ISSN No:-2456-2165

A General Perspective on Overlapping of Right to Privacy and Information Technology

[1]Arpit Vihan, Assistant Professor, Geeta Institute of Law, Panipat
[2]Bhawna, Assistant Professor, Geeta Institute of Law, Panipat

Abstract:- Eschewing the set of all freedoms, the concept of liberty sits at the soul of a democratic structure. Associated with varying connotations in different jurisdictions, Article 21 of Indian Constitution qualifies its enjoyment with the term 'personal' unlike its U.S. counterpart; probably the reason for reluctance of Indian Courts to recognize privacy as an essential ingredient of personal liberty for a long time.[1] Indian Jurisprudence is now settled on the issue of privacy and its safeguards in the modern era[2], it is nevertheless bound to face a resilient challenge while extending the guarantee in online sphere.

Online privacy being a mammoth subject; it is impossible to discuss all of its facets and the authors have confined the discussion to the most prominent privacy concerns associated with data handling and analysis, with special reference to the legal framework in India. The objective is therefore twofold: firstly, to determine the efficiency of national laws in ensuring online privacy by addressing its massive infringement by websites and the incapability of law in curbing it (Part III) and secondly, to suggest plausible remedies for the inherent flaws that exist therein considering the legal mechanism adopted in countries with a much matured understanding of privacy concerns (Part IV). Setting the stage, Part II provides an insight into the concept of online privacy, the pivotal role it plays in life and its infringement by exploitation of the cyber information pool while Part V contains the conclusive remarks of the author.

Keywords:- *Right to Privacy, ICT, Technology, IT Act.*

I. INTRODUCTION

The classic meaning of privacy, i.e., 'to be let alone' is the structural foundation that defines privacy in modern states. Extension of this foundational principle can be made to the realm of Internet. Privacy can therefore be assumed to be the security of personal data published through cyber means. It is a great cause of concern regardless of the services a user plans to avail, ranging from random social networking to huge monetary transactions. Convergence of computers with telecommunications and the advent of smart phones have paved way for an atmosphere of inexpensive and ready to access personal information pool which increments every single second, and if not handled carefully might lead to severe exploitation.

Internet privacy is economically important since it assures consumers that their personal particulars will not be released to unauthorized persons.[3] Its infringement thus poses great threat by breaching the trust of a user, detrimental to both social and economic interests. The risks it can generate include the theft of sensitive user data such as transaction PINs, bank account numbers, etc. The situation is worsened by the injection of malwares which damage both the computer resources and the data.

As far as the safeguard(s) of online privacy is concerned, Germany is probably the first jurisdiction to recognize online privacy after the abuse of information by state agencies, followed by Sweden where the high flow of personal information on the internet enabled a person to access all income tax returns by hunch of a few clicks. State agencies have ensured the security of online data by the system of encryptions, wherein no third party is legally allowed to intervene and extract the input data. In India, Information Technology Act, 2000 takes into consideration the system of key pair encryption for the recording and authentication of digital signatures.[4] The system though secure, is not infallible and there are innumerable instances of information being accessed by third parties.

Privacy interests are further jeopardized by the data collection done by websites, both explicitly and impliedly. Though one might wonder that the pop-up advertisements share utter relevancy with their cyber activities, majority of internet users are unaware of the fact that items such as banner ads, search queries, etc. are actually information receptors to Marketing Companies. They are happy to surf as long as no information is sought explicitly, and thus arises the need for massive state intervention to assure online privacy.

Cognizant of the outcomes of privacy infringement, there are multiple international directives such as OECD Privacy Guidelines, EU Data Protection Directivesand APEC Privacy Framework; all of which are designated to nullify the draconian effects of technology on privacy. Principles such as notice, consent, collection and usage limitation, access and corrections and openness cut across

[1]Kharak Singh v. State of U.P., AIR 1963 SC 1295
[2] See K.S. Puttaswamy v. Union of India, 2017 SCC OnLine SC 996, Maneka Gandhi v. Union of India, AIR 1978 SC 597; Ram Jethmalani v. Union of India, (2011) 8 SCC 1.

[3]Nandan Kamath, *Law Relating to Computers, Internet and E-commerce*, 287 (5th ed., 2012)
[4]Vakul Sharma, *Information Technology Law and Practice*, 111 (3rd ed., 2011)

ISSN No:-2456-2165

these frameworks along with the principle of enforcement. The EU Data Protection directive, OECD Guidelines and APEC framework additionally deal with the subject of Trans-border data flow, while Australia's ANPP specifically prescribes de-identification of the personal information.[5]

II. GLOBAL INFRINGEMENT OF PRIVACY: TRACING THE TRACKS

Significance of privacy in cyber space and the hardships users face thereof are now compellingly clear, which brings us to the discussion about the legal recourse available in such circumstances. However, it is preferable to discuss at first the privacy policies of the Reserve Banks of Data in India, i.e., Google and Facebook[6] to gauge the magnitude of infringement committed by them which would render help to test the logicality of Indian statutory provisions.

- *Google: The cyber spy*

The Privacy policy of Google states that Google collects information regarding device, IP addresses, user location, unique application numbers, cookies and similar technologies.[7] The fundamental question which arises at this juncture is, whether it conforms to the international standards and whether the information thus gathered is limited in usage or not. The policy itself offers some answer to it. Attention is sought to be laid on the highlighted words, which lead to the inference that Google can and will utilize data of any user if it is of some interest to Google itself, which if further interpreted means that Google is authorized to scrutinize every single bit of data to *protect Google*![8]

The policy further provides, *"Our automated systems analyse your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. We use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services..."*[9]

It should be mentioned here that cookies are small textual pieces sent to the web browser by a website visited by the user, and helps the website to remember information about the visit for the sake of future convenience. On the other hand, pixel tags are a kind of technology placed on a website or within the body of an email for the purpose of tracking activity on websites and are often used in combination with cookies[10].Pixel tags (web beacons) work and monitor activities even when a user is working on his/her e-mail. Google also provides personal information to its affiliates or other trusted businesses in compliance with its Privacy Policy or any other appropriate confidentiality and security measures.[11]

- *Unethically asocial Facebook*

While most of the policies of Facebook are synchronous with internationally recognized privacy standards, it provides, *"We offer a range of products and features that involve the use of these (Cookies, pixels and similar technologies) to reach you, based on your activity on and off our services.*[12]*"*

In implication, cookies monitor online activities of the user even when he has left the server.[13] It is a common experience that while browsing Facebook, the advertisements which are displayed are the ones which are relevant to us which is because the cookies sent by Facebook, as per the policy "*serve you ads that may be interesting to you on Facebook Services or other websites and mobile applications*[14]*".*

- *Byte-ing Cookie: Notsotasty*

A glimpse through the privacy policies of leading websites makes it amply clear that cookies are stored in the computer without user's consent and monitors the activities of the user even when (s)he has left the website. Though the browser provides settings using which cookies can even be turned off, many leading websites don't work properly on enabling such settings and users are forced to allow cookies, citing the absurd reason of improved user experience and overall service quality[15]. The targeted use of cookies is thus to monitor consumer habits which is unethical and illegal because such collection lies beyond a reasonable expectation of privacy and the collected information is deceitfully centralized.[16]

Since cookies are unwelcomed guests on a device, a typical computer user has no knowledge that cache files, temporary files and log files are being stored on his computer.[17] The international directives and principles speak vehemently that information should be collected with

[5] *Report of the Group of Experts on Privacy*, Planning Commission of India, available at http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf,

[6] *Top Sites in India*, Alexa, available at http://alexa.com/topsites/countries/IN,

[7] Ibid.

[8] https://static.googleusercontent.com/media/www.google.com/en//intl/en/policies/privacy/google_privacy_policy_en.pdf,

[9] Ibid.

[10] *Key Terms*, Google Privacy Policy, available at https://www.google.com/policies/privacy/key-terms/#toc-terms-pixel,

[11] Supra 8.

[12] *Privacy*, Facebook Help Centre, available at https://www.facebook.com/help/cookies/update,

[13] *Cookies*, Razorian Fly, available at http://razorianfly.com/cookies/, last seen on 25/03/2019

[14] Supra 14

[15] Supra 8

[16] Daniel Lin, Michael C. Loui, *Taking the Byte Out of Cookies: Privacy, Consent, and the Web*, Seventh Annual Meeting of the Association for Practical and Professional Ethics, Dallas, TX.

[17] Supra 12.

ISSN No:-2456-2165

consent of the user which should be an informed consent and the same is missing with respect to cookies.

It should be noted here that the directives issued by European Union allow websites to link actions of users during a browsing session for a variety of purposes which should be disposed on the expiry of the session or might even be stored on the device provided that the cookies must tell people that the cookies are there, explain what the cookies are doing, and obtain their consent to store a cookie on their device.[18]

- *Revenge Porn: Increasing menace and privacy concerns*

Revenge Porn is the sharing of private/sexual materials of another without their consent for the purpose of causing embarrassment or distress.[19] The content is sometimes accompanied by personal information about the subject, including their full name, address and links to their social media profiles. Revenge porn has a widespread nature, for that it travels faster with viewers multiplying exponentially and requires no expenditure to be made. Moreover, many targets hesitate to complain the ugliest form for infringing privacy for fear of being shamed and blamed.[20] Violation of sexual privacy, notably the non-consensual publication of sexually graphical images is a breach of trust and deserves criminal punishment. Denying subjects' ability to decide over sexual exposure to the public, it produces gross emotional and dignitary harms along with increasing the risks of physical assault.

Apart from the privacy concerns associated with private players, infringement of privacy by the state as a security measure is also a debatable issue. Cyber security cannot be enhanced without a proper understanding of the relationship between security and other national imperatives, primarily privacy[21]. A balance need be struck between the conflicting interests of privacy and national security applying the theory of social engineering[22]. On the contrary, statistics reveal that 708 URLs were blocked in 2012, 1,349 URLs in 2013, and 2,341 URLs in 2014, grounds of which are undisclosed.[23]

III. INDIAN LAWS: ARE WE PREPARED?

Indian law relating to online business is primarily governed by The Information Technology Act, 2000, which hardly recognises any concept of online privacy. It is sad to see that the objective of the Act clearly purports that the act is intended to deal with e-commerce and provides legal recognitions to these transactions.

There are tinctures of privacy concerns in an ocean called the IT Act, with S. 72 apparently being the single big molecule; which punishes an individual who, in pursuance of any of the powers conferred under the Act, rules or regulations made there under, secures access to any data and discloses it to third parties without consent.[24] The provision penalises those who abuse any of the powers conferred under this act, which necessarily restricts its application only on those empowered under this Act and excludes from its purview the entities such as private citizens, search engines and social networking sites.

The criminalization of privacy infringement, especially revenge porn is of utmost necessity to guard the citizens against devastating privacy invasions that chill self-expression and ruin lives[25], and the provisions of Privacy Bill, 2011 can come handy in achieving the target object.

The bill provides that every citizen shall have right to privacy and shall not be infringed except in accordance with procedure laid down in the Bill.[26] It states that the collection and disclosure of personal data, monitoring cyber activities, sending unsolicited communications shall constitute infringement of privacy[27].

[18] *Guidance on the rules on use of cookies and similar technologies*, The Privacy and Electronic Communications (EC Directive) Regulations, 2003, available at https://ico.org.uk/media/for-organisations/documents/1545/cookies_guidance.pdf, last seen on 27/03/2019.

[19] Olivia Wilson, *Revenge Porn Is More Than a Violation of Privacy: It Is Digital Sexual Assault*, The Huffington Post (26 June 2015), available at http://www.huffingtonpost.com/olivia-wilson/revenge-porn-is-more-than_b_7641876.html?ir=India&adsSiteOverride=in, last seen on 27/03/2019

[20] Sandhya Soman, *The seedy underbelly of Revenge Porn*, Times of India (23 August 2015), available at http://timesofindia.indiatimes.com/tech/computing/The-seedy-underbelly-of-revenge-porn/articleshow/48627922.cms, last seen on 27/03/2019

[21] Sunil Abraham, Elonnai Hickok, TarunKrishnakumar, *Security: Privacy, Transparency and Technology*, 2 CyFy Journal 107, 109 (2015).

[22] Ibid.

[23] Ministry of Information and Communications Technology, Government of India, No. 14 (74)/2014-ESD, available at http://sflc.in/wp-content/uploads/2015/04/RTI-blocking-final-reply-from-DEITY.pdf, last seen on 28/03/2019

[24] S.72, The Information Technology Act, 2000.

[25] Danielle Keats Citron**,** Mary Anne Franks**,***Criminalizing Revenge Porn*, 49 Wake Forest Law Review 314, 345 (2014).

[26] S. 3, Privacy Bill, 2011.

[27] S. 5, Privacy Bill, 2011.

ISSN No:-2456-2165

IV. FIXING THE FLAWS IN PRIVACY LAWS: REMEDIAL REMARKS

While addressing the flaws in legal framework of India while dealing with infringement of privacy, lead can be taken from other jurisdictions as remedial inputs. In the US, privacy protection is essentially liberty protection, i.e. protection from government.[28] The Privacy Act of 1974 can generally be characterized as an omnibus "code of fair information practices" that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies. The law with respect to privacy is further governed by a plethora of statutes such as The Electronic Communications Privacy Act of 1986, The Right to Financial Privacy Act and much more. Advancing a step ahead, legislations protecting right to privacy in private sector have also been enacted such as The Fair Credit Reporting Act (FCRA), The Identity Theft and Assumption Deterrence Act, The Children's On-line Privacy Protection Act, etc.

In Canada, privacy protection is focused on individual autonomy through personal control of information. [29] Canadian Government relies on the methodology of personal control to ensure privacy which holds well only with the presumption of a bona fide intention of all the citizens. However, the self-regulatory scheme can be effective only if businesses choose to become a part of it. While there are a large number of businesses likely to get on the bandwagon because they are already committed to privacy concerns or to gain commercial advantages, a larger number of businesses would still be opposed to self-regulation when there is no sanction to breach.[30] Further, such a model shall cease to be effective in the social context of India with huge social disparity unlike the egalitarian society of Canada.

- *SEAL Programmes: Certifying Trust of Users*

SEAL programmes render a highly significant solution to the concerns of cyber privacy by deploying agencies to certify websites based on their privacy policy and display the same on its home page so that whenever a user accesses it, he gets to know as to what the shall be repercussions of using the website on his privacy. This methodology is neither too harsh for the implementers to abide by, and assures an informed consent from the user.[31]

V. CONCLUSION

Infringement of privacy in cyberspace has become a global concern and it is no exaggeration to state that assurance of its safeguard in present circumstances is a myth owing to the macro level data analysis by almost all market players. While the Indian law stands absolutely helpless to cease such violation of privacy, the provisions of Privacy Bill, 2011 can be witnessed as a yardstick of change. Moreover, there are bulks of foreign statutory provisions as well as methodology as discussed above; which can be engaged to cater to the concern so as to keep the fundamental right to personal liberty alive and intact.

[28]Avner Levin and Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 7 University of Ottawa Law and Technology Journal 327, 330 (2015).
[29]Ibid, at 332
[30]Supra 4, at 400
[31] Certification Standards, Truste, available at https://www.truste.com/privacy-certification-standards, last seen on 29/03/2019