Social Media Monitoring

Amber Sinha
The Centre for Internet and Society, India

Introduction

In 2014, the Modi Government launched the much lauded and popular citizen outreach website called MyGov.in.[1] A press release by the government announced that they had roped in global consulting firm PwC to assist in the data mining exercise to process and filter key points emerging from debates on Mygov.in. While this was a welcome move, the release also mentioned that the government intended to monitor social media sites in order to gauge popular opinion. Further, earlier this year, the government set up National Media Analytics Centre (NMAC) to monitor blogs, media channels, news outlets and social media platforms.[2] The tracking software used by NMAC will generate tags to classify post and comments on social media into negative, positive and neutral categories, paying special attention to "belligerent" comments, and also look at the past patterns of posts. A project called NETRA has already been reported in the media a few years back which would intercept and analyse internet traffic using pre-defined filters.[3] Alongside, we see other initiatives which intend to use social media data for predictive policing purposes such as CCTNS and Social Media Labs.

Thus, we see a trend of social media and communication monitoring and surveillance initiatives announced by the government which have the potential to create a chilling effect on free speech online and raises question about the privacy of individuals.[4] Various commentators have raised concerns about the legal validity of such programmes and whether they were in violation of the fundamental rights to privacy and free expression, and the existing surveillance laws in India.[5] The lack of legislation governing these programmes often translates into an absence of transparency and due procedure. Further, a lot of personal communication now exists in the public domain which renders traditional principles which govern interception and monitoring of personal communications futile. In the last few years, the blogosphere and social media websites in India have also changed and become platforms for more dissemination of political content, often also accompanied by significant vitriol, 'trolling' and abuse.[6] Thus, we see greater policing of public or semi-public spaces online. In this paper, we look at social media monitoring as a tool for surveillance, the current state of social media surveillance in India and evaluate how the existing regulatory framework in India may deal with such practices in future.

Status of Existing Programmes

NETRA

NETRA (Network Traffic Analysis) was developed by the Center for Artificial Intelligence & Robotics (CAIR) laboratory under the Defence Research and would be installed at the ISP (Internet service provider) level at more than 1000 locations across India Each location will be called as "Node", with 300GB of storage space."[7] The basic idea behind this project was to enable real-time detection of suspicious "keywords" and "keyphrases" in social media, emails, blogs, tweets, instant messaging services, and in other types of Internet content. There was also talk of capturing "dubious voice traffic" over Skype and other voice channels.[8] From limited reports available, it appears that NETRA will essentially be a surveillance system designed specifically to monitor the nation's internet networks including voice traffic.[9]

MyGov.in

MyGov.in is a scheme launched under the Digital India Mission in 2014. It is a citizen engagement platform to promote the active participation of Indian citizens in their country's governance and crowdsource governance ideas from citizens.[10] The platform includes services such as survey polls, activities, discussions, blogs, and communication with the Prime Minister. In a short span of time, the platform has seen "34,53,330 comments in 620 discussions".[11] It was later also reported that the government had engaged the services of the consulting and analytics firm, Pricewaterhouse Cooper in order to help them mine the data crowdsourced from MyGov.in and other sources. News reports quoted government officials as stating that under MyGov.in, the government intended to "process and filter key points emerging from debates on mygov.in, gauge popular mood about particular issues from social media sites like Twitter and Facebook."[12] While soliciting feedback is one of the primary functions of the platform, there is no mention anywhere of what actually happens to the feedback provided. What this means is that there is no accountability measure for ensuring that the feedback collected is translated in a consumable format for the government ministries and departments, nor are there are controls, regulatory or otherwise, which put any restrictions on illegitimate uses of the information.

NMAC

In February 2016, it was reported that National Security Council Secretariat (NSCS) had proposed the setting up of a National Media Analytics Centre (NMAC). This centre's mandate would be to monitor blogs, media channels, news outlets and social media platforms. The centre intends to rely upon a tracking software built by Ponnurangam Kumaraguru, an Assistant Professor at the Indraprastha Institute of Information Technology in Delhi. The NSCS, the parent body that this centre will fall under, is a part of the National Security Council, India's highest agency looking to integrate policy-making and intelligence analysis, and advising the Prime Minister's Office on strategic issues as well as domestic and international threats. [13]

From limited reports available, it appears that the tracking software used by NMAC will generate tags to classify posts and comments on social media into negative, positive and neutral categories, paying special attention to "belligerent" comments. The reports say that the software will also try to determine if the comments are factually correct or not and the past pattern of writers' posts would be analysed to see how often her posts fell under the negative category, and whether she was attempting to create trouble or disturbance, and appropriate feedback would be sent to security agencies based on it. [14]

Social Media Labs

In 2013, the Mumbai police inaugurated the country's first Social Media Lab "to monitor the happenings on Facebook, Twitter and YouTube." The project is supported by the National Association of Software and Services Companies (NASSCOM) and is funded by Reliance Foundation. [15] The social monitoring app was developed by SocialAppsHQ.com which "tracks and provides sentiment analysis, identifies behavioural patterns, influencers and advocates, track increase in chatter and generate alerts in real-time on social media platforms." [16] Similar projects are also underway in other cities in India such as Pune and Kolkata.

It was reported that in Mumbai a team of 20 police officers will staff the Social Media Lab "and will work around the clock to keep an eye on issues being publicly discussed and track matters relating to public order." and that "the intent of the Social Media Lab is to prevent demonstrations and protests." [17] The stated intent to track citizen mobilisation efforts are particularly disturbing in light of the existing broad powers granted to law enforcement agencies to conduct preventive arrests in order to preserve 'peace and tranquillity' and prevent 'public disturbance'. In absence of any laws which govern the functioning of these applications, there is no way to ensure that basic human rights such as free speech, privacy and the right to assemble and protest are not curtailed.

Predictive Policing

Predictive Policing is the application of Big Data analytical techniques to identify targets for prevention of crimes through police intervention or use of statistical predictions to solve crimes. [18] Predictive Policing techniques typically look at various sources of data and one of the key sources of late has been social media data. The Crime and Criminal Network Tracking System (CCTNS) is an e-governance project under the Digital India mission which seeks to use ICT for better provision of citizen-centric services, connect approximately 14000 police stations across the country and facilitate investigation, detection and prevention of crime. Various states have decided to use predictive policing techniques, [19] and plan on leveraging the existing structural data along with the social media data. The idea is to use the already existing structured data collected from established legacy electronic data bases on geographic locations and the nature of crimes in locations, and databases of history sheeters and police reports, along with other alternative data available. [20] While predictive crime analysis is a major objective of the Centre, so far most states have not reached this stage as data migration and data digitization is still in progress.

Thus, we see a host of schemes either dedicated to monitoring of social media content, or involved in some part in tracking content on social media platforms. While NETRA has the ambitious objective of tracking all the content on the web for suspicious activity, Social Media Labs is dedicated entirely to Social Media Platforms. Yet other schemes like MyGov.in do not have monitoring of online content as their mandate at all, however, we see significant mission creep with news reports suggesting use of analytical and data mining tools at their disposal to monitor content on social media. The table below provides an overview of extent of surveillance being carried out by each scheme.

No.	Name of scheme	Nature of information intended to be monitored	Purpose of monitoring
1	**NETRA (Network Traffic Analysis)**	All Internet traffic including social media, emails, blogs, tweets, instant messaging services, and voice over IP	To detect suspicious activity for national security purposes
2	**NMAC (National Media Analytics Centre)**	Social Media content, blogs, news and media channels	Sentiment analysis of posts for security purposes and big data analysis for detection of pattern of posting. Both domestic law enforcement and national security purpose
3	**Social Media Labs**	Social Media platforms	To detect suspicious activity, and track mobilisation using social media for protests, and support domestic law enforcement.
4	**CCTNS**	Crime data, geolocation data, call data records, social media data etc.	One of the stated goals of CCTNS is predictive policing using among other things, real time tracking of internet data including social media data, for domestic law enforcement.
5	**MyGov.in**	Crowdsourced data on the platform, social media content and blogs.	While the main purpose is to serve as a platform from citizen engagement, it has been reported that data mining and analysis techniques will be used to follow public discourse and discussion on social media platforms and blogs.

Social Media and Privacy

Nature of Social Media Content

Social Media refers to a set of web-based services that rely on user generated content. According to Henry Jenkins, the main features of social media is that it is spreadable media. "Consumers play an active role in 'spreading' content" [21] Daniel Trottier and David Lyon identify five key characteristics of social media that distinguish it from more traditional forms of communications. [22] The first features is collaborative identity construction where posts by different individuals come together to create a dynamic and evolving identity and user profiles are informed by both the users and their connections. Second, social connections like friendships, followers etc. "provide unique surveillance opportunities as users often engage with a particular audience in mind." [23] Whereas earlier institutional surveillance occurred in definitely and easily identifiable settings, the use of social media data enables surveillance across different social spheres that individuals interact with on it. Third, a personal social network makes social ties visible and consequently, searchable and quantifiable. Fourth, an evolving user interface and privacy settings alter both users' visibility through the site, as well as the ability of the user to reasonably control it. Fifth, social media data is easily re-contextualised. [24]

Speaking of the peculiar nature of social media communication, Anders Albrechtslund refers to it as participative surveillance where users willingly share personal details, beliefs and preferences in order to 'socialize'. [25] Accordingly to Lyon, when the Internet got commercialized, the marketer's and subsequently other institutions like law enforcement and governments realised the potential of surfing data for profiling customers. [26] Further, with geo-tagging a whole new dimension is added to the data available.

Privacy in the Context of Social Media

It is often stated that privacy is non-existent with the rise of datafied societies and pervasive self disclosure of human activities on social media. [27] It is important to note that this is based on a conception of privacy which places a primacy on individual's ability and need to control their own data. Tavani has distinguished between the control theory, the restricted access theory and the limited control theory of privacy. [28] In line with the Warren and Brandeis idea of privacy as the "right to be let alone", the restricted access theory sees the goals of privacy as restricting the access of third parties to personal information. On the other hand, the control theory sees privacy as control and self-determination over information about oneself. Alan Westin who defined privacy as "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" was the most influential proponent of the control theory. According to Tavani, the restricted access theory tries to combine the above two ideas. This theory distinguished between the "between the concept of privacy, which it defines in terms of restricted access, and the management of privacy, which is achieved via a system of limited controls for individuals." [29] While the Westinian idea of privacy which places the onus of privacy protection on the data subject has been dominant over the last few decades, some theorists propose a conception of privacy which takes into account the interests of those that need to be protected from corporate and institutional domination. [30]

Social Media Monitoring

How Social Media Monitoring Works?

Unlike traditional technologies which involved visual tracking of persons or manually screening footage, emerging surveillance technologies work algorithmically, sorting data through a series of set instructions. [31] A 2014 Lexis Nexis study revealed the most likely forms of social media surveillance as "discovering criminal activity and obtaining probable cause for a search warrant, collecting evidence for court hearings, pinpointing the location of criminals, managing volatile situations, witness identification, and broadcasting information or soliciting tips from the public." [32]

Methodologically, social media monitoring can be performed in the following two ways. The first involves feeding the algorithm with a string of keywords, which leads to "producing an overview of the instances of online communication and their locations (forums, Facebook pages, Twitter accounts, etc.) in which these keywords are used." [33] The second way entails directing the algorithm towards a specific set of discussion forums and social networking sites, and to search them for a number of keywords. As opposed to traditional forms of monitoring, social media monitoring is real time and continuously. [34] Social media monitoring techniques have their origins in the private sector. These practices were, to begin with, aimed at market research and customer profiling. With time, law enforcement agencies have recognised their utility.

Machine Access to Data

Peter Marguilles analogizes algorithmic scanning and collection to physical searches, and compares the former to a quick visit and the latter to a lengthy

stay. “Scanning intrudes on privacy in passing, while collection contemplates the storage of data by the collecting entity.” The process of scanning involves access to vast troves of data, most of which is discarded by the algorithm, and material selected is collected and analysed further.[35] A directed search will usually involve ‘selectors’ or ‘identifiers’ chosen by analysts which are then used to sort through large datasets using these keywords. In contrast, an autonomous search will involve feeding the program training data so that it may learn to distinguish between relevant and irrelevant data. The program is then tested on another dataset to see if it is capable of generalizing lessons from the training data to apply them to the new dataset.

An ACLU study had found that Twitter, Facebook, and Instagram provided user data access to Geofeedia, a developer of a social media monitoring product that assisted law enforcement agencies in monitoring activists and protesters.[36] Geofeed creates tool that use the location data of social media posts to tag them on the maps and clients are able to specify a delimited geographic area and view all geotagged posts coming from that location in near real-time. Subsequently, the companies had reportedly taken steps to limit access to Geofeed. However, this revelation is illuminating about existing practices surrounding social media data.

Licensing arrangements between social media companies and social media monitoring tools has been highlighted as enabling use of data for law enforcement purposes.[37] The terms of services of most social media websites specifically prohibit scraping of data using automated tools.[38] However, special licensing agreements with social media monitoring tools like Geofeed allows the legal access to “data feed called the Topic Feed API” in the case of Facebook which allowed them get a ranked feed of public posts searchable on the basis of specific topic, hashtags, events and location. Similarly, such arrangements with Twitter could provide access to the Twitter Firehose or other APIs. The Twitter Firehose, for instance is an arrangement between Twitter’s partners and developers which allows real time access to 100% of the feed based on a search criteria. Other more limited arrangements include Twitter Search API which is not real time but searchable by content, and Twitter Streaming API which provides real time access with some restrictions in content.[39] While Twitter’s development agreement specifically prohibits use of its data for the purposes of investigation, tracking or surveillance of Twitter users,[40] other social media companies do not have any such terms. Even in the absence of these arrangements, there is little by way of enforcement of the terms of services in order to prevent scraping and use of social media data for the purposes of surveillance.

Sentiment Analysis

Sentiment analysis refers to the class of computational and natural language processing study of people’s opinions, appraisals, and emotions toward events, institutions or other subject matter in order to extract subjective information, such as opinions, expressed in a given piece of text.[41] The main purpose of sentiment analysis is to classify attitudes towards various topics into positive, negative or neutral categories.[42] The limited information available to us about the Social Media Labs and National Media Analytics Centre suggests that these initiatives will use sentiment analysis techniques. Ths essentially means that social media content collected by these programmes may be analysed to determine attitudes towards identified subjects and filter instances which are deemed as likely to lead to offences.

Sentiment Analysis techniques can be classified under the following five categories:[43] a) Document level analysis—analysis of a document with respect to an object, either on the basis of a finite set of classes (positive, negative, neutral) and training data supplied to a program for each class using common classification algorithms such as SVM, Naïve Bayes, Logistic Regression, or KNN, or calibrating the sematic orientation of specific keywords in a document using a Pointwise Mutual Information (PMI) against specified words determined as being at the end of the classes (eg. ‘excellent’ for positive, ‘poor’ for negative); b) Sentence level analysis— which looks at the range of sentiments expressed in a sentence, by first classifying a sentence into an objective or subjective sentence, and then classifying the subjective sentences in the different classes pre-determined; c) Aspect based analysis— which is considered preferable in cases where multiple aspects of an object are spoken about, usually done by extracting all noun phrases, narrowing down to some phrases which appear more frequently than a determined threshold, and using PMI analysis for each noun phrases or phrase dependency parser that utilizes known sentiment expressions to find additional aspect;[44] d) Comparative analysis— which identifies sentences or phrases with comparative sentiments, and determine the preferred entity in each sentence or phrase.

However, various questions have been raised about the reliability and the classification methods used in sentiment analysis. For instance, the assumption that an objective sentence is does not express sentiment and a subjective sentence does has been shown to be faulty, in many circumstances.[45] It is difficult for sentiment analysis tools to take into account context, regional variation of the same words, sarcasm and comparative statements.[46] These failures have implications for private sector use of sentiments analysis for purpose such as marketing, which can be accounted by making an educated guess about the degree of inaccuracy. However, in case of social media surveillance, they have real implications for the people surveilled which could

translate into individuals being placed under surveillances, monitoring of their electronic communications and other adverse impacts such as being denied visas or being put on no-fly lists.[47] Thus, social media posts by individuals used to determine their attitudes and intentions towards matters of deemed sensitive or pertinent of law enforcement and national security could lead to them ending up on heat lists, or viewed as suspects by the law in other manners.

Social Network Analysis

Social network analysis is a technique used to map and measure social relations. They are used in investigative tools to discover, analyze, and visualize the social networks of criminal suspects. The basic unit of any social network analysis is three points of data—two actors and the tie or link between them. Actors include "people, organizations, computers, or any other entity that processes or exchanges information or resources." while relationships are typically "ties, connections, or edges" representing "types of exchange, such as drug transactions between a seller and buyer, phone calls between two terrorists, or contacts between victims and offenders."[48] The centrality of nodes, such as those representing offenders, identifies the prominence of persons to the overall functioning of the network. It indicates their importance to the criminal system, role, level of activity, control over the flow of information, and relationships. Social network analysis has been widely used in predictive policing tools to create heat lists based upon research that found that those with close social ties to victims and offenders are more likely to be involved in future crime.[49]

However, in India the structural inequities in the existing crime data poses a huge problem for such analyses. For instance, there is a huge problem in police data on 'history-sheeters' from certain communities historically viewed and discriminated against as criminally inclined. This means that lists of suspects maintained by the law enforcement agencies is heavily biased against certain communities.[50] Therefore, a social network analyses of using social media data combined with the existing crime data is likely to be biased against individuals from these communities.

How Ethical is Social Media Monitoring?

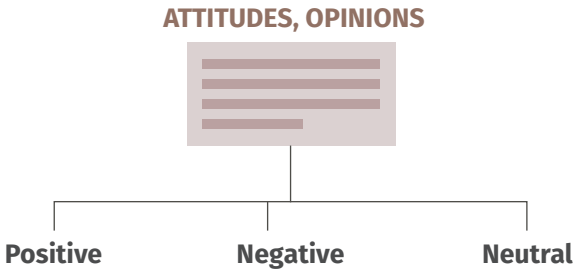
While the nature of content on social media is usually of a public or semi-public nature, it is important to understand how people usually use these platforms. Aside from use of social media for promotional purposes, the key forms of engagement with social media is for social engagement, venting and following content generators.[51] It is also important to recognise that unlike American law, there is no concept of denying the right to privacy when it comes to information 'knowingly exposed' by the individual in Indian jurisprudence on privacy. Therefore, as often argued, the blanket permission provided in the terms of use and privacy notices of social media platforms do not entirely compromise an individual's inherent right to privacy. Further, despite the acceptance of website terms and conditions as binding contract, it is important to note that blanket and binary terms which serve as condition to use online services[52] should not be considered as significantly limiting one's reasonable expectation of privacy.

It has been pointed that these activities were traditionally performed in private spheres or in a manner that the data created was of an ephemeral nature. Most social media users continue to have an implicit expectation of privacy despite being on public platforms due the following factors: (1) failure to understand data permanence, (2) failure to understand data reach, and (3) failure to understand the big data computational tools that can be used to analyze posts.[53] Therefore, often users do not understand the permanence of the content and metadata generated by them on social media. Many users feel that deletion of previous posts acts as erasure of past conduct. Further, users of platforms like Twitter feel that with passage of time, posts or tweets are beyond anyone's reach.[54] Finally, the advent of big data analysis which not only enables aggregation of data from multiple sources but also, analysis of the data to look for hitherto unseen patterns and inferences, making it unreasonable for an individual to have a clear idea of the extent of consent they provide to data about themselves.[55]

Social Media Monitoring Tools

SENTIMENT ANALYSIS

Sentiment analysis refers to the class of computational and natural language processing study of people's opinions, appraisals, and emotions toward events, institutions or other subject matter in order to extract subjective information, such as opinions, expressed in a given piece of text.

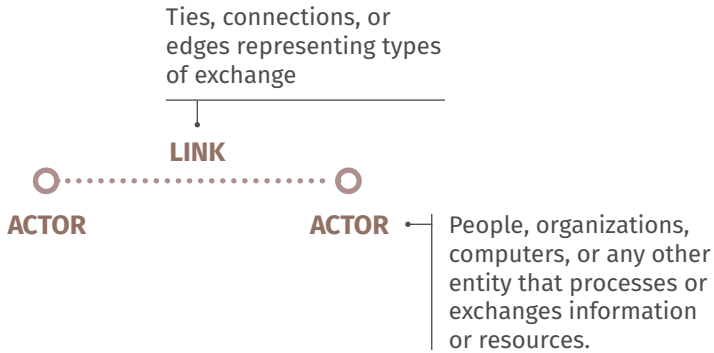


CATEGORIES

- **Document Level Analysis**
- **Sentence Level Analysis**
- **Aspect Based Analysis**
- **Comparative Analysis**

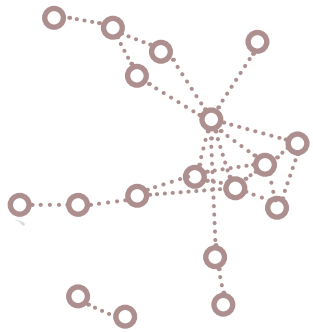
SOCIAL NETWORK ANALYSIS

Social network analysis is a technique used to map and measure social relations. They are used in investigative tools to discover, analyze, and visualize the social networks of criminal suspects.



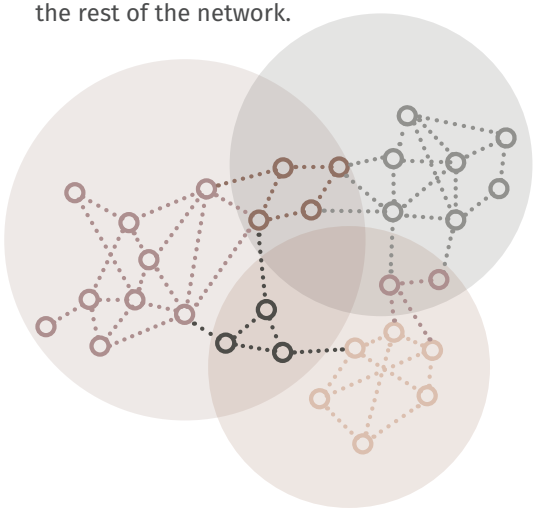
Centrality Analysis

Centrality analysis aims at determining more important actors of a social network so as to understand their prestige, importance, or influence in a network.



Community Detection Methods

Community detection methods identify groups of actors that are more densely connected among each other than with the rest of the network.



Legal Validity of Social Media Surveillance

Legal Basis for Data Collection

It is noteworthy that none of the surveillance projects mentioned in Section B have been born out of legislative actions. This is a feature of surveillance schemes launched by the central government in India in the last decade and all of them have been executive acts. The (Indian) Information Technology Act, 2000 is the legislation which governs all matters related to electronic data, and it includes numerous provisions on interception of electronic data and metadata. The most significant provision in this respect is Section 69, based largely on Section 5(2) of the Telegraph Act, 1951.[56] While the language in Section 69 is extremely broad and remains a lot to be desired in terms of clearly limiting the exigent circumstances in which it may be applied, as well as the scope of powers made available to the Central Government, it must be noted that it only provisions targeted surveillance which may only be authorised in case of a set of defined circumstances. Further, Section 69B deals with the interception and collection of Internet metadata.[57] This section, also, while extremely broad in its construction, only provisions targeted surveillance for the purposes of enhancing 'cybersecurity' and dealing with 'computer contaminants' and any collection of such metadata must conform to these conditions and procedure. In furtherance of these provision, the procedure to be followed for interception and monitoring of electronic data and metadata have been laid down under Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 and the Information Technology (Procedures and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009.

Additionally, there are other provisions under the Information Technology Act which deal with electronic surveillance under certain circumstances. These include a) Section 28 of the Act which allows authorised officials to access electronic data while investigating circumvention of the Act,[58] b) Section 29 of the Act which provides authorised officials the power to access computers and their data in case suspected contravention of Chapter VI of the Act,[59] c) Rule 6 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 which mandates a body corporate may disclose sensitive personal data or information about a subject without her consent to government agencies for the purposes of identity verification, prevention, investigations of offences etc.,[60] and d) Rule 3(7) of the Information Technology (Intermediaries Guidelines) Rules, 2011 requires intermediaries such as ISPs and platforms to provide all assistance and information to government agencies for the purposes of identity verification, prevention, investigations of offences etc. when mandated by a lawful order.[61]

While the above provisions suffer from vagueness, sweeping executive powers and lack of judicial oversight, it must be notes they are all provisions which enable only targeted surveillance, to be authorised under the defined set of circumstances and subject to either a time limit or executive oversight. However, none of the above mentioned clauses provide for perpetual and mass surveillance of data as envisaged by the schemes mentioned in Section B earlier. Therefore, the legal validity of these provisions remains an open question. It may be argued that most of these provisions only concern personal data whereas the social media monitoring schemes concern themselves with publicly available data from social media platforms. While the question whether social media data is personal communication or publicly available information remains an open question, (see D. (5) above) it is important to remember that the interception laws in India (Section 69 and 69A of the Information Technology Act) are not concerned with this question. The language used in these provisions is not in terms of personal data or reasonable expectation of privacy but states that the authorities must satisfy certain conditions in order to "intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource." Regardless of whether social media data collected is considered personal or public data, the conditions in the above provisions apply, thus, rendering the mass surveillance programmes on sketchy legal ground.

Intrusiveness of Algorithmic Surveillance

A common argument for greater use of algorithmic surveillance is that such methods are not as intrusive in nature.[62] According to this school of thought machine access on its own, without involving a human element is not intrusive on an individual's privacy. This argument stems from the idea that a certain level of consciousness that only human beings posses if required for intrusion.[63] However, what this argument ignores is that any examination of intrusion must stem not from the point of view of the actor surveilling but the actor being surveilled. Professor Julie Cohen has argued that algorithmic surveillance by private sector firms intrudes on our sense of control and self, and compromises the aspects of personhood.[64] Most of the literature of the chilling effects of surveillance draws from the idea of a disciplining 'panopticon' where direct violence has been replaced with softer forms of power in order to discipline, control, and normalize people.[65] This makes people more conscious of their actions leading to self-censorship, less experimentation and inevitably lesser personal growth. On the other hand, scholars arguing a non-panoptic

notions of Internet surveillance either use a neutral concept that assumes there are enabling as well as constraining effects.[66] However, these notions of internet surveillance tends to ignore power asymmetries and overlooks the fact that corporations and state institutions are the most powerful actors.[67] These factors will continue to operate regardless of the form of surveillance. Finally, it would be remiss to think of machines as non-judgmental[68] and the form of data processing that computers undertake is highly sophisticated rendering them more than capable of instilling a sense of loss of control on the data subjects.

Further, aside from the deontological objections to machine based monitoring, adverse determinations made by such tools about an individual can lead to tangible harms. The use of machine learning algorithms and big data multiply these harms by reducing the transparency and intelligibility of these decisions.[69]

Surveillance Discretion and Social Media Monitoring

Traditionally, the law enforcement agencies have always exercised some degree of discretion with regards to focussing their investigation on specific individuals or factors. No law enforcement agency can be expected to expend its resources on all possible leads and exercising judgements to filter out suspects from the general population has been integral to their job. Elizabeth Joh describes this judgment as 'surveillance discretion' i.e., focussing "police attention on a particular person or persons rather than others."[70] While the subject of enforcement discretion, the discretionary power to enforce laws against specific persons or not, has attracted some scholarship,[71] there is little literature available on the subject of surveillance discretion.

However, it is important to consider how the scope of surveillance discretion changes with use of new technologies such as predictive policing and social media monitoring tools. For instance, a big data approach to monitoring social media content is much broader in the scope of information it can survey, and promises to thrown previously unknown links and patterns.[72] Further social media data also offers much more information to conduct social network analysis in order to map social connections to events and relationships and their nature in criminal associations.[73]

First, the scale of data available might translate into a greater number of people being subjected to surveillance. Second, while big data tools like social media monitoring promise to introduce reduced bias and a more objective analysis of data, however, existence of structurally inequitous data can amplify existing biases further. Also, even for automated systems, decisions regarding which mathematical model to adopt, what data to use, and how to display that data remain discretionary. Finally, it also threatens to reconfigure traditional ideas of discretions based on personal judgments informed by contextual knowledge. This increased scope of policing requires greater transparency and accountability mechanisms.

Application of 'Knowledge'

A key question in use of technological tools such as social media monitoring which collect large quantities of data and subject them to algorithmic analysis, is the manner in which the knowledge gleaned from such tools is used. Under Indian criminal law, there is a good faith standard of reasonable suspicion which must accompany police actions such as arrests,[74] search and seizure.[75] If social media monitoring tools are being used for predictive analysis, any results derived from these tools are by their nature, probabilistic in nature and by themselves, do not meet the criteria of reasonable suspicion.

Therefore, the degree of automation that these tools provide becomes a significant question. Therefore for programmes such as Social Media Labs, National Media Analytics Centre and use of predictive policing in CCTNS, questions such as manner which data and insights are provided to law enforcement agencies, at what stage is the data provided, the capacity to critically evaluate the insights provided and account for common errors and biases as well as judicial scrutiny of the insights are integral to ensure proper accountability of such tools.

Conclusion

Applications of machine learning in law enforcement and anti-terrorism activities must take into consideration a crucial problem— the size of contextual data available. For instance, by its very nature, terrorism has little reliable data available on it.[76] Insufficient data will lead to "overfitting" the training data in its subsequent applications.[77] What this means is that such tools are likely to also emphasise on irrelevant attributes of known offenders and apply to its judgment of the unknown.

Most of all, uses of social media monitoring tools for surveillance raises the fundamental question about the degree and kind of constraint. While surveillance technologies are, to some extent, necessary to ensure care or protection, the legitimate forms of constraints and monitoring need to be clearly defined and observed. Rationales such as 'national security', 'prevention of crime', 'efficiency' and 'delivery of benefits and services' tend to have a strong persuasive value in justifying surveillance technologies. In some cases, the form of surveillance may be so implicit that the projects are not even recognised as employing surveillance technologies. For examples, the MyGov.in

initiative, which is primarily a citizen engagement platform, is reportedly being used to track and mine public opinions and popular discourse. Further, the advent of big data technologies and an entire identity based data ecosystem built around the Aadhaar number (being used as an identifier at MyGov.in) can feed into the unstructured social media data collected to mine and shape very granular and intimate profiles of citizens.

ENDNOTES

1. "Prime Minister launches MyGov: A citizen engagement towards Surajya." July 2015. Accessed December 30, 2016. http://www.narendramodi.in/prime-minister-launches-mygov-a-platform-for-citizen-engagement-towards-surajya-6402.
2. Ranjan, Amitav, "Now, govt cyber cell to counter 'negative' news." India Express. February 23, 2016. Accessed December 21, 2016. http://indianexpress.com/article/india/india-news-india/now-govt-cyber-cell-to-counter-negative-news/.
3. Xynou, Maria and Hickok, Elonnai, "Security, Surveillance and Data Sharing Schemes and Bodies in India." Centre for Internet and Society. Accessed December 22, 2016. http://cis-india.org/internet-governance/blog/security-surveillance-and-data-sharing.pdf.
4. 4 Bhatia, Gautam, "Free speech and surveillance." Centre for Internet and Society. July, 2014. Accessed December 22, 2016. http://cis-india.org/internet-governance/blog/free-speech-and-surveillance.
5. Prakash, Pranesh, "How Surveillance Works in India." The New York Times. July, 2013. Accessed December 29, 2016. http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=0.
6. Chaturvedi, Swati, I am a troll. (New Delhi: Juggernaut Books, 2016)
7. Supra Note 3.
8. "Government to launch 'Netra' for internet surveillance – The Times of India." http://theprivacyblog.com/surveillance/government-to-launch-netra-for-internet-surveillance-the-times-of-india/
9. Software Freedom Law Centre, "India's Surveillance State." Accessed December 14, 2016. http://sflc.in/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf.
10. "PM Narendra Modi launches portal, MyGov, for citizens to contribute in governance." The Economic Times. July 2014. Accessed December 17, 2016. http://economictimes.indiatimes.com/news/politics-and-nation/pm-narendra-modi-launches-portal-mygov-for-citizens-to-contribute-in-governance/articleshow/39040105.cms
11. Sabhikhi, Inayat Anaita, "How Participatory is My Government? A Closer Look at MyGov.in", The Hindu Centre. Accessed December 30, 2016. http://www.thehinducentre.com/the-arena/current-issues/article9411455.ece.
12. Dhoot, Vikas, "Pwc to help PMO mine MyGov.in data" Gadgets Now. November 26, 2014. Accessed December 20, 2016. http://www.gadgetsnow.com/tech-news/PwC-to-help-PMO-mine-Mygovin-data/articleshow/45283887.cms
13. Sinha, Amber, "Are we losing the right to privacy and freedom of speech on Indian internet?" Daily News and Analysis. March 2016. Accessed December 28, 2016. http://www.dnaindia.com/scitech/column-are-we-losing-the-right-to-privacy-and-freedom-of-speech-on-indian-internet-2187527.
14. Supra Note 2.
15. "Mumbai gets country's first 'Social Media Lab'." March 2013. Accessed December 25, 2016. http://www.thehindu.com/news/national/mumbai-gets-countrys-first-social-media-lab/article4516705.ece
16. "Mumbai Police tracks social media to gauge public sentiment." India Today. July, 2013. Accessed December 29, 2016. http://indiatoday.intoday.in/story/mumbai-police-social-media-sensitive-issues-protests/1/291283.html
17. Puri, Nitin, "India sets up social media monitoring lab." ZedNet. March, 2013. Accessed December 24, 2016. http://www.zdnet.com/article/india-sets-up-social-media-monitoring-lab/
18. Brayne, Sarah, Rosenblat. Alex and boyd, dana, "Predictive Policing, data and civil rights: A new era of policing and justice." Data and Civil Rights. Accessed December 20, 2016. http://www.datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf.
19. "About Crime and Criminal Tracking Network & Systems - CCTNS." National Crime Records Bureau. Accessed December 19, 2016. http://ncrb.gov.in/cctns.htm.
20. Routray, Bibhu Prasad, "Making a case for futuristic predictive policing in India." New Indian Express. Accessed December 20, 2016. http://www.newindianexpress.com/magazine/voices/article601920.ece?service=print.
21. Jenkins, Henry, Convergence culture. (New York: New York University Press, 2008)

22. Trottier, Daniel and Lyon, Daniel "Key features of social media surveillance" in Fuchs, Christian Boersma, Kees, Albrechtslund, Anders and Sandoval, Marisol ed., Internet and Surveillance The Challenges of Web 2.0 and Social Media (London: Routledge, 2012)

23. *Ibid* at 89.

24. *Id.*

25. Albrechtslund, Anders. "Online social networking as participatory surveillance." First Monday 13 (3) (2008) http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949

26. David Lyon, "Surveillance in cyberspace: the Internet, personal data and social control." Queen's Quarterly 109 (3) (2002): 135–149.

27. Sherry D. Sanders, "Privacy is Dead: The Birth of Social Media Background Checks." 39 S.U. L. REV. 243 (2012). https://ssrn.com/abstract=2020790.

28. "Tavani, Herman T., "Informational privacy: Concepts, theories, and controversies." in Himma, Kenneth Einar and Tavani, Herman T. ed. The handbook of information and computer ethics, 131–164. (Hoboken, NJ: Wiley, 2008)

29. *Id.*

30. Fuchs, Christian, Social media: A critical introduction (Sage Publication, New Delhi, 2014) at 471.

31. Hill, David W. "Jean-François Lyotard and the Inhumanity of Internet Surveillance" in Fuchs, Christian, Boersma, Kess, Albrechtslund, Anders and Sandoval, Marisol ed., Internet and Surveillance The Challenges of Web 2.0 and Social Media (London: Routledge, 2012).

32. "Social Media Use in Law Enforcement: Crime prevention and investigative activities continue to drive usage." LexisNexis, November 2014. Accessed December 26, 2016. http://www.lexisnexis.com/risk/downloads/whitepaper/2014-social-media-usein-law-enforcement.pdf.

33. Bekkers, Victor, Edwards, Arthur, de Kool, Dennis, "Social media monitoring: Responsive governance in the shadow of surveillance?" Accessed December 30, 2016. http://docplayer.net/9051597-Social-media-monitoring-responsive-governance-in-the-shadow-of-surveillance.html.

34. *Id.*

35. Marguiles, Peter, "Surveillance by Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights." Legal Studies Research paper Series. 68 Fla. L. Rev. (forthcoming). http://ssrn.com/abstract=2657619.

36. Cagle, Matt, "Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color." American Civil Liberties Union of North California. October, 2016. Accessed January 11, 2017. https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

37. *Id*.

38. Section 4 of Twitter's terms of service states that "You may not do any of the following while accessing or using the Services:..(iii) access or search or attempt to access or search the Services by any means (automated or otherwise) other than through our currently available, published interfaces that are provided by Twitter (and only pursuant to the applicable terms and conditions), unless you have been specifically allowed to do so in a separate agreement with Twitter (NOTE: crawling the Services is permissible if done in accordance with the provisions of the robots.txt file, however, scraping the Services without the prior consent of Twitter is expressly prohibited)". Similary Section 3 of Facebook's terms states: "We need your help to keep Facebook safe, which includes the following commitments by you:..You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission."

39. "Twitter Firehose vs. Twitter API: What's the difference and why should you care?". The Bright Planet. Accessed January 11, 2017. https://brightplanet.com/2013/06/twitter-firehose-vs-twitter-api-whats-the-difference-and-why-should-you-care/.

40. The Developer Agreement states as follows: "You will not knowingly: 1) display, distribute, or otherwise make available Content to any entity to investigate, track or surveil Twitter's users or their Content, or to obtain information on Twitter users or their Content, in a manner that would require a subpoena, court order, or other valid legal process or that would otherwise have the potential to be inconsistent with our users' reasonable expectations of privacy." https://dev.twitter.com/overview/terms/agreement-and-policy.

41. Feldman, Ronan, "Techniques and applications for sentiment analysis." doi:10.1145/2436256.2436274.

42. http://www.public.asu.edu/~gbeigi/files/BeigiSentimentChapter.pdf

43. Supra Note 38.

44. Zhang, Wu, Huang, Q and Wu, L., "Phrase dependency parsing for opinion mining." in Proceedings of Conference on Empirical Methods in Natural Language Processing (2009).

45. Some statement may be simple statements of fact, yet contain implicit emotion. On the other hand, statements containing opinions which are value neutral in nature have little sentiment to contribute to the analysis.

46. "Sentiment analysis: Why it's never 100% accurate" http://brnrd.me/sentiment-analysis-never-accurate/

47. "No-fly list uses 'predictive assessments' instead of hard evidence, US admits", The Guardian. August, 2015. Accessed December 17, 2016. https://www.theguardian.com/us-news/2015/aug/10/us-no-fly-list-predictive-assessments.

48. Johnson, Jennifer, Reitzal, John David, Norwood, Bryan F., McCoy, David M., Cummings, Brian and Tate, Renee R., "Social Network Analysis: A Systematic Approach for Investigating." FBI Law Enforcement Bulletin. March, 2013. Accessed December 29, 2016. https://leb.fbi.gov/2013/march/social-network-analysis-a-systematic-approach-for-investigating.

49. Gunnell, Daniel, Hillier, Joseph and Blakeborough, Laura, "Social Network Analysis of an Urban Street Gang Using Police Intelligence Data." Government UK Home Office. January, 2016. Accessed December 31, 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/491578/horr89.pdf.

50. Satish, Mrinal. "Bad Characters, History Sheeters, Budding Goondas and Rowdies': Police Surveillance Files and Intelligence Databases in India". National Law School of India Review, Vol. 23, No. 1, p. 133, 2011. November 6, 2010. Accessed December 28, 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1703762.

51. Mikal, Jude, Hurst, Samantha and Conway, Mike, "Ethical issues in using Twitter for population-level depression monitoring: a qualitative study." NCBI. April 14, 2016. Accessed December 29, 2016. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4832544/

52. Sinha, Amber, and Mason, Scott, "A critique of consent in informational privacy." Centre for Internet and Society. January 11, 2016. Accessed December 28, 2016. http://cis-india.org/internet-governance/blog/a-critique-of-consent-in-information-privacy.

53. *Id*.

54. *Id*.

55. Solove, Daniel, "Privacy self-management and consent dilemma." Harvard Law Review, 2013. Accessed December 28, 2016. http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2093&context=faculty_publications

56. Section 69 reads as follows: Power to issue directions for interception or monitoring or decryption of any information through any computer resource. - (1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.
(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.
(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to- (a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or (b) intercept, monitor, or decrypt the information, as the case may be; or (c) provide information stored in computer resource.
(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

57. Section 69B states as follows: Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security.-
(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.
(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.
(4) Any intermediary who intentionally or knowingly contravenes the provisions of subsection (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.
Explanation: For the purposes of this section,
(i) "Computer Contaminant" shall have the meaning assigned to it in section 43
(ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

58. Section 28 - Power to investigate contraventions. -
(1) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.
(2) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 (43 of 1961), and shall exercise such powers, subject to such limitations laid down under that Act.

59. Section 29 - Access to computers and data. -
(1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that 31 [any contravention of the provisions of this Chapter] has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.
(2) For the purposes of sub-section (1), the Controller or any person authorised by him may, by order, direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

60. Rules 6 states, *inter alia* — Provided that the information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government agency shall send a request in writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person.

61. Rule 3(7) states as follows: When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance.

62. Simon, William H., Rethinking Privacy, http://bostonreview.net/books-ideas/william-simon-rethinking-privacy-surveillance.

63. Posner, Richard A., "Privacy, Surveillance, and Law." 75 U. CHI. L. REV. 245, 254 (2008) (arguing that machine searches do not intrude on privacy because computers are not "sentient beings").

64. Cohen, Julie, "What Privacy Is For." 126 HARV. L. REV. 1904, 1909– 10 (2013).

65. Foucault, Michel, Discipline and punish: The birth of the prison. (Vintage, New York, 1995)

66. Albrechtslund, Anders. 2008. "Online social networking as participatory surveillance." First Monday. Accessed December 21, 2016. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949

67. Allmer, Thomas "Critical Internet Surveillance Studies and Economic Surveillance" In Fuchs, Christian, Boersma, Kess, Albrechtslund, Anders and Sandoval, Marisol ed., Internet and Surveillance The Challenges of Web 2.0 and Social Media (Routledge, London, 2012).

68. Supra Note 35.

69. Crawford, Kate and Schultz, Jason, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms (October 1, 2013). Boston College Law Review, Vol. 55, No. 93, 2014.

70. Joh, Elizabeth E., "The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing." UC Davis Legal Studies Research Paper Series. Research Paper No. 473. December 2015.

71. Miller, Marc and Wright, Ronald, "The Black Box." 94 IOWA L. REV. 125 (2008).

72. Sean Gallagher, Sena, "Staking out Twitter and Facebook, new service lets police poke preps." Ars Technica, Nov. 13, 2013. Accessed December 25, 2016. http://arstechnica.com/information-technology/2013/11/staking-out-twitter-and-facebook-new-service-lets-police-poke-perps/

73. Supra Note 43.

74. Section 41 (1) (a) of the Code of Criminal Procedure, 1973 states: When police may arrest without warrant. (1) Any police officer may without an order from a Magistrate and without a warrant, arrest any person (a) who has been concerned in any cognizable offence, or against whom a **reasonable complaint has been made, or credible information has been received, or a reasonable suspicion exists**, of his having been so concerned"

75. Section 165 of the Code of Criminal Procedure, 1973 states: "Whenever an officer in charge of a police station or a police officer making an investigation **has reasonable grounds** for believing that anything necessary for the purposes of an investigation into any offence which he is authorised to investigate may be found in any place with the limits of the police station of which he is in charge, or to which he is attached, and that such thing cannot in his opinion be otherwise obtained without undue delay, such officer may, after recording in writing the grounds of his belief and specifying in such writing, so far as possible, the thing for which search is to be made, search, or cause search to be made, for such thing in any place within the limits of such station."

76. Supra Note 35.

77. *Id*.