Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July 2021:8408 - 8412

Research Article

Surveillance Society: Its Nature And Characteristics

Jagriti Kalita

ABSTRACT

21st century has seen a growth in digital surveillance across the world. Countries like China, Singapore, the U.S strictly adheres to technology for monitoring their citizens. While supporters of surveillance has said it is important to monitor citizens' movements to reduce crime and mitigate danger, critiques have raised questions concerning privacy and human rights violation due to increased surveillance. The current Government in India has been currently on the news after the alleged spying done through the Israeli Pegasus malware.

This article will discuss the nature and characteristics of a surveillance society and the risks it possesses accordingly.

Keywords*:* Surveillance, data, privacy, risk management

INTRODUCTION

Surveillance is the monitoring of people's behaviour, activities, or other changing data in order to influence, manage, direct, or protect them. This can include remote observation using electronic equipment (CCTV) or the interception of electronically transmitted data (such as Internet traffic or phone calls). Human intelligence operatives and mail interception are examples of simple no-tech or rather low-tech methods. The term "surveillance" comes from a French phrase that means "to keep an eye on" (sur means "from above" and veiller means "to watch").

Governments utilise surveillance for intelligence gathering, crime prevention, the protection of a process, person, group, or item, and crime investigation. It's also used by criminal gangs to plan and carry out crimes like robbery and kidnapping, as well as by corporations to gather intelligence and private investigators.

WHAT IS WRONG WITH SURVEILLANCE SOCIETY?

Taking the risks and perils of surveillance society first, as Ulrich Beck puts it, any increase in the creation of "goods" also means a higher output of "bads." Some of the bads are political in nature, in addition to environmental ones. Large-scale technology infrastructures are prone to

[1]Postgraduate student, Department of Sociology, IGNOU. kalitajagriti@gmail.com

large-scale issues in particular. And, particularly in the case of computer systems, one inadvertent or ill-advised keystroke can quickly unleash disaster.

Second, there are issues of corruption and warped power perceptions. Some leaders use the guise of a greater good to legitimise unconventional or out-of-the-ordinary practises.

Surveillance allows for massive inequities in access and development. Unfortunately, the main surveillance modalities of the twenty-first century are exacerbating and institutionalising class, gender, race, location, and citizenship divisions.

Surveillance breeds suspicion, putting social cohesion and unity at risk. Trust is essential in social connections, and allowing ourselves to betray it appears to be slow suicide.

Surveillance diverts attention away from alternative methods and larger, more pressing issues.

CHARACTERITICS OF SURVEILLANCE

Surveillance is defined as the deliberate, routine, systematic, and focused attention paid to personal details for the purposes of control, entitlement, management, influence, or protection.

Purposeful attention- Initially, the attention is focused on a certain goal. There is a point to the watching that can be justified.

Routine- Surveillance is unavoidable while we go about our daily lives. It's how life is woven together.

Methodical- Surveillance is likewise methodical. It is planned and carried out on a rational schedule rather than a haphazard one.

Surveillance is laser-focused. Surveillance gets down to the nitty gritty. While some monitoring relies on aggregate data, the majority of it concerns identified individuals.

Dataveillance- The personal information may be in the form of CCTV photos, fingerprints, communication records, or numerical or categorical data, among other things. Roger Clarke refers to numerical data employed in bureaucratic institutions as "dataveillance."

THE PROCESSES OF SURVEILLANCE SOCIETY

SOCIAL SORTING

Social sorting is widespread in the surveillance society. In government and business, massive databases of personal information are analysed and classified to identify target markets and high-risk populations. Amazon.com, for example, profiles customers using sophisticated data mining algorithms that include both obvious and non-obvious relationship data. This allows them to identify not only who is most likely to buy what, but also which clients are credit risks.

Surveillance society is becoming increasingly defined by social sorting. It gives different groups varied possibilities and frequently amounts to subtle and sometimes unforeseen means of regulating societies and shaping policies without democratic debate. No one has ever voted in favour of such a system. They emerge as a result of integrated government, utility, and services outsourcing, as well as pressure from technology firms and the rise of actuarial procedures.

DATA FLOW

Surveillance-related data circulates over computer networks. To safeguard children from abuse or to decrease fraud in government services, frequent requests are made to access a growing number of databases. However, neither the general public nor data sharing organisations have a good understanding of where those data go. The concept of 'intelligence-led' policy interventions has gained traction, and this, along with the networking and data matching capabilities of today's digital infrastructures, means that surveillance appears to follow its own logic. One of the most important questions is how secure databases are against unauthorised access or leakage.

And a further more vital one is, to what extent should data be permitted to move from one sphere to another?

FUNCTION CREEP

Personal data acquired and used for one purpose and function frequently migrate to others, extending and intensifying surveillance and invasions of privacy beyond what was originally understood and deemed socially, ethically, and legally acceptable. While such data may remain in the same context, if their use expands, they may develop some harmful qualities. A good example is medical surveillance. Diagnostic tools that may be useful in certain circumstances may be permitted to seep into broader and broader contexts over time, reducing their predictive characteristics for positive diagnosis in the process. Those who have been misdiagnosed may be at a disadvantage.

As a matter of administrative convenience, function creep may occur silently and unobtrusively. However, it poses a significant barrier to FIPs, and it remains an issue despite the fact that it was highlighted as a concern several decades ago. All too frequently, the human repercussions of function creep are neglected, ignored, or minimised.

TECHNOLOGIES

Today, surveillance is frequently thought of solely in technological terms. Although technological advancements are critical, two points must be kept in mind:

One, direct human monitoring, unmediated by technology, continues to exist and is frequently paired with more technological forms.

Second, technical systems are neither the origin nor the total of today's surveillance.

Technology should be continuously analysed and analysed in order to fully comprehend the surveillance society. We need to know how they work, how they're used, and how they affect how an organisation operates. Furthermore, we must have a thorough understanding of these issues in order to impact policy and practise. One method is to conduct impact evaluations.

Similar technologies are being employed in various settings today, which is promoting the development of integrated surveillance. National ID card systems usher in a slew of new surveillance possibilities. After a system has been created, it is considerably more difficult to modify it.

A third issue with technology is that some suggest that technological solutions can alleviate concerns about a monitoring society. Some so-called privacy-enhancing technologies, for example, can help to limit the spread of technological surveillance, and their usage should be encouraged where possible.

SOME ISSUES IN SURVEILLANCE SOCIETY

Three key issues in surveillance are-

- SOCIAL EXCLUSION AND DISCRIMINATION
  Surveillance, invasion of privacy, and privacy protection differentiate amongst groups, benefiting some while disadvantaging others. Of course, it is not because of monitoring that the nation state thinks it can no longer provide the kinds of social security it previously did, or that it has scaled back its goals to just provide some forms of basic individual safety. Surveillance, on the other hand, grows in tandem with these changes, frequently supporting or facilitating them. Individual safety agencies can also be readily outsourced.
  Health and welfare from cradle to death, once a proud promise of social democratic administrations, has been reduced to risk management, and this is where the surveillance society comes in: such risk management necessitates complete information of the situation. As a result, dates are sought in order to determine where resources should be directed. Because surveillance networks allow for so much collaboration, insurance firms may simply collaborate with police or supermarkets with other data collectors. As a result, police hotspots are typically placed in primarily non-white regions, whereas supermarkets are located in posh neighbourhoods easily accessible by cars.
- CHOICE, POWER AND EMPOWERMENT
  It is extremely difficult to make a major change when the monitoring system is infrastructure-based and its workings are buried in technical obscurity. Consumers aren't aware of the extent of personal profiling carried out by major corporations until a major identity theft scandal breaks, and even then, the focus is usually on security—how to prevent similar fraud—rather than on limiting the power of businesses and government agencies to process so much data promiscuously and prodigiously.
- TRANSPARENCY, ACCOUNTABILITY
  Individuals and groups find it difficult to learn what happens to their personal information, who handles it when, and for what reason, despite the fact that business, transportation, and government infrastructures all have expanding monitoring capabilities. Given the power of enormous companies with advanced surveillance capabilities, it seems only right that ordinary people, even if only on a theoretical basis, should have a say. This can be found through specialised agencies, advocacy groups, and the media, among other places.
  Within organisations, accountability should be assumed, especially when high-powered surveillance is used on a regular basis with potentially harmful repercussions. Although workplace surveillance provides some useful examples of bad practises, companies have been forced to rein in the excesses of their monitoring in some cases due to active labour union engagement.

CONCLUSION

Some critics argue that supporters' claim should be changed to: "As long as we do what we're told, we have nothing to fear." For example, a member of a political group that opposes the national government's policies may not want the government to know their names or what they've been reading so that the government cannot easily subvert their organisation. Others argue that while a person may not have anything to conceal right now, the government may subsequently impose policies that they dislike, making opposition impossible due to widespread surveillance allowing the government to detect and eliminate political risks. Other critics also point out that the majority of individuals do have secrets. If a person is looking for a new job, for example, they may not want their current employer to know. Also, if an employer wants complete privacy to monitor and secure their employees' financial information, it may be hard, and they may not want to recruit individuals who are under observation. The greatest source of danger is securing the lives of those who willingly live under total surveillance, educating the public about those under peaceful surveillance, and identifying terrorists who use the same surveillance systems and mechanisms in opposition to peace, against civilians, and to reveal lives outside the law of the land. In addition, a significant risk of private data collection stems from the fact that this risk is too much unknown to be readily assessed today. Storage is cheap enough to have data stored forever, and the models using which it will be analysed in a decade from now cannot reasonably be foreseen. Furthermore, a considerable risk of private data collecting arises from the fact that this risk is now too unknown to be easily measured. Data can be held indefinitely since storage is cheap enough, and the models that will be used to analyse it a decade from now cannot be predicted.

Bibliography

1. Mahapatra, S. (2021). Digital Surveillance and the Threat to Civil Liberties in India. GIGA Focus Asien.
2. Moore, M. (2018). Democracy Hacked: Political Turmoil and Information. London: Edinburgh.
3. Bhattacharjee, K. (2021, July 21). Red line crossed by use of spyware, says UN High Commissioner for Human Rights. New Delhi, India.
4. Human Rights in the Digital Age. (2014). Retrieved from https://www.hrw.org/news/2014/12/23/human-rights-digital-age.
5. McGuinness, D. (2017). How a cyber attack transformed Estonia. Tallinn, Estonia.
6. (2019). The Personal Data Protection Bill. New Delhi: Ministry of Law and Justice.