Redefining a right

Dhruv Shekhar | June 20, 2018 11:00 pm

It might come as surprise to many, given the furore surrounding the recent Facebook saga, that privacy is a fairly recent construct. The initial definitional basis for privacy was grounded in the idea of the right of an individual to live as a stranger amongst strangers. Over the years particularly in the post-World War II era, this construct became applicable to actions of governmental institutions as well as private corporations.

The Oxford definition of the term privacy goes back to 1814, while the first serious legal treatise on this subject i.e. “The Right to Privacy” was written by Samuel Warren and Louis Brandeis in 1890. Even Google Books which has digitised and scanned a millennia worth of books, shows increased usage of the word only from the 1960’s onwards as part of it Ngram viewer.

This reinvigoration of interest in the construct of informational privacy and its basis as a legal defence is a direct consequence of industrialisation over the past two centuries, rapidly growing cities and a social fabric which once encircled one and all within a set of possibilities and expectations. Privacy can thus be surmised as a sanctuary initially from the physical presence of people to now the all intrusive and non-consent structure of the information age of the late 20th -21st century.

Scholars have often deemed privacy as a coping mechanism, deeming it as a haven for individuals from the increasingly regulated world that the modern man has migrated to. However, I believe that privacy as a construct is one which far outgrows the aforementioned description. Living in a time and place where individuals can be tracked by private and public actors, an aspect that can be used both for enhancing one’s quality of life as well destroying it, it thus becomes even more pertinent to assert and redefine this right for the new day and age.

https://www.thestatesman.com/supplements/law/redefining-a-right-1502651211.html
Redefining a right - The Statesman

8/11/2018

Recognition As a Human Right

Right to Privacy’s initial construction as a human right found its grounding in Article 12 of the Universal Declaration of Human Rights (UDHR) of 1950, wherein it was couched in the following terms:

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

The UDHR was followed by the European Convention of Human Rights (ECHR) espousing a similar ideology by means of Article 8 as it was adopted in 1953.

The final member of this trilectra came by way of the International Covenant on Civil and Political Rights (ICCPR) which was adopted in 1966, only to be enforced a decade later – in 1976. Subsumed within this convention was an understanding of privacy within Article 17, which many could consider as a replicate of the UDHR. However, a difference existed and was that Article 17 of the ICCPR not only prohibits ‘arbitrary’ interferences with one’s privacy and with more specific aspects of the private sphere, but also ‘unlawful’ ones.

In spite of these multiple conventions, privacy as it exists today far outstrips the simplistic codification it was considered as in the middle to the latter half of the twentieth century. This can be evidenced by General Comment 16 of the ICCPR (1988) on the issue of Privacy, one which could not have fathomed the way in which technologies such as instant messaging services and the explosion of social media websites amongst other information technology innovations that could affect the conception of privacy.

Since the ICCPR came into force in 1976, new information technologies have emerged, and both governments and private companies have at times employed them outside of any legal framework and without regard to individual privacy. In the wake of Edward Snowden’s leaks, lawyers and commentators have recognised that while surveillance and information technologies have developed rapidly, the law of privacy has not kept pace with these changes.

Although privacy law, at the international human rights level, is grounded in robust and pedigreed principles, it seems not to have been developed or adapted to fit the needs of 21st century society.

Remedying The Situation

An effective way to resolve this new age conundrum surrounding privacy would be by way of issue of a new general comment. General comments serve an integral role as they elaborate, develop by stating the jurisprudence as well as clarify its application to specific contexts.

This in turn ensures that the treaty monitoring body properly and consistently interprets the right in its practice of reviewing individual petitions and country reports. In addition, General Comments provide a framework allowing countries to ensure their continued compliance with protected rights.

Organizations such as ACLU (American Civil Liberties Union) have for long argued that a renewed understanding of privacy as a human right should come by way of a general comment which clarifies the existing position of what constitutes the basis of privacy as a human right. As well as the redefining the basis of its presence in the present and the foreseeable future.

The discourse on Privacy lays down two central propositions. The first focuses on the right to protection of the ‘home’ or ‘house’ or ‘domicile’ – and the other is the right to protection of one’s correspondence.

An individual’s house as a concept does very well occupy the virtual world such as social media websites and email inboxes. Any discussion on the conception of privacy in the 21st century should lead to the conclusion that online private spaces, alongside their accompanying hardware (personal computers and handheld devices) should be subject to the same protections as home. Such an interpretation would be in consonance with what Article 17 of the ICCPR describes as home i.e. “the place where a person resides or carries out their usual occupation”.

Such an interpretation is also in consonance with court practice regarding this issue. For instance, in Halford v. the United Kingdom, the European Court adopted a conception of the term “home” under Article 8 of the ECHR, by holding that the idea of privacy would be applicable to an individual’s phone calls as well as home phones. A similar stance was also taken in Bernh Larsen Holding AS and Ors. v. Norway, where the court stated that all data stored on a server as used by the three corporations in this case constituted a space that should be accorded the same protections as a home.

Thus, the conception of one’s home and private life when defined in such expansive terms, owing to the nature and functioning of the 21st century, can allow for privacy to be reflective of values representative of the day and age.

The term Correspondence was initially worried to maintain confidentiality of postal communication; however, this term should become an umbrella term under Article 17 to include all forms of electronic communication such as email and instant messages, as well as “telephonic and telegraphic” forms of communication. These conceptions find their roots in General Comment 16 but require updating with regard to aspects such as metadata i.e. the data about transactions or correspondence that excludes the content of what is communicated, which should be brought within the understanding of Article 17.

Metadata includes amongst other things information such as phone numbers dialled, the time, date and duration of calls made, location information for cellular phones (as recorded by cellular phone towers, for example); and the IP addresses or URLs visited while browsing the Internet. This data allows the government to infer new or hitherto unknown facts about an individual through data analytics algorithms which are collated and aggregated across time.
In certain instances, metadata can reveal information that is more sensitive than the underlying information. Furthermore, this information can be acquired at little or no cost and can easily be shared and be rapidly processed through algorithm surveillance to create digital profiles of individuals. On this one account, algorithms and location data are linked. Reports have emerged suggesting that despite metadata regulations, law enforcement surveillance techniques have been used to identify location of targets for lethal drone strikes or for that matter a general mapping of one's location at all times.

**GDPR & Human Rights**

The GDPR as brought in to force on the 25 May will be a game changer in the way in which private corporations contend with the issue of data privacy.

Effectively, the GDPR will require organisations with any ties to the personal data of individuals in the EU to examine and potentially change the methodology behind the collection, storage and processing of information for business operations. Crucially however this framework sets a precedent across the globe on the importance of personal information ownership and consumer protection. The prime aim that the GDPR is geared towards is to maintain integrity of personal data for individuals and not just organisations.

While this regulation is a promising development that many countries and regional organisations can seek inspiration from, equally there are gaps in the framework. These gaps will affect operation of the commerce of the cyber space arena as evidenced by the recent blocking of services to EU users by a variety of e-commerce and other online entities. This is due in part because of the expansive trade relations that the EU has as well as lack of clarity surrounding the GDPR regulations.

In addition, the relevance of redefining the scope of privacy as a human right will also ensure the inadequacies of laws pertaining to information technology on a domestic level (country specific) do not allow private parties to escape their obligations. For instance, with regard to the Facebook-Cambridge Analytica scandal, Facebook can potentially escape all liability in India as its contract with users is governed by American law and not Indian law. In other words, Facebook is exporting a service from America, to Indians in India, who by clicking on the 'I agree' button have agreed to be bound by American law.

Furthermore, Facebook if it can couch itself as an intermediary, possessing limited information about the exchange of user data, it would be protected as an intermediary under Section 79 of the Information Technology Act, 2000.

**Ruggie Principles**

In a scenario such as this with business contracts being spread over multiple jurisdictions, a pragmatic way of dealing with them would be via an international treaty which compels signatory countries to adopt similar rules on the principle of reciprocity.

While this suggestion could be something that governments work on for the future, for the present the framework as provided by the Ruggie Principles could serve as the basis for addressing concerns. Now, these principles work at a confluence of Human Rights protection and business by ensuring that the Respect, Protect, and Remedy framework is appropriately applied. This is to ensure that private and public entities review their policies, legislation, regulations and enforcement measures to ensure that their work does not result in human rights violations.

In the event of any gaps, appropriate steps must be taken such as imposing civil, administrative or criminal liability for enterprises domiciled or operating in their territory and/or jurisdiction that commit or contribute to gross human rights abuses. A similar treatment should be meted out to Governmental enterprises in the event of any violations.

An understanding such as this could be pivotal considering that the technologies which make industrial espionage and personal data security violations possible also form the basis of the 21st-century military. Examples of this are the collaborations between Google and the US military with regard to their drone mapping technology for Project Maven and their efforts to develop a cloud computing set up called JEDI for the Pentagon.

The dual nature of modern-day technology ensures its continued importance to both commerce and security. Against such a backdrop, it underlines the need to have a framework in place to ensure that global citizens' rights are both well represented and well protected.

By couching these terms in their broadest iteration within the confines of Privacy as a human right, they can address a variety of challenges from state or private actors. For instance, in the instance of a jurisdiction like India, privacy as a human right could lead to a more decisive take on the Aadhaar issue and the larger issue of biometric collection of data for state surveillance. On the private actors' front, a burgeoning financial technology industry would start taking these rights even more seriously if the issue of information is raised to the plane of human rights.

Redefining the scope of privacy as a human right would not immediately prevent any violations from not taking place. However, in similar vein to the K.S Puttaswamy v. Union of India judgment by the Supreme Court, it would raise the standard against which these rights are examined and explored in years to come.

The writer is a student of the Jindal Global Law School, Sonipat.
Bill to strengthen human rights institutions introduced in Lok Sabha

Odisha rights body without chairman for six years, pendency of cases mounts


Big Fan of Custom Motorbikes? Your Vote Counts Here


Harley-Davidson India

3-Tier Swimming Pool & Landscaping, Sculpture Garden & Orchard.

Aqua Garden

Watch the story of these childhood friends 'Sonu & Titu' on Prime Video by joining at just ₹129/month

Amazon Prime Video

Reside At Super Luxury Villa Township Near Delhi At Rs 3.79 Cr*

Sobha Homes Gurugram

WANTED: 500 people over 50 for free hearing aid trial
Do a HR certification from XLRI - Online Program

70+ CENTRES
ACROSS DELHI-NCR
✓ 9 AM-6:30 PM, 9 Months+ Kids.
✓ Live CCTV Camera & Mobile Updates.
✓ 100% Nutritious Food, 0% Junk.
✓ World Class Adult to Child Ratio.
✓ Smart Books & Talking Pen.

See Fee Card

TOP HEADLINES

1. 29 dead, 54,000 homeless as Kerala reels under floods amid unprecedented rain (https://www.thestatesman.com/india/death-toll-climbs-54000-homeless-kerala-floods-1502671875.html)


