THE INDIA FORUM
A JOURNAL-MAGAZINE ON CONTEMPORARY ISSUES

March 3, 2020

Consent and Privacy in the Age of Digital Technology

By: Radhika Krishnan

When Big Data reigns and the economy relies on mass surveillance and data collection, will humans end up as Pavlov's dogs? Taking back control of our data will require rebuilding digital technologies to make them compatible with greater democratic control.

The 18th century English philosopher and social theorist Jeremy Bentham visualized the panopticon as an institutional structure which would allow the all-round surveillance of individuals. Since then, the need for panoptical surveillance of prisoners, workers, and even children has been enshrined not just in governance but equally in our discourses.

The French philosopher Michel Foucault reminds us that the constant collection of information provides the basis for a regime of control and discipline. The question for us is: what is the nature of the modern panopticon, propelled by digital technologies? We are all perhaps familiar with the fictionalised account of a pizza delivery service interacting with a potential customer. Through the course of the conversation, the server reveals an awareness of the customer's medical condition, financial status, legal misdemeanors, and more. This situation, which was at one time seen as a joke or a frivolous exaggeration, is now strikingly close to our lived experiences.

> [Snowden] reminds us that everyone in the world now has a permanent record, maintained and updated by the US security establishment.

Our personal data is today the very fulcrum of a significant proportion of private business ventures. Digital technologies actively and silently record and process every instance of our lives. Detailed profiles are prepared, and this information is transformed into usable services which are now an integral part of our lives. While private businesses use our data, often without our explicit consent, governments are empowered to collect and use vast amounts of personal data. Sweeping powers make for a regime of anticipatory surveillance, where data can be collected and processed without having to cite a specific investigation. This point has been eloquently reiterated most recently in Edward Snowden's autobiography, *Permanent Record*. Snowden speaks of how technological tools and regulatory mechanisms have colluded to create an extensive system of mass surveillance. In particular, he highlights how traditional human-manned intelligence mechanisms have been made outdated by forms of cyber-intelligence. He reminds us that everyone in the world now has a permanent record, maintained and updated by the US security establishment.

These concerns have been reflected in India. Since its inception in 2009, the Aadhar project has given an additional momentum to existing concerns of governmental overreach and the loss of privacy. Several other initiatives are equally worrying. India has proposed a centralised telecom interception system to automate eavesdropping on conversations. The Modi government also plans mass surveillance of private conversations and posts on social media. Facial recognition systems are being introduced, not just for policing, but in an increasing range of public services. There is no structural mechanism or a framework for data protection and privacy in India to address this growing regime of surveillance. Given this backdrop, it is not surprising that we in India have been grappling with issues of large-scale surveillance and data collection over the past decade.

> As data moves seamlessly across application platforms, servers, and processors, the owner/generator of data often loses control and possession.

We are now talking about how to ensure civil liberties and limit the unauthorised usage of personal data in an increasingly data-driven world where both public and private actors constantly access personal information. This is easier said than done, because we are living in what cyber-intelligence analyst Pukhraj Singh terms "data dystopia", where the ownership, possession and control of data do not necessarily overlap. As data moves seamlessly across application platforms, servers, and processors, the owner/generator of data often loses control and possession. Data processors, in turn, might control data while maintaining an amorphous and tenuous possession over data. In this situation, we are urged to look for specific rights that might grant us some level of control over our data. The "right to explanation" (which translates to the right to a reasonable explanation for decisions/acts that are committed on the basis of data collected from an individual), the "right to erasure" (the right to demand that specific data generated by an individual be

forgotten/erased from the records after the purpose for which it is collected is served), and the "right to correction" of incorrect data have emerged in this context.

Consent and privacy have been the pivots around which any discussion of surveillance and data privacy takes place. It is in this context that Shoshana Zuboff's *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power* needs to be read for its description of the nature of modern surveillance systems.

Tracing the Contours of Surveillance Capitalism

"*Demanding privacy from surveillance capitalists or lobbying for an end to commercial surveillance is like asking…a giraffe to shorten its neck*"

Zuboff characterises the current economic model as "surveillance capitalism," where human experience is a raw material to be extracted and used to predict intentions, in order to produce and sell more goods and services. It crucially relies on new computing tools such as machine learning to exist. For example, personal data can be processed and converted into an application that is used by insurance companies to decide on the creditworthiness of its clients. It can be used to develop an application to help a car owner find an empty parking lot, or the least congested route to her destination.

Zuboff's central argument is that this regime poses a specific challenge because of its tumultuous impact on the very concepts of consent and privacy. What worries Zuboff the most is surveillance capitalism's potential to subtly modify behaviour, making it as a much a threat to human nature as industrial capitalism was (and is) a threat to the natural world.

A key feature leading to the development of surveillance capitalism out of earlier models of capitalism is what Zuboff calls the discovery of "behavioural surplus": the surplus value generated in mining enormous amounts of personal data and converting it into a marketable product. This surplus becomes available to corporations for uses beyond service improvement and its only purpose is to ensure exponential profits. The rush to increase behavioural surplus and thus ensure continuing profits leads corporations to move inexorably towards systems that not just infer personal behaviour, but are able to predict it with increasing accuracy. This is made possible through a continuous expansion of data that feeds into the prediction process and the use of computational tools.

> While Apple set the ball rolling, it was Google which ultimately emerged as the true pioneer of surveillance capitalism…

Zuboff traces the origins of this new regime to the launch of Apple's iTunes platform in 2011, seeing it as a pivotal moment wherein the individual becomes the central actor in the market. The desire to be uniquely catered to as a customer marks for Zuboff an important moment fashioned by and made possible by new digital, networked spaces. The digitalisation of music freed it from physical bounds and permitted reconfiguration at will, allowing Apple to cater to young people expressing "a new quality of demand: consumption my way, what I want, when I want it, where I want it". New information infrastructures and technologies made it possible to identifying individual mentalities and meeting individualistic demands.

Silicon Valley's notion of "permissionless innovation" resulted in a unilateral seizure of rights over data without consent in order to cater to these new needs. While Apple set the ball rolling, it was Google which ultimately emerged as the true pioneer of surveillance capitalism, with its elaborate model of computer-mediated transactions, where data is continuously extracted, behaviour is predicted, and user experience is personalised and customised. Personal data is now a rich vein to be mined by corporations.

The quest for behavioural surplus has moved to the offline world. Companies now track every moment of our daily lives in the physical world through smart-home devices, wearables, and applications such as Google Maps. Even human emotions are harnessed by computational methods that identify sentiments from textual and visual sources. The creeping incursion into daily routines slowly habituates people to them, but if a particular incursion generates too much of an uproar, companies adapt by promising reforms or by occasionally paying fines. This, however, fails to check the ever-growing range of data collection, made possible through tools such as ambient computing, ubiquitous computing and the Internet of Things (IoT).[1]

> In Zuboff's narrative, human beings are now essentially Pavlov's dogs, punished by the regime of surveillance capitalism for 'undesirable' behaviours and rewarded for 'desirable' ones.

From monitoring, surveillance capitalism has now entered a new domain: behavioural control. Not only is data being constantly collected, it is being processed and fed back to trigger certain desired commercial outcomes. Cars can be made to break down in order to facilitate loan recoveries; a Pokémon player is directed close to a MacDonald's outlet; advertisements are presented to individuals when they are emotionally vulnerable and most likely to respond impulsively. In Zuboff's narrative, human beings are now essentially Pavlov's dogs, punished by the regime of surveillance capitalism for 'undesirable' behaviour and rewarded for 'desirable' ones.

How has what Zuboff calls "digital dispossession" (humans being dispossessed of the control of their personal data) taken place? She argues that tech companies such as Google and Facebook have benefitted from an economic model that is based on libertarian notions of fundamental freedoms and a model that is deeply sceptical of regulation. In this milieu, companies have "ignored, evaded, contested and reshaped" laws which hinder the free generation of behavioural surplus. They equally benefitted from post 9/11 political milieu in the US, which accepted and allowed for exceptional levels of surveillance under the garb of fighting terrorism and protecting national security. Companies also fortified themselves by funding strong lobbies and building deep political connections. Zuboff reminds us that long before Cambridge Analytica, tech companies were working closely with political campaigns to build voter profiles and to advise on strategy. The 2008 Obama campaign, for instance, remodelled the electorate in every battleground state by collecting data on more than 250 million Americans.

> Efforts to foreground privacy and consent are doomed to fail, given that technology has become a useful handmaiden of surveillance capitalism…

A key takeaway from *Age of Surveillance Capitalism* is Zuboff's theorisation of how power works under surveillance capitalism. She terms it "instrumentarianism […] the instrumentation and instrumentalisation of behaviour for the purpose of modification, prediction, monetisation, and control." Instrumentation is the material computation architecture that allows human experience to be collected, collated and converted into a marketable form, while instrumentalisation denotes the social relations that make it possible for human behaviour to be used as raw material for surveillance capitalism. It is this combination, she argues, that makes surveillance capital the creature that it is. She draws parallels between instrumentarianism and totalitarianism. While the latter is an explicitly political project that converged with economics to overwhelm society, the former is a market project that converges with the digital to impose its own form of social control and domination. Just as othering is a crucial element of the totalitarian project, Zuboff argues that instrumentarianism functions by othering human experience and all notions of freedom. In other words, an autonomous, unpredictable, unknowable human being is the new 'other'.

Zuboff's arguments powerfully remind the reader that they are a mere pawns within an elaborate system of social control driven by technological tools controlled by big corporate houses or by governments. She convincingly argues that privacy and consent have been rendered toothless in this new regime of surveillance capitalism. Efforts to foreground privacy and consent are doomed to fail, given that technology has become a useful handmaiden of surveillance capitalism, containing and patterned by its "economic orientation". *The Age of Surveillance Capitalism* leaves the reader with a profound sense of doom and despair.

Technological Dystopia or Capitalist Nightmare?

In a recent interview, the Science and Technology Studies scholar Sheila Jasanoff argues that regulatory policy is structurally designed to lag behind developments in science and technology. For her, the absence of a strong regulatory framework is intentional, allowing technologies an uninhibited run. She argues that we need to "take back" control of technology. If we were to respond to Jasanoff's call to "take back" big-data analytics from the state and from big business, how successful would we be? In other words, how effectively would regulatory mechanisms work? In an increasingly data-driven world, is it at all possible for citizens to exercise control over data that they generate?

Historians and sociologists of technology have shown how communities and social movements have engaged to shape and reshape existing scientific and technological imaginations. Some of these alternative imaginations have come from within the world of science and technology. The existence of ideological battles in the domain of big data analytics is thus hardly surprising. More importantly, these contestations have the potential to change the course of technology.[2]

To begin, we have to identify the specific nature of technologies to understand the degree to which they are compatible with greater democratic control. As David Harvey suggests, technologies internalise certain mental conceptions and social relations, and reproduce particular notions of daily life. Or, as Langdon Winner has argued, some forms of technology are more compatible with particular

social systems. For instance, the use of nuclear energy encourages authoritarian forms of rule, given the tight controls required for such technologies; while the decentralised nature of solar energy lends itself to more democratic control. Socialism or democracy will need technologies which have mental conceptions of new social relations embedded in them.

> Zuboff sees surveillance capitalism as "rogue capitalism," a horrific aberration in a system which otherwise can be made to deliver.

It is here, in its lack of clarity of the role of technology in surveillance capitalism, that *Age of Surveillance Capitalism* disappoints. Zuboff sees surveillance capitalism as "rogue capitalism," a horrific aberration in a system which otherwise can be made to deliver. It emerges at a particular juncture in technological history, at a moment when crisis-hit digital technology firms were looking for a means to ensure their survival and stability. It is a product of the post 9/11 political world and of the strong neoliberal legacy in the US and not an inherent feature of digital technology. Surveillance capitalism would not necessarily be reproduced under a different set of political exigencies, Zuboff claims. She stops short of naming technology as a means of social engineering.

When Zuboff analyses the nature of knowledge, authority and power in surveillance capitalism, she speaks of the "new priesthood" in this form of capitalism, which is fundamentally dependent on technical advancements such as the integrated circuits enabling deep learning.[3] Machine intelligence is the means of production in Zuboff's account of surveillance capitalism, and yet she is reluctant to recognise the deep compatibility of digital technology with the economic system of surveillance capitalism. She is thus able to envisage a world where digital technologies can be employed in a regime marked by democratic control and not scarred by an all-pervasive loss of rights.

This distinction between forms of capitalism is often unconvincing, appearing instead as a plea to move back to old forms of capitalism. Harvey's framework would suggest a far deeper and more organic relationship between digital technologies and models of social domination and control. Given the extent of compatibility between the two, it would surely be difficult to imagine the existence of one without the other. To borrow from Winner's arguments, digital technologies appear as "forms of order", as means of social engineering and as being deeply compatible with authoritarian control. Unlike what Zuboff suggests, taking back the digital seems a difficult task, requiring the reconstitution and rebuilding of digital technologies themselves.

Footnotes:

1 In ambient computing, just about any type of object imaginable is outfitted with computing ability and connectivity. It allows the use of a computer or internet-enabled device, without human beings consciously using it. Ubiquitous computing is a concept where computing is made to appear anytime and everywhere. In contrast to desktop computing, ubiquitous computing can occur using any device, in any location, and in any format. These computing methods are part of part of the technological developments in IoT.

2 Big data analytics refers to the collection and processing of vast amounts of data, using a range of computational tools. This is often used for profiling, and to find hidden patterns, unknown correlations, market trends and customer preferences.

3 Deep learning is a subset of machine learning in artificial intelligence AI. It allows computers to learn from vast amounts of unstructured or unlabeled data, and this learning is not supervised by human beings.

References:

Harvey, David, *A Companion to Marx's Capital* (London and New York: Verso, 2010).

Snowden, Edward, *Permanent Record* (London: Macmillan, 2019).

Winner, Langdon, 'Do Artifacts Have Politics?', *Daedalus*, Vol. 109, No. 1, Modern Technology: Problem or Opportunity? (Winter 1980).