AN INSIGHT INTO PRIVACY AND PERSONAL LIBERTY

Anubhav Kumar Sahu, Dr. Ram Manohar Lohia National Law University

Introduction

According to Black's Law Dictionary, privacy is defined as "the right of a person to be left alone; the right of a person to be free from any unwarranted publicity; the right to exist without unwarranted public intrusion in areas with which the public is not necessarily interested." The promise of "a certain private realm of individual liberty shall be preserved substantially beyond the grasp of Government" underpins the concept of privacy.

When something is private to a person, it usually means that something is inherently special or sensitive to them. The domain of privacy partially overlaps with security, which can include the concepts of appropriate use and protection of information. Privacy may also take the form of bodily integrity. The right not to be subjected to unsanctioned invasions of privacy by the government, corporations, or individuals is part of many countries' privacy laws, and in some cases, constitutions.

The universal concept of personal privacy is a modern concept primarily related to Western culture, especially Britain and North America, and until recently remained virtually unknown in some cultures. However, most cultures recognize the ability of an individual to withhold certain personal information from a wider society, such as closing the door to their home.

Historical background

Privacy has historical roots in the philosophical debate of ancient Greece. The most famous of these was Aristotle's distinction between the two living spheres. In other words, the public sphere of police related to political life and the private sphere of Oikos related to family life. Privacy did not appear until the 1890s. With the enactment of US data protection law.

The debate over privacy issues dates back to the dawn of time. It began with the protection of one's body and house and quickly progressed to the control of one's personal information. In a famous paper published in 1891, American lawyers Samuel Warren and Louis Brandeis

defined the right to privacy as "the right to be left alone." With the release of Alan Westin's Privacy and Freedom in 1967, a new milestone was attained when he defined privacy in terms of self-determination: privacy is the right of individuals, organisations, or institutions to choose when, how, and to what extent information about them is shared with others.

Privacy is possibly the most difficult to describe of all the human rights in the international catalog. Privacy is defined in a variety of ways depending on the context and surroundings. The idea has been merged with data protection in many nations, which defines privacy in terms of personal information management. Outside of this relatively stringent setting, privacy protection is commonly considered as a way of defining how far society can pry into a person's personal concerns. The lack of a single definition should not be interpreted as a lack of significance. "In one sense, all human rights are facets of the right to privacy," one writer stated.

States of Privacy

Alan Westin has defined four states of privacy: experience. It's loneliness, intimacy, anonymity, and modesty. Solitude is a physical separation from others. Intimacy is a "close, relaxed and open relationship between two or more individuals" that results from the isolation of a couple or a small group of individuals. Anonymity is "the individual's desire for an era of" public privacy ". Finally, suppression is "creating a psychological barrier to unwanted invasion." Creating this psychological barrier requires respecting the need or desire of others to limit the transmission of information about themselves.

In addition to the psychological barriers of restraint, Kirsty Hughes has identified three other types of barriers to privacy. It is physical, behavioral, and normative. Physical barriers, such as walls and doors, prevent others from accessing and experiencing the individual. (In this sense, "access" to a person also includes access to that person's personal information.) Behavioral barriers are verbal, verbal, or non-verbal, personal space, Communicate with others through body language or clothing. -Do not want people to access or experience it. Finally, normative barriers such as law and social norms prevent others from accessing and experiencing others.

Status quo in an era of technology and data

Clive Humby coined the phrase "Data is the new oil" in 2006, implying that in the twenty-first century, whoever has more data is more powerful and wealthy, and since then, there has been

a slew of cyber attacks on individuals and

governments around the world, resulting in monetary frauds, identity thefts, rigged elections, government destabilization, illegal surveillance, and so on.

As technology has progressed, so has the way in which privacy is safeguarded and violated. The increasing ability to exchange information in some technologies, such as the printing press or the Internet, can lead to new ways in which privacy might be invaded. The 1890 article "The Right to Privacy" by Samuel Warren and Louis Brandeis is widely regarded as the earliest publication promoting privacy in the United States, and it was published mostly in response to the expansion in newspapers and photographs made available by printing technologies.

George Orwell's novel 1984 was published in 1948. 1984 is a classic dystopian novel about Winston Smith, who lives in Oceania, a totalitarian state, in 1984. The ruling party, led by Big Brother, is able to maintain power through mass surveillance and restrictions on freedom of expression and thought. George Orwell offers insight on totalitarianism's detrimental impacts, particularly on privacy and censorship. [6] There have been comparisons drawn between 1984 and modern censorship and privacy, with one noteworthy example being that large social media firms, rather than the government, may monitor a user's data and decide what can be stated online through their censorship policies, ultimately for monetary purposes.

Many firms, like Google, Amazon, and Facebook, have made significant profits from the "data economy," which involves amassing user data in order to enhance product or ad sales. Keeping client information secure, not sharing it with third parties without consent, and not utilizing data maliciously or irresponsibly are all examples of good information privacy practices.

Online users are extremely sensitive to security attacks, and there are numerous concerns about their safety. Only the most important aspects of online privacy are discussed here.

1) Tracking

Tracking is when a website collects information about how you use it or how you interact with it. Web trackers can gather more information about you than just your browsing habits on a website. They are also used by websites to collect personal information such as your IP address, origin, geographic location, and browser characteristics.

2) Surveillance

Every day, it becomes clearer and clearer that Internet restrictions and regulations are becoming the norm. Governments are continually enacting legislation that makes online surveillance and governmental cyber-policing easier. Concerns about online regulations can deter citizens from exercising their right to free speech or engaging in legitimate activities online, making Internet surveillance a pressing global issue.

3) Threat

Cybercrime is currently one of the most pressing issues confronting countries all over the world. The usage of the internet includes illegal access to information and breaches of security such as privacy, passwords, and other personal information. Cyber theft is a type of cybercrime that involves committing theft using computers or the Internet.

We are more vulnerable to data theft and monitoring than ever before in the age of social media and rapid payment channels. Big tech data businesses construct massive data centers in which they may clone your data, share your personal information, and even sell it to governments and other corporations. 'If you're not paying for it, you're the product,' as someone wisely put it. I'm not sure how many people are aware of or care about this sentiment. But remember that the next time you're surfing the web or watching a video on YouTube, Google is tracking your every action; it's the price you pay.

To quote Netflix's documentary 'The social dilemma':

Never before have a handful of tech designers had such control over the way billions of us think, act, and live our lives.

Legal view

Privacy has been a key legal issue across the globe from the past deacde, United States was the first state to bring a legislation for privacy and data protection

In 2018, the European Union (EU) General Data Protection Regulation (GDPR) came into force. This is a data protection law that replaces the 1995 Data Protection Directive. The GDPR requires consumers in the EU to have a complete and accurate knowledge of how businesses

use their data and have the right to receive and modify the data they hold. .. This will enforce stricter data protection laws compared to the 1995 Data Protection Directive.

'If you want to keep a secret, you must also hide it from yourself". Delhi High Court quoted the mentioned quote from Orwell`s novel 1984 while delivering Pegasus Judgement.

The Supreme Court from time to time has asserted that Article 21 is the heart of Fundamental Rights due to its extended dimension. On 24th August 2017 SC in a historic judgment declared the right to privacy as a fundamental right protected under the Indian Constitution in Article 21.

The landmark case of Justice K. S. Puttaswamy (Retd.) and Anr. V. Union Of India[1] was decided by the Hon'ble Supreme Court of India. The Bench's decision in the case gave citizens a new perspective on their right to privacy. According to Articles 14, 19, and 21 of the Indian Constitution, the right to privacy is a fundamental right.

After more than two years of heated debate, the Indian government finally presented the Personal Data Protection Bill[2] in Parliament on December 11, 2019. As India strives to build a comprehensive data governance framework, this law has far-reaching ramifications for nearly any organization wanting to do business in India. India has a unique potential to exert power over multinational digital businesses and shape global policy due to its population size, gross domestic product, and the influx of new internet users.

This bill will play an essential part in creating the regulation controlling today's increasingly data-driven geopolitical scenario, as many countries seek to develop data governance regimes. Meanwhile, the law has aspects of the protectionist and authoritarian-leaning data rules that are gaining traction around the world as countries seek to limit the global and open internet.

India's strategic goal is likely to be in ensuring that it fulfills its constitutional commitment to its people, prioritizing citizen rights and economic well-being over purely commercial or bureaucratic concerns. However, it is unclear whether this goal is met, owing to concerns about exemptions in the language of the Personal Data Protection Bill. It remains to be seen whether

[1] K.S. Puttaswamy (Privacy-9J.) v. Union of India, (2017) 10 SCC 1

[2] Arindrajit basu and Justin sherman, Key Global takeaways from india's revised data protection bill, LAWFARE, https://www.lawfareblog.com/key-global-takeaways-indias-revised-personal-data-protection-bill

the policymaking pendulum swings in the correct direction as the Joint Parliamentary Committee begins debates on the bill draught.

People at COVID 19 are being forced to stay at home and work at home, maintaining social gaps. This has resulted in a high level of reliance on digital platforms. In light of these conditions, India must move quickly to enact new personal data protection legislation. When and how the above regulations go into effect is still up in the air, and how they go into effect will influence the fate of data for millions of Indians.

Being a part of society frequently obscures the truth that we are first and foremost individuals. For all activities, each individual requires his or her own personal space (assuming it is legal here). As a result, the state grants each person the right to enjoy these private times with the people they choose, away from the prying eyes of the rest of the world. According to Clinton Rossiter, privacy is a unique form of independence that can be viewed as an endeavor to maintain autonomy in at least some personal and mental matters. This independence is something that one can appreciate. There, he is truly a free man.

Comment

Individual existence is in jeopardy nowadays, as others may easily influence our life thanks to the internet. End-to-end encryption, in which only individual users possess the information, is the need of the hour. Another method to secure our privacy is to use Zero Knowledge[3] Architecture, which protects us from hacks, leaks, secret subpoenas, and government overreach. This is a means to ensure that you and only you have control over who sees your data. Finally, Open Source Coding enables for independent verification of the system's dependability.

Conclusion

Justice Kaul has stated in Adhaar Judgement of his opinion that:

"The State must ensure that information is not used without the consent of users and that it is used for the purpose and to the extent it was disclosed"

[3] Istavan lam, What is zero knowledge encryption?, tresorit, https://tresorit.com/blog/zero-knowledge-encryption/

To quote angel investor and philosopher Naval Ravikant, "Social media breaks the world apart by bringing it together." The world is at the crossroads of technological progress and the threat to people's individuality due to technological progress. At this point, it's important to add some warnings to prevent the Big Tech giant from going out of control and not destroying people's social structure and privacy. We must pull the chain of social media algorithms before they overtake us. How social media controls and manipulates the mind and jeopardizes people's privacy. The ability and accuracy of social media giants to predict people's personalities is very worrisome and only deteriorates over time. With the integration of the platform, some social media companies are acquiring competitors, exercising monopoly power, significantly hindering the growth of privacy options and exacerbating the risk of social networking. Third parties, especially law enforcement agencies, may access and misuse personal data from social media companies. Excessive data collection, algorithm processing, and commercial use of users' personal data are the foundations of numerous social media networks. This needs to be changed.