DE JURE NEXUS LAW JOURNAL

Author:

Rihan Shareef

Symbiosis Law School, Noida

2nd Year, BA LL.B.

CYBER SURVEILLANCE BY LAW ENFORCING AGENCIES

Abstract

This article aims to examine the surveillance carried out by various law enforcement agencies around the world with the focus to India. It will examine the legislations, the constitutional safeguards recognised by the courts and executive actions taken by various governments over the years. It will also look into the judicial model adopted by India for its investigation, the history of abuse by law enforcement agencies across the world and its denial of the same. The recent controversies regarding the IT Rules and the Pegasus scandal have been discussed. Through this article a conclusion is drawn to understand what is required to ensure a constitutionally just and fair democratic society with respect to balancing of an individual's right to privacy and the interest of the State.

Keywords

Right to Privacy, State Surveillance, Constitutional Law, Cyber Law, Pegasus, IT Intermediary Rules 2021

Introduction

Recently with the Pegasus surveillance software's leak of potential targets has been released by a group of reputed organisations and media houses. The discussion on cyber surveillance by the government and its agency have reached its unprecedented heights and become a

mainstream subject. However, the issue and controversy around cyber surveillance is not new and has been taking place ever since the popularisation of the internet. Even before the use of internet, surveillance by executive and law enforcement agencies have been of much controversy with the use of other technologies such as telephones, popularly known as 'phone-tapping' or being 'bugged.' Although the technology has evolved, we will examine whether the law and judiciary have been able to keep up with it.

Formation of Right to Privacy and Surveillance

The conflict between the right to privacy recognised as a fundamental right in the landmark KS Puttaswamy Judgement and the use of investigative methods such as surveillance has been long present and debated by the Supreme Court. However, the conversation regarding right to privacy and surveillance by government agencies were discussed in foreign jurisdictions, primarily in the United States. Some of the landmark judgements given by US Supreme Court pre-dates Indian Supreme Court's position by decades.

The first of its kind was a judgement made by the United States Supreme Court in 1967, when overhearing telephonic conversation of a person with the usage of recording devices in a phone booth by the Federal Bureau of Investigation (FBI). The court held it to be unlawful search and seizure from which the individuals are protected through the fourth amendment rights.[1] Justice Harlan's judgement made it clear that "*a person has a constitutionally protected reasonable expectation of privacy*". This was one of the first-time courts held the right to privacy in relation with law enforcement agencies.

In the United Kingdom and other parts of European Union, it was through legislation that the right to privacy was formalised as a general right. In the year 2000, the European Convention of Human Right was held. Article 8 of the convention laid an explicit guarantee to the right to privacy as a general right.[2] Previously, the common law had recognised the right to privacy as a family right or to abortion, but these did not in its scope include the right against surveillance.

The status of right to privacy in India remains the on the most fragile grounds. The Supreme Court of India recognised the 'right to privacy' under the ambit of Article 21 in Right to Life and Liberty, in the landmark judgement of KS Puttaswamy v Union of India. This right is

[1]Katz v. United States, 277 U.S 347 (1967)
[2] European Convention on Human Rights, 2 October 2000, ETS 5, 8

subjected to the procedure established by law. The procedure established by law can be considered as a reasonable restriction on the right. However, despite not recognising right to privacy explicitly before this judgment . The Supreme Court did step-in the matters of Police surveillance of individuals and striking such actions down. The first instance of such sorts took place in MP Sharma v. Satish Chandra. The Supreme Court had held that visits to the residence of the accused by the police was violative of liberty constitutionally guaranteed. While the Court denied the existence of right to privacy as a guaranteed right in our constitution.[3] In another case, once again dealing with surveillance by police, the Supreme Court for the first time read in that the right to privacy flows from the right to life and liberty.[4] In a 1973 case law Supreme Court also recognised that listening to conversations of an innocent person's telephone is a violation of his fundamental rights.[5] I will explore how Indian Courts protected its citizens from laws that could be used for state surveillance through Constitutionality other than the right to privacy in the next section.

Two Models of Criminal Process

In order to understand the nature of surveillance framework that is dispensed by the law enforcement agencies. It is necessary to examine the legal framework that the country is built upon. US Jurist Herbert Packer classified legal framework of countries in two models based on their underlying values. The first model is the crime control model, this a process of criminal law which lays its emphasis on screening suspects, determining guilt, and trying convict them of crime. The second model is the due process model which protects and safeguards individual liberty from the actions of the state. It ensures that the procedure and process of investigation is taken in such a manner that the dignity of the individual would not be compromised. [6]Governments increasing have adopted practices which laydown certain vague terms such as national security, interests of the nation and similar phrases to put an undue suspicion on the individual. Most of which would fall under the first model of 'crime control.' The due process of law takes more of a secondary role. The idea essentially is that everyone is seen as a suspect to a crime and can be under the lens of the law enforcing agencies. While, understanding the effect of these laws it is not that these law would be misused by the government in a democratically elected country. The fact is that the far-

[3] MP Sharma v. Satish Chandra, 1954 SCR 1077: AIR 1954 SC 300: 1954 Cri LJ 865
[4]Gobind v. State of MP (1975) 2 SCC 148
[5] R. M. Malkani v. State of Maharashtra (1973) 1 Supreme Court Cases 471:1973 Supreme Court Cases (Cri) 309
[6]GAUTAM, THE TRANSFORMATIVE CONSTITUTION, ,303 (2019)

reaching powers that the government has under these rules, it can be an arena of possible abuse. This has been held by the Supreme Court in State of MP v. Baldeo Prasad when it held a law unconstitutional when far-reaching power were granted to the executive. [7]Thus, it is pertinent to ensure that such methods of investigation by law enforcement agencies which falls under the garb of surveillance are restricted. The very fear of such abuse of power through such an action can curtail an individual to act freely as it they are entitled to in a free democratic set-up. In a country such as India it is of utmost importance to follow, the due process model. This was accepted in the Selvi v. State of Karnataka judgement as well. [8] As citizens of marginalised communities are still extensively policed, and the justice machinery is disproportionately represented by those of the upper castes. The due process model holds a greater ideal of constitutional safeguards against any possible coercive action by the act of surveillance. The Shreya Singhal judgement which read down Section 66-A of the IT Act by the Supreme Court for curtailing the right to free speech as laid down in Article 19(a) made the importance of free speech in a democracy.[9] The jurisprudence laid down by the Supreme Court through the various judgements was all for limiting the influence of government law enforcing agencies.

Cyber Surveillance Around the World and India

The distinction between surveillance and cyber surveillance remains unclear as increasingly ordinary everyday items get connected to the cyberworld or uses and stores data on the cloud services online. Something as simple as door when made electronic makes it connected to the cyber world.

The reason there is little knowledge about Cyber Surveillance and even surveillance in general done by law enforcement agencies is the lack of public information regarding this. The dearth of reliable information is so extreme that, we are largely unaware of which law enforcing agency is conducting surveillance and on what basis such action is taken. Hence, the only information we get is through reports of investigative journalists and those working to keep internet a safe space. Journalists report that cyber surveillance is a reality all over the world as early as the 2000s and 2010s. However, by far the worst and the most totalitarian is that of China.

[7] State of Madya Pradesh v. Baldeo Prasad, 1961 AIR SC 293
[8] GAUTAM, THE TRANSFORMATIVE CONSTITUTION, 319 (2019)
[9] Shreya Singhal v. Union of India, (2015) 5 SCC 1

China being an anti-democratic country repressed information from and to the public by creating a wall which banned access to certain information. In order to keep this strict and controlled the government monitors, stores, analyses and acts on billions of telephonic records and internet communication. The scale of the operation is humungous to say the least. With the lack of any judicial oversight, and no barriers from a democratic society, it was free to do what it was doing. However, one would think things would be different in a democratic society such as United States.

The United States significantly changed its policy after the 9/11 attack in 2001 by Al-Qaeda. It started to aggressively monitor telephone lines and internet communication through the National Security Agency (NSA). This was done through an executive order by the President in a program called the Presidents Surveillance Program. In the United States such executive orders are equal to public law. This effectively made the program free from all judicial interference. Earlier, it had NSA had to file for a request to search in secret court, Foreign Intelligence Surveillance Court (FISA). This information came into knowledge of the public through a report by New York Times.[10] This led to distress and worry amongst citizens, especially criticising the executive nature of the order. Hence, the government retrospectively legalised the program through two legislations, Protect America Act (2007) and Foreign Intelligence Surveillance Amendment Act (2008). However, the US Surveillance Program was multiple times bigger than what was previously expected. All of which came into light when Edward Snowden, former NSA agent revealed it to the world through a series of interviews in 2013. Before Snowden's interview it was one of the deepest guarded secrets in the United States. The project was called STELLARWIND, it was used to collect data of anyone it wanted and hence no court could ever be able to meet the speed required to meet needs as surveillance was constant. The US government exploited a technicality to legalise the program. The government said to 'obtain' or ''acquire' the data did not require a warrant as warrants are only for 'search and retrieve.' This legal jargon was exploited by the government to spy on its citizens and citizens of the world. [11] However, the US Supreme Court is of strong opinion that the digital data reveal into the life of person and requires larger privacy as compared to other physical actions. It decided in Riley v. California, that when the law enforcing agency when going through a mobile phone without a warrant as an

[10] https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html
[11] SNOWDEN, THE PERMANENT RECORD, 177 (2019)

unconstitutional act and illegal search. The reasoning was that mobile had much more personal information compared to the interest of the government in procuring such data. [12]

The situation in India is extremely vague at the moment due to the absolute lack of information currently. There is no reliable source which has declared that any particular law enforcement agency does spy on its citizens or even the accused for that matter. However, the apparent conflict between Article 21 which guarantees right to privacy and laws which grant permission to Indian law enforcing agencies. Section 69 of the Information Technology Act grants the government power to intercept through any data to prevent a cognizable offence. [13]The power granted here is so wide that one could argue that government needs to provide no reason at all. Section 5 of the Telegraph Act gives governments the right to intercept any telephonic conversation if it is required for public safety. [14]There is no need for judicial oversight for the laws and the executive can act according to their own discretion. Despite this, the conversation on state surveillance was minimal in India. However, with the notification of the IT Intermediary Rules 2021 and the Pegasus Scandal controversy has reached a point like never before.

Recent Controversies

The first controversy arose when the Ministry of Electronics and Information Technology notified the new IT rules for intermediaries which provide platform for other to put in content. Previously, section 79 of the Information Technology Act, 2000 gave immunity to social media intermediaries to content posted by others. [15] However, with the effect of these rules, all intermediaries will be liable if they fail to comply with these rules. The compliance requirements are broad in nature, it includes appointment of grievance officers, following the orders of the government to share and take down any piece of content including private chats and any publisher of news or current affairs content shall need to inform about their activities to the government prior. The question arose whether the IT Rules had legalised surveillance of citizens to a certain extent. This was confirmed by the data published by Internet Freedom Foundation, which revealed than more than 12,000 tweets and two lakh WhatsApp accounts were given takedown notices and banned, respectively. The lack of transparency with regard

[12] 13-132 U.S. Reports 1 (2013) Riley v. California
[13] The Information Technology Act, 2000, §69.
[14] The Telegraph Act, 1885, §5(2).
[15] The Information Technology Act, 2000, §79.

to the takedown and bans was the troubling aspect. [16]There was no explanation given except for the fact that it was in the 'national interest' such an action was taken. It also necessary to note that all actions taken are by the government executive, the judiciary is not involved in this process. These are troubling aspects which would make us question whether we are going into a surveillance regime.

The Pegasus Scandal heated up the conversation further which lead to widespread protest into the parliament and filing of petitions by plethora of prominent personalities in the Supreme Court. The allegations made was the result of a report filed by massive team of investigative journalists from all over the world, under the Pegasus Project. The team also includes French media house Forbidden Stories and reputed human rights organisation Amnesty International. Pegasus is the most advanced software in the world operated by Israeli NSO group. The reason it is dangerous is that is can access everything on your phone, including all your photos, chats and it can even turn on your microphone and camera. All of this without your knowledge and any action of yours. [17]It can be injected to your phone without knowledge. If the Pegasus is used by governments across the world to spy on anyone other than the most dangerous terrorists of the world, it would fit the description, "the big brother is watching." The allegations made by the investigative journalists include tracking of reporters, lawyers. Human rights activists, Opposition leader and even the Information Technology Minister himself who denied the allegations in parliament by the Central Government. The Central government has denied all allegations in the Supreme Court as well.

Conclusion

Surveillance by government and law enforcement has steadily evolved over the years from intervening into telephonic conversations to the mobile phone covering every aspect of our lives. The jurisprudence regarding the same as evolved from earlier reluctance from the courts around the world to recognising the right to privacy as a fundamental right. However, we also realise that cyber surveillance largely takes place in a highly secretive form and is outside the knowledge of the public domain. Although reports have revealed different areas and methods of surveillance, the specifics remain unknown. This makes enforcing of

[16] Internet Freedom Foundation, *Yes, the Government is Following You*, 17th July 2021 Available at https://www.linkedin.com/posts/internet-freedom-foundation_revealed-transparency-reports-activity-6821819816098242560-G_WF/ (Last visited at August 14th 2021)

[17] Guardian, *Pegasus: the spyware technology that threatens democracy – video*, 19th July 2021 Available at https://www.theguardian.com/news/video/2021/jul/19/pegasus-the-spyware-technology-that-threatens-democracy-video (Last visited on August 15th 2021)

guaranteed fundamental rights difficult. Further the conflict between existing laws and constitutional provisions remains unsettled. The balancing act between legitimate government interest for best interest of the nation and an individuals need to privacy needs to be balanced. However, the former CIA agent and whistle-blower has called for ban of the surveillance industry as it is used only for civilians rarely to militants and terrorists. [18] As we have seen historically governments deny the usage of any such devices despite the surmounting evidence provided. They also brought in legislations to retrospectively to protect the previous abuses of law enforcement agencies. The need of the hour is for governments to accept abuses of law in the past and pave way for more constitutionally just path. There needs to a proper discourse among the leaders across the world and people from various industries including journalists, lawyers, human rights activists, and security experts and create a global solution to the issue. This will bring in clarity and prevent the world from slipping into dictatorial regime which is a common sight where surveillance begins.

[18] Guardian, *Edward Snowden calls for spyware trade ban amid Pegasus revelations* , 19TH July 2021 Available at https://www.theguardian.com/news/2021/jul/19/edward-snowden-calls-spyware-trade-ban-pegasus-revelations (Last visited on 16th August 2021)