**Digital Surveillance: A Security Blanket for the Cyber Age or a Threat to Privacy?**

**Arpita Saggar**

**MCA 2nd Year**

As artificial intelligence becomes increasingly ubiquitous, and human dependence on automation proliferates, a niggling worry plagues the current generation - Where does one draw the bounds of internet privacy? Indeed, does a clear frontier actually even exist, or is it just blurred lines?

The exchange of data and services forms the cornerstone of many new and exciting technologies. However, at the same time, the ability of governments and companies to keep people’s activities under surveillance has never been greater. A growing number of states are employing advanced AI surveillance tools to scrutinize, and possibly even censor citizens, in order to accomplish a range of policy objectives. While some may be lawful, others descend into a cesspit of human rights violations, and most fall into a murky middle ground. The ever-increasing efficiency of algorithms, combined the lust for power around the world, suggests that the collection of vast quantities of data may lead to catastrophe.

There is growing concern around the world that digital profiling is shaping business models. Digital rights groups such as Reporters Without Borders and the Electronic Frontier Foundation, have expressed trepidation regarding mass surveillance, warning that such measures restrict political and personal liberties. Such fear has resulted in legal challenges, such as the Hepting v. AT&T case in USA, which examined the role that telecom provider AT&T played in assisting the National Security Agency’s unlawful monitoring of communications, or the Levenson Inquiry in the UK, which investigated the practices and ethics of the British press, following the News International phone hacking scandal. On the illicit front, hacktivist group Anonymous has often hacked into government websites to convey their dissent.

Yet, even as the argument in favour of preserving digital privacy looms large, so does the one in favour of monitoring, albeit limited. Network surveillance is essential to monitoring Internet traffic, which helps keep transactions secure. Corporate surveillance ensures adherence to company policies and prevents misuse of resources and potential lawsuits, while state surveillance can enhance maintenance of societal harmony, as well as disruption of criminal activities. Because a society in which each individual conforms to every law, while also circumventing every social anathema will always cease to exist, establishments must employ some method to guarantee a degree of social and cultural conformity. And that process will inevitably violate some definition of privacy. Undeniably, for most, the persisting issue is defining the confines of scrutiny, rather than curtailing it entirely.

How this modern social contract will be established in this era of accelerating reliance on technology, is a matter which elicits endless, yet never banal, discourse, and will be vital in shaping societies of the future.