JCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol. 9, Issue.5, May 2021 E-ISSN: 2347-2693

Privacy Protection - Emerging Issues and Technological Responses

Ayush Gupta[1*], Manvi Gupta[2]

[1]Faculty of Computer Science and Engineering, University of Turku
[2]Faculty of Law, Vivekananda Institute of Professional Studies, New Delhi, India

[*]*Corresponding Author: ayush.a.gupta@utu.fi, Tel.: +358 466803764*

DOI: https://doi.org/10.26438/ijcse/v9i5.4754 | Available online at: www.ijcseonline.org

Received: 07/May/2021, Accepted: 18/May/2021, Published: 31/May/2021

Abstract – Privacy protection as a process of collection, processing and dissemination of Information is a burgeoning issue that is challenging researchers, scientists and regulators. A universal ethical concern of the organizations, individuals and society at large is how the Information is accessed and manipulated. Technology creates implications for the privacy of people in a variety of areas, and privacy Issues appear at a variety of platforms calling for the formation of standards and regulations. The regulations are still evolving and are not optimal since the technological contexts are highly dynamic. Our paper presents the privacy trends, regulation of privacy in some standard frameworks, technological contexts and emerging ethical considerations. We also highlight the ethical issues with privacy protection and motivates to develop new methodologies to handle privacy from a both legal and technological perspective. The technological context and legal framework go together for the protection of privacy. However, privacy issues are complex and will continue to evolve. People have to find the best ways of handling ethical issues in specific situations. Researches on the protection of privacy in various computing environments may be carried out given a specific technology environment that can in customizing for region-specific legislation.

Keywords - Privacy, Regulation, Standards, Data Security, GDPR, Technological Responses

I. INTRODUCTION

In the current times when technology is growing very fast, there is a flood of information which leads to various ethical and legal issues of which the right to privacy is prominent and has large implications. Ethics in general defined as a set of actions that are carried out within the criteria of being recognized as good. In the context of IT, the rational and honourable behaviour of people and organizations with respect to the security and privacy of Information can be regarded as Ethics. In today scenario world generating a huge amount of data on a daily basis directly hyping the privacy issue. "Data privacy describes the user's data must be utilized for its intended reason". Privacy can be defined as an individual condition of a human being characterized by exclusion from publicity [1]. In modern organizations, we find that there is a compliance officer who is responsible for the assurance of data privacy. Privacy is the right of every user, so every government or non-government organization needs to work on it. Today, data privacy is also a part of customer trust in the organization [2].

Data privacy is a very broader term that includes different forms of data which represent different dimensions [3]. Privacy includes the personal feelings, and a person's choice of selection related to society, religious practices, food and travel, everything which is directly concerned to a specific person, and it varies from person to person. Privacy of behaviour and action includes the things which are concern with people's sensitive issues, just like sexual preferences and the actions which a person wants to perform in public space or private space. Privacy of personal communication deals with the channel of communication and the use of mother tongue language at a public or private place. Privacy of data and image ensures the data of the person must not be available for others to perform the different types of editing or artwork over it. Privacy of thoughts and feelings imply that people must have right about not to share the feeling about anything and that not to be revealed publicly if he did privately. Loss of privacy of location and space imply applications collecting personal data and sharing over the web without the permission of the intended user, and if the user denies any particular option, then the application not performs appropriately. Privacy of association (including group privacy) includes all social groups as well, where one user can see the other user's personal group information. Privacy is different from secrecy in the sense that a set of data needs to be kept confidential for a variety of purpose but may not reflect on an individual when it is made public.

If the protection of privacy is not ensured, the privacy itself is meaningless. It is the fundamental right of a human being. Willingly, they can share their data, but without permission, if the data is parted to another person and organization, it is ethical. Leakage of personal data or Information creates trouble for peoples, and it hurts a person performance personally or professionally [4]. It creates unnecessary competitions and damages the reputation of a company or individual, so it becomes the biggest issue for all organizations [5]. Social networking platforms sharing their user's data for their personal or commercial benefits, which creates complexity for end-users [6]. The financial loss due to privacy breach these days can be substantial to people and organizations.

Privacy Framework is typically required to build better privacy grounds for organizations where users can save their data with an open mind. This framework defines the basic structure of the implementation of data privacy, which we can use to gain the end-user's trust by providing privacy on their data. The Privacy Framework consists of three parts: Profiles, Core and Implementation Tiers. Each layer strengthens the privacy of the end-user data, which may belong to the student, professional or academician category [7].

(a) The Core enables a dialogue—All privacy protection activities take place from top to bottom.
(b) Profiles-Enable the prioritizing, which gives most suitable set of activities which meets the organizational needs.
(c) Implementation Tiers-It provides the support for whole processes related to the management of the data privacy

Data privacy becomes a higher priority for all government and private organizations for developing the best data privacy framework but data privacy framework policy will vary from organization to organization. A kind of framework structure is required which targets all vulnerable activities and meet the expectations of the organizations by which they gain the trust of the third parties. The concerns of privacy differ across entities and context, thus requiring different privacy protection responses [8] has stated various reasons why organizations need a privacy framework. Though data protection and privacy regulations worldwide are intended to be similar, many MNC companies face issues in data privacy because privacy policy varies from country to country. At whatever point protection is undermined, it harms both the organization and the client. A privacy framework is needed to ensure the less likely occurrences of data privacy attacks. Frameworks are the fast track to compliance and risk management. The framework provides the set sequence of activities for data privacy and security. Privacy law is subject to change; the framework must be sufficiently capable of adapting to the new changes in laws. Whenever the merger or acquisition issue comes into the picture, the frameworks guide to implement the data privacy or guide how to isolate the data of both companies on the same space. This paper presents the privacy trends, regulation of privacy in some standard frameworks, technological contexts and emerging ethical issues and considerations.

In this paper, we have analyzed the literature and published opinions of experts and analysts to highlight the data privacy issues in a technological context. We have highlighted the ethical issues with privacy protection and motivates to develop new methodologies to handle privacy from a both legal and technological perspective. The paper is organized as follows. The introduction part (Section I) discusses the issue of privacy framework in the technology context. Section II describes the privacy trends and implications. Section III provides an overview of the regulation, and Section IV discusses the technological responses. Section V presents the privacy issues in a technological context, and Section VI shows the Emerging Issues and Ethical Considerations. Finally, Section VII concludes the paper.

II. Privacy Trends and Implications

An analysis of the literature and opinions of experts and analysts reveal the following emerging data protection and privacy trends.

Privacy culture and public awareness – the awareness and protection of privacy have been growing with the pace of technology. It is required that privacy awareness should increase in an almost similar ratio as technology [9].

Privacy landscape will increase in complexity - Many countries like India and China are in the continuous process of promulgating privacy regulations similar to GDPR. India and China are in the race of creating their own tech hub, so they must need to create and plan about the data security and privacy procedure of their data.

Uncertainty over international data transfers will persist - The uncertainty on the manner and quantum over international data transfer is likely to persist.

Privacy Professional will have a mature view of automation potential. During the covid situation, many privacy and other professionals worked from different location. They stored their data according to their understanding without following any standard norms and procedure, which creates a problem for all industries. So, now it becomes complex to store that data in such a manner that helps in performing different types of mining or extraction operations over it.

Common view on the use of encryption - Due to end to end encryption algorithm people share some illegal data which is not tracked by the legal authorities, and when they try to explore the Information about that data by communicating with the end-user then it becomes more complex for them to get access on that data by asking the key from end-user.
In the year 2020, it is confirmed by penetration testing firm that half of the total data breaches attacks are connected to ransomware. According to Heidi Shey, a senior security analyst, these attacks not only about the data security and privacy attacks, but these attacks target the CIA triode as well.

An increase in privacy laws implies an increase in costs of data collection - The cost of data collection has gone up significantly because of the multiplicity of privacy of laws since a large diversified bunch of professionals are required for compliance. Today, we depend on lots of smart or IOT based gadgets for our daily routine tasks, and they lack in implementation of proper data privacy or security policy. It creates the most vulnerable situation for our data.

Collecting fewer data makes more sense - Due to the collection of the massive data from a different application, it requires much space along with the sound algorithms for saving it securely. It takes lots of efforts and resources. So, companies need to store only limited data of their customers as well as employees.

Privacy gets senior management attention in organizations - today, data privacy is the major concern for the whole industry, and the end-users are also concerned about it. As the users of the latest technologies getting increase day by day along with this awareness of data security or privacy are also getting an increase in the same manner. So, the companies which are involved in the end-user data handling need to take this issue seriously or on priority; otherwise, they have to lose their users. As we have a recent example of WhatsApp social app, which is declared earlier about the change in the data privacy policy in which they mentioned to sharing of WhatsApp user data with Facebook. It poses a negative impact on their users, and immediately due to this lot of WhatsApp users switched to other alternative applications.

Ransomware's rise makes data availability increasingly important - With the growth of ransomware, data security and privacy has become increasingly important. In many recent cases, it has been seen that data security isn't just about the data, but it also includes the data being stolen and destroyed.

Disinformation becomes a greater data threat - Attackers using misinformation for targeting the end user's data over the web in a recent couple of months. Companies need to build strong relationship and communication with their clients for better adoption and implementation of data privacy policy.

According to the Gartner report of 2020, privacy regulations will cover 65% of the relevant population in the near future. However, multiple regulatory frameworks will create complexity, especially for companies operating internationally. According to experts, the companies would prefer to extend their data privacy rights over and above the jurisdictions to streamline with the international regulatory framework. An emerging issue for various countries, including US would be tackling the global regulatory framework through patchworks or complete modifications in the existing laws.

III. REGULATION OF DATA PRIVACY

Data privacy is directly or indirectly regulated in various nations depending upon the context and forms in which breach occurs. Legal Right to Privacy is protected by the constitution in various societies of a democratic nature, and we find a variety of Legislations to protect privacy. In Finland, the right to privacy is postulated as a fundamental right under the Constitution of Finland. The general law that deals with the collection, storage and use of personal data is GDPR, Information Society Code, and law are dealing with privacy protection in working life. Personal data "means any information on an identified or identifiable private individual". A data controller means "the natural or legal person, or a number of them, determining the purposes for the processing". Data controllers are not compulsorily required to register with the Finnish data protection authority and the Data Protection Ombudsman.

General Data Protection Regulation (GDPR) of 2016 aims to protect the personal data and privacy of EU citizens for various transactions that happen within EU member states [10]. It also regulates the personal data exported outside the EU [11]. Across the 28 members states, the standards are uniform for companies whose transactions fall in the ambit of GDPR. In a report published by RSA in 2018, , stolen data is a worry to consumers worldwide since it has significant financial implications. It has been observed in various research studies that the issue of "ethical use of data" is similar across regions and people perceive personalization as intrusive and unethical[12].

GDPR ensures to protect the data like identity, web locations and searches, health and biometric details, sexual orientation and political inferences and opinions. It is mandatory in GDPR for every company which has access to personal Information about EU citizens to protect privacy even if it has no business presence in the EU states. The penalties under the GDPR are "up to €20 million or 4% of global annual turnover, whichever is higher", for non-compliance. It has been conventionally observed that penalties that have been imposed are not big.

Data processors have been defined to include the people or organization that maintain and process, in part or full, the personal data record stated in the regulation, including the outsourced organizations. The regulations place the onus on the data processors for breach of privacy or non-compliance with the regulations. The cost of adhering to the GDPR regulation is relatively high for compliant companies.

In the US, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides for establishing national standards that protect the sensitive Information of the patent health information, which must not be disclosed without the patient's consent or knowledge. The coverage of this legislation includes health providers, health plans, clearinghouses and business associates. Individually identifiable health information created, received, maintained or transmitted by an entity in electronic form is called as "electronically protected health information" (e-PHI). In order to comply with the HIPAA Security Rule, the entities covered by the regulations shall maintain the confidentiality of health records in electronic form with full integrity. They are also bound to protect these records from security threats and non-permissible disclosures. Full compliance must be ensured by their staff. Under the Family Educational Rights and Privacy Act (FERPA), the student records must be protected for privacy and disclosed only after obtaining their consent.

The Gramm-Leach-Bliley Act, 1999 provides for the protection of the customers' private Information by financial institutions and the manner in which this Information will be shared. In order to comply with GLBA, "financial institutions must communicate to their customers how they share the customers' sensitive data, inform customers of their right to opt-out if they prefer that their personal data not be shared with third parties, and apply specific protections to customers' private data in accordance with a written information security plan created by the institution."

California Consumer Privacy Act (CCPA) allows any consumer belonging to California to inspect all Information which any company has saved on him and at any time require the company to disclose to whom the private Information was given. The customer can sue companies if the privacy guidelines are violated, even if there is no breach [13]. According to UNCTAD (2020), "As more and more social and economic activities have placed online, the importance of privacy and data protection is increasingly recognized. Of equal concern is the collection, use and sharing of Personal Information to third parties without notice or consent of consumers. 128 out of 194 countries had put in place legislation to secure the protection of data and privacy." In spite of evolving frameworks for the protection of privacy, there is still some issue that is unresolved. For example, in Europe, different regulations are applicable to businesses depending upon location and sector. Protection of cross border data is another issue that needs to be resolved.

Some authors like [14] have argued that compliance with GDPR across the nation may be subject to serious limitations given the possibilities of circumventing the GDPR for various advantage by companies. [15] has put forth the view that GDPR can put a limit on the types of data collected by organizations, though there are controversial opinions. In various Asian countries like India, Vietnam, Malaysia etc., there are multiple regulations dealing with the privacy of data. As such, it is difficult to exclusively implement the legal code.

IV. Technological Responses to Privacy Protection

With the increasing strategic importance of data being visualized in all walks of life, the privacy and protection of data is a top concern. Continuous efforts are being made to develop technologies that can enhance privacy and develop robust systems for data security. Privacy Enhancement Technologies (PETs) includes all technologies that ensure the security of data and contribute to the preservation and enhancing of privacy during searches or analytics. PETs are meant to offer an effective technological response to the protection of privacy. The common privacy enabling technologies are described as follows(Figure 1).

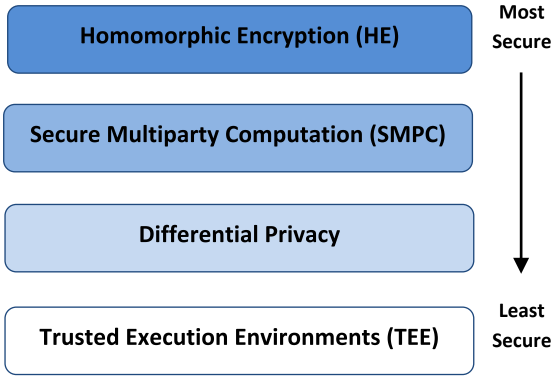
Homomorphic Encryption (HE)
Secure Multiparty Computation (SMPC)
Differential Privacy
Trusted Execution Environments (TEE)
Most Secure
Least Secure

Figure 1 - Common Privacy Enabling Technologies

Source: https://www.helpnetsecurity.com/2020/06/16/a-look-inside-privacy-enhancing-technologies/

Homomorphic encryption is believed to be the strongest security positioning, and Trusted execution environments is the weakest, said to be the least privacy-preserving [16]. Homomorphic encryption "is a form of encryption allowing one to perform calculations on encrypted data without decrypting it first. The result of the computation is in an encrypted form when decrypted the output is the same as if the operations had been performed on the unencrypted data" [17]. In a cloud environment, the issue of sensitive and confidential(private) data processing is a major concern [18]. The HE can perform operations on encrypted data without knowing the secret key and can offer an effective solution to strengthen the confidentiality of private information.

Fully homomorphic encryption (FHE) can provide effective privacy protection for IoT that is now versatile in physical, cyber and social spaces [19]. However, homomorphic encryption suffers from the serious limitation of real-world implementation to solve the privacy protection problems. The slow speed and complexity limit its application in real-world [20].

Secure multiparty computation techniques allow the multiple parties to jointly operate on data while keeping their individual inputs private. It is an old conventional technique continuously reached. Privacy and security of data depend upon the technique used. Definitions of security need to be relaxed from the notion of fully secure instead of using a highly efficient protocol unproven secure under any model so that secure and efficient protocols can be built. Therefore, research on privacy, in general, must be coupled with answering the question of permissible information leakages [21].

Differential privacy is a mathematical framework that aids to quantify and manage the risk of privacy. It involves the collection of individual Information using statistical procedures and probability setting. The introduction of noise into the outcome results prevents the leakage of private information on an individual. The approach of distorting data for privacy protection offers security challenges [22]. Application of differential privacy requires qualified personnel and a suitable computing environment. There is a lack of tools and trained individuals to verify the correctness of differential privacy implementations [23]. Though this approach is used in various privacy protection protocols, the trade-off between accuracy and privacy is difficult to achieve [23].

Trusted Execution environment (TEE) is the concentrated area of a processor which can run parallel to the operating system in a secluded environment. It gives assurance about the confidentiality and integrity of the loaded data and code in TEE. The TEE is the least secure of PETs and sometimes it is also referred to SET (Secure Enclave Technologies). TEEs are the small perimeter-based security model, and the security of this perimeter is available in a hardware chip. Suppose someone breaks this perimeter then, he can gain access easily to the data available in this perimeter. TEEs have a very fast computational capability which gives a good sound of privacy and security posture. The Intel SGX is the profitable available space in TEEs. After the detection of the Meltdown and Spectre vulnerabilities, space is continuously engaged in security issues. TEEs are the chip level hardware-based security model which provides security on the stored data along with the data available in processing. There is an API abstraction layer. Also, available for the application portability in different configuration hardware. A typical modern TEE architecture is meant to be ensuring a strong isolation among the different types of security domains. But, when we prevent the sharing of resources, the TEE is no practical use. The challenge of privacy protection lies in every technology. It all depends upon the user and context how the privacy extending technologies are optimally utilized.

V. Privacy Concerns in Specific Technological Contexts

The issue of privacy can be examined in specific technology application contexts. Of these, the prominent are cloud, big data and IoT. We present these issues in the following paragraphs.

Cloud Computing - The requirement and the popularity of cloud storage and computing is increasing day by day, which accentuates the cloud service provider to focus on cloud data privacy along with its security. In cloud computing environments, two major problems in data security and privacy are encountered [24]. First, departments in an organization are not ready to share data with other departments with whom they have trust issues for the protection of their data. Second, the users don't have up to the mark resources and don't have a proper model for data security/privacy. If they use an outsourced model, then the risk of leakage of data will increase. Therefore, there is a need to develop the framework for better data security and privacy with some latest machine algorithms. Today usage of cloud storage becoming much popular in small scale and medium scale organization. In these organizations, they prefer cloud storage of data because of its effective and efficient techniques of data management, which helps in performing different operations on data and generating reports as per their requirement. The fundamental challenge is still there about data privacy or security. The biggest challenges are (1) how to separate sensitive and confidential data from the bulk storage of data (2) how to implement access mechanism of data according to user requirement from bulk storage of data [19].

Big Data - Latest technologies dealing or taking very sensitive data of technology end-users, so in the early stages, it must be decided what type of technique and algorithm we have to apply over the data to ensure data security and privacy. It is broadly accepted by different technology experts if there is a large amount of data available of individual user or organization, then the probability of hitting or leakage of data get an increase in multiples Nils[25]. When we are working on a web application, then there are two types of data generated – (1) Active data generation, which is generated by the application user willingly and he knows what type of information he is sharing with the third-party applications and (2) Passive data generation which is generated in the same manner over the web when we are working but here is user consent is not involved, and even he does not know data is generating or not. In the passive data generation, third-party applications collecting user data over the web in this sensitive information are also included, which users do not want to share if he knows about the data generation.

In Big Data, a high volume of data collection and storage is no issue, but the biggest challenge is the storage of data securely and shares it responsibly with the authenticated users, even with the consent of the end-users. At this level, if any type of lapses comes over the Big Data storage companies or data security/privacy, then it becomes a very critical situation to save the sensitive information of the users. Therefore, we have to ensure the data security and privacy of end user's data by applying all the latest data security and privacy algorithm, which are based on the latest technologies like Artificial Intelligence or Machine learning [26]. Data Security and privacy issues get increased due to the high frequency of web application usage, any time anywhere accessibility feature and small or medium size organization's trust getting increased due to these reasons (1) Big Data Storage techniques (2) diversify of data sources (3) their different formats of data storage (4) streaming nature of data generations (5) Cloud migration facility[27]. *Too Much Data* - IOT based product generates a huge amount of data, and by 2025 more than 500 billion IOT devices will be connected worldwide, creating a heavy load on the Internet. On a daily basis, more than150 a million data moving over the internet as per the ongoing scenario. Thus, we see that security and privacy issues are getting increased day by day due to the high frequency of data storage, accessibility along with availability of cloud infrastructures on large scales and availability of data generation in multiple forms like Active and passive forms [28].

Internet of Things (IoT)- includes a wide range of smart gadgets which are enabled with the latest technology features and sufficiently capable in handling the complex task with the high computation speed of data in few Nanoseconds. These are the internet-based intelligent devices that are enabled with Artificial Intelligence features also. These types of devices can be controlled easily from a remote location by [29] state that IoT is the kind of invention that has its own security and protection layers. It is based on the integration of heterogeneous and homogenous networks. The biggest issue in IoT is to handle the vulnerability and complexity which arises due to those smart devices and gadgets which is developed by their own infrastructures.

The current privacy policy of IoT devices is much confusion because these devices are not sufficiently capable of taking input and producing output to the end-users with the help of external devices. IoT devices don’t have the popular resource connectivity features just like keyboard and mouse. The uses of Sensor devices are also having the issue of data security and privacy. These devices are used in the collection of both (Active and Passive) type of data show poor security mechanism [30].

Unwanted Public Profile: It is a common practice that any user signing the terms and condition pages in a consent form or agreement doesn’t read the whole document. It becomes difficult to identify genuine users because they may not give accurate Information, and they just signed the document without reading the terms of the privacy policy. In today scenario, we have some gadgets which check the health of the user and generate the result or report. This type of smart gadgets helps in acknowledging the doctor and insurance companies about the health of the smart gadgets’ users. *Eavesdropping*: Today, Intruders can easily explore the Information of smart homes with the help of spying and vulnerable gadgets. By using these IOT based gadgets, intruder even can tell about what program running on TV. All Tech experts have their different opinion on uses of IoT devices “few are in favour but after the implementation of strong data security and privacy mechanism and few are still opposing the use of smart gadgets at least in inside the home”. *Consumer Confidence*: IoT industry needs to gain confidence in front of the smart device audience by implementing some strong data security and privacy mechanism. But if they still lacking in this issue, then it can’t target that much audience, which it can do after implementation of data security and privacy mechanism.

It has also been observed that an increase in awareness about organizational threats reduces the potency and impact of threats, while in the social media context, the increased awareness prompts threats.

VI. Emerging Issues and Ethical Considerations

Data Security and Privacy have been used synonymously in practice in varied contexts. *Data security* guides us in protecting data from outside attackers or hackers and malicious users. The primary concern is to protect data from unauthenticated users and breaches or leaks. *Data Privacy* governs the ways of data collection, which will not compromise at any level or responsibly handling the data. It is concerned about sensitive data must not be leaked or compromised due to any lapses from the organization, and it must be utilized or shared only with the consent of the concerned person. However, we find that often privacy is construed as data security which leads to incorrect conceptualization and treatment. The summarized view of data privacy issues can be summarised as follows.

New laws and regulations - An emerging issue for the business and organizations is the uncertainty about the new regulatory framework for privacy protection in terms of its implications and adoptions.

Need for Privacy Protection Scientists - With the issue of privacy protection become extremely important, a dire need for experienced professionals to effectively organizing the management and protection of private data is strongly felt.
Training and Awareness of Employees - The role of employee awareness regarding data management plays a crucial role in the security of the data and storing it in an organized form. An education support and resources top employee in organizations is imperative to adaptation and reinforcement of best practices for data privacy and security.

Cloud solution security: With a growing rush towards cloud computing, security issues have become more and more critical[31][32]. In the context of cloud security adaptation and leveraging the machine leveraging tools for data protection within organizational frameworks and processes is important there is a need for data protection in a manner that it can be integrated with information security to build up an “Intelligent Enterprise”.

Management of third-party risks - It always needs to build trust and ensure all parties which are involved in providing support to the customer must not share their data with any other competitors in the market.

In a digital world, we use the IoT or AI-based devices which store and access their maximum data over the web. All these latest technology-based gadgets are collecting some confidential or sensitive data. Applications running on these latest technology-based gadget or devices collect the end user data, sometimes with the user's consent and sometimes without the user's consent. The major concern is the security of data that is collected by the different applications running on the end-user devices.

The ethical norms for every identity that has access to private Information are - Truthfulness (Factual correctness), Freedom from intrusion and privacy, legal protection of Human Rights. An IT Professional is regarded as an *infopreneur* who deals with various person-related and private Information. He is concerned with various ethical issues like - (a) deciding as to entitlement of private Information, (b) confidential treatment of gathered Information, (c) authenticity of Information, (d) purposes for which Information may be used and (e) right to privacy of the person whose Information is gathered.

VII. Conclusion and Future Scope

Technology has obvious implications on the collection, processing and dissemination of Information. The main ethical concern of Information Technology is how the Information is accessed and manipulated. Accessing a person's private information has become easier in modern times because of a variety of technologies and interfaces. The use of Technology, cannot be regarded as Ethically Neutral when the data is processed in various computing environments. Technology creates implications for the privacy of people in a variety of areas that include monitoring of people by electronic means in the workplace, intercepting messages, intruding into databases containing Personal Information. Privacy Issues appear on a variety of platforms, for example, applying for financial products, health treatments, buying of products and services and various E-Commerce activities. Since all computer systems are more or less vulnerable in one or another form because absolute security doesn't exist. Hackers and crackers create significant threats to privacy and raise issues of IT Ethics. Intrusion into privacy creates an impact on individual and society. Loss of Private Data affects the individual in the sense of loss of dignity and spontaneity coupled with threats to freedom. Researchers have established that technology itself is a threat to privacy, though it is viewed as a solution to problems.

Various Businesses gather large sets of person-related Information in their business and endeavours, thus creating a threat at the processing or post-processing stage. In the current scenario, we need a kind of data privacy framework that help the companies and organizations to define or implement the data privacy policies by which they can assure the customer about the retention of their data with privacy. Along with data privacy, they have to give assurance about the authentic access of the data with the responsible use. Also, the regulations dealing with privacy must be universal and adaptable with financial feasibility on the part of concerned parties.

Future Directions

Researches on the protection of privacy in various computing environments may be carried out given a specific technology environment that can in customizing for region-specific legislation.

REFERENCES

[1] Neethling, J., Potgieter, J.M. & Visser, P.J. *Neethling's law of personality*. Durban: Butterworths. **1996**.

[2] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, "*Data Security and Privacy in Cloud Computing*," International Journal of Distributed Sensor Networks, Vol. **10**, Issue **7**, p. **190903**, **2014**.

[3] R. L. Finn, D. Wright, and M. Friedewald, "*Seven Types of Privacy*," European Data Protection: Coming of Age, pp. **3–32**, **2012**.

[4] Feng, D.-G, Zhang, M., Li, H., "*Big data security and privacy protection*", JisuanjiXuebao/Chinese Journal of Computers, Vol. **37**, pp. **246-258**, **2014**. 10.3724/SP.J.1016.2014.00246.

[5] P. J. Susn, "*Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions*," in IEEE Access, Vol. **7**, pp. **147420-147452**, **2019**. DOI: 10.1109/ACCESS.2019.2946185.

[6] A. Ho, A. Maiga, and E. Aimeur, "*Privacy protection issues in social networking sites*," 2009 IEEE/ACS International Conference on Computer Systems and Applications, **2009**.

[7] Boeckl, K. and Lefkovitz, N.,"*NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management"*, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.CSWP.01162020,**2020**.

[8] Gruzd, A., & Hernández-García, Á., "*Privacy concerns and self-disclosure in private and public uses of social media*", Cyberpsychology, Behavior, and Social Networking, Vol. **21**, Issue **7**, pp. **418-428**, **2018**. doi:10.1089/cyber.2017.0709.

[9] C. Pilton, S. Faily, and J. Henriksen-Bulmer, "*Evaluating privacy - determining user privacy expectations on the web*," Computers & Security, Vol. **105**, p. **102241**, **2021**.

[10] I. Fish, "*GDPR: Global Privacy Regulations*," ITNOW, Vol. **61**, Issue **2**, pp. **30–30**, **2019**.

[11] F. Nahai, "*General Data Protection Regulation (GDPR) and Data Breaches: What You Should Know*," Aesthetic Surgery Journal, Vol. **39**, Issue **2**, pp. **238–240**, **2018**.

[12] Treiblmaier, Horst & Madlberger, Maria & Knotzer, Nicolas & Pollach, Irene, "*Evaluating Personalization and Customization from an Ethical Point of View: An Empirical Study",* Proceedings of the Hawaii International Conference on System Sciences, **37**, **2004**. 10.1109/HICSS.2004.1265434.

[13] J. S. Baik, "*Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA)*," Telematics and Informatics, Vol. **52**, p. **101431**, **2020**.

[14] Zarsky, T., "*Incompatible: The GDPR in the age of big data*", Seton Hall Law Review, Vol. **47**, pp. **995-1020**, **2017**.

[15] R. Lenz, "*Big Data: Ethics and Law*," SSRN Electronic Journal, **2019**.

[16] K. P. L. Coopamootoo, "*Usage Patterns of Privacy-Enhancing Technologies*," Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, **2020**.

[17] M. A. Will and R. K. L. Ko, "*A guide to homomorphic encryption*," The Cloud Security Ecosystem, pp. **101–127**, **2015**.

[18] K. El Makkaoui, A. Ezzati and A. B. Hssane, "*Challenges of using homomorphic encryption to secure cloud computing*," 2015 International Conference on Cloud Technologies and Applications (CloudTech), Marrakech", pp. **1-7**, **2015**, Doi: 10.1109/CloudTech.2015.7337011.

[19] D. Chen and H. Zhao, "*Data Security and Privacy Protection Issues in Cloud Computing*," 2012 International Conference on Computer Science and Electronics Engineering, **2012**.

[20] V. Biksham and D. Vasumathi, "*Homomorphic Encryption Techniques for securing Data in Cloud Computing: A Survey*," International Journal of Computer Applications, Vol. **160**, No. **6**, pp. **1–5**, **2017**.

[21] Lindell, Yehuda, Pinkas, Benny, "*Secure Multiparty Computation for Privacy-Preserving Data Mining*". IACR Cryptology ePrint Archive. **2008**. 10.29012/jpc.v1i1.566.

[22] S. Balamurugan, Dr. Sanjay Pande, "*Data Security and Cryptography in Cloud Environment*", International Journal of Engineering Research & Technology (IJERT), Vol. **4**, Issue **6**, **2015**. Doi:10.17577/IJERTV4IS061013.

[23] S. L. Garfinkel, J. M. Abowd, and S. Powazek, "*Issues Encountered Deploying Differential Privacy*," Proceedings of the 2018 Workshop on Privacy in the Electronic Society, **2018**.

[24]Feldman, M., Friedler, S. A., Moeller, J., Scheidegger, C., and Venkatasubramanian, S., "*Certifying and Removing Disparate Impact*", In Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining - KDD '15, pp. **259–268**, Sydney, NSW, Australia, **2015**. Doi: 10.1145/2783258.2783311.

[25]Gruschka N., V. Mavroeidis, K. Vishi and M. Jensen, "*Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR*," 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, , pp. **5027-5033**, **2018**. doi: 10.1109/BigData.2018.8622621

[26]Y. Shi, "*Data Security and Privacy Protection in Public Cloud*," 2018 IEEE International Conference on Big Data (Big Data), **2018**.

[27]Shirudkar, K. & Motwani, D. "*Big-Data Security*", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. **5**, Issue **3**, pp. **1100-1109**, **2015**.

[28]R. Tahboub and Y. Saleh, "*Data Leakage/Loss Prevention Systems (DLP)*," 2014 World Congress on Computer Applications and Information Systems (WCCAIS), **2014**.

[29]Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., and Kwak, K. "*The internet of things for health care: a comprehensive survey*". IEEE Access, Vol. **3**, pp. **678–708**, **2015**.

[30]Solangi, Zulfiqar, Solangi, Yasir, Murad, Shah, S Abd Aziz, Madihah, Hamzah, Mohd, Shah, Asadullah. "*The future of data privacy and security concerns in Internet of Things*". Vol., **1-4, 2018.** 10.1109/ICIRD.2018.8376320.

[31]A Mallareddy, R Sridevi, Ch G V N Prasad, "*A Survey of Data Hiding methods for data security in Cloud*", International Journal of Computer Sciences and Engineering, Vol.**7**, Issue.**5**, pp.**690-694**, **2019**.

[32]Supriya J., Srusti K.S., Gamana G, S. Sukhaniya Ragani, Raghavendra S., Venugopal K.R., "*A Survey on Efficient and Secure Techniques for Storing Sensitive Data on Cloud*", International Journal of Computer Sciences and Engineering, Vol.7, Issue**.5**, pp.**1766-1777**, **2019**.

AUTHORS PROFILE

Ayush Gupta is of Masters of Technology (Cyber Security and Cryptography), Faculty of Computer Science and Engineering, University of Turku, Finland. He has presented papers in national and international conferences in the area of Information and data security. His area of research interest is cryptography and information security.

Manvi Gupta is a student of BALLB programme of Guru Gobind Singh Indraprastha University in Vivekananda Institute of Professional Studies, New Delhi. She has also obtained certification in cyber law from Indian Law Institute Delhi. Her area of interest is Information Security Law and Practice.