

State and Privacy

Armaan Natt

Student (IV Year), Rajiv Gandhi National University of Law, Patiala, Punjab, India

Abstract: - With increased surveillance over the digital sphere, it has naturally led to concerns regarding individual privacy and autonomy. The set up of the modern state is such that it requires the extensive use of these methods in order to achieve its desired goals. There is a balance that needs to be maintained between national security and privacy and thus both these concepts operate by their very nature, in a give and take relationship often being traded off against each other. The digital trail has also resulted in a complex challenge for privacy since every move can now be stored and tracked, greatly hinging the anonymity and privacy of Internet users. The need for secrecy around intelligence agencies, whose primary task is to collect information through use of surveillance, has also led to various privacy advocates raising a multitude of concerns. In particular there has been a raging debate over the creation of a Big Brother State through the use of these methods. The following chapter deals with the nature of the modern day state, the interplay between intelligence gathering and privacy with regard to the digital trail and also the need for surveillance to achieve the goal of national security, while dispelling fears with regard to the Big Brother concern.

I. STATE: DEFINITION AND SCOPE

The concept and understanding of a Nation State, its role and functions, has developed through the course of human history. The evolution of the State and its institutions has also had an impact on the relation between the State and its citizens. Thus it is important to first understand the nature of a state and its functions, and also between a state and its population.

It can be universally agreed upon that the state is a necessary institution. It is a form of an organized political association of individuals. Thus, it can be said that the state is the creation of the people; it is the result of our desire to have an organized community that functions on the rule of law. Thus the existence of a state is intrinsically linked to the relation between the state and its citizens and the functions it is expected to perform. Since the State is an association of humans, it can only perform its functions when its institutions are viewed as supreme and the individual as subordinate. Thus the state then may be defined as an institutional structure, which exercises its authority over a predefined jurisdiction. As Max Weber put it “The state is thus the supreme legitimate authority”¹ The state is an institution that exercises powers over individuals and groups. This view is similar to the one expressed by John Rawls, according to Rawls “a community is a society governed by a shared comprehensive, religious,

philosophical, or moral doctrine. we must abandon hope of political community unless we are prepared to countenance the oppressive use of state power to secure it”²

The Social contract theory also focuses on statehood, and the influence states have on the individual. The individual desire for security, or safety, demands fulfillment through a collective agreement. Through this collective agreement a primitive association of human beings transforms itself into an organized society, giving birth to a state.

Thomas Hobbes' also presented an idea behind the origin and role of the state. Hobbes presented his opinion stating that the pre state world was characterized by anarchy and people acting to pursue their own individual interests. It was a “war of all against all” and as a result of this state every individual lived in fear. The most abundant fear was the fear of death and the omnipresence of violence. People realizing that this was no free way to live decided to give up violence. however, there was no way to ensure that everyone would comply by this and not follow individual whims. A ruler – Hobbes names this ruler “Leviathan” – thus was needed to be installed to ensure this compliance. This Leviathan may use force, even against its own population, as long as the benefit of the population is pursued.³

German philosopher Hegel in his writings explained the sphere of liberty to comprise the whole state. Freedom, he argued, was not so much an individual's right, as it was the result of human reason. Freedom was not the capacity to do as one liked but was the alignment with a universal will toward well-being. All the comprising parts of society and state were to be nourished as a whole. Similarly was the view of Bentham, that the state worked to produce a unity of interest and acted as a device to maintain its stability.⁴

MacIver defines the state and its sphere of influence as “an association which, acting through law as promulgated by a government endowed to this end with coercive power, maintains within a community territorially demarcated the universal external conditions of social order.”⁵

Further stressing upon the need for the institution of a state to have an absolute and superior nature Harold Laski defined the

¹ ANDREAS ANTER, MAX WEBER'S THEORY OF THE MODERN STATE (Palgrave Macmillan, 2014).

² JOHN RAWLS, POLITICAL LIBERALISM (Columbia University Press, 2d ed. 1996).

³ (Mar. 24, 2018, 10:05 AM) <https://plato.stanford.edu/entries/hobbes-moral/>

⁴ Castells, M., The Information Age, Volumes 1-3: Economy, Society and Culture. Cambridge (Mass.); Oxford: Wiley-Blackwell. 1999.

⁵ MATTHEW GRIMELY, CITIZENSHIP, COMMUNITY, AND THE CHURCH OF ENGLAND: LIBERAL ANGLICAN THEORIES OF THE STATE BETWEEN THE WARS (Clarendon Press, 2004).

State as “a territorial society divided into Government and subjects claiming, within its allotted physical area, a supremacy over all other institutions.”⁶ Reiterating the view that the state should be viewed as the supreme power.

This view and understanding of the State naturally extends itself then to what the nature of the relationship between the State and society should be. According to Professor Gettell, citizens are the members of that political society who are obliged to discharge their duties to that society and have the right to enjoy all the benefits from that society.⁷ A citizen should enjoy the state given status and as Prof Laski expressed “A person is a citizen who enjoys the facilities of the state and pays obedience to state.”

The understanding of the state in terms of the relationship between the governors and the governed, has also developed over time. The function of the state and its duty towards its citizens have evolved over time. Earlier the utility of the state was to maintain and impose law and order, and to prevent the situation of war and provide security to its people. The modern state while performing all those functions also performs another important function, that is to ensure the welfare of its citizens. Consequently the modern state has evolved to become the welfare state, ensuring a symbiotic relationship, where the state takes something in return for what it provides to its citizens.

State operations are performed for adding value to and securing the interests of its citizens. The modern State performs not just the role of a protector but also the role of a provider. The state is provider of goods and services that individuals cannot provide individually for themselves, hence providing for the benefit of its citizens. Such as the creation of an economic infrastructure or providing means of physical travel, such as roads, airports etc. A more expansive concept of government as provider is the social welfare state as explained by T.H Marshall in his essay *Citizenship and Social Class* - “The extension of the social services is not primarily a means of equalising incomes. In some case it may, in others it may not. The question is relatively unimportant; it belongs to a different department of social policy. What matters is there a general enrichment of the concrete substance of civilised life, a general reduction of risk and insecurity, an equalisation between the more and the less fortunate at all levels - between the healthy and the sick, the employed and the unemployed, the old and the active, the bachelor and the father of a large family. Equalisation is not so much between classes as between individuals within a population which is now treated for this purpose as though it were one class. Equality of status is more important than equality of income”⁸

This is precisely what the modern state is trying to achieve however it is important to understand that a welfare state cannot function effectively without the participation of its citizens. It is the duty of the state to provide for an environment where the individuals can flourish and pursue their own goals, a balance however needs to be maintained between individual interests and needs and the concerns of the state. The subordination of the individual for the interests of the society as a whole is important if a welfare state is to be effective. Hence the aims of the state such as protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and the extension of social welfare benefits to all would always trump the specific needs of the individual.

II. NOTION OF PRIVACY AND THE DIGITAL TRAIL

The concept of privacy and what it entails is essential to understand the scope and nature of surveillance practices, since essentially all surveillance practices involve some form of invasion of privacy. Many jurists and academicians have tried to provide a contextual understanding of privacy, only with limited success. As Colin Bennett notes, “Attempts to define the concept of ‘privacy’ have generally not met with any success.”⁹ and as Judith Jarvis Thomson observes, “nobody seems to have any clear idea of what it is.”¹⁰ The concept has been at the center of much debate between those who see it as one of the core building blocks of modern civilization and those who view it as a commodity that must be traded in order to gain security and protection.

Several jurists have contended that the concept of privacy is best defined in terms of intimacy of the human, focusing upon the fact that privacy is an individual right.

- Julie Inness - The content of privacy cannot be captured if we focus exclusively on either information, access, or intimate decisions because privacy involves all three areas.¹¹
- Thomas Emerson - privacy is based upon premises of individualism, that the society exists to promote the worth and the dignity of the individual. The right of privacy is essentially the right not to participate in the collective life—the right to shut out the community.¹²
- John Stuart Mill – the only part of the conduct of anyone, for which he is amenable to society, is that which concerns others. In the part, which merely concerns himself, his independence is absolute. Over

⁹COLIN J. BENNETT, *REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES* p.25 (1992).

¹⁰J. THOMSON, *THE RIGHT TO PRIVACY* in, *PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY* 272, 272 (Ferdinand David Schoeman ed., 1984).

¹¹JULIE C. INNESS, *PRIVACY, INTIMACY, AND ISOLATION* p.56 (1992).

¹²THOMAS I. EMERSON, *THE SYSTEM OF FREEDOM OF EXPRESSION* pp.545, 549 (1970).

⁶(Mar.24, 2018, 12:15 PM)<https://medium.com/twenty-one-hundred/data-is-the-new-oil-a-ludicrous-proposition-1d91bba4f294>

⁷<http://repository.ums.ac.id/bitstream/handle/123456789/15989/F.%20Chapter%20II.pdf?sequence=6&isAllowed=y>

⁸(Mar.25, 2018, 08:05 AM) <http://delong.typepad.com/marshall-citizenship-and-social-class.pdf>

himself, over his mind and body, the individual is sovereign.¹³

Thus when defined in this manner, the concept of privacy essentially entails the right of a person to be free from any interference by the public in matters with which they are not ordinarily concerned. This view of privacy stresses on the fact that privacy is the ability to lead life away from the public's gaze and scrutiny. It is a sense of freedom away from the eyes of the public or the government. Privacy exists to limit the amount of interference in a person's life by others.

Overtime, with the changing social context and the dynamic relations that humans have with each other and with public institutions, there has been a shift in the way the concept of privacy is viewed and understood. Privacy should be understood as an important and sacred right of human beings but not one that is absolute, due to the societal nature of our existence as a species.

- Etzioni - Privacy is not an absolute value and does not trump all other rights or concerns for the common good.¹⁴
- John Dewey - We cannot think of ourselves save as to some extent social beings. Hence we cannot separate the idea of ourselves and our own good from our idea of others and of their good.¹⁵

This understanding of privacy lends itself to understanding the term as an inter-relation between the individual and his community. Privacy interplays with social interests and is of the view that privacy should be curtailed for and trumped by greater public interests. It is the society's interest at large that should win against those of the individual. As Dewey further goes on to argue, the good of both the individual and society are often interrelated rather than antagonistic since the individual is shaped by society.¹⁶

The rapid rise achieved in technological advancements coupled with the advent of the digital age have further complicated the understanding of the concept of privacy and what it entails. Technology has made life fundamentally interconnected and changed the interpretation of what can be viewed as the private realm of the individual.

Alan Westin provided a definition of privacy that has fully integrated the complexities of the information age and aims to explain privacy in terms of control. Privacy, Westin defines, "is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."¹⁷

Westin has provided an interdisciplinary approach to analyze the nature and functions of privacy. The modern understanding of the concept of privacy is incomplete without placing adequate importance to issues such as new technologies for surveillance, as well as the demand for new and stricter privacy standards and protections.

Westin's model of informational privacy defined four distinct functions or reasons of privacy and four distinct states of privacy.

Four distinct functions -

- Personal autonomy
- Emotional release
- Self-evaluation,
- Protected communication

Four distinct states of privacy -

- *Solitude* - freedom from observation
- *Intimacy* - closeness among a small group of people
- *Anonymity* - freedom from being identified in public settings
- *Reserve* - the freedom to withdraw from communication.

Privacy for Westin was a fundamental part of civil liberty and he stressed on the importance of control that a person should have with regard to information disclosure.¹⁸ This view is largely the majority view with regard to privacy as most advocates of privacy argue that while some intrusion is fine and even undeniable, due to the nature of the information age, eventually the user should have the power to consent what aspects of and till what limit information should be shared with those conducting surveillance activities.

Privacy has various shades and is often best defined keeping the contextual framework in mind. Thus the advancement of technology has had a big impact on what can be considered the private realm of an individual and to what extent a reasonable expectation of privacy exists. Privacy as a right developed, keeping in regard the historical development of the right, keeping in focus the physical world and the worldly possessions of men. The realm of privacy extended over tangible objects and spaces, however in an increasingly interconnected digital world, technology has forced us to redefine the concept of privacy to extend over the digital world as well. It needs to be balanced against the bigger gains that can be achieved through the technological revolution.

"When privacy and its purportedly outdated values must be balanced against the cutting-edge imperatives of national security, efficiency, and entrepreneurship, privacy comes up the loser. The list of privacy counterweights is long and growing. The recent additions of social media, mobile platforms, cloud computing, data mining, and predictive analytics now threaten to tip the scales entirely, placing

¹³(Mar.25, 2018, 09:25 AM) <https://eet.pixel-online.org/files/etranslation/original/Mill,%20On%20Liberty.pdf>

¹⁴ AMITAI ETZIONI, THE LIMITS OF PRIVACY p.196 (1999).

¹⁵ JOHN DEWEY, LIBERALISM AND CIVIL LIBERTIES (1936).

¹⁶ Ibid.

¹⁷ National Research Council. 2007. *Engaging Privacy and Information Technology in a Digital Age*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/11896>.

¹⁸ Ibid.

privacy in permanent opposition to the progress of knowledge.”¹⁹

In the present day and age there are always tradeoffs taking place between what we value as private and the benefits that we may receive. Often we do not realize how much personal data and information we share in the course of everyday activities. The following are just some of the trade offs of privacy that we indulge in almost everyday.

- The monitoring of citizens in public places through CCTV cameras for the purpose of increasing public safety
- Collection of private details by e-commerce and social network sites in exchange for using their free services
- Collection of personal financial information by banks in order to evaluate credit rating of a person for the purposes of a loan

The vast reach of the internet and the seamless integration of a vast amount of digital devices in our life has redefined the relationship between an individual, his privacy, and the society. Technology has touched and revamped almost every aspect of our life be it entertainment, commerce, education, the modes of communication and even national security concerns. It has made the sharing of at least some form of information absolutely necessary and this has had an impact on what aspects of our information we can consider private anymore. The concern now should shift from the sharing of information to what purpose the information is being analyzed and used for. There are increased threats to privacy in the traditional form, but there are also great benefits to be achieved from it.

We may not be able to define privacy due to multifaceted nature of the concept, however it is a notion that is experienced and desired in some form or the other by all. Privacy is important because it provides a confidential space where people can express their true self and indulge in what ever activities they desire away from the gaze and knowledge of the outside world and society. “Only when we believe that nobody else is watching us do we feel free - safe - to truly experiment, to test boundaries, to explore new ways of thinking and being, to explore what it means to be ourselves. for that reason, it is in the realm of privacy where creativity, dissent, and challenges to orthodoxy germinate.”²⁰

That realm of privacy should be respected and protected, however, as soon as the consequences of an individual's act reach beyond him it becomes the concern of society at large. As more and more aspects of our lives get integrated with technology it is important that we put in place a regime that allows us to reap its benefits while saving us from

manipulation. Technology should now be seen as the opponent of privacy but as a concept that can revolutionize and enhance it.

III. SURVEILLANCE – INTELLIGENCE AGENCIES – PRIVACY: INTERPLAY

The word surveillance has its origin in the French language, derived from the words *sur* (over) and *veiller* (to watch)²¹. The term thus means to observe and watch a place(s) or person(s) for ongoing activity in order to gather information. The term encompasses the observation and scrutiny of both verbal speech and physical behaviour. Surveillance is not a new phenomenon, since time immemorial we can find various instances of either private parties or the government (whatever form it may take) conducting surveillance practices. Espionage is one of the oldest, and most well documented, political and military arts. Surveillance activities and privacy are essentially contradictory notions since the fulfillment of one would lead to intrusion upon the other. In the present with technology is playing such a big role in almost all aspects of life, intelligence and law enforcement agencies have had to alter their approach to surveillance. Essentially however they perform the same function, it is just that their field of operations has expanded. Due to the creation of a digital identity, much like a physical identity, intelligence gathering to has had to expand its digital presence. Thus digital and physical surveillance are two sides of the same coin. The changing nature of threats has meant that the state has to extend policing activities on to the digital sphere.

The nature of intelligence and law enforcement activities is such that it relies on information. There are 3 main information related activities that these agencies conduct.

- collecting and analyzing information to determine if there has been some violation of the law.
- If in case there has been a violation of the law, then to identify from the information available who is responsible for such a violation
- To gather proof against the person so that he may be tried and convicted by the established procedure of law

Information gathering is in the very nature of intelligence activities, and surveillance is the method to gather this information. If majority of the information sharing is being done online and through digital devices, then these are the resources that intelligence agencies must focus on. This directly leads to increased digital surveillance and some level of intrusion.

Surveillance tools and equipment can help identify terrorists and criminals and thereby protect the security of

¹⁹ Julie E Cohen, “What Privacy Is For”, *Harvard Law Review* (2013), Vol. 126, at page 1904.

²⁰ (Mar.23, 2018, 11:05 AM)

https://www.ted.com/talks/glenn_greenwald_why_privacy_matters

²¹ (Mar.22, 2018, 04:00)

<http://ro.uow.edu.au/cgi/viewcontent.cgi?article=2510&context=infopapers>

society. Through means such as observance and reconstruction crime can be reduced and more criminals and lawbreakers can be caught.

“ Throughout American history, intelligence has helped secure our country and our freedoms, intelligence is central to liberty, not in tension or at odds with it ”²²

The tension and conflict between privacy and security arises mostly due to the nature and intrusive scope of these intelligence-gathering and analysis activities.

For the purpose of national security, the role of law enforcement and intelligence gathering agencies is to ensure that its government knows all the secrets of its adversaries or potential adversaries while at the same time ensuring that these adversaries know none of the government's secrets. Hence not only do surveillance practices help in catching a suspect after a law has been violated, but they can also warn about possible future threats.²³ This why intelligence-related technological capabilities are often kept secret. The process itself requires and inherent need for secrecy.

A lot of intelligence work is based on second guessing and connecting the dots, this is the main reason why intelligence activities need a wider net of information interception.

“ In an extraordinarily difficult job, one in which actions are second-guessed, success is unreported, and failure can be catastrophic, the men and women of the intelligence community, including the NSA, consistently follow protocols designed to protect the privacy of ordinary people. they know that if another 9/11 or massive cyber-attack occurs, they will be asked, by Congress and the media, why they failed to connect the dots.”²⁴

The mantra that Prevention is better than cure holds as much importance in matters of national security as it does in medical matters. The primary aim of the authorities is to prevent hostile acts from taking place in the first instance, hence the need to be proactive. Unfortunately, due to the changing nature of modern threats it is often impossible to determine, before the fact, where the threat might arise. A wide net must therefore be cast in order to determine whom to target. While this gathering of information may pose some risk to the right of privacy it is needed to enhance national security. These agencies are then often caught in the middle of a difficult situation; if they fail to prevent an attack they are criticized for not using the latest techniques and technologies and if they gather information they are criticized for invasion of privacy. It is often not known in advance what specific information must be sought in order to recognize a suspicious

pattern, especially as circumstances change. From the perspective of intelligence analysis, the collection rule must be “collect everything in case something might be useful.” Such a stance generates obvious conflicts with the strongest pro-privacy advocates who argue, “Don’t collect anything unless you know you need it.”²⁵

Freedom comes with reasonable restrictions, in terms of protecting and securing the nation and its society the restriction is government surveillance. Nowadays, the greatest threat is terrorism from non-state actors. It is originating from unknown sources and targets. While technology has provided a platform to innovate and bring about positive changes, it can also be abused by other less desirable elements to carry out their sinister plans. Just as it facilitates and helps you to communicate with your parents located in another continent, it also helps terrorists and criminals communicate with each other. The internet does not know which is which, this is the job of intelligence agencies. Fringe elements and groups like ISIS and Al Qaeda have increased their virtual presence, using the internet to spread their propaganda and recruit people. Just to provide a few examples

- In February 2016, the National Intelligence Agency (NIA) arrested software engineer Mudabbir Mushtaq Shaikh along with several others. He was reportedly recruited by a Syria-based Indian who trawled through the Internet looking for recruits in India. The modus operandi is reportedly to search for accounts of people who post on the topic of Islam and watch videos of fiery speeches by clerics so on. Such people are then traced, contacted and then wooed to join ISIS. In 2013; Shaikh came across an account run by a man called Yusuf al-Hindi. A former Indian Mujahideen member and the leader of ISIS's Indian cell. The two of them first met in a group called "Dajjal-e-Akbar" and started interacting through Skype.²⁶
- ISIS has developed sophisticated Internet technology for attracting new recruits and planning attacks. It has developed its own encrypted chat for spreading its propaganda. As discovered and reported by the counter-terrorism network Ghost Security Group, which had previously flagged ISIS communications over the app Telegram, terrorists are communicating over a new secure Android app Called “Alrawi”. The encrypted chat app makes it harder for governments and security agencies to spy on terrorist plans.²⁷
- According to a BBC report, Isis extensively uses Twitter to provide details of its operations, including the number of bombings, suicide missions and

²² Barack Obama - Llyod.C.Gardner, The War on Leakers: National Security and American Democracy, from Eugene V. Debs to Edward Snowden, (New Press, 2016).

²³ National Research Council, Division on Engineering and Physical Sciences, Computer Science and Telecommunications Board, Committee on Privacy in the Information Age, National Academies Press, 28-Jul-2007.

²⁴ Barack Obama - <https://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html>

²⁵ John L. Hennessy, David A. Patterson, and Herbert S. Lin National Research Council, Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, (The National Academies Press, Washington, D.C. 2003).

²⁶ (Mar.21, 2018, 10:25 AM) http://www.huffingtonpost.in/2016/03/22/isis-uses-internet-to-rec_n_9519976.html

²⁷ (Feb. 20, 2018, 10:25 AM) <https://techcrunch.com/2016/01/16/isis-app/>

assassinations it has carried out, and of checkpoints and towns it controls. The top Twitter hashtags used by the group include: "#Baghdad_is_liberated" and "#Iraq_is_liberated". In addition to the hashtags, the group produces professional promotional videos and urges support for its "one billion campaign", which calls on Muslims to post messages, photos and videos on Twitter, Instagram and YouTube in support of Isis. One video, posted on 17 June 2014 showed an Isis member speaking in French and asking Muslims to support Isis's cause online. Many videos are also posted with English subtitles or translation.²⁸

- Reports have suggested that the Paris attackers used sophisticated tools like burner cellphones and encrypted laptops to eliminate any digital trail.²⁹
- Minister of State for Home Haribhai Parathibhai Chaudhary said in Rajya Sabha, "ISIS is using various internet-based platforms for propaganda and to propagate its ideology. The intelligence and security agencies monitor the cyberspace closely to identify potential recruits and keep them under surveillance and take further action, if necessary."³⁰

It is the primary responsibility of the state to ensure that the basic objectives for its formation - welfare, national security are guaranteed and protected. This can be ensured through effective surveillance. There is always a tradeoff between privacy and security since information gathering is the job of intelligence. Governments by definition have to prioritize security and legality over morality and popularity.³¹

"Highest on the list of "lessons learned" from the September 11th terrorist attack was the need for a retooled intelligence enterprise that could "connect the dots" and keep us safe. The intelligence apparatus in place on September 10th was not built for that purpose. The imperatives of the Cold War were to deter conflict and maintain the peace; the overarching challenge, which US intelligence met so brilliantly, was to collect ever more refined insights about a known antagonist. Today, the collection targets are unknown (what are the indicators of terrorist activities that we should be watching?), and our principal objective is to take action to defeat and dismantle threats in order to keep us safe.

Don't intrude but keep me safe. How to square such a circle?

Interconnected global networks of digital data have become the single most important source of intelligence warning of

*threats, enabling our defense at home and the advancement of freedom abroad. To say "hands off," as some shortsighted privacy advocates have been doing, will not preserve our liberties, it will endanger them. It should be possible for an enlightened citizenry to empower government action in that sphere without forfeiting the very rights that our government exists to secure. That challenge is, at the very least, a part of the continuing experiment that is our democracy."*³²

- Michelle Van Cleave, Head of US Counterintelligence under President George W. Bush

IV. THE BIG BROTHER CONCERN

There is a strong need to dispel concerns and notions associated with surveillance that portray it in a "Big Brother" manner. The chief concern is that of data misuse or abuse and its consequences.

There are often various apprehensions relating to the fact that if the data being collected is being used for the right or intended purpose. This is an issue of concern because even though a specific dataset might not have information that can be misused, but through the practice of fusion or integration with other datasets it can effectively prepare a comprehensive profile of a person. It is imperative that the data collected is only used for its specific purpose and not for data fusion. In the modern age there does exist a great imbalance between the power of the state to collect information and the power of the individual to withhold such information. The scales are tipped in the favour of the state and it is only natural that such an imbalance would cause people to worry about the possible misuse of these powers by the state. Privacy thus becomes an important concept in this context and data sharing is but one element of this concept of privacy. Privacy is necessary for exercising liberty and other guaranteed fundamental rights such as the freedom of thought and expression. The concern that surveillance and privacy raise are that, and as has been pointed out by various pro-privacy advocates, surveillance causes people to self-censor and change their behavior. For example - surveillance may reduce the likelihood of someone attending a public protest or demonstration out of the fear that he may be targeted for dissenting. This sort of an effect can affect the entire society by breeding homogeneity.³³ They argue that surveillance does not leave a physical trail but works insidiously upon the minds of the targets, restricting their actions and thoughts into heterodoxy and conformism.³⁴ This kills the plural fabric of society and takes society from

²⁸ (Feb. 21, 2018, 09:25 AM) <http://www.bbc.com/news/world-middle-east-27912569>

²⁹ (Feb. 22, 2018, 11:30 AM) <https://theconversation.com/burner-phones-social-media-and-online-magazines-understanding-the-technology-of-terrorism-56727>

³⁰ (Feb. 21, 2018, 12:50 PM) <http://business.financialpost.com/investing/why-data-is-the-new-oil-and-what-it-means-for-your-investment-portfolio>

³¹ (Mar. 12, 2018, 07:32 AM) <http://www.zdnet.com/article/state-surveillance-may-be-a-fact-of-modern-life-but-having-nothing-to-hide-is-not-an-excuse-for-apathy/>

³² (Mar. 12, 2018, 10:45 AM) <http://www.worldaffairsjournal.org/article/what-it-takes-defense-nsa>

³³ National Research Council, Division on Engineering and Physical Sciences, Computer Science and Telecommunications Board, Committee on Privacy in the Information Age National Academies Press, 28-Jun-2007.

³⁴ (Mar. 15, 2018, 10:12 AM) <http://www.rediff.com/news/column/why-privacy-is-important-and-all-need-it/20171004.htm>

being composed of citizens and leaders to one comprising of subjects and rulers.³⁵

The main problem with these concerns and this line of thought is that it interprets surveillance in an incorrect manner. The above listed problems have nothing to do with the carrying out of surveillance practices. These concerns are caused by the friction and trust deficit in the relationship between Man and Society on one hand and Man and State on the other. It is not the collection of information through Surveillance but the consequences of the processing and analysis of such information that create this problem. If an individual is satisfied that his personal information will only be used for the relevant required purpose and not to target him, then he will not hesitate to provide this information. Thus this is not a debate about whether such capabilities should exist and be used but about what aims are being achieved by using such technology. It is not a problem of the policy in place but the problem of the implementation of that policy. Emphasis should be put on the use of information and not its collection. As far as the problems of killing dissent and non conformity are concerned, these are problems that are brought about by the nature and set up of society. Surveillance doesn't kill the existence of a free and open society, but often it is the members that comprise this society that constrain an individual and his expression. The society should allow for dissent, non- conformity and the expression of individualism. Surveillance is like a watchful eye that needles out the troubling elements, who and what these troubling elements are is decided by the society and the people. As in the case of the example provided above, it is upto to the society to view whether someone attending a demonstration is bad or not. Just the mere fact that surveillance is being conducted does not lead to a "Big Brother" scenario. The government should build trust amongst society so that people do not fear it. After all the government is for the people and not the other way around. This can be done by bringing in adequate oversight measures and external constraints on the use of such gathered data.

A Group of Experts constituted by the Government of India proposed a framework for the protection of privacy concerns, which would serve as a conceptual foundation for any future data protection legislation.³⁶

The framework suggested by the expert group was based on five salient features:

- (i) Technological neutrality and interoperability with international standards;
- (ii) Multi-Dimensional privacy
- (iii) Horizontal applicability to state and non- state entities

³⁵ Edward Snowden - <https://techcrunch.com/2014/10/11/edward-snowden-new-yorker-festival/>

³⁶ Report of the Group of Experts on Privacy" (16 October, 2012), Government of India, available at http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf. Taken from Writ Petition (Civil) No 494 of 2012, J.Puttaswamy v Union of India.

- (iv) Conformity with privacy principles
- (v) A co-regulatory enforcement regime.

In this regard the California Electronic Communications Privacy Act³⁷ enacted by the state of California, USA has a comprehensive data protection regime in place. Some of the main provisions of the act are –

- Government entities will have to obtain a warrant in order to collect or gain access to electronic information, including both content and metadata.
- In the case of metadata, four exceptions have been provided where a warrant may not be obtained
 - When consent from the information's owner has been received
 - If the device containing the sought information is taken from a prison inmate
 - In an emergency situation involving danger of death or serious physical injury
 - If the device is believed to be lost, stolen, or abandoned, and if access is sought in order to try to "identify, verify, or contact the owner or authorized possessor of the device"
 - In emergency situations, the government must file an application for a warrant within three days of obtaining the electronic data.
- The warrant must expressly describe the information. Any information that has been obtained but was not expressed in the warrant "shall be sealed and not subject to further review, use, or disclosure" without a separate court order.
- When a service provider voluntarily shares data with the government, the information must be destroyed within 90 days, subject to certain exceptions
- The law also allows any individual involved in a judicial proceeding to move to suppress and destroy any information "obtained or retained in violation of the Fourth Amendment" or of the law.

V. CONCLUSION

Alan Dershowitz - No state has ever survived without some surveillance, and no state deserves to survive if it has too much surveillance.³⁸

As the digital age progresses and newer innovations are introduced, it will bring about fresh challenges and concerns. The use of technology in surveillance is like a double-edged sword; in the right hands it can be a tool for empowerment and in the wrong a tool for tyranny. There is a need to strike a balance between privacy and surveillance, but such a balance should not eliminate the power of the government to conduct surveillance activities. Some control and oversight is

³⁷

(http://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=20152016_05B178

38 (Mar.18, 2018, 10:42 AM) <https://www.theglobeandmail.com/opinion/is-state-surveillance-a-legitimate-defence-of-our-freedoms/article18368244/>

necessary and important but they must not hamper the goal of national security.

Another important issue that needs to be addressed by nations around the world is the interplay of privacy – technology - surveillance. The gathering of information alone cannot said to be a violation of privacy, however it is important to maintain a check on how that information is collected, and what goal the analysis of this information achieves.

It is also important that governments build a trust relationship between the people and their intelligence agencies. The more trust there is between the two, the easier it will be for these agencies to continue carrying out their important work and for the government to address and reasonable concerns that the public might have. It is important that a transparent and well functioning system backed by adequate check and oversight is put into place. Citizens who have faith in their government are more likely to cooperate. The creation of such a system requires a balance to be achieved between individual interests and the legitimate concerns of the state.

The right to privacy, while important and necessary, must accommodate some exceptions. These exceptions must be based on the principles of legality, the concerns of the state and proportionality. The issue should not be government agencies should be allowed to engage in particular forms of surveillance or information collection but rather about the goals, type of technology, and data involved, and what kinds of oversight and accountability procedures are in place.

We are witnessing the creation of a democratic form of surveillance where individuals willingly exchange data and allow themselves to be subjected to monitoring and algorithmic processes in exchange for the benefits of services, welfare and security.³⁹ The choice is not between liberty and privacy on one hand and national security on the other, both can be achieved together.

³⁹ (Mar.18, 2018, 11:50 AM) <https://thewire.in/170689/right-to-privacy-data-protection/>