The International Journal of Indian Psychology
ISSN 2348-5396 (Online) | ISSN: 2349-3429 (Print)
Volume 11, Issue 1, January- March, 2023
DIP: 18.01.090.20231101, DOI: 10.25215/1101.090
https://www.ijip.in

Research Paper

"What About My Privacy?": Exploring Perceptions Towards Increased Surveillance

Adrija Sanyal[1], Salonee R. Jukar[2]*

ABSTRACT

In the past few years, states and organisations have made use of technology to increasingly track, and monitor the population; the onset of COVID-19 was further used to validate and justify these surveillance systems. During the pandemic, the administration was focused on detecting the trends of the diseases for which, the surveillance systems require information about what is happening inside our bodies, such as our body temperature and heart rate, in order to determine whether we are ill (Eck & Hatz 2020). These noticeable trends marked a significant change in surveillance techniques from "over the skin" to "under the skin" surveillance which is not just restricted to monitoring overt behaviour but also recurrent patterns of traits, habits and feelings (Harari, 2020). The study aimed to explore people's perceptions about the government and corporations using their personal data for extensive surveillance. Law enforcement and the security mechanism use the vast amount of data gathered to fulfil their security objectives, eventually leading to the institutions breaching the boundaries of their control. Focus group discussion (n=9) was conducted to gain insights regarding political surveillance and its relational understanding of an individual's sense of privacy, perceived control, and trust in political institutions. Using thematic analysis, key themes ranged from the absence of institutional trust in citizens, privacy and its susceptibility to breaches to pandemic-induced changes in surveillance. In conclusion, the consequences and the broader impact of such views held on an individual level are discussed.

Keywords: *Institutional Trust, Privacy, Surveillance, Pandemic*

Surveillance is a long-standing social practice. It has long been a part of institutional processes and social interactions among people, however, it has been the dominant organisational strategy of late modernity over the last 40 years (Locke 2010).

The monitoring, gathering, and/or processing of personal data by a government is state surveillance. Online activity monitoring, GPS or Bluetooth location tracking, tracking financial transactions, video surveillance, facial recognition software, and biometric data

[1]SVKM's Mithibai College of Arts, Chauhan Institute of Science and Amrutben Jivanlal College of Economics (Autonomous), Mumbai, Maharashtra
[2]SVKM's Mithibai College of Arts, Chauhan Institute of Science and Amrutben Jivanlal College of Economics (Autonomous), Mumbai, Maharashtra
*Corresponding Author

Received: December 19, 2022; Revision Received: February 20, 2023; Accepted: February 22, 2023

© 2023, Sanyal, A. & Jukar, S. R.; licensee IJIP. This is an Open Access Research distributed under the terms of the Creative Commons Attribution License (www.creativecommons.org/licenses/by/2.0), which permits unrestricted use, distribution, and reproduction in any Medium, provided the original work is properly cited.

collection are a few examples of this. The types of information that states are able to gather and connect are numerous, precise, and frequently of a private nature (Eck & Hatz 2020).

Commercial entities have contributed to the monetization of information and, as a result, have created an insatiable demand for consumer data (Turow 2005). Through various "e-government" projects, the nation-state, which has long been a prominent actor in collecting data on citizens (Agar 2016; Higgs 2003), is radicalising the breadth of governmental surveillance. In order to increase school safety, students from kindergarten through university are increasingly being tracked, measured, and marked (Monahan, Torres et al. 2009).

After the onset of COVID-19 and it being declared a pandemic by WHO, several countries launched mobile apps developed to gather users' geolocated mobility information in order to assist authorities in tracking the COVID-19 outbreak. The apps developed by Norway, Kuwait and Bahrain were declared as 'the most invasive' tracing apps by Amnesty International in 2020 (Amnesty International, 2021). These apps have signified a global rise in state surveillance. By the end of 2020, 34 countries initiated surveillance and out of them, 22 were democratic in nature (Gershgorn, 2021).

REVIEW OF LITERATURE

Surveillance allows for the detection of dissent and the targeted application of repression. As state law enforcement and security organisations use the vast infrastructure of data gathered by other governmental bureaucracies and incorporate it into security objectives, institutional boundaries also become less clear. Many studies on surveillance in the field of political science concentrate on how authoritarian regimes use it to combat domestic political threats. This is because surveillance enables the detection of dissent and the extraction of intelligence, allowing for the targeted application of repression (Gohdes, 2020).

Surveillance has ironically grown more obvious and more covert in recent years. On one hand, it is difficult to ignore the increasing number of cameras, requests for official records, and public discussions about internet data surveillance as we go about our daily lives, yet there exists an odd obscurity that surrounds these behaviours. With the exception of a small group of insiders, the actual workings of surveillance, the precise nature and degree of its penetration, as well as the processes for how one is picked out for suspicion or reward, are opaque (Ball, Haggerty, & Lyon, 2012). Another trend is the democratisation of surveillance, where even previously largely unobserved groups are now occasionally observed by other citizens as well as major institutions. (Mathiesen 1997; Goldsmith 2010).

Surveillance is one strategy that democratic countries are increasingly adopting. In addition to using closed-circuit television (CCTV), drones, mobile phone usage data, and biometric tracker bracelets, public surveillance of population movements during a lockdown is another form of surveillance measure that has been adopted (Weller, 2012).

But the introduction of mobile apps that enabled tracking during COVID-19 has become the most often-used method of surveillance. The fundamental idea is to use digital technologies to scale up conventional contact tracing. Although digital utopianism sees mobile phones as a way to assist protect against disease and worries of privacy invasion, there is tension there. Worries about government overreach online are not new, the COVID-19 pandemic's high stakes have caused official state monitoring operations to be accelerated and securitized in ways that are novel to the digital sphere. (Eck & Hatz, 2020). If we look at the Norwegian app, Smittestopp, the app's advantages were eventually thought to be insufficient to justify its

invasion of citizens' privacy. Indeed, the design of contact tracing apps has drawn criticism from several governments' own monitoring organisations. For instance, Slovakia expedited various changes to its telecom law that widened telecom providers' responsibilities to keep track of each customer's location information. Due to their "vagueness and insufficient protections against misuse," these regulations were contested before the Slovakian Constitutional Court and subsequently suspended (Rodriguez, 2020). Even in India, the government and numerous significant private businesses require workers to download the official COVID-19 tracking software, which is allegedly voluntary. Critics have noted that there is no national data privacy law in India and that it is unclear who gets access to the app's data and under what circumstances (O'Neill, 2020).

There is a possibility that governments won't be willing to give up the additional surveillance capabilities these applications provide and there is also a possibility that personal data may be gathered indefinitely and utilised for unexpected purposes. In reaction to the September 11, 2000, terrorist attacks, the US Patriot Act was passed in 2001, giving the government wide monitoring authority with no oversight. Despite the lack of any evidence pointing to a current threat of a foreign attack on US land, it is still in effect today (Eck & Hatz 2020). The government of the United Kingdom intends to keep the information it gathers for up to 20 years and only grants people a complete right to have their data removed upon request (Sabbagh & Hern, 2020).

However, with private organisations acting as a conduit or relay in a wider network of state monitoring, access by the state to other institutions is becoming a more explicit legal obligation (Ball, Haggerty & Lyon, 2012). Online information exchange has emerged as a cutting-edge method for businesses to get crucial data for market trends and decision-making research. Many businesses and organisations manage the shared information between individuals to provide valuable data for their business plans (Hajli & Lin, 2014). Similar to the government, the commercial sector now has access to vast amounts of information on us and regularly exchanges and uses that information in order to market to us. Anyone who has used Amazon in the past ten years will be able to attest to the fact that businesses have grown increasingly skilled at fusing consumer data with personal information to create sophisticated consumer profiles that can accurately forecast each person's consumption habits (Goold, 2010).

These surveillance applications have different strategies based on whether they were created by public or private initiatives, thus there is no one strategy that works for all of them. These strategies are based on questions like what kind of technology is utilised to monitor interpersonal contact, whether the app is optional, whether there are restrictions on data collecting, whether there are plans for discarding the data, whether the data is anonymised, whether data storage is centralised or decentralised, and whether the app is transparent (Bradshaw, Murphy, & McGee, 2020). Most democratic governments have reaffirmed their dedication to protecting privacy in this situation, yet worries still exist. For instance, anonymized data are susceptible to reidentification, and while data may be stored locally rather than centrally to reduce privacy issues, there are worries that the data may be compromised (Eck & Hatz, 2020).

The public may receive a particularly unfavourable message about how the state sees them and how much they can rely on the state to trust them from the rising usage of surveillance technologies. To foresee how the public will respond to the loss of trust, it is crucial to comprehend the circumstances under which the state acquires and uses its surveillance

power. It could be simpler to focus on the culturalistic approach and deal with the broad and detailed effects of monitoring on public trust separately (Goold, 2008).

From a culturalist vantage point, it is obvious that states' increasing use of surveillance technologies against their citizens risks undermining the confidence that society has in its leaders. A society's capacity to resist shifting toward more authoritarian forms of administration depends in part on the implicit value that democracy and democratic institutions are accorded by the general populace. It can be claimed that the state runs the risk of eroding the normative commitment of people to democratic government and, consequently, their commitment to ideals like the defence of individual rights and civic responsibility. Simply put, if the state loses public trust, it's possible that the people may also lose faith in the state. The state has been challenged in its claims to be the only source of order and (in extreme situations) to have a monopoly on the use of force as people have become increasingly responsible for their own safety and have a better grasp of the hazards they face. In nations like the United States, the public's reaction to the state's exit from some aspects of law enforcement may be seen in the emergence of private policing and gated communities. It is also conceivable that the public could lose faith in some governmental institutions, and with it, their willingness to submit to such organisations' rule of law. (Goold, 2008).

Again, there are two distinct views of the connection between trust and governance that may be found in literature: institutional theories and cultural theories. Although both theories emphasise the importance of trust in the development and upkeep of democratic forms of governance, they have different explanations. According to cultural theories, trust is somehow socially ingrained and passed down from one generation to the next because of a community's deeply ingrained devotion to democratic norms. In order for the executive to pursue controversial aims in the short or medium term without worrying about losing democratic support or legitimacy, trust is necessary to establish and maintain a relationship between the government and the public (Mishler & Rose, 2005). Due to people's overall trust in the government and conviction that the institutions of the state are really concerned with their welfare and well-being, they accept decisions that they may not like or agree with. Trust is also important because it ensures that the wider population actively fights non-democratic alternatives to current political systems. When democracy is threatened, it helps to strengthen its legitimacy. The notion that trusts is crucial for promoting political engagement and democratic participation is the final point to consider. In this approach, trust "strengthens people's ideas that government is responsive and motivates citizens to express their needs via engagement in activities ranging from voting to joining organisations". Contrarily, institutional theories view trust as a byproduct of institutional performance that may be strengthened or weakened depending on how the government and its agencies behave. While acknowledging that these are all possible ways for trust to function in society, institutional theorists disagree with cultural theorists in that they contend that neither these ideals nor specific kinds of trust are inevitably influenced by culture. They contend that rather than being passed down through generations, trust is instead continually replicated in response to the activities of the government. Trust is said to be developed as a specific response to institutional performance. When viewed in this light, trust is less of an act of faith—which is essential for the democratic endeavour to succeed—and more of a logical response to how well the government is performing (Mishler & Rose, 2005).

Privacy in online forums exists predominantly in two domains: a sense of control and dignity. To date, the notion of privacy as having control over one's personal information has been

more prevalent than the other. Technology, business policy, legislation, and regulation are frequently assessed and studied in terms of the level of control that individuals have over their personal data. Leading social networks like Facebook and MySpace spread the idea that users can regulate their privacy. The premise of privacy as control, however, is fundamentally challenged by online social networks (OSN). Even with rigorous controls, it is still possible for online socializers to post unpleasant, malicious, or private information about one another, which would then be accessible to a sizable, if not unrestricted, online audience (Levin & Abril, 2009).

Many people interact online and share personal information without appearing to give it much thought about the possibility of losing control, but these same people become angry when their personal information is accessed, used, or disclosed by people they believe to be outside of their social network. However, online socialisers have developed a novel and arguably legitimate concept of privacy known as network privacy that, if embraced by OSNs, will provide online socialisers control and protection over their reputation and dignity. This suggests that information is considered private by online socializers as long as it does not affect their established online personae if it comes from others or if it comes from them if it does not get shared outside of the network to which it was initially provided. OSNs should be obligated to offer effective protection to online socializers, who are typically young and vulnerable, in accordance with their understanding of network privacy above and beyond conventional methods of personal information control. OSNs are companies that make money from online social networking (Levin & Abril, 2009). It has been found that perceived control is adversely connected with attitudes toward sharing information and perceived privacy risk, which in turn affects how information is shared. To the extent that a person believes social networking sites give them control over how their information is used through privacy settings, Hajli and Lin define perceived control of information, which is unique to social networking sites. 2014 (Hajli & Lin).

Advocates of a privacy-centric strategy highlight the importance of privacy discourses and structures as the most viable method of limiting surveillance and provide examples of how these strategies have successfully prevented egregious privacy intrusions. (Bennett, 2010). Those who emphasise the constraints of privacy as a concept and a regime are at the other extreme of the spectrum. For them, the fact that a surveillance society has developed around us despite a sizable and active privacy bureaucracy is blatant evidence of the failure of private institutions. In summary, it is claimed that the privacy infrastructure has demonstrated its inability to stop the spread of surveillance through its relentless growth of intensive surveillance techniques (Whitson and Haggerty, 2008).

Privacy risk has been seen as a crucial element in the context of SNS that affects users' social interactions and usage patterns. All user interactions on SNS are recorded for possible use in data mining for commercial and other purposes. Some users deal with their privacy worries by having faith in their ability to govern the information they disclose on social networking services (SNS) like Facebook (Acquisti & Gross, 2006). Additionally, research demonstrates that Facebook users share a lot of private information without being aware of the site's privacy settings (Hajli & Lin, 2014). Users' SNS usage habits have an impact on the privacy issues they face. There is evidence that these privacy hazards affect people's psychological impressions and desire to use technology (Van Slyke et al. 2006).

Even after the widespread release of several social media websites reusing and selling the user's data, participants have shown an ambivalent response to how their personal

information might be reused by social contacts, strangers and organisations (Shipman & Marshall, 2017). There is no specific consensus among the general population about the security and privacy of their data. According to data from the technology press, there is a display of less personal information by people over social media (Beck, 2018). Even though user discontent is on the upswing, there is still somewhat reluctance by the population to stop the complete sharing of details over media (Shipman & Marshall, 2017).

METHODOLOGY

Sample and Procedure

Using purposive sampling, 9 participants of all age groups participated in a focus group discussion. The respondents were early adults, in the age group of 18-25 and were from most of the metropolitan cities in India. Purposive sampling was used given the limited resources that the study had to be conducted, we ensured that people who were relatively more aware of the topic were invited to form, frame and discuss their opinions. This ensured that the exploratory study could lead to substantial findings for the researchers to formulate future research questions.

Ethical Protection of Participants

Participants were assured confidentiality for the data they gave during the focus group discussion. All the participants were adults who had given consent to being in the study. Participants' names and identities have been protected throughout the analysis of the transcript. There were no risks associated with being in the study.

Data Collection Procedure

The data collection procedure used to understand the perception of the people was a Focus Group Discussion. The participants were asked to read and respond to an informed consent form before the discussion began.

A focus group is a qualitative research method that assembles a small group of individuals to respond to questions in a controlled environment. The questions were intended to provide light on an interesting topic, and the group is selected based on predetermined demographic characteristics. There are some characteristics of a focus group discussion that made it more suitable for the data collection necessary for this paper. One, focus groups are qualitative methods of data sourcing. Two, it focuses on the interaction among group members and three, there is an active role of the researcher (Morgan, 1996).

The data collection method of focus group discussion begins with the research design. The researcher establishes the objectives of the study, identifies and recruits the sample population for the study and again identifies a suitable location for the conduction. For the second stage of collecting data, the researcher starts with the pre-session preparation by being aware of the questions and the script and deciding on the seating arrangements, group dynamics and recording facilities. The researcher also has to facilitate the meeting by introducing the topic and informing the participants about confidentiality, discussing the problem throughout the entire discussion, and concluding the discussion. The researcher then analyses the discussion with the help of thematic, content, discourse or conversation analysis (O. Nyumba et al. 2018).

This paper analysed the data with the help of thematic analysis. The practice of finding patterns or themes in qualitative data is known as thematic analysis. It is one of the primary data collection methods that is taught in qualitative because, "..it gives essential abilities that

will be valuable for undertaking many other kinds of analysis." In contrast to many qualitative techniques, it is not bound by a certain theoretical or epistemological stance and is a flexible strategy for the analysis of data (Braun & Clarke, 2006).

DISCUSSION

A thematic analysis was conducted with the data from the focus group discussion. The major themes that emerged primarily dealt with a lack of trust of the citizens both at an individual and a collective level in political institutions, the justifiability of surveillance during times of crisis, changes in the surveillance due to the pandemic, privacy concerns related to online forums, and the opinion of the general public on the same.

1. Absence of Institutional Trust in Citizens

We place a high value on privacy, among other things because it is necessary for the exercise of personal liberty and a strong self. But even though it may be simple to understand how privacy is fundamentally important to each of us as individuals, it is necessary to keep in mind that privacy also has a significant public dimension (Goold, 2010).

Many participants in the focus group discussion mentioned their inability to trust the government with their personal data. They believed that they would not have full disclosure about the way data is being used by the government and it might be used for reasons of monitoring and surveillance against their will. There were also references to recent imprisonments of people based on their social media activity which further reinforced the idea. A participant mentioned, ".....once you put your data out there, it's for everyone to see, interpret and analyse." This elaborates on a common belief among the citizens about governments and political institutions of the country not being completely transparent.

By making it apparent that there are some limitations the state cannot cross and other things it cannot expect to know, privacy serves to set boundaries for the state. It is also understood, that trust in political organisations is difficult to achieve but very easy to lose. It is, thus, advisable for all democratic institutions to not push their limits to the threshold after which they will most likely lose mass support (Goold, 2010).

The legitimacy of public institutions is crucial for building peaceful and inclusive societies. While levels of trust in institutions vary significantly across countries, opinion surveys suggest that there has been a decline in trust in public institutions in recent decades (United Nations, 2022).

2. The justifiability of Surveillance in specific contexts

While most of our participants were critical of mass surveillance, some discussed the benefits of this, especially in times of crisis. Most of them spoke about the lack of health infrastructure, especially in third-world countries like India, which would benefit from surveillance. Even in emergency situations, like accidents, where the immediate family is not readily available, upon the availability of health data accessible by the hospitals, treatment of the patient would be facilitated. Surveillance by corporations was also found to be justified provided they used the data for improving the experience of using the applications they built, rather than for using them to manipulate our opinions. While most spoke about ethics limited to health, some also claimed surveillance enhances the security of the state. Constant monitoring reduces deviance from normal behaviour and antisocial behaviour among members of society.

Personal data "needs" for institutions are actually very flexible. At one extreme, certain types of personal information are indeed required for particular organisational functions. For example, if someone subscribes to a publication, they must provide a physical address or an email address in order for it to be delivered. These requirements are "functionally necessary," but other alleged "needs" for personal information are not prerequisites; rather, they only increase the organization's advantage in dealing with the individuals in question (Cho, 2022).

3. Opinions regarding legal mechanisms for storage and use of data

Opinions regarding the need for privacy both at an individual and a collectivistic level were very strong among all the participants. All of them realised the immediate need for specific privacy laws related to data surveillance, both by governments and corporations. There was a sense of exploitation as some felt that their data was being used for the benefit of governments and corporations at their disposal. The discussion also included the lack of awareness about the absence of laws related to privacy breaching in online forums and monitoring online behaviour. The discussion concluded that this lack of awareness is a borderline infringement on an individual’s right to privacy.

While we spoke about the lack of privacy laws, there is also a sense of hopelessness in citizens that limits them from taking sufficient action. The discussion related it to mostly the lack of awareness among common people about the ardent need for privacy. Some people also claimed to feel helpless, and not influential enough to make a change. There was a consensus that ordinary people don't have the means to confront data extraction through governments and organisations, data once published can be accessible by all. There is also a certain context of influential multinational corporations and governments preventing such privacy-related laws for their personal benefit.

Online privacy protection has grown to be a compelling and important problem. The threats of privacy loss and infringement activities have come to light as a result of numerous cases involving the invasion of personal information privacy. These include activities that compromise users' data security, such as the sale of personal information and the development of online sociopsychological profiles. They show that governmental legislation and privacy rules don't adequately handle this moral conundrum. A recent example is EasyJet, where we recently found that more than 9 million accounts of their customers were hacked and all their personal data was leaked, including information like credit card information (Prince, Omrani, Maalaoui, Dabic, & Kraus, & 2021). Relating to privacy helplessness, there is a large number of people who exhibit such feelings and give up the concept of their own data management (Cho, 2022)

4. Trends of Data Tracking Awareness

While we spoke about the lack of common knowledge in people about the general data tracking done by corporations and governments, there is very little news about it. The discussion spoke about data extraction through illegal means by corporations, data extracted being used as actionable intelligence, and to study the trend of the society, or make strict laws in the society. But there was also a sense of reluctance to remove personal data from online forums, or re-check their privacy settings.

One tactic that democratic governments are increasingly using is surveillance. Public surveillance of population movements during a lockdown is another type of surveillance method that has been employed, in addition to the use of closed-circuit television (CCTV), drones, mobile phone usage statistics, and biometric tracker bracelets. The commercial sector

now has access to enormous amounts of information on us and regularly shares and uses that information in order to market to us, just like the government (Goold, 2010).

Overall, the opinions of the participants are consistent with recent research showing people's complacency with continually evolving security regulations and data breaches. Consequently, keeping up to date is exhausting, and when individuals do make the effort to update their settings, read regulations, etc., they are immediately discouraged or perplexed by the deluge of information they are presented with. Individuals are freed from worrying that businesses may take or use their data when they are in a state of denial regarding potential risks and threats to personal data and are able to use social media unrestrictedly (Hinds, Williams, & Joinson, 2020).

5. Privacy and its susceptibility to breaches with regard to social media

There was a very common theme in the discussion of the lack of privacy and consent in social media. Especially in the context of Cambridge Analytica, the participants expressed feelings of fear of manipulation, helplessness, and anger. Some of the topics that were discussed in lieu of this were about social media being used by governments as a tool to spread propaganda. People are manipulated through selective data based on their algorithms. Something that was also discussed was about past choices, past decisions about one's life being tracked and used to sway one for political thoughts.

Anonymized data in social media is susceptible to reidentification, and while data may be stored locally rather than centrally to reduce privacy issues, there are worries that the data may be compromised (Eck & Hatz 2020). The premise of privacy as control is fundamentally challenged by online social networking. Even with rigorous controls, it is still possible for online socializers to post unpleasant, malicious, or private information about one another, which would then be accessible to a sizable, if not unrestricted, online audience (Levin & Abril, 2009).

6. Pandemic-induced changes and needs for surveillance

The discussion primarily led to two dominant views. While one mostly dealt with how crisis situations require radical measures and in those situations data tracking is acceptable, if and only if, the data is just used for emergency-related purposes and removed after the emergency at hand is over. There was also a factor of complete transparency with the citizens and informed consent throughout the process. The second view was about whether a government, powerful with complete surveillance of its citizens, would ever give it up, or would the under-the-skin surveillance increase as we progress, eventually leading to a dystopian society.

Governments may not be ready to give up the enhanced surveillance tools these programmes offer, and there is always the chance that personal information will be collected forever and used in unforeseen ways. The UK government plans to preserve the data it collects for up to 20 years and only gives individuals the full right to have their data erased upon request. The US Patriot Act, which granted the government-wide monitoring ability without any supervision, was passed in 2001 in response to the terrorist attacks of September 11, 2000. It is still in force today even though there is no proof that a foreign assault on US soil is currently a threat (Eck & Hatz 2020).

CONCLUSION

The paper deals with the knowledge of online communication, be it state-mandated technologies or social media, is already regulated, primarily by search engines and recommender systems, whose goals and parameters may not be publicly known. There is very less awareness of public policy and laws that deal with online data monitoring of people. There is an asymmetrical relationship between the users and the platforms. This was especially evident in 2020 with the advent of the pandemic. Data monitoring apps that began with aim of storing and recording health-related information slowly progressed to complete data monitoring through those applications in several democratic countries. The paper tried to understand the perception of people regarding surveillance, especially their notion and understanding of their privacy levels.

Better laws like national human rights action plans might concentrate on how state actors employ digital surveillance techniques to determine whether there are human rights violations occurring would help people address their complaints and seek judicial help. When the use of contact tracing apps does not adhere to the obligations of international human rights legislation, transparency through effective multilateral and multistakeholder can be used to hold governments accountable. There are now several instances of domestic review systems that have been successful in reversing overzealous governmental surveillance during the COVID-19 pandemic. The recently updated, hastily passed telecom law in Slovakia was found to include illegal provisions by the Constitutional Court. The modifications aimed to give state authorities access to telecommunications data for contact tracing, but they were rejected because they weren't sufficiently clear and didn't include safeguards against abuse (Sekalala, Dagron, Forman, & Meier, 2020).

States have barely taken substantial action to prevent under-the-skin surveillance of their citizens both by themselves and private organisations. But some of the things that states can do to increase transparency and accountability is to have regular risk assessments to have evidence-based decision-making. There should be sufficient reason for citizens to be monitored, and those justifications should be given to the citizens. Data of all citizens should be treated equally, irrespective of their social background. States must include a termination clause in any laws that permit digital public health monitoring due to the threats to privacy, which stipulates in advance what information is being collected, for how long it should be kept, and when the right to keep it will expire.

REFERENCES

Agar, J., & Aspray, W. (2016). The Government Machine: A Revolutionary History of the Computer (History of Computing) (Reprint). The MIT Press.

Amnesty International. (2021, August 13). Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy. https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/

Acquisti, A., & Gross, R. (2006, June). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In International workshop on privacy enhancing technologies (pp. 36-58). Springer, Berlin, Heidelberg.

Beck, J. (2018, June 8). Did Cambridge Analytica Change Facebook Users' Behavior? The Atlantic.https://www.theatlantic.com/technology/archive/2018/06/did-cambridge-analytica-actually-change-facebook-users-behavior/562154/

Bennett, C. J. (2010). The Privacy Advocates: Resisting the Spread of Surveillance. MIT Press.

Bradshaw, T., Murphy, H., & McGee, P. (2020, April 28). Coronavirus apps: the risk of slipping into a surveillance state. Financial Times. https://www.ft.com/content/d2609e26-8875-11ea-a01c-a28a3e3fbd33

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative research in psychology, 3(2), 77-101.

Cho, H. (2021). Privacy helplessness on social media: its constituents, antecedents and consequences. Internet Research, 32(1), 150–171. https://doi.org/10.1108/intr-05-2020-0269

Eck, K., & Hatz, S. (2020). State surveillance and the COVID-19 crisis. Journal of Human Rights, 19(5), 603–612. https://doi.org/10.1080/14754835.2020.1816163

Franko Aas, K., Gundhus, H.O., & Lomell, H.M. (Eds.). (2008). Technologies of InSecurity: The Surveillance of Everyday Life (1st ed.). Routledge-Cavendish. https://doi.org/10.4324/9780203891582

Gershgorn, D. (2021, December 14). We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World. Medium. https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9

Gohdes, A. R. (2020a). Repression Technology: Internet Accessibility and State Violence. American Journal of Political Science, 64(3), 488–503. https://doi.org/10.1111/ajps.12509

Gohdes, A. R. (2020b). Repression Technology: Internet Accessibility and State Violence. American Journal of Political Science, 64(3), 488–503. https://doi.org/10.1111/ajps.12509

Goldsmith, A. J. (2010). Policing's New Visibility. British Journal of Criminology, 50(5), 914–934. https://doi.org/10.1093/bjc/azq033

Goold, B. J. (2010). How much surveillance is too much? Some thoughts on surveillance, democracy, and the political value of privacy. Some thoughts on surveillance, democracy, and the political value of privacy.

Goold, B.J. (2010). Technologies of surveillance and the erosion of institutional trust. In Katja Franko Aas, Helene Oppen Gundhus, & Heidi Mork Lowell (Eds). Technologies of Insecurity: The Surveillance of Everyday Life. Routledge Cavendish

Gunitsky, S. (2015). Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability. Perspectives on Politics, 13(1), 42–54. https://doi.org/10.1017/s1537592714003120

Hajli, N., & Lin, X. (2014). Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. Journal of Business Ethics, 133(1), 111–123. https://doi.org/10.1007/s10551-014-2346-x

Harari, Y. N. (2020, March 20). Yuval Noah Harari: the world after coronavirus | Free to read. Financial Times. https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

Higgs, E. (2003). The Information State in England: The Central Collection of Information on Citizens since 1500(2003rd ed.). Red Globe Press.

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. International Journal of Human-Computer Studies, 143, 102498. https://doi.org/10.1016/j.ijhcs.2020.102498

Hope, T. L., & Gilliom, J. (2003). Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy. Contemporary Sociology, 32(3), 295. https://doi.org/10.2307/3089153

KING, G., PAN, J., & ROBERTS, M. E. (2017). How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument. American Political Science Review, 111(3), 484–501. https://doi.org/10.1017/s0003055417000144

Levin, A., & Abril, P. (2009). Two notions of privacy online. Vanderbilt Journal of Entertainment and Technology Law, 11(4), 1001-1052.

Lippert, R. (2008). David Lyon, Surveillance Studies: An Overview. Canadian Journal of Sociology, 33(2). https://doi.org/10.29173/cjs2004

Locke, J. L. (2010). Eavesdropping: An Intimate History (1st ed.). Oxford University Press.

MATHIESEN, T. (1997). The Viewer Society. Theoretical Criminology, 1(2), 215–234. https://doi.org/10.1177/1362480697001002003

Morgan, D. L. (1996). Focus groups. Annual review of sociology, 22(1), 129-152.

Monahan, T., Torres, R. D., Kupchik, A., Bracy, N., Apple, M., Hirschfield, P., Casella, R., Gilliom, J., Hope, A., Lewis, T., Lipman, P., Matthew, R., Simmons, L., Steeves, V., Wall, T., & Weiss, J. (2009). Schools Under Surveillance: Cultures of Control in Public Education (Critical Issues in Crime and Society) (None ed.). Rutgers University Press.

Mishler, W., & Rose, R. (2005). What are the political consequences of trust? A test of cultural and institutional theories in Russia. Comparative Political Studies, 38(9), 1050-1078.

O'Neill, P. H. (2020, May 7). India is forcing people to use its covid app, unlike any other democracy. MIT Technology Review. https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-COVID-app-mandatory/

O.Nyumba, T., Wilson, K., Derrick, C. J., & Mukherjee, N. (2018). The use of focus group discussion methodology: Insights from two decades of application in conservation. Methods in Ecology and Evolution, 9(1), 20–32. https://doi.org/10.1111/2041-210x.12860

Prince, C., Omrani, N., Maalaoui, A., Dabic, M., & Kraus, S. (2021). Are we living in surveillance societies and is privacy an illusion? An empirical study on privacy literacy and privacy concerns. IEEE Transactions on Engineering Management.

Rodriguez, K. S. W. (2020, September 9). International Proposals for Warrantless Location Surveillance To. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2020/05/global-contact-tracing-international-proposals-track-COVID-19

Routledge Handbook of Surveillance Studies. (2012). Routledge.

Sabbagh, D., & Hern, A. (2020, July 1). Privacy group prepares legal challenge to NHS test-and-trace scheme. The Guardian. https://www.theguardian.com/world/2020/may/31/privacy-campaigners-prepare-legal-challenge-to-uks-test-and-trace-scheme

Sekalala, S., Dagron, S., Forman, L., & Meier, B.M. (2020). Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis. Health and Human Rights, 22, 7 - 20.

Shipman, F. M., & Marshall, C. C. (2020). Ownership, Privacy, and Control in the Wake of Cambridge Analytica. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3313831.3376662

Trust in public institutions: Trends and implications for economic security | DISD. (n.d.). https://www.un.org/development/desa/dspd/2021/07/trust-public-institutions/

Turow, J. (2005). 11. Cracking the Consumer Code: Advertisers, Anxiety, and Surveillance in the Digital Age. The New Politics of Surveillance and Visibility, 279–307. https://doi.org/10.3138/9781442681880-012

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. Journal of the Association for Information Systems, 7(6), 1.

Weller, T. (2010). The Information State: An historical perspective on surveillance. In Routledge Handbook of Surveillance Studies. (2012). Routledge.

Whitson, J. R., & Haggerty, K. D. (2008). Identity theft and the care of the virtual self. Economy and Society, 37(4), 572–594. https://doi.org/10.1080/03085140802357950

Acknowledgement

To the participants, without whose insightful contributions to the topic, it would have been merely impossible for us to progress with this paper. To the college for providing us with all the necessary infrastructure and facilities, we are required to go ahead with the paper and to the Principal and the Professors in the Psychology department for their immense support and guidance, we thank you. And, to all the esteemed researchers who contributed to the topic before us, we would like to express our utmost gratitude.

Conflict of Interest

The authors declare no conflict of interest.

How to cite this article: Sanyal, A. & Jukar, S. R. (2023). "What About My Privacy?": Exploring Perceptions Towards Increased Surveillance. *International Journal of Indian Psychology, 11(1),* 874-886. DIP:18.01.090.20231101, DOI:10.25215/1101.090