LUMS | Centre for Business and Society

SHOULD INTELLIGENCE AGENCIES BE GIVEN ACCESS TO SOCIAL MEDIA AND TECHNOLOGY FOR SURVEILLANCE PURPOSES?: *Policy Analysis*

Abstract

The advent of globalization and increasing interconnectedness of the world has opened new avenues for security agencies as well as miscreant groups. Moreover, information creation, dissemination, and storage has skyrocketed with the exponential rise of the internet, broadcast media, and social media. The plethora of personal information that is present on the internet is a highly valuable resource for security and security agencies internet, broadcast media, and social media intelligence agencies that thrive on Big Data as part of their struggles for viable intel and potential threats. Despite promises of strong privacy mechanisms, consumers are becoming insecure about their private data which is highly susceptible to infringements by security and/or intelligence organizations. Pakistan, like most states, has become increasingly active in public surveillance which is argued to be another manifestation of the total autonomy and utter lack of accountability of the state security apparatus. Therefore, this report aims to critically review the various factors at play behind the increasing role of security agencies in mass surveillance especially through online monitoring using the lens of the security organizations as well as the common man. Subsequently, this policy brief evaluated a set of effective policy alternatives using the Policy Delphi rankings and certain assessment criteria such as political feasibility, social feasibility, economic feasibility and implementation in order to propose the best practices and solutions to tackle the issue of unrestrained access to personal information and activities due to mass surveillance activities carried out by security and/or intelligence agencies in Pakistan.

Key findings

The findings highlighted that Pakistan still lacks a foundational privacy commission. Very few and vague legal provisions were found for the protection of personal data from privacy breaches. Antithetical to Pakistan's democratic system, there was seen a lack of transparency and accountability in the whole process of security agencies engaging in mass surveillance that ultimately results in the abuse of power and exploitation of people. The government entrusted the intelligence and security agencies with more and more autonomy to identify security threats. This involved mass surveillance which encompassed phone taps, social media monitoring and account hacking. Since the government prioritized security over privacy, these agencies developed more effective mechanisms for abducting individuals, and they could even pose a threat to national security without any evidence at all. Further analysis identified structural legal causes behind this huge biasness of the Pakistan's legal system towards the state security apparatus, including several legal issues that allow this issue to exist and persist and the Constitution of Pakistan that allows individual privacy to be breached in the case of "proper discharge" of the Army and intelligence organizations. Moreover, force field analysis presented that the main tension is between privacy and security that has afflicted Pakistani policy making. Although the Pakistani state would be prioritizing national security by sticking to its policies of mass surveillance, however, by holding onto such laws the state would only ensure further privacy infringements and allow for continual repression by the security apparatus. Furthermore, it was found very difficult in terms of resources and potential feasibility to stand up against the military establishment that has a huge vested interest in public surveillance. In addition to that, major policy actors including government, state institutions (i.e. security agencies, armed forces and intelligence bodies), civil society, academia and NGOs were also found influencing the policy process as being directly or indirectly involved with mass surveillance in Pakistan. However, the analysis provided that if no proper legal reforms would be taken to increase transparency, accountability, and limit institutional power then the state-security apparatus would continue to infringe on citizen privacy under the pretext of security when the real motivation would be to remove any sort of opposition to their hegemony. Therefore, the study proposed significant policy alternatives in the broader context such as the government should introduce new legislation which ensures that online surveillance is transparent, agencies must go through certain conditions before they can monitor a person's activities online and offline (targeted as opposed to conducted broadly), addition of a clause for illegally obtained information, being non-admissible when registering for a social platform or setting up gadgets, a mass awareness campaign must be enacted whereby the public is informed of their fundamental right to privacy and its associated ramifications, and no action policy. According to the Delphi results, the alternative that mass surveillance should be transparent was found to be the most suitable option for being easily implementable and politically feasible, but in the social and economic contexts it could not score well. Subsequently, the second ranked alternative, that agencies must go through certain conditions before they can monitor a person's activities online and offline, was found to be the most practical option for being politically feasible and effective. Whereas, alternative three and four scored equally since the results ranked them both at third position with minor differentiation and alternative five scored the least since taking no action was found to be an inviable option. However, according to the alternative ranking results, conducting a mass awareness campaign was found to be the simplest alternative since it would be easier to implement and the government body would also support it. Subsequently, the addition of a clause would be more viable to implement before an outrage raised by agencies. This would give the governmental body more time to ease the agencies into further procedural steps. However, the alternative of having a transparent surveillance was ranked least due to the various complications in its implementation process.

Implications

The study suggests that, in Pakistan, the government should conduct mass awareness campaigns to make people aware of their rights to privacy and its ramifications. Similarly, the public needs to be educated enough to understand the system, their privacy rights and how their information can be used online. In this regard, the government can conduct workshops or use television advertisements and posters all over the country to spread basic awareness about mass surveillance and privacy rights. Moreover, the Pakistani government needs to make sure all agencies have registered their activities or have given rights to oversee their work. In this way, the government can check and confirm whether their activities are legal. However, in the long term, making a policy where every agency must go through a proper governmental check to get the permission for conducting mass surveillance would be a fruitful action plan. Furthermore, there should be an addition of a clause for illegally obtained information being non-admissible when registering for a social platform or setting up gadgets in the current policy act. Similarly, the government should reinforce that any information through illegal surveillance must be discarded. Government should also work towards making the system transparent to ensure equal knowledge transmission to all stakeholders (more specifically the public). In addition to that, it can be vital for the government to have project heads for each element of the action plan since there will be a direct team in contact during the implementation process. This would also help to ensure whether the goals are achieved effectively. Moreover, there should be unbiased and neutral people in charge of these projects who can efficiently work for the interest of all stakeholders especially for protecting the rights of the general public. However, these notions would take a while to yield productive results since the procedure would require many legalities to be overcome and the policy to be passed. This would also involve teams working for a few years to produce enough substantial footwork for taking approval from the court especially due to the political implication and the expected backlash from the agencies that are involved.

Keywords

Security Agencies
Internet
Social Media
Intelligence Agencies
Privacy Rights
Public Surveillance
Personal Data
Citizen

SDGs

16 PEACE, JUSTICE AND STRONG INSTITUTIONS

*The full paper has been made available following consent from all concerned parties that hold ownership of this intellectual output.

Citation

Qureshi A.I., Nisar M.A. (2018) Should intelligence agencies be given access to social media and technology for surveillance purposes?: policy analysis. *Term Project, Suleman Dawood School of Business*