Widening the Horizons of Surveillance

Lateral Surveillance Mechanisms: Issues & Challenges

8 January 2021*

By: Mira Swaminathan & Shubhika Saluja
Edited by: Arindrajit Basu, Aayush Rathi, Shweta Mohandas.
The Centre for Internet and Society, India

* The research was submitted for review in May 2020 and accepted for publication in June 2020.
Acknowledgements

We thank Amber Sinha for his advice and insights into the research and the final paper. We thank Shweta Reddy and Torsha Sarkar for the endless discussions and believing that this paper will be published one day.
# Table of Contents

**Background**  
2  

**Research Overview**  
3  
Objective  
3  

**Neighbourhood Watch: A form of Lateral Surveillance**  
4  
1.1 Introduction to Lateral Surveillance  
4  
1.2 Forms of Lateral Surveillance: From Neighbourhood Watch Schemes to Mobile Applications  
5  
1.3 Examples of Technologization of Lateral Surveillance  
7  

**Dangers arising from Lateral Surveillance**  
9  
2.1 Impact on the society and other structures  
9  
2.1.1 Increasing Social Distrust and building the Culture of Surveillance  
9  
2.1.2 Issues with Privatization of Law Enforcement  
12  
2.2 Impact on Fundamental Rights  
13  
2.2.1 Right to Privacy  
14  
2.2.2 Right to Freedom of Speech and Expression  
16  

**Conclusion & Recommendations**  
17  
4.1 On the human front: Building a culture of mutual care and trust instead of surveillance  
19  
4.2 On the tech front: Implementation of privacy practices/principles  
20  

**Limitations & Scope for Future Research**  
21
Background

Neighbourhood watch arrangements are peer to peer surveillance practices aimed at countering criminal activities in the local area. These arrangements have been used to tackle changes in the urban environment, and can be seen as a shift from traditional policing to community policing. Though these neighbourhood watch schemes originated in the United States due to increased crime rates, in India, these arrangements grew in light of the heavily understaffed and under-resourced police force. According to the Bureau of Police Research and Development, India’s police to population ratio is 198 per lakh of population. Further, larger cities have increased incidents of crime which may be attributed to urban anonymity. National Crime Record Bureau statistics for the year 2018 showed an increase of 10% over 2017 in the cognizable crimes registered in 19 metropolitan cities.

Since the outbreak of the pandemic, several authorities in India have launched neighbourhood watch arrangements to shore up security while reducing alienation of individuals from society. While these new initiatives are a positive step undertaken by the law enforcement agencies in good faith, they raise concerns about the normalization of a culture of surveillance, especially due to the regulatory challenges around a range of issues including privacy and security concerns about the data collected through this initiative and the possible impacts on the freedom of expression.


Research Overview

Objective

Neighbourhood watch integrated with community engagement is emerging worldwide to target anti-social behavior and crime. Initially, started by law enforcement agencies on the ground, it has been enabled by the use of surveillance technology, and facilitated often by private entities. Technology has further enabled easy access into the private lives of citizens, either by their own volition or by the laws of the state or the practices of the society.

In India, the use of high powered technology by law enforcement agencies to surveil has raised concerns over privacy and data protection, especially due to the lack of a full-fledged privacy law. Privatization of the functions of law enforcement agencies, also warrants invasion of privacy, especially in the times when surveillance technology is affordable and easily accessible by ordinary citizens as well, giving rise to a new form of surveillance, peer to peer or lateral.

The objective of this study is to analyse the working of the several lateral surveillance mechanisms backed by the state or private entities and their potential social and constitutional impacts. This paper provides doctrinal research on the legal issues involved in the working of different portals and applications dealing with neighbourhood watch and community policing. Be that as it may, the analysis has been made to understand the practical implications of the emerging technology and not in any way suggests that these issues will actually arise. The paper then recommends certain basic safeguards required to be adhered to by data collecting entities to ensure privacy and security of the data.

---


Neighbourhood Watch: A form of Lateral Surveillance

1.1 Introduction to Lateral Surveillance

The concept of lateral surveillance is based on a novel application of the concept/technique of surveillance, i.e., the act of ‘watching over’. The conventional understanding of the term, surveillance, is its use in hierarchical sense, i.e. vertical relationship between the person watching and the person being watched, which is usually the State and its citizenry. Lateral or social or peer to peer surveillance differs from typical surveillance. The power dynamic between the one watching and the one being watched is not structural or hierarchical but more decentralized and balanced; and the surveillance takes place between individuals themselves, without the involvement of any organizational entity. Lateral surveillance, as described by Mark Andrejevic, is characterised by surveillance relationships that are mutual, with horizontal relationships between persons. He further describes it as “the use of surveillance tools by individuals, rather than by agents of institutions public or private, to keep track of one another, covers (but is not limited to) three main categories: romantic interests, family, and friends or acquaintances.”

Surveillance of any kind shows an imbalance of power between the person who surveils and the person being surveilled. Lateral surveillance, however, depicts a shift from the hierarchical form of surveillance, i.e., state over citizen, to citizen over citizen wherein the

---

imbalance of power no longer exists. Informal watching of communities by their members has been a part of the society, however, the same have become more organized in the form of neighbourhood watch programmes and made more intrusive through “the assemblage of surveillance mechanisms”.

1.2 Forms of Lateral Surveillance: From Neighbourhood Watch Schemes to Mobile Applications

The origins of neighbourhood watch schemes may be attributed to the rise of community policing in the 1980s in the USA and UK. Neighbourhood watch initiatives encourage citizens to take the responsibility of detecting and preventing crime through surveillance of their neighbourhoods. These neighbourhood watch schemes may originate in association with local law enforcement agencies or independently by the citizens of the neighbourhood and hence, are a kind of community policing. The assumption underlying these programs is that they reduce opportunities for crime through observation and reporting of suspicious activities to the police. Several campaigns have warned citizens to keep alert, look out for

suspicious or unusual behaviours,\textsuperscript{22} and appealed with slogans like ‘if you see something, say something’ or ‘be suspicious of anything unattended’.\textsuperscript{23}

Neighbourhood watch is said to have several benefits like reducing crime rates, improving the quality of life, building community pride and unity and enabling individuals to become the “extra ‘eyes and ears’ of law enforcement agencies”.\textsuperscript{24} Watch programmes which were implemented in the 1970s and 1980s in the USA were intended to mobilize the local residents ‘to become reflexive with respect to risks for crime prevention’, making them responsible for policing their own territories.\textsuperscript{25} Similarly, the new lateral surveillance technologies emphasize on local knowledge of the citizens in association with policing authorities.

With rapidly evolving technology, monitoring of people and their behaviour has become easier and collection of information by a myriad of public and private institutions for the purposes of governance and engaging in public activities has become normal.\textsuperscript{26} Specifically in the sphere of crime prevention, there has been a transition in the outlook from a ‘punishing state’ to a ‘preventive state’.\textsuperscript{27} This trend has emerged post the terrorist attacks which have led the states to focus more on prevention of major crimes in the society and

\begin{footnotesize}
\begin{enumerate}
\end{enumerate}
\end{footnotesize}
reduction of the harms caused,\textsuperscript{28} instead of simply bolstering the criminal justice system that encourages deterrence. Thus, everything from introduction of CCTV cameras in public spaces to security check-ins are methods through which a ‘preventive society’ is being created.\textsuperscript{29} This pervasive, decentralised and uncoordinated regime of surveillance systems has been termed as “surveillant assemblage” by Haggerty and Ericson.\textsuperscript{30} Further, the arrangements of mutual watching where citizens’ monitoring themselves and others through corporate channels of data flow, i.e., operated by private entities, feed back into state surveillance of citizens have come to be termed as “veillant panoptic assemblage.”\textsuperscript{31} Due to lack of coordination, such information collected from these sources can be used for different purposes that the ones they are collected for.\textsuperscript{32}

The contribution of the state in technologisation of lateral surveillance for the purposes of law enforcement and public engagement reaffirms the idea “that surveillance is driven by the desire to bring systems together, to combine practices and technologies and integrate them into a larger whole [...] with such combinations providing for exponential increases in the degree of surveillance capacity.”\textsuperscript{33} Surveillance technologies have eased the participation of citizens by arming them with mobile applications and other platforms which can help them watch over others\textsuperscript{34} to help law enforcement (public) or private entities gain knowledge about individuals. Search engines like Google and social media networks such as Facebook


and other advancements in technologies have made it cost-less and effortless ‘to listen to, watch, record, and research’ anyone. This results in the ‘explosion of personal data’ capable of producing massive amounts of data which can further become a target of surveillance.

### 1.3 Examples of Technologization of Lateral Surveillance

Lateral surveillance initiatives are undertaken by both public and private entities. With the development of technology, new initiatives have come to rely heavily on such technology to mobilize citizens or to provide them with information sharing platforms to enable peer to peer or citizen communication. The table below elaborates the objectives and working of some lateral surveillance technologies across the world and we further go on to discuss the general concerns about these applications raised by privacy and free speech advocates.

<table>
<thead>
<tr>
<th>Name of the Application</th>
<th>Location</th>
<th>Objectives/Working</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citizen App</td>
<td>United States of America</td>
<td>This application provides real-time safety alerts and live video incidents happening near the user. It is meant to protect the citizens. The application uses the location data of the user to send users 911 alerts for crimes happening nearby.</td>
</tr>
</tbody>
</table>

---


<table>
<thead>
<tr>
<th>App</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nextdoor App</td>
<td>United States of America &amp; Australia</td>
<td>This application provides a social media network [facebook styled] for people to share information with their local community. Apart from encouraging sharing of goods and recommendations, it has a ‘crime and safety’ section and it allows users to report crime or suspicious activity. The information collected by the application includes basic contact information, network data, social media data, payment information among other things.</td>
</tr>
<tr>
<td>Neighbors App (Ring)</td>
<td>United States of America</td>
<td>This application [linked to the home-security system, Ring] was created to detect real-time crime and safety alerts from neighbors and local law enforcement. Its objective is to keep people informed about the crimes happening in their area, and allows them to share updates in order to keep their neighbourhood safe.</td>
</tr>
<tr>
<td>C-Plan App</td>
<td>Uttar Pradesh, India</td>
<td>This application launched for keeping a tab on anti-social elements, is designed to receive input from certain identified individuals in villages across the State. These individuals have been given the responsibility to solve local problems, provide information about simmering communal tensions or land disputes taking place in their respective villages through the application.</td>
</tr>
</tbody>
</table>

Dangers arising from Lateral Surveillance

2.1 Impact on the society and other structures

In the absence of research proving the effectiveness of neighbourhood watch efforts, it may be said that lateral surveillance is promoted by governments not necessarily because of their effectiveness, but due to “more symbolic and emotional factors that contribute to the adoption of such initiatives”. It is likely that such initiatives are undertaken by local governments for the message they send rather than the substance. It is becoming increasingly difficult to differentiate a surveillance practice dedicated to ‘security’ from its many other applications, as surveillance mechanisms constituted for one purpose may assume other uses. Social relations and emotional factors such as love, affection, care for elderly are a major driving force for lateral surveillance mechanisms. By the effect of these factors, people may voluntarily or involuntarily take up the exercise of checking up on their neighbours to be of help or prevent loneliness, which could soon turn into vigilantism and surveillance. Therefore, we argue that the aforementioned applications actively promote lateral surveillance under the facade of community building.

---

42 Hawkeye. Hyderabad City Police (Version 3.0.7) [Mobile application software]. https://hyderabadpolice.gov.in/HawkEye.html.


2.1.1 Increasing Social Distrust and building the Culture of Surveillance

Culture of surveillance and constant suspicion: The use of lateral surveillance tools or technologies by ordinary citizens for observing and reporting threats in the neighbourhood normalizes the ‘culture of suspicion’, thus creating potential social distrust.\(^{46}\) Trust among citizens is based on a mutual understanding about the need to provide security protection and the need to respect rights like privacy in a democratic society.\(^{47}\) This trust and social cohesion erode when people start putting aside either privacy or security in favour of the other.\(^{48}\) While citizens become more aware of the various types of criminal activities and methods of prevention, they also alter their behaviour in order to feel more secure and sustain the practice of ‘keeping an eye on another’.\(^{49}\) It could range from curiosity about a neighbour’s absence in community gatherings to reporting of a suspicious person to the police. In this process, citizens are sensitized to security threats whether or not there is an actual imminent danger.\(^{50}\) The mere possibility of discovering a threat convinces them to continue looking. Thus, their suspicion over neighbours creates an air of distrust.\(^{51}\)

Once a specific way of what a neighbourhood should be, is normalized, any act which is not in accordance with this way is regarded as suspicious and hence a potential threat to the society. As stated by Janet Chan in her article, “The New Lateral Surveillance and a Culture of Suspicion,” new lateral surveillance is not a means to develop and sustain trust and building healthy communities but ‘a call for eternal vigilance and constant suspicion’.\(^{52}\) Research has

---


shown that such watch programmes or lateral surveillance initiatives can actually heighten the fear of crime. People believe that they are constantly under threat and are also responsible for the safety and security of their neighbourhood. Further, such perceived threat has a tendency to “increase intolerance, prejudice, ethno-centrism, and xenophobia”.

The consequence of the constant contact among neighbours may result in “ethnic profiling, vigilantism, increased anxiety, communication overload and potential tensions” among them.

Fear is used as a ‘disciplinary power’ in order to control the mindset of the society, not only against crime but also non-conforming social behaviour. A study of Singapore's lateral surveillance mechanism has proved that most people feared the negative publicity and hence, involved themselves in this form of surveillance to check their own behaviour as well.

**Tool for social exclusion:** The surveillance technologies act as tools for social control and social exclusion in shaping the socio-economic relations in the society and relation between the state and its citizens. Acceptance of these technologies and the desire for more security increases the likelihood of people detecting threats in every image or situation different from the one they have of themselves or the society they live in.

Though the stated goal of neighbourhood watches is the unification of community, there is an inherent exclusionist intent of community crime prevention which often does not come to


the fore. The neighbourhood members who decide what qualifies as crime or suspicious activity are the so called ‘like minded individuals’ whose inherent biases may creep in while deciding who the crime-creating undesirables are. Then, the neighbourhood becomes a gated community with restricted access to anyone considered an outsider and tends to privatize normally public spaces. Hence, leading to the exclusion of those considered not fit for protection of the community. Hence, neighbourhood watches have the potential to re-characterize a community, neighbourhood or place, and establish new norms about criminality, suspicion and surveillance in that place, leading to the stigmatization or re-stigmatization of target groups who are already disadvantaged. Furthermore, wrong suspicions can trigger police investigations and preliminary searches and more surveillance.

2.1.2 Issues with Privatization of Law Enforcement

Initiatives which encourage lateral surveillance make the citizens responsible for ‘policing their own territories’. In order to prevent crimes, citizens are becoming increasingly eager to join hands with the law enforcement agencies to create safer neighbourhoods by engaging in policing efforts and facilitating the investigation processes. Though the involvement of citizens has shown to strengthen the local security networks, if citizens lack trust in the police, an air of mistrust and frustration between the police and citizens might be created.

A major problem which has surfaced with active citizen involvement in crime prevention or neighbourhood watch schemes is that citizens may overstep their boundaries and act as private law enforcers.\textsuperscript{67} Since active involvement, to a great extent, warrants a shift in the responsibility of the law enforcement agencies onto the citizens, who are not only required to monitor their neighbourhood, but to safeguard it.\textsuperscript{68} This greater responsibility in managing potential security threats and risks blurs the fine line between solving neighbourhood issues and acting as police themselves, especially in crimes that directly impact people such as thefts, assaults, and domestic violence or meagre cases of neighbourhood nuisances. There is thus a misprioritization of what might come under the police priorities and citizen priorities.\textsuperscript{69} Therefore, in light of the exclusionist intent of community involvement in crime prevention discussed above, citizens might overreach their roles as mere ‘watchers’ and transform from reporters to actors for countering crime. In order to prevent such blurring of the boundaries between police, citizens and suspects, it is important to clarify the role assumed by the participants of such so-called community building initiatives.

\section*{2.2 Impact on Fundamental Rights}

Lateral surveillance mechanisms \textit{prima facie} threaten the two most fundamental rights of citizens in any modern democratic state. These initiatives impact the right to privacy and the freedom of speech and expression. The two rights, “\textit{privacy and freedom of expression are interlinked and mutually dependent; and infringement upon one can be both the cause and consequence of an infringement upon the other}”.\textsuperscript{70} Considering the impact lateral surveillance has on the society, it may lead to intrusion of privacy, if checks and balances are not imposed and also threatens those who express dissent.

In the case of lateral surveillance, the ‘fear of being watched’ is constant as the ‘watchers’ are always in the vicinity. Briefly, the constant watching leads to people altering their behaviour

\begin{itemize}
\end{itemize}
in order to conform to societal standards or norms.\textsuperscript{71} This creates a “chilling effect” on free speech, i.e., people tend to indulge in self-censorship.\textsuperscript{72} Further, the minority groups in religion, gender, caste, and others are the ones who are disproportionately impacted by such restraints due to the higher risk of being different and non-conformist, hence, at a higher risk of being considered ‘surveillance worthy’ by fellow citizens. The impact on both these rights with reference to lateral surveillance mechanisms is explained below.

### 2.2.1 Right to Privacy

In India, the right to privacy was declared to be a part of the right to life under Part III (Chapter on Fundamental Rights) of the Constitution by a nine judge constitutional bench in *Puttaswamy v Union of India* (I).\textsuperscript{73} The Supreme Court has observed that “the contours of the right to privacy include the right to be left alone; the right to respect for private and family life, home, and correspondence; protection against intrusion and surveillance; and a recognition of an individual's decisional autonomy”.\textsuperscript{74} The right to be let alone is not an absolute right.\textsuperscript{75} An individual's right to privacy has to be balanced against the state’s responsibility to ensure the safety and security of the State and maintain public order.\textsuperscript{76}

Surveillance measures of any kind would have to be assessed against the tests laid down by the court. While the elements of the test have suffered from a lack of clear majority opinion in the decision,\textsuperscript{77} we use the test applied by the majority in the *Puttaswamy v Union of India (II)*\textsuperscript{78} (the “Aadhaar” judgement) for our analysis. Surveillance measures are said to be reasonable restrictions on the right to be let alone if they achieve the right balance between the exercise of the right to privacy and the state action infringing privacy. *Puttaswamy v Union of India (I)* laid down a three fold test to ascertain if the restriction on the right to privacy is legitimate and this includes-(i) existence of a law; (ii) legitimate state aim; (iii) proportionality.\textsuperscript{79} The Supreme Court in *Modern Dental College & Research Centre v State of"

---


\textsuperscript{73} K.S. Puttaswamy v Union of India (2017) 10 SCC 1.

\textsuperscript{74} Karmanya Singh Sareen & Another v Union of India and Others SLP (C) No. 804 Of 2017 & Antony Clement Rubin v. Union of India W.P. No. 20774/2018.

\textsuperscript{75} K.S. Puttaswamy v Union of India (2017) 10 SCC 1.

\textsuperscript{76} State of Privacy in India. (2019, January 26). Privacy International. \url{https://privacyinternational.org/state-privacy/1002/state-privacy-india}.


\textsuperscript{78} K.S. Puttaswamy v Union of India (2019) 1 SCC 1.

\textsuperscript{79} K.S. Puttaswamy v Union of India (2017) 10 SCC 1.
Madhya Pradesh,⁸⁰ specified the requirements of proportionality standards, which are (i) a measure restricting a right must have a legitimate goal; (ii) it must be a suitable means of furthering this goal; (iii) there must not be any less restrictive, but equally effective alternative; and (iv) the measure must not have any disproportionate impact on the right holder. This was later adopted by the Supreme Court in 2018 in the judgment on the validity of Aadhaar in Puttaswamy v Union of India (II).⁸¹

State surveillance is a preventive measure to reduce crime, and ensure safety of all the citizens. However, measures that purport to improve security might actually reduce security⁸² by disturbing the balance between competing interests of privacy and collective security. There are different surveillance mechanisms that inadvertently collect some data directly, however under the lateral surveillance mechanism, data is collected through the means of social control of citizens.⁸³ Social control can be exercised not only by the introduction of accessible and affordable surveillance technology but also through indirect means including pressurizing citizens to conform to societal norms citizens via their awareness schemes.

The introduction of lateral surveillance applications online or offline constitute infringement of one’s right to privacy as individuals would be effectively surveilled on a daily basis by other citizens, and these applications when sanctioned by the state are likely to fail the test of proportionality as laid down in Puttaswamy I for the following reasons:

(i) Measure restricting a right must have a legitimate state aim and must be rationally connected with the aim

This step is known as the “legitimate goal test” wherein the measure taken by the State should be a suitable means of furthering its goal.⁸⁴ While the objective of these applications is to increase interaction between the neighbours, build a sense of community and reduce crime rates, these applications only make it easier to share personal information about neighbours on their platforms, through the use of CCTV cameras or other features. As a result of this, the connection between the aim of the state to reduce crime rate and manner in which the right to privacy is restricted is most likely to be unclear.

---

⁸⁰ Modern Dental College & Research Centre v State of Madhya Pradesh (2016) 7 SCC 353.
⁸⁴ K.S. Puttaswamy v Union of India (2017) 10 SCC 1; Anuradha Bhasin and Ors. v Union of India and Ors. (2020) 3 SCC 637.
(ii) There must not be any less restrictive but equally effective alternative

If there exist less restrictive and better alternatives, then such measures are likely to fail the test. For the purposes of countering crime rates and depression in the urban jungle, less restrictive and less intrusive mechanisms that can be equally effective such as ground measures to reduce crime with citizen participation or community policing initiatives. For instance, ‘behavioural impact’ programmes in schools and colleges to introduce counselling and awareness services regarding criminal behavior or other awareness initiatives at the community level. One such model is the Youth Guidance Behavioural programmes\textsuperscript{85} in Chicago wherein weekly group sessions were introduced in public schools.

(iii) The measure must not have any disproportionate impact on the right holder.

Lateral surveillance technologies are likely to create a culture where anonymity of individuals is not respected on the pretext of preventing crimes and loneliness. On this basis, such technologies infringe upon the right to privacy of an individual either directly or indirectly. It infringes privacy directly because it encourages people to update information of their neighbours, and indirectly because it encourages a culture of surveillance which ultimately infringes on the right to anonymity in public spaces. Further, the prospects of what can result in organized surveillance with the combination of the information available on these applications raises concerns not only about privacy violations but the increased control in the hands of ordinary citizens which might embolden citizens to take actions they should not.\textsuperscript{86} Thus, there is a definitive disproportionate impact on the right holder, especially if the right holder belongs to a vulnerable group- people belonging to religious minorities, lower caste and the LGBTQIA community, among many others.

2.2.2 Right to Freedom of Speech and Expression

The functioning of these applications is likely to impact the right to free speech and expression protected under Article 19(1)(a) of the Constitution. Though the right can be reasonably restricted, it forms the basis of a democratic society.\textsuperscript{87} The establishment of a ‘full proof and a powerful’ surveillance system is a mark of a totalitarian regime wherein the requirement of privacy is looked down upon and is termed as ‘anti-national’, ‘anti-social’ and immoral in nature.\textsuperscript{88}

\textsuperscript{85} UChicago Urban Labs. \textit{Reducing Violence and Increasing Graduation}. \url{https://urbanlabs.uchicago.edu/projects/becoming-a-man}.


\textsuperscript{87} Constitution of India, Article 19(2).

Dissent is an essential component of democracy.\textsuperscript{89} It could be dissent against the state or dissent of opinion between two individuals. The right to freely express one’s opinion without it having to be curbed is an essential fundamental right and it needs to be respected. Justice DY Chandrachud in a speech clearly stated that “the blanket labelling of dissent as anti-national or anti-democratic strikes at the heart of our commitment to protect constitutional values and the promotion of deliberative democracy.”\textsuperscript{90} The very famous Shreya Singhal judgment\textsuperscript{91} struck down Section 66A of the Information Technology Act that disproportionately suppressed dissent.

Implementation of lateral surveillance mechanisms has the potential to threaten dissent in society. In an environment of increasing intolerance to minority conduct and other socio-political factors, the social pressure to conform to the society along with the disincentivization of dissent results in curbing one’s freedom of speech and expression. This could lead to pre-censorship. Much like how the citizens unwilling to light the candles ultimately participated in the activity, more people might ‘pre-censor’ and conform to the societal standards of ‘normalcy’ in order to belong or be accepted by the neighbourhood.

The right to anonymity is also an aspect under the right to freedom of speech and expression and is of more importance for minority groups and dissenting individuals. Further, various judicial pronouncements in the United States have ensured that recognition of a right of anonymity is based on the belief that compulsory disclosure may deter the expression of ideas and the participation in associations both of which are protected by the first and fourteenth amendments.\textsuperscript{92} While there is an ongoing debate on whether or not the deterrent effect of disclosure may result in an infringement of freedom of speech and expression.\textsuperscript{93} It is essential to note the importance of anonymity in public spaces. These forms of excessive surveillance being normalised are a direct blow at the right to anonymity under the right to freedom of speech and expression.

\begin{flushright}
\textsuperscript{91} Shreya Singhal v Union of India (2013) 12 SCC 73.
\end{flushright}
Conclusion & Recommendations

Surveillance always begins on a justifiable commonly agreeable public goal in a systematic way.\textsuperscript{94} Surveillance being a focused activity involves aggregation and storage of data that can be transmitted, retrieved, compared, mined, and traded.\textsuperscript{95} As discussed above, emerging technologies have made it easier for the state as well as the citizens to constantly watch those with non-conforming behaviours as set by the society or the law. Technologies such as CCTV cameras and mobile applications have privatized and decentralized law enforcement placing greater responsibility on the citizens ultimately creating a ‘culture of surveillance’.

The proliferation of lateral surveillance mechanisms, especially mobile applications which either provide a social media kind of platform or other modes of community participation for the purposes of crime prevention is increasingly becoming the new ‘normal’. Moreover, the promotion and sanction of such mechanisms by governments ensure that their objective of surveillance is met through citizens themselves with little or minimal involvement sideling the benefit to the community.\textsuperscript{96} What we see then is the mobilization of the citizens either by ‘soft persuasion’ or ‘coercion’ by the state to integrate lateral surveillance into their daily lives.\textsuperscript{97}

Especially, in the wake of a pandemic, different kinds of applications were brought for the purpose of contact tracing and enforcing quarantine.\textsuperscript{98} Further, these measures increase the chances of users learning about who could be the source of infection\textsuperscript{99} by showing the timing when an infected person visited a particular location on interactive maps or using identification tags seeking active involvement of neighbours. We discussed how lateral surveillance also poses a threat to the social fabric of the society as it normalises suspicion and distrust towards fellow citizens ultimately becoming a means for social exclusion of the minority. In this culture of risk aversion, fearing strangers and security obsession, it is important for these technologies to be structured in a way that restrains or at least, redirects...

surveillance. Redirection of surveillance essentially would mean doing it for appropriate purposes while ensuring it does not foster fear.

There is a need to balance the conflict between the common objective of community building and safer neighbourhoods and privacy interests of the individuals forming part of the community. Though the use of technology promoting lateral surveillance cannot be avoided due to the increasing need for security and human contact in civilised and technologized societies, its harms can be significantly reduced by placing certain safeguards and changing the citizens’ approach to such initiatives. Therefore, the following recommendations have been made in light of the above. These recommendations are based on two aspects, on the human front and technology aspect, i.e. first, the focus should be on sensitizing people who would consciously or otherwise take part in lateral surveillance and then, on how the technology used should be based on privacy principles.

4.1 On the human front: Building a culture of mutual care and trust instead of surveillance

Lateral surveillance can supposedly be ‘turned on the head’ in order to ensure that there is an effective mechanism created to sustain a system wherein mutual trust and welfare is encouraged instead of suspicion. This stems from the distinction between the ‘top-down’ and ‘bottom-up’ approach prescribed by Offe. The ‘top-down approach’ induces compliance from citizens through legitimate and competent governance to generate horizontal trust by following the principles of transparency and fairness. On the other hand, in the ‘bottom-up approach,’ more reliance is placed on citizens to get involved with strangers in open associative communities and learn to trust each other. If the latter approach is adopted in

---

the absence of the possibility of transparent and fair government mechanisms, the burden is on the people to use lateral surveillance mechanisms not as a tool of control but as a more positive initiative for interactive citizenship. This can be done only when the focus shifts from desire for security to mutual care.\textsuperscript{105}

In a ‘world of rising suspicion’ where people are becoming more distrustful of one another, Onora O’Neill in Reith Lectures\textsuperscript{106} observes that stringent ways to control those who are suspected would be harmful.\textsuperscript{107} Instead, trust must be rebuilt as it is noticed that “appropriate development of trust enables not only basic relationships to flourish but also confidence, wisdom, and discretion.”\textsuperscript{108} Though spoken in the context of parents and children, the same may be applied to relationships between strangers. Thus, basic trust between neighbours is absolutely essential as it then creates a mutual understanding about the need to care about community safety. Be that as it may, the need to respect one’s right to privacy cannot be compromised. The balance between the two seemingly conflicting needs (i.e., need for community safety and individual privacy) should be maintained with implementation of a mechanism wherein one does not impede the other. For instance, an application could encourage people to implement initiatives on ground where they would check in on each other with respect via WhatsApp groups or innovative ideas. This must be translated and implemented effectively through the application in order to prevent the creation of an atmosphere of ‘constant threat’ when there isn’t any.

4.2 On the tech front: Implementation of privacy practices/principles

It is recommended as is for all ‘datafication programmes’ in India that the policy should be crafted to ensure institutionalization of robust transparency and accountability measures.\textsuperscript{109} This is particularly critical in the absence of any comprehensive data protection legislation.


Any application should ensure that it follows the basic principles of privacy protection in order to stand the scrutiny of law and sustain the confidence of the users.

Most applications encouraging lateral surveillance are based on the collection of data from neighbours about neighbours by a law enforcement agency or a private entity that stores the data. The data collected can range from basic demographic information to sensitive personal data such as location data. Though the purpose of collection is to ultimately provide better connectivity among the neighbours or more information about the neighbourhood events, it must be noted that, it is rare that data collected for one purpose will be used for just that.¹¹⁰ In relation to privately controlled applications, privacy policies can be changed to modify the uses of the collected information while the users may be given a take it or leave it option to continue using the services. Data is easily repurposable, information about one group can be used for controlling another group, which is referred to as “refractive surveillance”.¹¹¹ In the context of government or law enforcement controlled applications, the possibility of purpose creep, i.e., the use of when information for a purpose other than the original specified purpose,¹¹² cannot be ruled out. Further, certain research studies suggest that community policing applications, though effective in translating traditional functions of the police authorities into digital services, tend to overlook the importance of privacy and safety.¹¹³

In order to prevent instances of loss of privacy, stigmatization and rights violation, the law enforcement agencies or the data collecting entity must remain accountable. It is important for an application to properly implement privacy principles in its functioning. The harms of surveillance can be avoided by a clear prescription of the functioning of the applications and further, minimizing collection of unnecessary information from individuals in terms of such provisions in the privacy policy and terms of service. The minimization of data collection reduces the risk of excessive information being sought or being made available to the neighbours in the first place.¹¹⁴ The storage and security practices must be fool proof so as to prevent leakage of data. Further, limited access to collected data, secured data storage practices, and promotion of transparency, inclusiveness and openness are important privacy

principles to be considered for the privacy policy of existing applications. The functioning of the application should also place some restrictions on the use by the neighbours, so as to prevent the individuals from spreading incorrect information about any incident which might have adverse consequences. This is specifically important to tackle the spread of misinformation and preventing the ‘heightened fear of crime’ among citizens.

**Limitations & Scope for Future Research**

It is critical to understand that the lateral surveillance mechanisms by the state thrive on the ambiguity of citizens’ public and private responsibilities. However, this understanding has been developed recently and there exists no concrete study on the effects of such shifts in responsibility from the state to person in terms of law enforcement. Though scholars have written about the potential impacts of lateral surveillance and its technologies on societal bonds and community building, an immediate research is required to better understand the implications of such mechanisms on people on a larger scale with no geographical limitations.

Further, in the context of Indian authorities engaging in lateral surveillance, directly or indirectly, there is no specific study which focuses on these types of initiatives, online or offline, and their social and legal implications. The available research on neighbourhood watch and lateral surveillance is rooted in foreign jurisdiction, various COVID applications as analyzed before and is characterized by a shortage of in-depth ethnographic information. Research in the context and culture specific local initiatives, with and without the involvement of an application will help us gather a better understanding of the actual impact of such mechanisms and if their effects differ depending on different factors such as living conditions, income levels, caste and societal hierarchies, etc. in the society.

---

