

Data Privacy in Bangladesh: A Review of Three Key Stakeholders' Perspectives

[Kamal Hossain, Khabirul Alam & Umme Saara Khan]

Abstract

The study focuses on data privacy in the context of Bangladesh. The objective of this study is threefold: first, to know consumers' perspective on the importance of data privacy, second, to understand the industry experts' point of view towards data privacy and third, to analyze Government's stake and initiatives to protect personal data. This paper focuses on the current status of data privacy in Bangladesh and entails with recommendation to further develop data protection aspects in Bangladesh.

Keywords: data privacy, Bangladesh, consumer, industry expert, government, perspective.

i. INTRODUCTION

In this age of globalized connectedness, we are constantly in need to connect through sharing our personal data. Everyday terabytes of personal data are used through different technologies to access and operate various technological devices [1]. It has become a matter of concern how these data are being stored, accessed and used [1]. The need for a modern data protection law, considering the growth of e-commerce, cloud computing, social networks and online games has become pivotal across the globe [2]. As such, more and more nations are enacting Personal Data Protection laws such as GDPR in Europe [1,2].

Kamal Hossain

Senior Lecturer
eBusiness & Computer Information Management
BRAC Business School
BRAC University, Bangladesh.

Md. Khabirul Alam

Business Development Manager
Kazi IT Center, Bangladesh

Umme Saara Khan

Research Assistant
BRAC Business School
BRAC University, Bangladesh.

A. The Concept Of Data Privacy

Theories by scholars such as Floridi, discusses two data privacy theories: i) the reductionist interpretation and ii) the ownership-based interpretation [3]. According to the reductionist interpretation, to avoid the undesirable consequences possibly caused by a breach of privacy, data privacy is necessary and valuable as it guards against it. According to the ownership-based interpretation, each person owns his or her information or data [3]. These two theories emphasize on different aspects of data privacy, however, there are arguments regarding their incompatibility [3]. Two newer theories are suggested as more appropriate which highlight variations of the restricted access and control while analyzing issues affecting data privacy [4]. According to the restricted access theory, “zones” of privacy (specific contexts) need to be established so that people have informational privacy to limit or restrict others from access to information about them. In control theory, having privacy is directly linked to having control over information about oneself and personal choice [4].

Despite the widespread use of these two theories, scholars came to a decision that though both restricted access theory and the control theory notes something important about data privacy, it does not provide a satisfactory explanation of data privacy [4]. A framework attempting to merge all the important elements of data privacy into a single theory is the Restricted Access/Limited Control (RALC) theory [5].

The RALC theory considers privacy and control as two separate concepts. In this theory, privacy is defined having a fundamental role in case of protecting from intrusion and information gathering by others [5]. On the other hand, individual control of personal information is defined as a part of the justification of privacy that plays a role in the management of privacy [5].

B. Historical Background of Data Protection

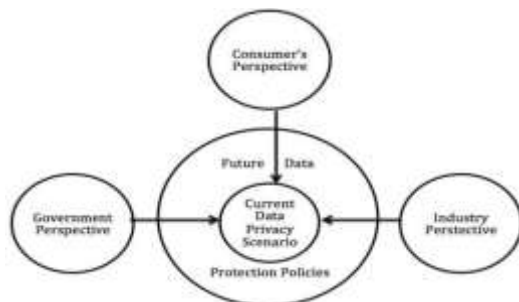
The first ever computer specific statute of a Data Protection Act was introduced in 1970 in the German State of Hesse [6]. In those days, computers were used in order to store and process large amounts of personal data, people were concerned about the misuse of those records under the Nazi regime. In order to resolve the concerned problem, The Data

Protection Act was pursued [6]. In the case of Sweden in 1973, an introduction of data protection was seen for the very first time and that was the first national statute [7] In 1981, to ensure free flow of information and infringement of personal privacy, the Council of European Convention established standards among member countries. The first Data Protection Act was introduced in UK three years later [7]. It was made mandatory for public and private organizations to register with a Data Protection Registrar to access computer-held personal data. However, this act failed to specifically recognize the individual's right to privacy [7,8]. With the explicit aim of protecting the right to privacy, the Data Protection Act was changed and introduced in 1998 and this time it was built on an EC directive of 1995[8]. This act broadened the definition of data while tightening restrictions on the usage of sensitive information and specifying conditions for the data processing. This act not only separated the functions of registration and enforcement but also increased the powers of a government regulator in the fields of freedom of information now also known as the Information Commissioner [8].

ii. METHODOLOGY

For the purpose of the study the authors have conducted a thorough literature review from various authentic and credible sources. In addition, a primary research through survey to understand users' perspective has been conducted with 81 data user respondents. Industry experts in the BPO sector of the country have been interviewed to get the insight of the area covered in this article. All the secondary data are collected through different search engines, different online journals and articles available online. Qualitative techniques were used to analyze the collection of data.

iii. FRAMEWORK



The framework depicts that there are three stakeholders who influence the current scenario of data privacy in the country which needs to develop into a strong data protection policy framework. The authors aim :- i) to know consumers' perspective on

the importance of data privacy, ii) to understand the industry experts' point of view towards data privacy and iii) to analyze Government's stake and initiatives to protect personal data. This study intends to have an insight of data privacy from these three key stakeholders' perspective and analyze the current scenario.

iv. FINDINGS AND ANALYSIS

A. Consumers' Perspective

In order to understand the consumers' point of view, primary research was conducted through a survey with 81 respondents. Through the survey respondents were asked several questions related to their extent of knowledge and concerns about data privacy and how important data privacy is to them. Out of 81 respondents, 64.2 % (52) were male and 35.8% (29) were female who are mainly university students. The respondents represent different age groups from 16-34 and most of them fall in the age group of 20-24 (84%) and the rest falls under the age group of 16-19 (3.7%), 25-29 (9.9%) and 30-34 (2.4%) respectively. To understand their exposure to Internet, the authors identified their Internet usage per week. The result says, 10 out of 81 respondents use internet less than 5 hours per week, 25 respondents use for 6-10 hours, 10 respondents for 11-15 hours, 16 respondents for 16-20 hours and 20 respondents for 21-25 hours per week which is 12.3%, 30.9%, 12.3%, 19.8% and 24.7% respectively.

After understanding their Internet usage, the respondents were asked whether they know about data privacy and their intensity of knowledge on data privacy. Among the respondents some agreed that they know somewhat about data privacy though they are regularly using the Internet and other social media to communicate and avail different online services and they are sharing their data regularly on those sites or media. The result was acceptable but not satisfactory considering the importance of data privacy.

To get a clearer view, the respondents were also asked about the importance of data privacy to them. As most of the respondents belong to an age group who are well known about the recent facts and more conscious about the recent news on Facebook Cambridge Analytica scandal, they were asked whether they consider data privacy as important or not. In response, 63.0% (51 out of 81) claimed data privacy as very important, 35.8% (29 out of 81) claimed as important and 1.2% (1 out of 81) claimed data privacy is not very important to them. From this we can understand that previously data protection

might not be a concern of consumers, but due to the exposure to the adversity of data theft and other negative consequences, nowadays consumers are getting more conscious about data privacy.

In order to get an understanding about consumers' concern on data privacy while purchasing online or visiting any website, the respondents were asked about their concern on this. With the advancement of technology and availability of Internet, nowadays people tend to shop online and they are likely to visit different websites to search for information on a regular basis. Among 81 respondents around 54.4 % of the respondents stated that they are not concerned about privacy while doing online shopping. Some of the reasons behind this alarming report were: buying from pages already known to them, buying products from the same online shop regularly, not experiencing any adverse effect of sharing personal data, little knowledge about data privacy and its importance etc.

The result changed when it came to importance of privacy while visiting any website. 64.2% respondents marked it as very important, 30.9 % as important and 4.9 % as not so important. According to them, while visiting some websites for information or any other purpose, they are sometimes asked to log in or sign up with their Facebook id and they find it insecure. Some said that while visiting some websites there are times when there are pop ups regarding cookies and that discourage them to visit that website.

B. Industry Perspective

In Bangladesh the BPO (Business Process Outsourcing) industry follows GDPR (General Data Privacy Regulations) as EU highly abides by GDPR and this industry falls under one of the trade agreements we have with the EU. BPO industry has clients worldwide and currently has a market share of \$180m and more than 40,000 people are working in this particular industry [9]. UK, Denmark, Germany, Netherlands, Sweden, and Switzerland; EU nations are also clients of BPO companies like Datasoft, Brain Station 23, Dream 71 Bangladesh, Lead Soft, and others. These companies either individually or institutionally deal with EU and exchange data between trading partners companies thus companies such as Taskeater, Genex Infosys Ltd, Digicon Technologies Ltd, Syntech Solutions along with these companies are getting affected by GDPR [9].

Bytominer is a rising SME BPO company and targets the UK as one of its markets. Saima Islam, Managing Director of Bytominer, in an interview, confirmed the imposition of restricted unsolicited emails targeting potential customers as one definite impact of GDPR among so many on the company. However, she also

highlighted the positive aspect of GDPR for companies. According to her, companies will be focusing more on a varied, solicited omni-channel approach in order to reach smaller target markets ensuring better relationship management and outcomes.

The Business Development Manager in Kazi IT Center, in an interview said, in Bangladesh Context, being a private company they do not require to publicly declare their privacy policy. They only need to provide documents mentioning their existing system, operations as a part of documentation. He also mentioned that as they mostly work with BPOs there is exactly no generalized rule that they need to abide by. As there are no such mandatory rules, Kazi IT focuses on their data security management such as office access, network setup, locked USB, limited access to only necessary information, restriction on unauthorized devices (personal device) etc. They also focus on cyber-security by ensuring secured user id and password known as Credential Management with a software called Lastpass to encrypt user id and password.

C. Government Perspective

At present, one of the greatest significance for innovations is data. Nowadays, personal data is considered as the most valuable commodity in the world [10]. The commodification of personal data collected by multinational corporations (e.g. Alphabet, Apple, Microsoft, and Facebook), risk threats of breach of privacy and misuse or abuse of private information belonging to ordinary citizens [10]. To counter these threats, Countries across the world have enacted legislations or implemented policies to protect their citizens to counter these threats [10].

National digital revolution has been sparked with the Bangladesh government's vision of a „Digital Bangladesh“ [10]. The expansion of cellular subscriptions, digitization of state-related activities (such as e-TIN registration, application for passport, registration for examinations, publication of results and notices, access to public information, etc.) are two of the highlights of this vision [10]. The project of Bangladesh government also includes implementation of various projects and programs in order to develop the ICT sector [10]. To that end, the government has enacted legislations and drafted policies. Those legislations and policies are also there to safeguard against abuse [11]. The government has enacted The Information and Communication Technology (ICT) Act, 2006 has already been enacted by the government and already in action [11]. In order to ensure cyber-security and prevent

cyber-crime, Bangladesh government has proposed Digital Security Act, 2016[11]. However, it is quite unfortunate that the government has not yet formulated any formal legislation or policy on data protection specifically [10,11].

v. *DISCUSSION*

With the improper use or inadequate protection of consumers' privacy numerous issues can arise and can further affect a consumer. Individuals face numerous complexities and ethical issues regarding data privacy and its protection. Those numerous ethical issues can be sum up as PAPA: *privacy* (the information one requires to divulge about one's self to others), *accuracy* (authenticity, fidelity and accuracy of information), *property* (owner of the information), and *accessibility* (someone's right to obtain information) [12]. These four areas are widely taken in action while deciding whether or not to share personal information. There are other four areas to be focused concerning consumer privacy: *collection of personal information, improper access to personal information, unauthorized secondary use of personal information, errors in personal information* [13]. Though there are some considerations on ensuring privacy of personal data, consumer's lack of control, their lack of knowledge on the future usage of data and lack of participation how data will be used in the future, and their lack of participation [13].

According to a BTRC report of June 2016, the total Internet users in Bangladesh are 63.29 million that is almost equal to the total population of UK [14]. According to the same report, there are 131.37 million mobile phone users that is roughly about 80% of the population, whereas India has 78% and Pakistan has 66% mobile penetration [14]. This report gives an overall idea on how people are getting in touch of Internet, which depicts the importance of data protection. In Bangladesh, the concept of privacy is relatively new [14]. BTRC Director General Brigadier General Mustafa Kamal said that, BTRC will soon take initiative to ensure an acceptable information Security Policy, after discussing with be taking all the companies, banks, hospitals. [15] The Constitution of Bangladesh does not explicitly mention the word 'privacy', though it safeguards the sanctity of the home and the confidentiality of communications from government intrusion [16]. Article 43 of Constitution renders, "Every citizen shall have the right, subject to any reasonable restrictions imposed by law in the interest of the security of the State, public order, public morality or public health: (a) to be secured in his home against entry, search and seizure; and (b) to the privacy of his correspondence and other means of

communication" [16] Bangladesh Constitution has the same standpoint as the USA Constitution.

At times there are evidences of Bangladesh being on the verge of major threats of privacy and personal data leakage [10]. In the national dailies we often see upsetting news regarding privacy infringement and personal data loss from medical records, banks, educational institutions, Bkash outlets, spa center, hotel, shops and so on [10]. However, it may appear that Bangladesh has Information and Communication Technology (ICT) Act of 2006 in order to bring proceedings against perpetrators of such intrusion and unauthorized access, but the ICT Act has several loopholes too; e.g. failure to take into account all heinous incidents as perpetrators carry out their operations anonymously [11]. Thus, it becomes very difficult to identify them in most of the cases. There is a lack of a preventive framework at the pre-breach level and it is simply non-existent [11]. To curb future challenges of protecting citizens' privacy it is a demand that Bangladesh must have data protection law as the mere presence of legislation on post-breach offences is not providing adequate protection [11]

vi. *RECOMMENDATIONS*

Some enactment may be applied to safeguard personal data, as the idea of privacy is not so clearly mentioned in Data Protection laws of Bangladesh. Article- 43(b) of the Constitution provision includes chapter of fundamental rights, which compels the state to implement the privacy of citizen, otherwise the victim can use their rights right to move the High Court Division in accordance with clause (1) of article 102 [Article-44]. As per section- 7(h), 7(i) and 7(r) of the Right to Information Act, 2009 [16].

As per section- 2(10) of the Information and Communication Technology Act, 2006, data means any information, knowledge, facts, concepts or instructions which are prepared in a formal manner and is intended to be processed, is being processed or has been processed in a computer system or computer network, in any form including computer printouts, magnetic or optical storage media, punched cards, punched tapes or stored in the internal memory of the computer [11]. As the definition of personal data is not clearly mentioned here, so it can be clearer in the new proposed law [17]. With a clear indication of personal data definition, purposes for processing personal data, punishment for obtaining, transferring or selling of personal data without lawful authority etc. can be a part of the comprehensive statute [17]. Another mandatory provision can be the prohibition of processing collected data without the consent of

the person concerned except any statutory legal excuses [17].

vii. CONCLUSION

In today's information age the privacy of personal information is considered to be very important and with time the concept of privacy has transformed and evolved. Starting from availing services to social interactions, everything requires revealing of personal data, hence we feel the need of protecting data. The topic of privacy has been brought to the fore as a result of involvement of large companies and personal information of millions of people in numerous public incidents. Consequently, the need to promote and govern legislation has come to light. For both consumers and organizations privacy is very important. In today's information-oriented society, privacy of information has become an important and complex issue affecting our lives. With the continuous progress of society and technology, it will inevitably become more complex hence requires ongoing thought, research and intellectual engagement. In order to find the right balance between the demands of the individual and the society, the nature and implementation of data privacy demands considerations.

References

- [1] M. Zamir, "The collection, sharing and projection of data", *The Daily Star*, 2018. [Online]. Available: <https://www.thedailystar.net/news-detail-38946>. [Accessed: 29-Sep- 2018].
- [2] "Data protection", *European Commission - European Commission*, 2018. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection_en. [Accessed: 29- Sep- 2018].
- [3] L. Floridi, "The Ontological Interpretation of Informational Privacy", *Ethics and Information Technology*, vol. 7, no. 4, pp. 185-200, 2005.
- [4] H. Tavani, "Informational Privacy: Concepts, Theories, and Controversies", *The Handbook of Information and Computer Ethics*, pp. 131-164.
- [5] H. Tavani and J. Moor, "Privacy protection, control of information, and privacy-enhancing technologies", *ACM SIGCAS Computers and Society*, vol. 31, no. 1, pp. 6-11, 2001.
- [6] P. Bakshi, *Bharat's handbook of cyber and e-commerce laws*. New Delhi: Bharat Publishing House, 2002.
- [7] "The Swedish Personal Information Act", *People.dsv.su.se*, 2018. [Online]. Available: <http://people.dsv.su.se/~jpalme/society/eu-data-directive-freedom.html#EU>. [Accessed: 29- Sep- 2018].
- [8] EDPS, "The History of the General Data Protection Regulation - European Data Protection Supervisor", *European Data Protection Supervisor*, 2018. [Online]. Available: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. [Accessed: 07- Oct- 2018].

- [9]"What does GDPR mean for Bangladesh?", *Dhaka Tribune*, 2018. [Online]. Available: <https://www.dhakatribune.com/op-ed/2018/07/02/what-does-gdpr-mean-for-bangladesh>. [Accessed: 29- Sep- 2018].
- [10]2018. [Online]. Available: <https://www.thedailystar.net/opinion/human-rights/protecting-data-digital-bangladesh-1401592>. [Accessed: 29- Sep- 2018].
- [11]"Department of Information and Communication Technology", *Ictd.gov.bd*, 2018. [Online]. Available: <https://ictd.gov.bd/>. [Accessed: 29- Sep- 2018].
- [12]R. Mason, "Four Ethical Issues of the Information Age", *MIS Quarterly*, vol. 10, no. 1, p. 5, 1986.
- [13]H. Smith, S. Milberg and S. Burke, "Information Privacy: Measuring Individuals' Concerns about Organizational Practices", *MIS Quarterly*, vol. 20, no. 2, p. 167, 1996.
- [14]"BTRC | Bangladesh Telecommunication Regulatory Commission", *Btrc.gov.bd*, 2018. [Online]. Available: <http://www.btrc.gov.bd/>. [Accessed: 29- Sep- 2018].
- [15] S. Report, "ICT sector fails to attract investment: minister", *The Daily Star*, 2018. [Online]. Available: <https://www.thedailystar.net/online/cyber-attack-in-bangladesh-government-organisation-faced-4600-times-1643437>. [Accessed: 07- Oct- 2018].
- [16] *Hrlibrary.umn.edu*, 2018. [Online]. Available: <http://hrlibrary.umn.edu/research/bangladesh-constitution.pdf>. [Accessed: 29- Sep- 2018].
- [17]*Hg.org*, 2018. [Online]. Available: <https://www.hg.org/legal-articles/need-of-personal-data-protection-laws-in-bangladesh-a-legal-appraisal-48450>. [Accessed: 29- Sep- 2018].

AUTHORS



Kamal Hossain is a Senior Lecturer of eBusiness and Management Information Systems at BRAC Business School, BRAC University.



Mr. Khabirul Alam is the Business Development Manager at Kazi IT Center, Bangladesh. Skilled in Marketing, Branding, and Communication. Strong B2B sales professional with an Executive MBA majored in Marketing.



Umme Saara Khan, studying Bachelors of Business Administration at BRAC Business School in BRAC University, Bangladesh. She is working as a research assistant. She likes to write articles in different national and international journals.