KnowLaw Journal

Socio-Legal and Contemporary Research

A Publication of KnowLaw

Volume 02 Issue 01 KnowLaw

Understanding Digital Privacy through Intellectual Property and the Future Outlook

Kanak Purohit[1]

Abstract

Data privacy commonly means the capacity of someone to decide for themselves when, how, and to what extent the privacy of a person is shared with or communicated to others. Information privacy is essential to the broader right to privacy. It is every human's right but unfortunately, the world has reached a point where the internet will not function properly unless some of the user data is sacrificed. A precise knowledge of the significance of privacy, and why it desires safety, is fundamental for a user's role. In many jurisdictions, privacy is taken into consideration as an essential human right, and data protection laws exist to shield that right. Data privacy is likewise vital due to the fact so as for people to be inclined to have online interaction, they must consider that their private data is being dealt with care. Evolving Technology and De-volving Privacy the Internet of Things (IoT) is predicted to carry the entirety from washing machines to scientific implants online.

[1] 4th Year, Jindal Global Law School, O.P. Jindal Global University, Sonepat, kanak3103@gmail.com

KnowLaw Journal

Socio-Legal and Contemporary Research

A Publication of KnowLaw

Volume 02 Issue 01 KnowLaw

Introduction

Privacy is every human's right but unfortunately, the world has reached a point where the internet will not function properly unless some of the user data is being sacrificed. From social media platforms to cell phones everything requires some or the other form of personal information or location and more. Data privacy commonly means the capacity of someone to decide for themselves when, how, and to what extent the privacy of a person is shared with or communicated to others. These non-public facts maybe one's name, location, or online or real-world behaviour. Just as a person might want to exclude someone from a private conversation to maintain privacy regarding what the conversation is about, the same way people online want to control and oversee what kind of their data is being collected.

To many of us, how organisations collect and use our data is often a mystery. There are regular stories of customer information that is being stolen from the database, but we still, willingly, deliver ours due to the fact the opportunity is cloud services and social networks locking us out. The solution relies upon how the internet evolves withinside the future. One fashion that's predicted to extrude the panorama is the boom in non-pc gadgets and the use of the net to hook up with cloud services.

KnowLaw Journal

Socio-Legal and Contemporary Research

A Publication of KnowLaw

Volume 02 Issue 01 KnowLaw

Evolving Technology and De-volving Privacy

The Internet of Things (IoT) is predicted to carry the entirety from washing machines to scientific implants online. One gain of those clever gadgets is that we'll be capable of managing them remotely. Soon, we'll be capable of managing the entirety of our houses with an app. But clever gadgets like those depend on sending records regarding our activities to providers. Once most of the gadgets are online, our complete lifestyles may be too. A precise knowledge of the significance of privacy, and why it desires safety, is fundamental for a user's role. A device to help you carry out an entire task all by itself will require all the personal information about the user to carry out that task explicitly for that user personalised.

Privacy is acknowledged as a character of human proper in diverse global treaties and conventions including the International Covenant on Civil and Political Rights (ICCPR). In Victoria, a right to privacy is protected in section thirteen of the Victorian Charter of Human Rights and Responsibilities Act 2006,[2] which says that everybody has the right to not have their privacy, family, domestic or correspondence unlawfully or arbitrarily interfered with. Information privacy is essential to the broader right to privacy and pertains to a person's ability to decide for themselves when, how, and for what cause their non-public records are dealt with through others. Protecting privacy is fundamental to making sure human dignity, protection and self-determination. It permits people freely expand their personal personalities. The right

[2] N A, "The Importance of Privacy," Office of the Victorian Information Commissioner, June 30, 2021, https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-officer-toolkit/the-importance-of-privacy/.

to privacy is likewise acknowledged as a permitting right because it allows the entertainment of different human rights consisting of freedom of expression; freedom of thought, sense of right and wrong and religion; freedom of meeting and association; and the right to be free from discrimination. In this way, it serves as a basis for a democratic society. In many jurisdictions, privacy is taken into consideration as an essential human right, and data protection laws exist to shield that right. Data privacy is likewise vital due to the fact so as for people to be inclined to have online interaction, they must consider that their private data is being dealt with care. Organizations use data protection practices to illustrate to their clients and customers that they may be dependent on their private data.[3]

Interferences with an individual's privacy can result in many different types of harm to an individual such as:

- Reputational damage
- Embarrassment or humiliation
- Emotional distress
- Identity theft or fraud
- Financial loss
- Physical harm
- Intimidation

[3] "What Are Your Digital Rights?," World Economic Forum, accessed October 9, 2022, https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer/.

- Disruption of government services
- Discrimination
- Feeling of disempowerment

But failing to respect the right to privacy also can have wider societal impacts. It can cause the erosion of public consideration and a loss of willingness to interact with authorities. For governmental organizations, this could imply the failure of programs, tasks and operations and the general public effects that they are looking to achieve. As such, it is important that the public sectors are transparent which will create trust in the community.

Personal data may be misused in some of the methods if it isn't kept private or if people don't have the power to control how their data is being used:

- Criminals can use private data to defraud or harass customers.
- Entities might also additionally promote personal data to advertisers or different outside parties without personal consent, which may bring about customers receiving undesirable advertising or advertising.

- When a person's activities are tracked and monitored, this will put a limitation on them from expressing themselves freely, especially under repressive governments.

Laws around Data Privacy

As technological advances have progressed in data collection and surveillance capabilities, governments around the globe have begun passing laws regulating what sort of data may be gathered regarding users, how that data may be used, and the way data need to be saved and protected. Some of the most vital regulatory privacy frameworks to know include:

- General Data Protection Regulation (GDPR): Regulates how the private data of European Union (EU) data subjects, which means people, meaning individuals, can be collected, stored, and processed, and gives data subjects rights to control their personal data (including a right to be forgotten).
- National data protection laws: Many countries, along with Canada, Japan, Australia, Singapore, and others, have complete data protection laws in a few forms. Some, like Brazil's General Law for the Protection of Personal Data and the UK's Data Protection Act, are pretty just to the GDPR.
- California Consumer Privacy Act (CCPA): Requires that purchasers be made aware of what personal data is collected and offers purchasers control over their private data, which includes a right to inform organizations not to sell their personal data.

There also are industry-precise privacy guidelines in a few countries: for instance, withinside the United States, the Health Insurance Portability and Accountability Act (HIPAA) governs how private healthcare data have to be dealt with. However, many privacy advocates argue that people nevertheless do now no longer have enough control over what happens to their personal data. Governments around the world might also additionally pass additional data protection laws in the future.

In Article 10(2) of the TRIPs Agreement, the security of "data" is acknowledged. According to Article 10(2) of the Agreement, "data compilation" or "other material," whether in machine-readable form or another format, "must be covered as such" since "the selection or arrangement of its contents comprises intellectual production." The Article further states that any copyrights located in the data or material itself are unaffected by these rights, which do not apply to the data or material itself.

Only the use of creative creations in the collection or arrangement of the information supports the justification for data protection.

Therefore, the gathering or arrangement of the things cannot be considered data property if no intellectual effort was put into them. However, the same would also hold true for copyright defences since these are based more on how the items are presented as such than on their actual content. At this point, it must be made clear that the assertion of copyright is independent of the registration process formalities. Copyright protection will also be provided as long as the contents are displayed in their original form. The person who owns the data has options.

He has a right in the form of databases that are available as a collection or arrangement of intellectual creations, on the one hand. However, he is entitled to the copyright of the information or content that is made available to him. In other words, copyright is available in the data or material itself because the duration is the same, however, the right to data protection is only available in the type and manner of intellectual selection or arrangement and not in the data or material itself. Therefore, both databases and copyrights are appropriately covered by the Copyright Act of 1957. Therefore, the data security system's current structure is sufficient to abide by the TRIPs Agreement[4] and the Indian Constitution's regulations. The best way to address any problem is not by enacting a tonne of laws, but by vigorously and consistently carrying them out. The courts must apply the law in a progressive, modern, and impartial way. It is important to realise that the bestowment of the highest, most effective, and most effective security for every cause does not depend on the enforcement of the law, but rather on the intention, the desire, and the commitment to embrace and execute it in its true text and spirit. In addition to a quantitative effort, these rights must also be enforced qualitatively.

[4] The Agreement on Trade-Related Aspects of Intellectual Property Rights

KnowLaw Journal

Socio-Legal and Contemporary Research

A Publication of KnowLaw

Volume 02 Issue 01 KnowLaw

Analysis and the Predictable Future

As people more and more conduct their lives online – shopping, socializing and sharing data– our virtual rights, especially the rights to privacy and freedom of expression, have become even more important than ever. People need to understand how their data is being utilized by corporations, governments and net giants along with Facebook and Google. Is it being dealt with pretty and scrupulously, or bought or shared without our consent? Revelations about surveillance programmes and virtual hacking have sparked political and diplomatic wrangles. National Security Agency (NSA) whistle-blower Edward Snowden has called for new international laws to govern data privacy and protect it. He argues that people might be aware of mass data surveillance it's time to "assert our fundamental and virtual rights in order that we are able to defend them".

Ranking Digital Rights, which is primarily based totally at the New America Open Technology Institute think tank, assessed the user agreement policies of sixteen of the world's largest networking and telecommunications corporations for its 2015 Corporate Accountability Index. The index permits customers, investors, activists and policy-makers to examine how – and whether – corporations are making efforts to recognize our virtual rights. Rebecca MacKinnon, director of Ranking Digital Rights, stated: "Our wish is that the index will result in more

company transparency, which could empower customers to make greater knowledgeable choices approximately how they use technology." [5]

Governments, corporations and cybercriminals can without difficulty accumulate private data and track our actions and communications. But maximum people wouldn't realize who precisely has got access to the data trail that is created. In 2014, Facebook, Microsoft, Yahoo and Google commenced publishing information about how oftentimes the government requested them for data.

Should people be worried about hackers getting hold of our non-public information? In the contemporary of a string of high-profile cyberattacks, UK telecoms organisation TalkTalk's firewall became hacked, which placed non-public information of up to four million clients at risk. According to Ernst and Young's 2015 Global Information Security Survey, corporations are worried about the risk of cyberattacks and are trying to grow to spend on safety measures. Should we trust governments regarding our data?

Snowden's revelations[6] about the extent of the US, government spying spread shockwaves around the arena. Microsoft has spoken back by saying plans to construct data centres in Germany to hold European clients' data out of the palms of US officials. Meanwhile, withinside the UK, campaigners are calling for judges, in preference to the house secretary, to signal warrants that authorize safety companies to have a take observe citizens' data.

[5] "What Is Data Privacy? | Privacy Definition |," 2021, https://www.cloudflare.com/learning/privacy/what-is-data-privacy/.
[6] "Snowden Revelations," Lawfare, October 31, 2019, https://www.lawfareblog.com/snowden-revelations.

While it can be difficult to defend privacy withinside the virtual age, it appears that evidently human beings around the globe have become more and more aware of their digital rights and are organized to combat them again in opposition to net surveillance.

Netflix had made a documentary, "social dilemma"[7] which clearly shows what goes behind the scenes in big social media corporations such as Google, Facebook, Instagram etc. With the advancing technologies, these platforms have curated algorithms that keep predicting what kind of content to show up next on the user's feed to increase their usage of their platforms.

The Developments for a Better Future

Data Protection refers back to the set of privacy laws, rules, policies and techniques that intend to minimise intrusion into one's privacy as a result of the collection, storage and dissemination of private data. Personal records commonly refer to the facts or records which relate to someone who may be recognized from that information or data whether collected by any Government or any personal business enterprise or an agency.

The Constitution of India does not patently grant the fundamental right to privacy. However, the courts have read the right to privacy in relation to other existing fundamental rights, i.e., freedom of speech and expression under Art 19(1)(a) and right to life and personal liberty under Art 21 of the Constitution of India. However, there can be reasonable restrictions imposed on

[7] "Social Dilemma", *Netflix*, 2021

those Fundamental Rights under the Constitution of India given under Art 19(2) of the Constitution that can be imposed by the State. Recently, withinside the landmark case of Justice K S Puttaswamy (Retd.) & Anr. vs. Union of India and Ors[8]., the constitutional bench of the Hon'ble Supreme Court has held the Right to Privacy as a fundamental right, subject to reasonable restrictions.

India currently does not have any specific rules governing data safety or privacy. However, the applicable legal guidelines in India managing data safety are the Information Technology Act, of 2000 and the (Indian) Contract Act, of 1872. A codified regulation close to data safety is likely to be delivered in India within the near future.

The (Indian) Information Technology Act, 2000 offers issues referring to the payment of compensation (Civil) and punishment (Criminal) in case of wrongful disclosure and misuse of private data and violation of contractual terms in appreciation of private data.

Under section 43A of the (Indian) Information Technology Act, 2000, a company who is possessing, dealing or handling any sensitive private information or data, and is negligent in enforcing and preserving affordable protection practices ensuing in wrongful loss or wrongful advantage to any man or woman, then such company can be held liable to pay damages to the man or woman so affected.

The Government has notified the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The Rules most

[8] (2017) 10 SCC 1

effectively offer the safety of "Sensitive private information or data of a man or woman", which incorporates such private data.

Conclusion

The trend is that everyone is sharing data about themselves through more devices. The Internet of Things will boom similarly, and techniques for organizing and reading huge data are evolving too.

Similar to the US, India lacks a well-developed framework to adequately safeguard data and the rights of its residents with regard to data privacy. Companies are allowed unlimited access to user data, which reduces their profit margins and forces them to store data, as an illustration of India's immaturity in this area. As a result, a number of businesses made money by analysing the data they had gathered, which brings us back to the danger of users' personal information being misused. Recently, the government in India ordered VPN service providers to keep connection logs, completely defeating the point of the service. In order to comply with the new regulations mandating these businesses to preserve their name, address, and IP address, India will now grant VPN providers and cloud service operators an additional three months.

of their clients. This provides some respite to businesses as they rush to adhere to the new regulations and consider their options for leaving the South Asian market.

Fortunately, there are initiatives underway to strengthen Indian law and safeguard user data. In addition to current rules intended to secure its citizens' data, a new data protection bill that was

written in late 2021 would include legislation requiring the notification of data breaches within 72 hours. Along with other legislative initiatives in India to address invasions of privacy, such as an investigation into antitrust issues with WhatsApp, this bill was introduced.