed in the list. In 2014 a federal judge found the whole process opaque and declared the No Fly List as unconstitutional (Cramer, 2018).

In the case of Thompson Reuters' World-Check database, it screens customers, partners, employees and transactions to help banks from starting or continuing any relationship with people or institutes that may pose a high risk to the banks (Verhage, 2008). A database referred by most US banks and government agencies in the world, banking services are denied to people, organisations and institutions that are featured as 'politically exposed persons and heightened risked individuals' on the list. As per the 2016 leaks, two million individuals and religious institutions were listed as 'terrorists' if any government agency listed them as possible suspects or have been referred as terrorists in social media. Such opaque practices by both the state and private sectors reveal the evidence of data driven discrimination in this modern big data society (Cramer, 2018).

2.4 Surveillance and threat to Freedom of Expression

Freedom of Expression is suppressed and violated by state surveillance activities. With the fear of being under surveillance, individuals adopt self-censoring techniques to avoid being repressed or be picked up and punished for their contents. Social science experiments aimed at studying surveillance and self-censorship reveal social, political engagement and behavioural changes as consequences. On being monitored, people tend to behave in a different way which gradually affects their freedom to express in a free and fair manner, thereby endangering the right to freedom of expression (Morachimo & Rodríguez, 2015).

Violations of freedom of expression are demonstrated by targeting dissenting opinions, filtering content, obstructing content and at times even denying access to technologies. In Iran, producers and participants of a YouTube video titled 'Happy in Tehran' were subjected to one year imprisonment along with ninety one lashes for having a women featured with no headscarves. Filtering and blocking social media websites have been rampantly prevalent in Iran. In another case, during a campaign against 'rumours' in China, social media users were intimidated and arrested extensively. The Great Firewall of China is known for its robust six internet gateway points that filters and blocks (if necessary) online content from other countries. Some countries like Russia lean on new legislations to enhance censorships and restrict freedom of expression. A bill signed by Vladimir Putin permitted the state to block websites reporting on Euromaiden protest in Ukraine and Crimea. Furthermore, a new law was introduced for bloggers and social media users to register with the state's telecommunications regulator. During the weeks leading up to elections, the Iranian and Turkish governments have resorted to either internet speed slowdowns and temporary disconnections or blocking and intercepting social media sites. Freedom of expression has largely been violated and more often inflicted by the very governments that should be safeguarding it (WAGNER, BRONOWICKA, BERGER, & BEHRNDT, 2015).

2.5 Surveillance and threat to Freely Assemble and Form Associations

Apart from word of mouth and hand written letters print mediums like newspapers, handbills and pamphlets were used to build associations by early groups. Today the same is achieved through blogs, websites, emails and social media networks through internet technologies. Associations are formed to exercise the right to petition, to assemble, to have coordinated activities, to march, to protest and to use social networks. People assemble to debate, share ideas, organise, demonstrate, to critique, to celebrate and engage in philanthropy and more. These associations enable the public a platform to voice their dissent or support. Democracy gives individuals the liberty to assemble for sharing ideas, voting or taking actions where they become a part of the developmental process. Preventing the state from recording, tracking or observing through mass surveillance, enhances this liberty (Desai, 2014). Digital technologies has been extensively used by citizens to organise social and political movements like the 'Umbrella Revolution' in Hong Kong and the protest around Gezi Park in Turkey. To stop people from coordinating, gathering, protesting and demonstrating, respective governments resorted to blocking and shutting down internet services (Wagner, Bronowicka, Berger, & Behrndt, 2015). Unfortunately, state enforced modern surveillance jeopardises associational freedom. Time and again surveillance has suppressed free thinking, dissenting and challenging groups and associations. In the absence of associational freedom, the very existence of self-governance in democracy erodes (Desai, 2014).

2.6 Surveillance and threat to Personal Liberty

While conferring the relationship between surveillance and personal liberty granted in the constitution, the apex court of India (in Karak Singh v. State of UP) noted that intrusion into an individual's house without proper authorization was interference to personal liberty. The court recognised that the right that protected citizens from unreasonable searches and seizures was not to be violated. Justice Subba Rao opined that innocent citizens were placed under risk by surveillance powers (Arun, 2014). In a dissenting view he expressed that the right to privacy was an essential ingredient of personal liberty. As rights protect people from restrictions and encroachments, he found all surveillance methods to be unconstitutional (Bhatia, 2014).

The Communist Party of China is identified with surveillance measures, one that is used to crackdown upon activists of civil and political liberties. In the 2015 wave of detentions, authorities have harassed them through constant surveillance and unwarranted arrests. From phones and emails being tapped and monitored to police officials stealthily trailing them, one was subjected to both online and offline state surveillance. Measures by the Chinese state to 'operate in the shadows' through residential surveillance and soft detentions denied individuals their physical liberty. Activists' partners and family members too were exposed to ordeals of surveillance and house arrests. Like in the case of Liu Xia after her husband Liu Xiaobo was arrested in 2008. Despite never being charged for any crime she spent several years under surveillance and house arrests. Xiaobo was later convicted for 'inciting subversion of state power' and for co-authoring a political manifesto that called for democratic transformation in China (Nesossi & Franceschini, 2018).

3. NEED FOR SAFEGUARDS

After a young women was unlawfully placed under surveillance by the Gujarat government for illegitimate reasons, the need for better safeguards was made even more apparent in India(Arun, 2014). Lack of proper safeguards in context to mass and targeted surveillance threatens a healthy democracy. Excess executive powers that create power imbalance as a harmful result of surveillance, undoubtedly damage the social structure. The UN Special High Commissioner Navi Pillay too has emphasised that in the absence of an independent external monitoring system rights would be threatened(Arun, 2014). Surveillance should be resisted because it is indicative of an expansion of state power, inevitably bringing with it more bureaucracy and an intrusive government. Ensuring a robust legal system to safeguard fundamental rights is one way to resist unrestrained proliferation of mass surveillance (Wright, Friedewald, & Gellert, 2015).As unconstrained surveillance threatens a cognitive revolution it therefore needs to be constrained by legal and social regulations. Our liberties and rights can be safeguarded by recognising the harms of surveillance and crafting stringent laws (Richards, 2013).

Although international laws and standards are constantlyevolving, comprehensive safeguards is the need of the hour to protect citizens' rights from the increasing Orwellian powers of the government.

References

Arun, C. (2014). PAPER-THIN SAFEGUARDS AND MASS SURVEILLANCE IN INDIA. *National Law School of India Review*, 105,109,112.

Bhatia, G. (2014). State Surveillance and The Right to Privacy in India: A Constitutional Biography. *National Law School of India Review*, 127& 131.

Boghosian, H. (2013, March). The Business of Surveillance. *Human Rights*, p. 2 &23.

Borogan, A. S. (2013). Russia's Surveillance State. *World Policy Journal*, 29,30.

Brown, I. (2013). The Global Online Freedom Act. *Georgetown Journal of International Affairs*, 153,154.

Cramer, B. W. (2018). A Proposal to Adopt Data Discrimination Rather than Privacy as the Justification for Rolling Back Data Surveillance. *Journal of Information Policy*, 5,6,11, 12&22

Desai, D. R. (2014). Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding. *Notre Dame Law Review*, 585,631.

Guzik, K. (2016). Grasping Surveillance. In K. Guzik, *Making Things Stick* (p. 179 and 180). University of California Press.

Hagen, J., & Lysne, O. (2016). Protecting the digitized society—the challenge of balancing surveillance and privacy. *The Cyber Defense Review*, 75, 77, 84 & 87.

Kaminer, W. (2015). Human Rights Freedom's Future. In G. S. Morson, & M. Schapiro, *The Fabulous Future? America and the World in 2040* (pp. 81,82). Northwestern University Press.

Luna, J. R., & Buzarquis, M. S. (2016). *State Communications Surveillance and the Protection of Fundamental Rights in Paraguay.*

Lysne, J. H. (2016). Protecting the digitized society—the challenge of balancing surveillance and privacy. *The Cyber Defense Review*, 84.

Morachimo, M., & Rodríguez, K. (2015). *State Communications Surveillance and Protection of Fundamental Rights in Peru.* Electronic Frontier Foundation.

Nesossi, E., & Franceschini, I. (2018). Human Rights in the Age of Prosperity. In *China Story Yearbook 2017: Prosperity* (pp. 258,266 & 267). ANU Press.

Ramanathan, U. (2010, July 24). A Unique Identity Bill. *Economic and Political Weekly*, 11.

Regan, P. M. (1986). Privacy, Government Information, and Technology. *Public Administration Review*, 629-634.

Richards, N. M. (2013). Dangers of Surveillance. *The Harvard Law Review*, 1934, 1936, 1945 & 1964.

Verhage, A. (2008). The beauty of grey? AML as a risk factor for compliance Officers. In P. C. Duyne, S. Donati, J. Harvey, A. Maljević, & K. v. Lampe, *CRIME, MONEY AND CRIMINAL MOBILITY IN EUROPE* (pp. 214,222). Belgrade: Wolf Legal Publishers.

Wagner, B., Bronowicka, J., Berger, C., & Behrndt, T. (2015). *Surveillance and censorship: The impact of technologies on human rights.* Belgium.

Wright, D., Friedewald, M., & Gellert, R.¨. (2015). Developing and testing a surveillance impact assessment methodology. *International Data Privacy Law*, 41.

[i] **Mr. S Freddy Singaraj**

Assistant Professor, Bachelors of Mass Media, Mithibai College, Ville Parle, Mumbai