International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

PRIVACY ISSUES IN CYBERSPACE: AN INDIAN PERSPECTIVE

Amit Kumar Gupta
Research Scholar, The Glocal University, Saharanpur, U.P

Dr. Dharm Pal Khatri
Research Supervisor, The Glocal University, Saharanpur, U.P

ABSTRACT

Cyber privacy is contentious and as yet unsolved subject in legal jurisprudence all throughout the globe. In the new century, the existing cosmos is enveloped by the force of new mantra called 'Information Technology'. Knowledge abounds in the era of the "Information and Communication Technology Revolution," and this unprecedented plethora of information has dramatically pushed the issue of personal privacy to the forefront of the field of Jurisprudence. It's questionable how far residents in democracies would go to reveal private information. Cyber spying, cyberstalking, corporate espionage, devastating cyber-attacks, and website defacement pose serious threats to online privacy, but it is the obligation of the legal sector to craft a sufficient policy to defend it. The growing commercialization of the Internet and the development of new and more powerful information technologies have heightened these worries in recent years in India, the United States, and other countries. Cyberspace is shorthand for the web of consumer devices, computers, and communication networks that interconnects the globe. To be privy to one's own thoughts, feelings, and actions without interference from others is the essence of privacy. The right to privacy in cyberspace is protected by the current legal framework. The current study article consequently focuses at investigating the situation of Privacy in Cyber Space in India. India must do more to ensure that its data protection law is both effective and tangible.

Key Words: Cyber Privacy, Cybercrimes, Fundamental Right to Privacy, The Information Technology Act, 2000.

INTRODUCTION

A worldwide, inventive, and Internet-reliant "Digital Society" runs on the cheap and plentiful gasoline provided by the information and communication technology sector. There have been significant security risks to critical national infrastructure as a result of the rapid development of cutting-edge Computer Science technology and its ability to collect, store, and analyze vast quantities of personal information. The delicate and apparently unsolvable issue of nearly limitless internet freedom has prompted a rethinking of privacy norms in the digital sphere. More and more people are using the internet, and many of them are making their private lives public by posting details about themselves on social media websites. This includes details about their schooling, their relationships, their families, their interests, and even their hobbies. Because to this, sensitive information was exposed, including the KOOBFACE, which was stolen in a fraud. KOOBFACE is malicious software with several different parts. Each part performs a different purpose.

KOOBFACE is unique among malware in that, rather from cramming all of its features into a single executable, it separates them into several files that work together to create a botnet.

Since entering the online realm, nearly nothing has remained secret. By providing a safe haven for users' private data, privacy protection helps make it possible for more people to enjoy the many advantages the Internet has to offer. Exposure of sensitive, personal information to unexpected parties as well as financial losses are only two of the many negative outcomes that may result from a breach of privacy. Every time someone clicks their mouse on the Internet, a digital trail is left behind, usually without the user even knowing it. These digital traces give valuable insight into the user's personality and pursuits thanks to the information they carry. Credit bureaus, payment processors, businesses, tax authorities, service providers, ad networks, and social media all collect private data online. It's a rather typical practice to make use of cookies, which the user's browser then installs on their hard drive. Without the user's knowledge or consent, certain cookies may transmit sensitive information about the user to an advertising agency, which may then share this information with another advertising agency in the same or a different line of business. In the eyes of the world, this is a major problem.

LITERATURE REVIEW

Johnson, Swartz, & della Cava, (2016) After the FBI was unable to get access to the shooter's iPhone, the company was forced by a judge to do so. Since the company claims it would have to develop a modified version of iOS to unlock the phone, it has chosen to challenge the ruling in court. After locating a third party to help unlock the phone, the FBI ultimately retracted their request, but the situation reignited discussion about many areas of privacy and governmental spying.

McMillan, (2016) In 2014, Yahoo said that hackers had broken into their system and stolen information connected to more than 500 million user accounts. The corporation has made what is likely the greatest breach disclosure in history.

Brustein, (2015), In February of 2015, RadioShack, a household name in American consumer electronics, declared bankruptcy. It auctioned out the personal information of over a hundred million clients. Several parties are challenging RadioShack's right to make this transaction, with some arguing that the data is not RadioShack's to begin with and others alleging that the retailer is breaching its own privacy standards.

Marc Pelteret (2016) In today's technological age, when information can be quickly taken, saved, and shared, protecting individuals' privacy has become more crucial. It has been front and center in the news media and the focus of legislation on every continent in recent years. Despite decades of study across many disciplines, privacy continues to be a nuanced and intriguing topic with plenty of room for exploration. To prove its significance to both consumers and businesses, this article presents a narrative summary of the nature of information privacy by highlighting the intricacies and obstacles that each encounter when making choices about it. With this work as a foundation, we give a multidisciplinary perspective on consumer-focused information privacy research. It shows the issues that bother people and the aspects that go into people's and businesses' privacy choices. We hope that this perspective will inspire further interdisciplinary study of this important topic.

Mark Burdon (2012) In response to the widespread unauthorized exposure of personal information by public and private sector entities, legislation mandating the notification of affected individuals after such a breach has been enacted. Legislative interest has been piqued all over the globe since these laws were first enacted at the state level in the United States

during the previous decade. We argue that obligatory data breach notification regulations are not as broadly applicable as they would seem, both conceptually and practically, especially in light of preexisting information privacy law frameworks. In this article, we highlight these concerns in the context of recent legislative developments in the European Union and Australia.

THE LACK OF PRIVACY IN CYBERSPACE

There seems to be some ambiguity in cyberspace, as there is in the modern physical world, about what constitutes and what does not constitute privacy. According to Ruth Granson, "the notion of privacy is a crucial one in most debates of contemporary Western culture, but only lately have there been serious attempts to understand what what is meant by privacy." The definition and scope of privacy have been dramatically distorted throughout the years. As many people as there are who study privacy in the legal and academic communities, there are just as many different definitions and notions of privacy. Judith DeCew, another academic, investigates multiple understandings of privacy: "Different legal experts have different notions of what constitutes private. Because the concept of privacy can refer to the partitioning of spheres of activity, the restriction of governmental authority, the prohibition of knowledge and experience, the restriction of access, and the conception of group membership, it is often taken to encompass a wide range of related topics." The concept of privacy as a means of seclusion for a person has evolved significantly.

Once upon a time, a person's safety was ensured by the logistical boundaries erected by geography. However, there is another another aspect that has undergone significant alteration. Neither our legal system nor the creation of the Internet or, more recently, the World Wide Web are to blame for the collapse of the geographical wall of protection. The absence of these once-impassable walls is not reflected in the current body of knowledge. In today's world, "effective protection of personal data and privacy is emerging into a crucial prerequisite for societal acceptance of the new digital networks and services." Even in the safety of one's own house, one cannot presume privacy. Instead, privacy is considerably more difficult to build and defend since it is so much easy to breach. There hasn't been much of a shift in how we think about personal privacy throughout the years, and in some situations, people have actively fought against new ways of thinking. Despite this, privacy has grown from a niche industry to a multifaceted behemoth. We need a fundamental paradigm change in our understanding of privacy. For now, "privacy" should be considered a cornerstone idea, much like "life," "liberty," and "the pursuit of happiness," all of which are fundamental to our society. To make progress toward this paradigm shift, it's important to look back at the history of the concept of "privacy" in popular culture and consider how it has developed through time so that we can assess the entire effect of new technology..

SECURITY AND PRIVACY ISSUES RELATING TO TECHNOLOGY AND THE LAW CRIMES OVER CYBERSPACE

When computers and the internet are utilized in the court system, questions regarding the privacy of information exchanged and stored on them inevitably emerge. During a legal case, you could have to provide personal details about your finances, health, or family. The parties involved in the disclosure will typically only wish to make the information available to those who require it to carry out the agreed-upon work. Every time you gather, store, or transmit sensitive information, you raise the likelihood that it may fall into the wrong hands. It's partially

due to the fact that there's more area for data to expand, and partly due to the fact that there are more opportunities for data to be compromised in digital form. Concerns about personal information being compromised due to the widespread use of computers to access legal publications are a real possibility. Access to potentially relevant personal information for a legal report has also been simplified by technological advancements. In addition, there has to be a trustworthy method of identifying the author of any particular piece of digital information.

In order for a message to be trusted, for example, it must be possible to determine with absolute certainty that a document has not been altered in any way. If these problems can be fixed, then a computerized court system may be trusted and secure. In the absence of adequate guarantees of security and a respect for the privacy of information, the rise of electronic judicial procedures is unlikely to be universally welcomed by the legal profession and the wider public. this study delves into privacy concerns in terms of ensuring the safety of data during transmission and storage. It does so by detailing how much security the current legal system must provide. The article then evaluates the feasibility of complying with the mandated standard by using presently accessible technological solutions. We conclude by assessing whether this level of security is enough to deal with safety concerns posed by computerized court proceedings. In Section 3, we explore privacy concerns surrounding the circulation of PII via electronic law reports. It clarifies the need for law reports and why the rules now in place permit some details to be left out of them. The report concludes by assessing whether or not the current legislative provisions provide adequate remedies for any privacy issues that may arise.

Hacking: To "hack" is to get access to a computer or network without permission and alter its settings in a way that prevents the intended user from using it. An invasion of both data and personal privacy. A woman's whole profile is changed to something filthy and nasty, making it clear that the hackers' goal is to humiliate her. People cast aspersions on her moral fiber and purity. Several popular social networking platforms allow users to tailor their privacy settings and keep their accounts confidential, including Facebook, Orkut, Instagram, etc. People who have their privacy violated by a profile may also register a complaint with them.

Cyber Stalking: Stalking is defined as "a healthy pursuit or attitude." It may be used for what is known as "online harassment," in which an individual makes repeated attempts to track another individual's whereabouts and activities over the internet. In this kind of cyberbullying, the offender repeatedly sends vulgar comments to the victim through email, as well as posts threatening or harassing messages on the victim's favorite message boards and enters the chat rooms where the victim often hangs out. Although both sexes may be victims of cyber stalking, women, particularly those between the ages of 16 and 35, are more often targeted by male perpetrators. We estimate that women make up over 75% of the casualties. By using the victim's identity, the stalker will access their personal information such as their name, family history, phone numbers, and daily routine, and then publish this information on dating service websites. It's a euphemism for keeping tabs on someone in a covert manner, or "hide hunting." It refers to persistent, unwelcome attempts at social interaction that may make a person feel intimidated or harassed. For e.g., The stalker in the case of Ritu Kholi published her home phone number and solicited calls from random people. Because of this, she began getting calls at inconvenient times, casting serious doubt on the stability of her marriage. The stalker was arrested when she filed a complaint against him for violating the modesty of a woman (Sec. 509). Another case in point is the DU Case, in which a law student from Delhi University fabricated online personas for a woman after she rejected his marriage proposal. He went so

far as to upload photos of the woman, claiming she was his wife. As a result, the girl filed a complaint under Section 66A of the Information Technology Act, stating that she had been the target of cyberstalking and identity theft. Another lady, 28-year-old Neha Ghai, was taken aback when she began receiving offensive phone calls, text messages, and sexually explicit emails. As a result, she went to the cyber cell and learned that she had been the target of cyber stalking and had been tracked online.

Cyber –Bullying: These days, all it takes to connect with someone else is a click of a button, thanks to the incredible advancements in technology. However, this action exposes them to many risks. In most cases, bullying occurs when one person uses his or her greater power to coerce another person into doing something. Consequently, cyberbullying is the use of the Internet to coerce another individual into doing an action. Using a mobile phone or other electronic device to harass or threaten another person. Bullying in the digital era is defined as "the intentional and repetitive damage perpetrated by using computers, mobile phones, or other electronic devices by sending messages of an intimidating or threatening character." 15 For.e.g., The child, just 12 years old at the time, had her photo used as her profile picture and was subjected to online threats because of it. Someone who lives in her area has threatened to use her personal data.

Harassment via Emails: Electronic mail (or email) is the transmission of text or files from one computer to another through the Internet. If that's the case, then it's impossible for there to be cyberbullying. The material in question might be a letter, email, or other written communication that includes an incitement to violence. Emails may be used to harass in many different ways, such as by sending repeated love proposals, blackmailing, etc.

Voyeurism: When used as an adjective, it refers to the practice of engaging in sexual gratification through seeing other people when they are undressed or engaging in sexual behavior. The Merriam Webster Dictionary describes voyuerism as the practice of receiving sexual enjoyment via seeing others. Leaks of private movies and photos are commonplace on the internet, where they are often viewed with glee. There is a parallel to be drawn with pornography. Is pornography the individual themselves in engaged or is forced to become involved. Conversely, voyeurism is the questioning of a person's modesty by photographing or filming them when they are undressed. The victim is completely unaware of any of this. For e.g., Many women are filmed as they change their clothing in the dressing room and such recordings are shared on social media which is evident act of voyeurism.

Morphing: The term "morphing" refers to the practice of altering a photo of a person by another person before distributing it online. Morphjacking occurs when a malicious individual poses as another person online in order to steal photos from another person and then uploads or reloads the edited photos. 16 When an image is uploaded to a social networking site like Facebook, Orkut, etc., it may be easily copied and uploaded again by users with phony accounts, which amounts to identity theft and morphing.

Email Spoofing: A faked email is one in which the text is taken verbatim from an actual email but the context is altered to give the message a false sense of authenticity. E-mail spoofing is the forging of the original e-mail header with different content and origin. Email spoofing refers to the fraudulent practice of altering an email's header information so that the recipient does not recognize the sender as the original sender of the message. By modifying some attributes

of the email, such as its header, from, Return-Path and Reply- To fields etc., hostile users may produce faked email.

Cyber Defamation: Publishing material that may incite anger, ridicule, or harm the reputation of the target among the reasonable members of society is considered defamatory. Cyber defamation is posting of negative information against another person via the internet which may impair the individual's reputation and image. For e.g., A nasty customer review against a firm might damage a tiny business . An unjustified charge of infidelity has the potential to ruin an otherwise fulfilling marital relationship. Though it may take years to construct anything, it may be destroyed in a flash.

Cyber Pornography: In this context, "pornography" refers to any visual media that graphically depicts or describes sexual organs or sexual action. Internet sexually explicit content is called cyber pornography. It's the production, dissemination, and exhibition of pornographic or obscene materials and the arousal of sexual desire over the Internet. A Swiss couple in Mumbai, for instance, rounded up a group of young kids and subjected them to sexual abuse. As also, they posted it online for everyone to see. It was an obvious case of cybershaming, in which young children's modesty was violated.

CONCLUSION

As the digital economy has developed over the last decade, the need for increased cybersecurity measures has become universal. The 'Internet of Things,' which includes wearables,'smart' home gadgets, autonomous cars, and unmanned aerial systems, has also contributed to the growing significance of cybersecurity in recent years (also known as drones). Yet against this background of digital transformation, it is becoming obvious that both the public and private sector are failing to keep pace with cybersecurity risks. Various legislative and regulatory initiatives have been implemented in India to improve data protection and privacy. The primary conclusions from this study about data protection and privacy in India are: Indian law and policy provide some degree of confidentiality and privacy for personal information. There are number of laws in India which safeguards specific areas of data protection and privacy. Legal framework includes the Indian Constitution, the Information Technology Act of 2000, the Indian Contract Act of 1872, the Copyright Act of 1957, and the Indian Penal Code of 1860.

REFERENCES

1. Johnson, K., Swartz, J., & della Cava, M. (2016, March 29). FBI hacks into terrorist's iPhone without Ap-ple. USA Today. Retrieved from http://www.usatoday.com/story/news/nation/2016/03/28/apple-justice-departmentfarook/82354040/

2. Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. Busi-ness Horizons, 59(3), 257–266.

3. Brustein, J. (2015, March 24). RadioShack's bankruptcy could give your customer data to the highest bid-der. Retrieved April 24, 2015, from http://www.bloomberg.com/news/articles/2015-03-24/radioshack-s-bankruptcy-couldgive-your-customer-data-to-the-highest-bidder

4. Pelteret, Marc, and Jacques Ophoff. "A review of information privacy and its importance to consumers and organizations." *Informing Science: the International Journal of an Emerging Transdiscipline*, vol. 19, annual 2016, pp. 277+. *Gale Academic OneFile*, link.gale.com/apps/doc/A485809228/AONE?u=anon~cc2400aa&sid=googleScholar&xid=3f3bb486. Accessed 20 Aug. 2022.

5. Burdon, M., Lane, B., & Von Nessen, P. (2012). Data breach notification law in the EU and Australia - Where to now? Computer Law and Security Review, 28(3), 296 - 307. https://doi.org/10.1016/j.clsr.2012.03.007

6. Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. Information Systems Journal, 23(5), 401–417.

7. de Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? Computer Law & Security Review, 32(2), 179–194.

8. King, N. J., & Raja, V. T. (2012). Protecting the privacy and security of sensitive customer data in the cloud. Computer Law & Security Review, 28(3), 308–319. http://doi.org/10.1016/j.clsr.2012.03.003

9. Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academy of Sciences, 110(15), 5802–5805.

10. Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. Busi-ness Horizons, 59(3), 257–266.

11. Peters, R. M. (2014). So you've been notified, now what: The problem with current data-breach notifica-tion laws. Arizona Law Review, 56, 1171–1202

12. Ponemon Institute. (2015). 2015 cost of cybercrime study: Global (Research Report). Traverse City, MI: Ponemon Institute.

13. Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. Information Systems Research, 22(2), 254–268.

14. Trepte, S., & Reinecke, L. (Eds.). (2011). Privacy online: Perspectives on privacy and self-disclosure in the social web. Berlin, Germany: Springer Science+Business Media.

15. Rubinstein, I. S. (2013). Big data: The end of privacy or a new beginning? International Data Privacy Law. Retrieved from http://idpl.oxfordjournals.org/content/early/2013/01/24/idpl.ips036.abstract