ExpertView

Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)

05/17

BALANCING RIGHT OF PRIVACY AND NATIONAL SECURITY IN THE DIGITAL AGE

Gp Capt Ashish Gupta
Senior Fellow, CAPS
24 September 2017

The unbridled enthusiasm for Information and Communications Technology (ICT) and its proliferation, coupled with ubiquity of internet access and mobile connectivity have dramatically impacted the everyday lives of almost all the people across the globe. The information is being collected, collated, analysed and disseminated almost in real time. It has emerged as a strategic resource contributing to competitive dominance, capability aggrandisement and for evaluation of potential threats. Information can be garnered through persuasion, inducement, enticement, coercion or can be compromised due to technological inadequacies and human frailties. The types of personal and social interactions that are played out through the milieu of social media and their uninhibited sharing, either wittingly or unwittingly, lead to many privacy breaches and violations. The all-pervasive digital technologies and the changing nature of human interaction using online tools have affected radical changes in notions, perceptions and expectations of privacy.

Privacy is a legitimate expectation, an inalienable right and an indispensable precondition for an inclusive society that ensures human dignity to each and every person. A person's fundamental need for privacy is a psychological as well as sociological manifestation of the sense of being human with dignity.[1] Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.[2] The explicit conception of privacy is not easy and has intrigued and vexed generations of philosophers, anthropologists, legal theorists and experts in jurisprudence.

In a historic judgment, August 24, 2017, a nine-judge Supreme Court bench unanimously ruled that privacy is a fundamental right, protected as an intrinsic part of the right to life and personal

liberty and as part of the freedoms guaranteed by the Constitution.[3] The judgement also delineated the limits to the state's intervention in the lives of citizens.[4] However, the bench took due cognisance of the challenges being thrown up by technology and recognised the need of having a balance between the right to privacy and imposition of certain restrictive measures within the legal framework by the state for aims such as national security, prevention and investigation of crimes and distribution of welfare resources etc.[5]

With ICT touching upon various facets of our daily lives, the objective understanding of its implications on 'privacy' is limited. Some of such factors include the volume, magnitude, complexity, and persistence of information; the expanding number of ways to collect information; the number of people affected by information; and the geographic spread and reach of information technology. These technologies have emerged as a new medium for mediation of most of the private and public communication, social interactions and business transactions. These technologies form the linchpins of contemporaneous infrastructures and institutions such as banking, healthcare, defence, education, industry and entertainment, etc.

The burgeoning information technology revolution has created a paradigm challenge to privacy as it facilitates and fosters uninterrupted surveillance, restricts erasure of footprints in cyberspace and gives instant visibility of information across the globe. The concerns about the possible misuse of data garnered and stored in large stand-alone computers by the government and other institutions since the mid to end of twentieth century, have given way to outright trepidation about privacy invasion and mass surveillance from the range of present-day systems, including the Internet; the World Wide Web; smart mobile phones; biometric surveillance; global positioning system (GPS); social networks; big data; cloud computing; mobile computing; Database Analytics; data mining; and more. Besides, the ubiquitous social media has deeply influenced the way we decide to reveal or conceal personal information. Although many individuals are still sticklers for a certain measure of privacy in their lives, the social media has fanned the narcissistic, exhibitionistic and voyeuristic desires of a large section of society which comes at the high price of loss of privacy.

The vociferous and ongoing debate between privacy and security and its consequences has led to an increasing tension between the principle of 'security' and that of 'privacy'. The threats of internal extremism, global terrorism, radical insurgency, threats from rogue nations and asymmetric threats from non-state actor shave all resulted in deepening and intensification of security discourses across the full spectrum of political, economic, social, constitutional and legal landscape. A pressing question recurrently posed, not only by the citizenry but by experts as well, is whether it is possible to strike a

balance between security and privacy. In the midst of security imperatives, will it be even plausible to not tread upon fundamental rights and civil liberties. In the present security environment - underpinned by the rationality of a "war on terror" and buttressed by all the possible means, methods and materials – the privacy concerns seem trivial compared to overarching security necessities. Security concerns are readily discernible since national security, human security and economic security stakes are far too high than somewhat abstract and vague conception of privacy rights.

The contemporary compulsions and security imperatives fueled by the growing public and political fear over the rising scourge of terrorism have, to some extent, impinged upon the 'Right to Privacy'. Since increasing number of political, economic and social functions are facilitated, supported and mediated through cyberspace; it has given ample opportunities to law enforcement agencies to garner unprecedented levels of information and unparalleled means to engage in surveillance. In the digital realm, it's nearly impossible to live without generating streams of data about what we read, watch, buy and who we support, idolize, sympathize, and empathize – and all this data can be accessed remotely. National security concerns may trump privacy as perceived stakes are much higher in terms of loss of life or limb. Given a choice between being secured and being privacy conscious, many will happily trade privacy for a certain level of security. However, protecting right to privacy of individuals need not be fatally impinging on efficacy and legitimacy of security measures; it merely demands accountability, oversight and effective regulatory mechanisms.

More ironically, information revolution has contemporaneously coincided with the evolution of terrorism in its current form, putting digital surveillance to a higher level of importance than other activities of law enforcement agencies. With growing threat of terrorism and mounting national security concerns, the law enforcement agencies have also expanded their arsenal of techniques to snoop through the digital packets transiting through the networks and gather records and data, carry out audio and visual surveillance and track movements. Despite constitutional provision and statutory enactments for protection of privacy, the first casualty of the war on terrorism is perhaps personal privacy. George Orwell's depiction of a totalitarian society in 'Nineteen Eighty-Four' in which the citizenry is subjected to a high degree of control and intrusive surveillance might not only be a metaphoric construct but closer to present day realities. As the 'Orwellian metaphor' has underscored, the public and the social realm cannot exist without protecting privacy and freedom.[6] The digital surveillance has become far more pervasive and intrusive and is perceived as natural a manifestation of problems of modern times, somewhat relegating the issue of privacy to incongruity.

The resolution of the debate on privacy vs national security rests on the extent to which national security concerns outweigh the rights of citizens to privacy of their associations and communications,[7]and on the extent to which democratic concepts such as privacy and freedom can be accommodated within a larger security conception and framework. There is no denying the fact that the global scourge of terrorism can only be exterminated through the collaborative and integrated efforts-of global political leadership, military, law-enforcement, intelligence and security agencies, financial institutions and public and private companies even if it requires transcending parochial partisan interests and objectively balancing the degree of risk that might be warranted by potential benefit.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

Keywords: Digital Privacy, Internet, Information and Communication Technology

Notes

[1] The Social Science Research Network, "Right of Privacy. Constitutional Issues and Judicial Responses in USA and India Particularly in Cyber Age", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1440665, accessed on August 28, 2017.

[2] Daniel J. Solove, "Conceptualizing Privacy", *California Law Review,* July 2002, Vol. 90, Issue 4, Article 2, p. 1088.

[3] Amit AnandChoudhary&DhananjayMahapatra, "Supreme Court gives India a private life", *The Times of India*, August 25, 2017.

[4] Ibid.

[5]Ibid.

[6] DionysiosPolitis, *Socioeconomic and Legal Implications of Electronic Intrusion* (London: IGI Global, 2009) p. 131.

[7] Richard H. Rovere and Gene Brown, *Loyalty and Security in a Democratic State*, (New York: Ayer Company Publishers, 1977), p. 354.