STATE SURVEILLANCE AROUND THE WORLD

Written by ***Armaan Natt***

5th Year BA LLB Student, Rajiv Gandhi National University of Law, Patiala

ABSTRACT

The growth and evolution of technology has brought about far reaching changes. Surveillance activities have been conducted since time immemorial. Almost all regimes have used some form of surveillance, while history has numerous examples of such practices. The modern day state coupled with innovations resulting in increasingly sophisticated technology has led to a transformation in how surveillance is now conducted. The means and methods of surveillance have developed and this has resulted in surveillance shifting from the physical realm onto the digital realm. The digital space and the Internet are now fertile grounds for conducting such activities, Further, modern surveillance practices over the Internet have also been discussed along with providing a glimpse into various surveillance laws around the world. The development of laws in countries such as USA, UK, India along with international organizations has been examined along with specific surveillance programs conducted in these countries. Lastly suggestions have been provided that should be incorporated in modern data laws so that users are provided certain rights and protection against surveillance activities.

INTRODUCTION: THE IMPACT OF TECHNOLOGY

Technology has without doubt had a massive impact on society. As a matter of fact, we experience this effect in our daily lives. It has an effect on the growth of the economy, our culture and our living standards. The world has changed in a multitude of ways in the past two decades owing to the rapid advancement of technology. Today big data, artificial intelligence, smartphone technology are all being used to deliver solutions for real-world problems in the

furthermost corners of the globe. We are seeing societal transformation in a way that has never been seen before. Digital technology is permeating every part of our lives, and aiding access to education, health, or availability of clean water.[1]

While it is true that technology and the internet have undoubtedly made our lives simpler and easier, it is important to keep in mind that technological advancement has affected human life both positively as Well as negatively. There are several indications of threats to life and society in the future due to the misuse of modern technology. While the development of technology has brought about economic development, it has at the same time brought about radical changes in the social and cultural spheres of society. The main concerns with widespread use of technology and this infinite amount of data creation are the issues of privacy and regulation.

On one hand, this data can be used to make tools and services better, and more personalized but on the other, there is a very real possibility that this data can also be used to manipulate consumers or worse be used for identity thefts and other crimes. Once a sufficient number of people have independently 'consented' to exchange personal information in return for services and efficiency, the resulting social structure can no longer sustain a culture of privacy, even for those who withhold.[2] Respect for privacy rights and expectations is integral to ensuring trust in the Internet, and maintaining its near universal use and access. Privacy concerns have also developed with regard to surveillance that can be conducted on users based on the data generated. Personal devices used by many people such as those which consist of the Internet of Things collect and analyse highly personal data. Combined with different data bases on the same user they can create a virtual digital portrait of a person and reveal much more information about him than a single dataset can. For example, a user's Internet-enabled toothbrush might capture and transmit innocuous data about a person's tooth-brushing habits. But if the user's refrigerator reports the inventory of the foods he eats and his fitness-tracking device reports his activity data, the combination of these data streams paint a much more detailed and private description of the person's overall health.[3] Data analytics when applied to large and multiple

[1] *Available at* http://www.livemint.com/Home-Page/2cZuBVmUOh1eVSY3MIWldP/For-greater-good-How-digital-technology-is-redefining-socia.html

[2] *Available at* https://thewire.in/170689/right-to-privacy-data-protection/

[3] *Available at* http://www.cbc.ca/news/technology/data-is-the-new-oil-1.4259677

databases, can cause a substantial risk of privacy invasion and potential discrimination. In a world increasingly being dominated by the internet and now the ever expanding 'internet of things', there are a long list of services such as social media, tailored products, national security that will require this constant barter between data collection and delivering services thus making digital privacy even more difficult to achieve.

INTERNET SURVEILLANCE

The means and methods of carrying out surveillance have developed at a rapid pace. Modern technology has introduced sophisticated devices for conducting surveillance. Since the mode of communication has changed dramatically, surveillance practices have followed suit. Now most of the communication and activity takes place and digitally and thus that is the realm that needs to be monitored. The widespread use of technology can replace the extensive deployment of manpower needed earlier, as most of these operations can be carried out by unmanned machines thus leaving officers to focus on other aspects of the investigation[4] Some of these practices have been criticized by privacy right activists who argue that the use of technology has resulted in mass surveillance programs, where entire populations have been subject to constant monitoring thus affecting their civil liberties, instead of targeted surveillance which the earlier traditional methods focused on.

In the modern age digital surveillance has become the norm rather than the exception. Technology has resulted in the creation of digital self, apart from the physical being. Surveillance has thus shifted from the physical to the digital realm. It is now of as much if not more to monitor the digital presence of a person as carefully as his physical presence. It can rightly be said that a man's castle has moved from his home to his phone. It has resulted in a state where it can be undeniably said that man is more honest with his search engine than his family. The most important and revolutionary innovations of this age have turned into virtual snooping devices, aware of your every move. Our relationship with technology and the internet has reached a very high level of connectedness. This is why digital surveillance has replaced

[4] *Available at* http://work.chron.com/types-surveillance-criminal-investigations-9434.html

traditional methods of intelligence gathering. Digital surveillance involves the monitoring of computer activity and the data generated and transferred as a result of these activities. Digital surveillance has different forms. The reach of these technologies is astonishingly broad: there are now technologies in place that can listen in on cell phone calls, use voice recognition to scan mobile networks, read emails and text messages, censor web pages, track a persons every movement using GPS, and even change email contents while en route to a recipient.[5] Some tools are installed using the same type of malicious malware and spyware to steal credit card and banking information. They can secretly turn on webcams built into personal laptops and microphones in cell phones not being used. And all of this information is filtered and organized on a massive scale in virtually limitless databases. It is estimated that the world's capacity to store information has reached 5 zettabytes (expressed as $10^{21)}$ in 2014.[6] It is then imperative that we develop a better understanding of the technical jargon involved in digital surveillance. Some important terms involved have been expalined in order to gain a better understanding of what digital surveillance entails and how it is carried out over the internet.

- IP (Internet Protocol)

IP (Internet Protocol) is a connectionless protocol used for transmitting data over a network. Data is divided into independent packets containing the IP address of both the sender and the recipient. Each computer or network device has its own unique IP address.[7]

- IP Address

An IP address is the unique address of a computer or network device connected to that network. IP addresses allow those network computers and devices to locate each other and transfer data back and forth.[8]

[5] Musa Khan Jalalzai, *The Crisis of Britain's Surveillance State: Security, Law Enforcement, and the Intelligence War*, Algora Publishing, 2014

[6] *Gillings, Michael R.; Hilbert, Martin; Kemp, Darrell J. (2016). "Information in the Biosphere: Biological and Digital Worlds" Trends in Ecology & Evolution*

[7] *Available at* https://www.videosurveillance.com/glossary/

[8] ibid

- Data Packet

A data packet is a basic unit of communication over a digital network. When data has to be transmitted, it is broken down into smaller structures called packets. Once they reach their destination these packets are then reassembled and reconstructed to form the original data. IP packets travel over the Internet through nodes, which are devices and routers found on the way from the source to the destination. Every activity on the Internet involves the use of these data packets, from every webpage you visit to every email you send.[9] An IP packet includes amongst other technical data a combination of

- The source and destination IP address, which are the IP address of the machine sending and receiving information
- The sequence number of the packets so that the data can be reassembled[10]

- Splitters

Modern day communication involves the use of optic fibers to transmit information from one place to another. Since the communication grid of the Internet involves the whole world, there are often large undersea cables that are used to transmit data across continents. A splitter is essentially a device that can be used to tap into these cables and monitor the data that is passing through. The splitter that takes a single input of optical light and divides it into two or more outputs, thereby replicating the data passing through these fibers so that is sent simultaneously to both the intended recipient and to a monitoring station or device. [11]

- Cookies

Cookies are messages that web servers pass to your web browser when you visit Internet sites. Your browser stores each message in a small file, called cookie.txt. When you request another page from the server, your browser sends the cookie

[9] *Available at* https://www.techopedia.com/definition/6751/data-packet

[10] *Available at* https://www.lifewire.com/what-is-a-data-packet-3426310

[11] *Available at* http://www.cablinginstall.com/articles/print/volume-21/issue-3/features/tapping-its-not-just-for-phones-anymore.html

back to the server.Cookies are most commonly used to track website activity. It acts as your digital identification card. In this way, a web server can gather information about which web pages are used the most. The most common use of cookies has been by e-commerce sites which record a users personal information and track their shopping patterns and then provide recommendations based on that pattern.[12]

- Metadata

Metadata can effectively be described as data that describes other data. Thus it plays the important role of summarizing basic information about data.For example - a digital image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created**.** Metadata is crucial to the efficiency of information systems to classify and categorize data. Having the abilty to filter through that metadata makes it much easier for someone to locate a specific document and it allows analysts to unlock meaning in big data. [13]

Metadata is a sensitive topic because there is great potential for abuse. When conducting surveillance, metadata becomes a very important commodity. Even without the content of the communications, metadata can reveal a tremendous amount of information.

For example phone companies for the purposes of improving services maintain a record of the metadata of its users. This can contain information like whom the user called, for how long they spoke, how often, and the location of the customers. This is where information integration across databases can cause a real privacy concern. An information analysis across different databases such as criminal records, financial records and social media can paint a digital portrait of a person.

- Encryption

[12] *Available at* https://techterms.com/definition/cookie

[13]*Available at* http://data-informed.com/what-is-metadata-a-simple-guide-to-what-everyone-should-know/

Encryption involves the process of encoding and decoding messages, like cryptography but for digital communications. Computers, with a much more advanced mathematical prowess as compared to humans, have allowed for much more complex encryption schemes. The function of data encryption is to convert the data into a code so that the confedentiality of the data is protected when it is being transmitted across networks. Only those with access to the decryption key can access such encrypted data. The process is such that data is encrypted with an encryption algorithm and an encryption key. The process results in ciphertext, which only can be viewed in its original form if it is decrypted with the correct key.[14] Thus even if there is physical access to data, it would be worthless without the encryption key to decode it.

The main problem with ecryption of data is while it protects data and its confidentiality, this can often get in the way of law inforcement investigations. The same encryption that helps us secure our communications can also be abused by criminals and terrorists to secure and encrypt their communications. While it is a tool that can help prevent crimes like identity theft, it can also aid in secretly and securely planning and carrying out criminal and other nefarious activities.

Governments and law enforcement agencies across the world thus have been vocal critics of strong encyption practicies that the technological revoloution has brought about. They often seek access to encryption backdoors or other methods of decoding such data. A "backdoor" is a method of bypassing normal modes of authentication. In encryption terms, a backdoor allows access to encrypted information. To address this issue, the U.S. government proposed in the 1990s a concept of encryption known as key escrow, in which strong encryption systems would be allowed subject to the proviso that the decryption keys for such systems be placed in a database that could be accessed by the government under certain conditions.[15] Even the United Kingdom has criticized encryption practices and asked for technology companies to include backdoors into their encryption

14*Available at* https://digitalguardian.com/blog/what-data-encryption

[15] National Research Council, *Cryptography's Role in Securing the Information Society*, Kenneth W. Dam and Herbert S. Lin, eds., National Academy Press, Washington, D.C., 1996

processes that the government can access.[16] Encryption is one of the most difficult challenges that modern technology has presented before law enforcement agencies, because governments cannot conduct surveillance and provide for the security of the nation if the data intercepted in impenetrable.

This conflict between law enforcement and technology came to the forefront in the aftermath of the San Bernardino Shooting in USA. Following the shooting, FBI officials had recovered the IPhone of gunman Syed Rizwan Farook, however they were unable to access any information stored on the phone due to Apple's encryption practices. The FBI requested the company's assistance in order to gain access to the phone and even obtained a court warrant, but Apple rejected the same. The agents requested a backdoor into the encryption algorithim however the company reiterated that providing such a backdoor would set a dangerous precedent and encryption was necessary for the protection and confidentiality of its customers data. Eventually the FBI was able to hack into the device with the help of a private third party, but the incident once again put into limelight the bigger concern involving the issue of whether technology companies could be forced to develop computer codes to assist in criminal investigation and also about how far the government could go in forcing companies or individuals to provide this service.[17]

Another recent and similar incident of Devin Kelly has again reignited the debate. Devin Kelly was responsible for the November 5th 2017 mass shooting at a church in Sutherland Springs, Texas killing 26 people in the process. The FBI recovered the Apple Phone that Kelly was using and wanted aceess to the data on the phone to help in their investigation of whether he had any other militant links. However the agency couldn't hack into the phone and has again served Apple with a warrant demanding them to provide access to his phone and ICloud account. The

[16] *Available at* http://www.zdnet.com/article/backdoors-encryption-and-internet-surveillance-which-way-now

[17] *Available at* http://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html

FBI has frequently complained that encryption had prevented them from accessing the shooters phone and had hampered investigations.[18]

All actions over the Internet result in the creation of large amounts of data, ensuring the creation of a traceable digital trail. Electronic record keeping makes data easily collectable, storable, and accessible. To better understand how surveillance over the Internet is carried out and what it entails, information has been provided on some programs used by governments around the world to monitor the Internet.

- PRISM Programme

The PRISM programme is a tool used by the US National Security Agency (NSA) to collect private electronic data belonging to users of major Internet services like Gmail, Facebook, Outlook, and others. It began under President Bush with the Patriot Act, and expanded to include the Foreign Intelligence Surveillance Act (FISA). The basic idea behind the programme is that it is a mechanism that allows the government to collect user data from companies like Google, Yahoo, Facebook, Microsoft, Apple etc. Both the companies involved and the government insist that data is only collected with court approval and for specific targets allows officials to collect material including search history, the content of emails, file transfers, chats, cloud stored files among other things. The program facilitates extensive, in-depth surveillance on communications and stored information. The law allows for the targeting of any customers of participating firms who live outside the US, or those Americans whose communications include people outside the US.[19]

- XKeyscore

It is a top secret National Security Agency program that allows analysts to search through vast databases containing emails, online chats and the browsing histories

[18]*Available at* https://www.theverge.com/2017/11/20/16679426/apple-search-warrant-icloud-iphone-sutherland-springs-shooting

[19]*Available at* https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

of millions of individuals and that too with no prior authorization. The NSA had boasted in training materials (part of the documents revealed by Edward Snowden) that the program is its "widest-reaching" system for developing intelligence from the Internet. XKeyscore thus in essence provides the ability to target persons for extensive electronic surveillance without any oversight. Analysts can simply perform searches by typing in any of the following information of their target. Name, telephone number, IP address, keywords, the language in which the internet activity was conducted or the type of browser used. Beyond emails, the XKeyscore system allows analysts to monitor a vast amount of internet activities such as websites visited or search queries entered, including those within social media such as Facebook chats or private messages. In 2012, there were at least 41 billion total records collected and stored in XKeyscore for a single 30-day period.[20]

- NETRA (Network Traffic Analysis System)

It is surveillance software developed by the Centre for Artificial Intelligence and Robotics under the aegis of the Defence Research and Development Organization. The software is primarily used by Indian Spy agencies such as the Intelligence Bureau (IB) and the Research and Analysis Wing (RAW) with some capacity being reserved for domestic agencies under the Home Ministry. The software is meant to monitor Internet traffic on a real time basis using both voice and textual forms of data communication, especially social media, communication services and web browsing. It was built with the intent of combating internal and external threats to the security of the country. NETRA has the capability to intercept and analyse data (including voice traffic) passing through Google, Skype, and other social networking forums. Apart from that can also track specific keywords across datasets such as emails, tweets, Facebook

[20]*Available at* https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

status updates, comments, blogs, messages on forums, and even images shared over the Internet.[21]

The majority of the information gathered by intercepting this data is then analysed by computer algorithims, much like the process of data mining and analysis works, to create organized databases which the human analysts can then search through and monitor. Thus the devices that consumers pay for, have been turned into virtual snooping assistants that help conduct surveillance activities on their users and it can be done remotely over long distances. Thus modern day surveillance activities have the capability to track, analyse and store information on and about everyone you meet, talk to, or activities you perform while using the internet. The digital trail that you leave behind can be analysed and traced.[22] This mass surveillance is usually conducted in the following manner –

- Initial Interception – Obtaining a raw signal from a source (e.g. tapping a fiber optic cable).
- Extraction – Copying the signal and converting or reconstructing it into an intelligible format.
- Filtering – Selecting particular information of interest (either content or related communications data or both) through the use of identifiers or selectors and discarding low value internet traffic.
- Storage – Retaining filtered information in a database for potential future analysis or dissemination.
- Analysis – Querying, examining, data-mining or otherwise analysing information stored in databases.
- Dissemination – distributing the results of analysis to other persons, agencies, organizations.

[21] *Available at* http://www.news18.com/news/tech/privacy-in-internet-era-four-government-surveillance-programs-you-must-know-about-1493541.html

[22] Diffie, Whitfield; Susan Landau (August 2008). "Internet Eavesdropping: A Brave New World of Wiretapping". *Scientific American.*

- Dissemination – Distributing the results of analysis to other persons, organisations or agencies.[23]

SURVEILLANCE LAWS AROUND THE WORLD

Surveillance and information security has increasingly come into focus around the world as many governments and international organizations are diverting their resources into this field. There is increasing evidence that almost all countries in the world have the ability and resources to carry out modern surveillance techniques and are putting these abilities to use. Questions of privacy and surveillance remained at the forefront of debate in international law. Hence it is imperative to understand the global scenario with regard to State Surveillance.

The international understanding of privacy and what it entails is enumerated in various international texts.

- Article12 of Universal Declaration of Human Rights (1948) and Article17 of International Covenant of Civil and Political Rights have identical provisions that state –

  "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attack upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks."
- Article 8 of European Convention on Human Rights states - "Everyone has the right to respect for his private and family life, his home and his correspondence; there shall be no interference by a public authority except such as is in accordance with law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the

[23] European Court of Human Rights (Human Rights Organizations v United Kingdom) *Available at* https://privacyinternational.org/sites/default/files/2017.09.29%20BBW%20%26%20Ors%2C%20BIJ%20%26%20Anr%2C%2010HROrgs%20-%20Applicants%27%20Consolidated%20Observations%20-%2029%20September%202017.pdf

country, for the protection of health or morals or for the protection of the rights and freedoms of others."

Thus these texts regard privacy as a fundamental human right, which has the protection of law, but can also be curtailed and restricted due to reasonable concerns and by procedure of law. It is also reflected in case law developed pursuant to ICCPR Article 17 and ECHR Article 8: both provisions have been authoritatively construed as requiring national implementation of the basic principles of data privacy laws[24]

UNITED NATIONS AND OTHER ORGANIZATIONS

Keeping in mind the rising incidents of surveillance around the world and concerns raised by privacy activists, mostly in part due to the Snowden revelations, the United Nations took various steps in this regard.

- In December 2013, the United Nations General Assembly adopted resolution 68/167_which expressed concern at the negative impact that surveillance may have on human rights. It called upon all States to respect and protect the right to privacy in digital communication. The General Assembly called on all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data.[25]

[24] In relation to Article 17 of the ICCPR, see General Comment 16 issued by the Human Rights Committee on March 23, 1988 (UN Doc. A/43/40, pp. 180-183), paragraphs 7 and 10. In relation to Article 8 of the ECHR, see the judgments of the European Court of Human Rights in, e.g., Klass v. Germany (1978), Series A of the Publications of the European Court of Human Rights ("A"), 28; Malone v. United Kingdom (1984), A 82; Leander v. Sweden (1987), A 116; Gaskin v. United Kingdom (1989), A 160; Kruslin v. France (1990), A 176-A; Niemitz v. Germany (1992), A 251-B; Amann v. Switzerland (2000), Reports of Judgments and Decisions of the European Court of Human Rights 2000-I. See further, L.A. Bygrave, "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties," International Journal of Law and Information Technology 6:247-284, 1998.

[25] *Available at* http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

- Underscoring the importance of this issue, In July 2015, the Human Rights Council appointed Prof. Joseph Cannataci of Malta as the first-ever Special Rapporteur on the right to privacy. Special rapporteurs are independent experts appointed by the Human Rights Council who serve in a personal capacity and are mandated to report on human rights. The independent status of the mandate-holders is essential for the UN to impartially fulfill its functions. The Rapporteur has been given the following responsibilities.[26]

➢ To play a crucial role in developing common understandings and furthering a substantive interpretation of the right to privacy in a variety of settings.

➢ To carry out systematic analyses, research, and monitoring the right to privacy across the world.

➢ Provide guidance to states and companies on its interpretation of the right to privacy.

➢ To report on alleged violations, wherever they may occur, of the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, including in connection with the challenges arising from new technologies, and to draw the attention of the Council and the United Nations High Commissioner for Human Rights to situations of particularly serious concern[27]

- UN High Commissioner for Human Rights Navi Pillay's report of 2014 pointed out that the secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn, demands greater precision in the rule governing the exercise of discretion, and additional oversight." The report further stated that judicial involvement can help assess whether such surveillance meets the standards required by international human rights law. It called for States to establish independent, institutions to monitor

[26] *Available at* http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

[27] ibid

such surveillance. The report emphasized that when conducted in compliance with the law, including international human rights law, surveillance of electronic communications data can be necessary and effective for legitimate law enforcement or intelligence purposes. "Where there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in surveillance." With regard to the laws governing such surveillance, the report stated that these laws must be publicly accessible and must contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims and that these laws must be sufficiently precise and provide for effective safeguards against abuse.[28]

Another International Text that deals with data protection is the General Data Protection Regulation (GDPR). It was adopted by the European Parliament and European Council in April 2016 and will become enforceable in May 2018. It replaces the previous 1995 data protection directive and provides a new framework for data protection laws. This regulation will be implemented in all 28 countries. Some of the major points of the regulation are as follows[29]

- The regulation applies to all companies processing the personal data of subjects residing within the jurisdiction of the European Union, regardless of the company's location. Thus even Non-EU businesses processing the data of EU citizens can be held liable.

- A breach of the regulation for the most serious infringements, such as not having consent to process data, can lead to a maximum fine of up to 4% of annual global turnover or €20 Million (whichever is greater).

- The conditions for consent have been strengthened. The request for consent must be given in an intelligible and easily accessible form, with the

[28] *Available at* http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14875

[29] *Available at* http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

purpose for data processing attached to that consent and it must be as easy to withdraw consent as it is to give it.

- Right to be forgotten - This is one of the most robust provisions of the regulation. It provides that the data subject has the right to ask the data controller to erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, are outlined in article 17, this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

- Right to Access – the data subjects can obtain from the data controller confirmation as to whether or not their personal data is being processed, where and for what purpose. The controller is liable to provide an electronic copy of the data to the subject free of cost

- The regulation will allow users to claim damages in the instance of data loss as a result of unlawful processing, including collective redress

In terms of other international legal instruments, there does not exist a truly global convention or treaty dealing specifically with data privacy despite calls for such a treaty by various people. There are however steps being taken in this regard. Entitled the “The International Treaty on the Right to Privacy, Protection Against Improper Surveillance and Protection of Whistleblowers,” or informally, the “Snowden Treaty ” is an attempt at establishing an international regime regarding state surveillance and the manner in which whistleblowers like Edward Sowden are treated. It was conceieved by David Miranda, a founding editor of *The Intercept. It has been sent to the governments of various states for their review and observations*

A full text of the treaty is yet to be released however discussions with various proponents of the treaty have led to the following details about the provisions of the treaty.[30]

- Signatories will be required to outlaw mass surveillance activities along with incorporating data protection laws and the right to privacy in all future policies
- The preservation of privacy is a fundamental responsibility of governments
- Oversight of state surveillance activities will also need to be revamped independent tribunals will need to be established that review these surveillance activities to ensure transparency and accountability.

DIFFERENT COUNTRIES AROUND THE WORLD

Many countries are also introducing laws granting intelligence agencies new surveillance powers. A breif look is provided at the surveillance laws of some countries around the world.

UNITED STATES OF AMERICA

The United States of America conducts the most extensive surveillance programme anywhere in the world. Its technological capabilities are far superior to the rest of the world and it has put them to effective use through these programs. The National Security Agency is responsible for carrying out majority of these surveillance programs..

The Foreign Intelligence Surveillance Act (FISA)(sec 702) and the Patriot Act (sec 215) have established the current legal framework for national security intelligence gathering in the United States.

[30]*Available at* https://thewire.in/11654/snowden-treaty-calls-for-end-to-mass-surveillance-protections-for-whistleblowers/

FISA, and a series of executive orders based on it, allow for the surveillance) of "a foreign power or an agent of a foreign power," including U.S. persons who fall under the definition of an agent of a foreign power.

Under FISA a special court of 11 federal district court judges has been established who review requests for warrants. These warrants can cover both electronic surveillance and covert physical searches. To obtain a warrant, law enforcement authorities must demonstrate to the FISA Court that there is probable cause to believe that the target of the warrant is an agent of a foreign power. FISA warrants do not require a statement of what information is being sought through the warrant

Section 215 of the USA PATRIOT Act also allowed the FISA Court to issue orders granting access to any records and tangible items from any entity. This provision substantially enlarged the range of items subject to FISA jurisdiction.[31]

Since a large amount of the world's Internet data passes through the United States, the U.S. has the ability to observe and record the communications of much of the world's population.

UNITED KINGDOM

The United Kingdom along with the United States of America conducts one of the biggest state sponsored surveillance programs. The GCHQ (Government Communications Headquarters) is the primary agency entrusted with carrying out this task. Part of the Five Eyes alliance, GCHQ and the NSA have an intelligence sharing partnership. The Investigatory Powers Act is the legal instrument through which the power to conduct these surveillance practices are derived. Soe of the main provisions of this act are[32] -

- The provisions of the bill empower the security services such as GCHQ, MI6, MI5 to hack into the computers of targets. Security services will be legally empowered to bug computers and phones upon approval of a warrant

[31]*Available at* https://thewire.in/130237/u-s-spy-agency-abandons-controversial-surveillance-method/

[32]*Available at* http://www.telegraph.co.uk/technology/2016/11/29/investigatory-powers-bill-does-mean-privacy/

- ISPs and CSPs are required to save the internet and communications history of users for uptil one year so that it can be called upon in investigations. This refers to the meta data of web browsing and communications, and not the content. Some 48 authorities will be able to request access to this information, including the Met Police, British Transport Police, GCHQ, the MoD, the Department of Health, HM Revenue and Customs, and the Home Office.
- The Act creates a framework of oversight intended to prevent abuse. An independent body, Investigatory Powers Commission, has been tasked with reviewing and reporting on the government's surveillance activities.
- It also introduces the need for a judge's sign-off on "the most intrusive powers", as well as a new Investigatory Powers Commissioner to monitor how they're used. Intercept warrants will need ministerial authorization and will be further reviewed by judges.

INDIA

There are no laws that officially allow for mass surveillance in India. There are however two legislations deal with interception and monitoring of communications. These are the Indian Telegraph Act of 1885 and the Information Technology Act of 2000, along with its 2008 amendments. The aim of these laws is to allow for targeted surveillance in certain specific instances.

The Telegraph Act allows for interception of communications only on two accounts.

1. on account of a public emergency
2. or, for public safety.

If either of those two preconditions is satisfied, then the government may cite any of the following five reasons, to be recorded in writing -

1. the sovereignty and integrity of India
2. the security of the state

3. friendly relations with foreign states

4. for maintaining public order

5. for preventing incitement to the commission of an offense.[33]

In 2007, Rule 419A was added to the Indian Telegraph Rules (1951) framed under the Indian Telegraph Act. This rules entailed that the orders for the interception of communications must be issued by the Secretary in the Ministry of Home Affairs in the case of the Central Government and the Secretary to the State Government in-charge of the Home Department in the case of a State Government. However, the Rules provide that in unavoidable circumstances an order can also be issued by an officer, not below the rank of a Joint Secretary to the Government of India, who has been authorised by the Union Home Secretary or the State Home Secretary.[34]

The provisions of the Information Technology Act are similar to those of the Telegraph Act. Section 69 of the Information Technology Amendment Act, 2008 gives power to the government to intercept, monitor or decrypt any data or information stored on any computer resource.

Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, Defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub - section (2) for reasons to be recorded in writing,, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted o r monitored or decrypted any information transmitted received or stored through any computer resource.

[33] *Indian Telegraph Act, 1885* s.5

[34] *Available at* https://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=0

(2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out shall be such as may be prescribed

(3) The subscriber or intermediary or any person in charge of the computer resource shall,, when called upon by any agency which has been directed under sub section (1) extend all facilities and technical assistance to -

(a) provide access to or secure access to the computer resource containing such information; generating, transmitting,, receiving or storing such information; or

(b) intercept or monitor or decrypt the information, as the case may be; or,

(c) provide information stored in computer resource..

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub - section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.[35]

Thus the government is sufficiently empowered to carry out surveillance activities. There is some sort of data protection provided to the citizens under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 but that holds the body corporates liable (fine upto 5 crore) and not the government. a body corporate means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities. It is also worth noting that the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 declare that any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules[36]

[35] *Information Technology Act, 2000,* s. 69

[36] Rule 3 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

In the licenses that the Department of Telecommunications grants Internet service providers, cellular providers and telecoms, there are provisions that require them to provide direct access to all communications data and content.[37]

The government of India conducts the following surveillance programs along with NETRA(explained earlier)

Central Monitoring System (CMS)

The premier mass surveillance programme of the Indian Government. Its primary goal is to replace the current on-demand availability of data from service providers with a "central and direct" access which involves no third party between the captured information and the government authorities.[38] The CMS is primarily operated by Telecom Enforcement and Resource Monitoring Cell (TERM) within the Department of Telecom, The data collected by the CMS includes voice calls, SMS, MMS, fax communications on landlines, CDMA, video calls, GSM and even general, unencrypted data travelling across the internet using the standard IP/TCP Protocol.[39]

National Intelligence Grid (NATGRID)

The National Intelligence Grid (NATGRID) is a semi-functional integrated intelligence grid that links the stored records and databases of several government entities in order to collect data, decipher trends and provide real time (sometimes even predictive) analysis of data gathered across law enforcement, espionage and military agencies. The programme intends to provide 11 security agencies real-time access to 21 citizen data sources to track terror activities across the country. The citizen data sources include bank account details, telephone records, passport data and vehicle registration details, the National Population Register (NPR), the

[37] *Available at* http://dot.gov.in/sites/default/files/internet-licence-dated%2016-10-2007_0.pdf

[38] *Available at* http://ijlt.in/wp-content/uploads/2015/08/IJLT-Volume-10.41-62.pdf

[39] *Available at* http://www.thehindu.com/scitech/technology/in-the-dark-about-indias-prism/article4817903.ece

Immigration, Visa, Foreigners Registration and Tracking System (IVFRT), among other types of data, all of which are already present within various government records across the country.[40]

Lawful Intercept And Monitoring Project

This is a secret mass electronic surveillance program operated by the Government of India for monitoring Internet traffic, communications, web-browsing and all other forms of Internet data. It is primarily run by the Centre for Development of Telematics (C-DoT) in the Ministry of Telecom since 2011. The programme consists of installing interception, monitoring and storage programmes at international gateways, internet exchange hubs as well as ISP nodes across the country. This is done independent of ISPs, with the entire hardware and software apparatus being operated by the government. [41]

OTHER COUNTRIES

- Australia passed the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 whereby the government has the power to compel telecommunications companies to store metadata information about users phones and computers for up to a period of two years.[42]
- The French Intelligence Act of 24 July 2015 permits the French government to carry out surveillance activities. Among the main provisions of the act are the requirements of installing black boxes by Internet service providers to store and retain metadata of users and to make this data available to intelligence agencies. Further the law also gives powers to the government to break into the homes of suspected terrorists and plant bugs and surveillance cameras and

[40] *Available at* https://cis-india.org/internet-governance/blog/the-design-technology-behind-india2019s-surveillance-programmes

[41] ibid

[42] *Available at* https://www.legislation.gov.au/Details/C2015A00039

equipment like keystroke loggers. Monitoring the calls of people without prior authorization from a judge is also permitted.[43]

- Narus, a technology firm, has provided Egypt Telecom (Egypt's biggest call and internet service provider which is State run) with Deep Packet Inspection equipment (DPI), a content-filtering technology that allows network managers to inspect, track and target content from users of the Internet and mobile phones, as it passes through routers.[44]

SUGGESTIONS

Concerns with increasing use of technology are issues regarding regulation of the datasphere and so far it has been a struggle to contain and regulate these procedures. Managing and regulating the data economy is not easy, mostly in part due to the fact that it is the responsibilty of a nation, with a finite jurisdictional authority, to regulate the practices of what are essentialy in the modern day and age global borderless corporations. A handful of tech giants now surpass the size and power of many governments. For example Facebook now has about two billion users, while Canada has a population of just over 36 million. Data collected by these companies is often sent across different jurisdictions and boundaries for the purpose of storage. This can casue a real legal and social problem when it is taken into account that data regarding people of one country may be saved on the company's servers located in another country which has vastly different data protection laws and thus does not offer the same level of protection. Often data protection laws are incompatibleacross countries and based on the sheer scale of these large tech companies, it is difficult for countries to enforce any kind of regulation or bring about a global framework within which they must operate irrespective of what country they operate in.

The right of the state to conduct surveillance is not absoloute and unchecked. Every person has a reasonable right to expect a private sphere, where they can expect to shut out the community

[43]*Available at* https://www.theverge.com/2015/5/5/8553271/french-parliament-terrorism-surveillance-bill-charlie-hebdo

[44]*Available at* https://www.huffingtonpost.com/timothy-karr/one-us-corporations-role-_b_815281.html

and have an exclusive zone where they are the soveriegn. A sphere where no other entity is allowed to intrude.

Thus it becomes important to have strong oversight measures to put in place a regime where there is accountability of intelligence agencies. There is a need to maintain a clear boundary between privacy and national security and for that we need clear and transparent laws. A strong data protection law can empower the people and provide adequate safeguards such as a system of judicial review. Further it can strengthen the surveillance abilities of a state by providing clear guidelines on what it can and cannot do. Some suggestions on what should be incorporated into such a data protection law and what it should adequately cover have been provided under

- Clear identification of what type of data is to be collected and gathered.
- How the data is to be collected and from what sources.
- Whether any data sort of collection can be allowed without warrants or do all collection and interception activities need warrants. Also which authority provides these warrants
- Categories of people who may be subject to surveillance along with the definition of those categories, so as to understand who may be covered under those categories – ideally collection of data should be targeted at specific people instead of wholesale blanket surveillance
- A provision for how long targets may be subject to surveillance and for how long that data is to be retained.
- An exhaustive list of the agencies who are empowered to collect information and conduct surveillance along with an exhaustive list of who might access this data and under what conditions
- Clearly defined instances where surveillance may be authorised, such as for building a case for prosecution or national security concerns.
- Where the data is to be stored and who is responsible for the security of such data
- Clearly define for what purpose data analysis can take place and when integration of various datasets may be permitted
- Oversight measures that have been put in place. Adequate safeguards are needed so that these powers are not misued. They may range from a provision that requires judicial review of every warrant, or the creation of an intelligence

committee whose job is to ensure that these procedures are being followed and provide a review report.

- Stringent punishments for the breach of these provisions
- To what extent these provisions apply to private companies and parties and if any additional provisons apply to them.

The data protection law can also ensure further protection for the people by providing certain protections and additional rights

- The creation of a national privacy commision, which is tasked with providing periodic assesments of privacy law related developments and to review the various provisions of the act.
- Provide the citizens with a right to sue the government or private parties if they cause a breach of privacy or if information is compromised or leaked
- The creation of a separate court, along the lines of the FISA Court, that deals exclusively with the authorization of warrants. The court could also exclusively deal with cases that involve the violation of the provisions of the act.
- Allow the individual to retain control over potential future uses of the information provided, so that no future use may be permitted without obtaining their consent.
- Provide for a publication of the number of requests made by the government for surveillance warrants

'No state has ever survived without some surveillance, and no state deserves to survive if it has too much surveillance.'[45]

As the digital age and 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,

[45] *Available at* https://www.theglobeandmail.com/opinion/is-state-surveillance-a-legitimate-defence-of-our-freedoms/article18368244/ - Alan Dershowitz

but such a balance should not eliminate the power of the government to conduct surveillance activities. Some control and oversight is 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 right to privacy 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.