PRIVACY IN INTERNET ERA

By Arundhati Banerjee
From Mewar Law Institute, Ghaziabad Uttar Pradesh

INTRODUCTION

"**Information privacy is a social goal, not a technological one. To achieve information privacy goals will require social innovations, including the formation of new norms and perhaps new legal rules to establish boundary lines between acceptable and unacceptable uses of personal data."**
Pamela Samuelson[1]

WHAT IS PRIVACY AND INTERNET?

Privacy is a concept that is neither clearly understood nor clearly defined .Of all Human Rights in the International catalogue, privacy is perhaps the most difficult to define. It is a fundamental human right recognized all over the world, enshrined in numerous international human rights instruments.[2] It protects human dignity and other values such as freedom of expression, information and association. Thus, it has become one of the most important human rights in modern age.[3]
In most of the countries Privacy is fused with Data protection, which interprets privacy as management of personal information. Privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organizations.[4] People enjoy having private spaces, and want to keep them. In rather strict context, Privacy protection is seen as a way of drawing a line of how far a society can intrude a person's affairs.

Ability of others to access and link databases, with few control on how they use, share or exploit the information, makes individual control over information about oneself difficult. Privacy in cyberspace is the most flagrantly violated right of the individual. It has multiple dimensions, including privacy of the physical person, privacy of personal behavior, privacy of communications and privacy of personal data. The last two are commonly bundled together as 'information privacy'.

Dataveillance or intellectual privacy is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons. Universal Declaration of Human Rights defines Right to Privacy under Article 12.[5] Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8) are expressed similarly.

Internet offers many benefits. Web sites provide a vast world of information,

[1] Pamela Samuelson, Privacy as Intellectual Property? , 52 STAN.L.REV.1125, 1169 (2000).
[2] Universal Declaration of human Rights Article 12, United nations Convention on Migrant Workers Article 14, UN Convention of the Protection of Child Article 16, International Covenant on Civil and Political Rights Article 17.
[3] Marc Rotenberg, Protecting Human Dignity in the Digital Age (UNESCO 2000).
[4] Clarke, Roger, Information Privacy On the Internet Cyberspace Invades Personal Space.
[5] "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

entertainment, and shopping at our fingerprints. Electronic mails, instant messaging, and chat rooms enable us to communicate with friends, family, and strangers in ways we never dreamed of a decade before.

The internet has become an indispensable tool for data retrieval, communication, and business transactions. Companies increasingly look to the internet to attract potential clients and customers and to stay in contact with current clients and customers. But with the ease in collecting and processing information, there exists the danger that Internet Business transactions can render party's information susceptible to interception, misappropriation, or even loss.

Internet exposes Companies to the danger that third parties may access private, confidential client data, resulting in potential liability to those companies. The privacy and security concerns generated by its usage increase the importance of a company's privacy policy.[6]
Internet privacy involves the right or mandate of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the Internet.[7] Internet privacy is a subset of data privacy. Privacy concerns have been articulated from the beginnings of large-scale computer sharing.[8]

RISKS TO PRIVACY

Companies are hired to watch what websites people visit, and then use that information, for instance by sending advertising popups based on one's web browsing history. There are many ways in which people can divulge their personal information, for instance by use of "social media" and by sending bank and credit card information to various websites. Moreover, directly observed behavior, such as browsing logs, search queries, or contents of the Facebook profile can be automatically processed to infer potentially more intrusive details about an individual, such as sexual orientation, political and religious views, race, substance use, intelligence, and personality.[9]

Several social networking websites try to protect the personal information of their subscribers. On Facebook, for example, privacy settings are available to all registered users: they can block certain individuals from seeing their profile, they can choose their "friends", and they can limit who has access to one's pictures and videos. Privacy settings are also available on other social networking websites such as Google Plus, Twitter etc. The user can apply such settings when providing personal information on the internet. The Electronic Frontier Foundation has created a set of guides or

[6] Wendy S Meyer, Insurance Coverage for Potential Liability Arising from Internet Privacy Issues, journal of Corporation Law, Winter 2003
[7] The Editorial Board (March 29, 2017). "Republicans Attack Internet Privacy". *New York Times*. Dated on March 29, 2017
[8] E. E. David; R. M. Fano (1965). "Some Thoughts About the Social Implications of Accessible Computing. Proceedings 1965 Fall Joint Computer Conference" Dated on 06-07-2012.
[9] Kosinski, Michal; Stillwell, D.; Graepel, T. (2013). "Private traits and attributes are predictable from digital records of human behavior". *Proceedings of the National Academy of Sciences*.

guidelines so that users may more easily use these privacy settings.[10]

In late 2007 Facebook launched the Beacon program where user rental records were released in the public for friends to see. Many people were enraged by this breach in privacy, and the *Lane v. Facebook, Inc.* case ensued.[11]

Children and adolescents often use the Internet (including social media) in ways which risk their privacy: a cause for growing concern among parents. Young teenagers also may not realize that all their information and browsing can and may be tracked while visiting a particular site, and that it is in their own hands to protect their own privacy.

They must be informed about all these risks. For example, on Twitter, threats include shortened links that lead one to potentially harmful places. In their email inbox, threats include email scams and attachments that get them to install malware and disclose personal information. On Torrent sites, threats include malware hiding in video, music, and software downloads.

In 1998, the Federal Trade Commission of USA considered the lack of privacy for children on the Internet, and created Children Online Privacy Protection Act (COPPA). COPPA limits the options which gather information from children and created warning labels if potential harmful information or content was presented. In 2000, Children's Internet Protection Act (CIPA) was developed to implement safer Internet policies such as rules, and filter software. These laws, awareness campaigns, parental and adult supervision strategies and Internet filters can all help to make the Internet safer for children around the world.[12]

LAWS RELATED TO PRIVACY IN INDIA

There was no mention of right to privacy within the context of communication surveillance and data protection in the National Report submitted by India. The right to privacy was not raised as an issue of concern neither by UN Member States nor external stakeholders.

The Constitution of India does not contain any provision granting a general right to privacy. But 'Right to Privacy' has been recognized by the Indian Judiciary as implicit in Article 21 and Article 19 (1) (a) of the Constitution in many cases. Right to Privacy has many dimensions and the most likely aspect of privacy that would be affected in cyberspace is **informational privacy**. There are currently no laws in India requiring websites to disclose how the information they gather about visitors is being used; and online businesses are largely free to use data obtained on their websites without oversight by the consumer. In India, consumers have no statutory right to control the dissemination of their personal information to others by third parties.

Protection of privacy is one of the crucial issues that must be resolved. Will the "Digital

[10] "Protecting Yourself on Social Networks". *Surveillance Self-Defense*. Last seen on 04-06-2019.

[11] Grimmelmann, James (2009). "Saving Facebook". Iowa Law Review

[12] Valcke, M.; De Wever, B.; Van Keer, H.; Schellens, T. (2011). "Long-term study of safe Internet use of young children"

Age" be one in which individuals may maintain, lose, or gain control over information about themselves? In the midst of this uncertainty, there are some reasons to be hopeful. Of course, individuals operating on the Internet can use new tools for protecting their privacy.

DATA PROTECTION LAWS IN INDIA

The Government of India has notified the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The Rules only deal with protection of "Sensitive personal data or information of a person", which includes such personal information relating to:-

- Passwords;
- Financial information such as bank account or credit card or debit card or other payment instrument details;
- Physical, physiological and mental health condition;
- Sexual orientation;
- Medical records and history;
- Biometric information.

The rules provide the reasonable security practices and procedures, either the body corporate or any person who on behalf of body corporate collects, receives, possess, store, deals or handle information is required to follow while dealing with "Personal sensitive data or information". In case of any breach, the body corporate or any other person acting on behalf of body corporate, may be held liable to pay damages to the person so affected.

But it is not just individual's self-interest leading us towards increased privacy protection. Lack of privacy protections is a major barrier to consumer participation in electronic commerce, businesses are beginning to take privacy protection seriously. Numerous efforts at self-regulation have emerged; such as TRUSTe[13]. A growing number of companies under public and regulatory scrutiny, have begun incorporating privacy into their management process and actually marketing their "privacy sensitivity" to the public. The collective efforts pose difficult questions about how to ensure the adoption and enforcement of rules in this global, decentralized medium. Government is also struggling to identify their appropriate role in this new environment.

RESTRICTIONS TO RIGHT TO PRIVACY

The constitutional right to privacy in India is subject to a number of restrictions. These restrictions have been culled out through the interpretation of various provisions and judgments of the Supreme Court of India:

- The right to privacy can be restricted by procedure established by law which procedure would have to be just, fair and reasonable.[14]
- Reasonable restrictions can be imposed on the right to privacy in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or to

[13] TRUSTe, is an industry sponsored self-regulation watchdog group. TRUSTe: Building a Web You Can Believe In

[14] Maneka Gandhi v. Union of India 1978 AIR 597, 1978 SCR (2) 621

an offence; (Article 19 (2) of the Constitution of India, 1950).

- The right to privacy can be restricted if there is an important countervailing interest which is superior.[15]
- The right to privacy can be restricted if there is a compelling state interest to be served.[16]
- The protection available under the right to privacy may not be available to a person who voluntarily thrusts her/himself into controversy.[17]
- Like most fundamental rights in the Indian Constitution, the right to privacy has been mostly interpreted as a vertical right applicable only against the State, as defined under Article 12 of the Constitution, and not against private citizens.[18]

AREAS OF CONCERN

Communication surveillance in India is broad and fragmented. It is primarily regulated by two different statues The Telegraph Act, 1885 ("Telegraph Act") (which deals with interception of calls) and the Information Technology Act, 2000 ("IT Act") (which deals with interception of electronic data).

In India, there are at least sixteen[19] different intelligence agencies that have been established. Most of the intelligence agencies in India do not have clearly established their oversight mechanisms other than the departments that they report to. For example, CBI and RAW report to the Prime Minister's Office, Directorate of Revenue Intelligence reports to the Finance Ministry, and the Military intelligence agencies do not come under the purview of Parliament, the Right to Information Act, and their functions are not subject to audit by the Comptroller and Auditor General – despite these agencies being funded from the Consolidated Fund of India.

In 1996 the Supreme Court of India noticed the lack of procedural safeguards in the provisions of the Telegraph Act and laid down certain guidelines for interceptions. These guidelines formed the basis of the Rules defining the procedures of interception that were codified by introducing Rule 419A in the Telegraph Rules in 2007. These guidelines were, in part also reflected in the Rules prescribed under the IT Act in 2009. Section 69 of the IT Act, 2000 allows for the interception, monitoring and decryption of digital information in the interest of the sovereignty and integrity of India.

The "IT Interception Rules" include safeguards stipulating who may issue directions of interception and monitoring, how such directions are to be executed, the duration those remain in operation, to whom data may be disclosed, confidentiality obligations of intermediaries, periodic oversight of interception directions by a

[15] Gobind v. State of M.P 1975 AIR 1378 1975 SCR (3) 946 1975 SCC (2) 148

[16] Gobind v. State of M.P 1975 AIR 1378 1975 SCR (3) 946 1975 SCC (2) 148

[17] R.Rajagopal v. Union of India 1995 AIR 264, 1994 SCC (6) 632

[18] Zoroastrian Cooperative Housing Society v. District Registrar Appeal (Civil) 1551 of 2000

[19] National Technical Research Organization; Research and Analysis Wing (R&AW); The Aviation Research Centre (ARC) and Radio Research Centre (RRC), which are a part of the Research and Analysis Wing (R&AW); Electronics and Technical Service (ETS), which is the ELNIT arm of R&AW; Intelligence Bureau; Narcotics Control Bureau; Directorate of Revenue Intelligence; Central Economic Intelligence Bureau; Central Bureau of Health Intelligence; Denfence Intelligence Agency; Joint Cipher Bureau; Signals Intelligence Directorate; Directorate of Air Intelligence; Directorate of Navy Intelligence; Directorate of Military Intelligence; Directorate of Income Tax (Intelligence and Criminal Investigation); Directorate General of Income Tax Investigation and Joint Intelligence Committee.

Review Committee under the Indian Telegraph Act, the retention of records of interception by intermediaries and to the mandatory destruction of information in appropriate cases. Rule 3 allows the "competent authority" to issue directions for monitoring for any number of specified purposes related to cyber security.

THE AADHAAR DATA BREACH (2018)

In Justice K.S.Puttasawmy v. Union of India[20], the Apex Court unanimously affirmed that the right to privacy is a fundamental right under the Indian Constitution. The Attorney General for India had stood up during the challenge to the Aadhaar Scheme and declared that the Constitution did not guarantee any fundamental right to privacy.

Aadhaar, which means 'foundation' is a 12 digit unique-identity number issued to all Indian residents based on their biometric and demographic data. The Unique Identification Authority of India (UIDAI), a statutory body that oversees the world's largest biometric identity card scheme, following a report in The Tribune[21] claimed unrestricted access to any Aadhaar number for a paltry sum of Rs. 500. Biometric data, unlike the UIDAI'S statement, is not the only privacy concern with this breach. The disclosure of demographic data, such as an individual's name, date of birth, address, PIN, photo, phone number, e-mail, etc., is not any less of a privacy concern. This data forms the basis of many cybercrimes, be it publishing or identity theft.

WHEN CAN GOVERNMENT INTERFERE WITH DATA

Under section 69 of the IT Act 2000, any person, authorized by the Government or any of its officer specially authorized by the Government, if satisfied that it is necessary or expedient so to do in the interest of sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, for reasons to be recorded in writing, by order, can direct any agency of the Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource. The scope of section 69 of the IT Act, 2000 includes both interception and monitoring along with decryption for the purpose of investigation of cyber-crimes. The Government has also notified the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, under the above section.

The Government has also notified the Information Technology (Procedures and Safeguards for Blocking for Access of Information) Rules, 2009, under section 69A of the IT Act 2000, which deals with the blocking of websites. The Government of India has so far blocked 2388 social media URLs in 2018 under the Rule 7 Section 69A of IT Act, 2000 as per the data maintained by NCRB (National Crime Records Bureau).[22]

[20] Writ Petition (CIVIL) No. 494 of 2012

[21] Rachna Khaira, Tribune News Service, Jan 4, 2018, https://www.tribuneindia.com/news/punjab/no-formal-probe-in-aadhaar-breach-cops-come-sniffing/523829.html last seen on June 6, 2019

[22] https://www.business-standard.com/article/economy-policy/2-388-social-

CONCLUSION

The importance of right to privacy for the maintenance of dignity and integrity of an individual is beyond explanation. The legislative measures are adopted in India in this regard though seem to be enough on paper but when it comes to implementation, lack of awareness amongst the users, the internet habits of the users in India and lack of expertise amongst the enforcement agencies are presenting serious challenges.

In today's privacy politics, the strong medicine of a privacy commission will be politically infeasible until weaker medicine has been tried. In the meantime, most of us could agree that policy makers and academics alike should work to improve public understanding of cyberspace privacy.

India need to work more for enduring an effective and concrete legislation for data protection. However, while creating the laws, the legislature has to be well aware for maintaining a balance between the interests of the common people along with amicably handling the increasing rate of cyber crimes. Technological advancements such as micro cameras and video surveillance had a profound effect on personal privacy.

Everyone, be it an individual or an organization has a right to protect and preserve their personal, sensitive and commercial data and information. India at this moment needs a dedicated law protecting the data and personal privacy of an individual. A national privacy policy is still missing in India. The laws should be made keeping in mind both the genders rather than protecting only female rights. A gender neutral is as crucial as a technological neutral legislation.

For privacy intactness, proper training and awareness, monitoring and auditing, and incident response is required. Expression through speech is one of the basic needs provided by the civil society and variances in the scope of freedom of expression, combined with more online communication, has produced concerns about censorship in cyberspace. Freedom of opinion and expression should be free from any kind of political, commercial or any other influences. It should be applied in non-discriminatory and non-arbitrary manner, and also should be supported by applying safeguards against any kind of abuse, hate speeches, religion biasing etc.

Alan Westin (1967) in 'Privacy and Freedom' defined privacy as the "desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and behavior to others."[23] The absolute protection of privacy on the internet is difficult to imagine and achieve. The self-restraint by the users on his 'web-habits' is the basic solution which may yield positive results in this direction.[24]

*****

media-urls-blocked-or-removed-in-2018-under-it-act-ahluwalia-118121200628_1.html last seen on June 6, 2019

[23] Alan Westin, Privacy and Freedom, 25 Wash. & Lee L. Rev. 166 (1968) https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20/ last seen on June 6, 2019

[24] Dr. Pankaj Kakde, Right to Privacy and its Infringement in Cyberspace https://www.academia.edu/5635495/Right_to_Privacy_and_Its_Infringement_in_Cyberspace last seen on June 6, 2019

VOLUME 12 ISSN 2456-9704