International Journal of Research in Engineering
www.engineeringpaper.net
Online ISSN: 2664-8784; Print ISSN: 2664-8776
Received: 04-08-2019; Accepted: 05-09-2019; Published: 12-09-2019
Volume 1; Issue 4; 2019; Page No. 15-17

Data privacy and security issues in India: An empirical study

Sachin Bhutani[1], Harsh Goel[2], Dr. Deepak Chahal[3]
[1-2] MCA Student, Department of IT, Jagan Institute of Management Studies, Sector-05, Rohini, New Delhi, India
[3] Professor, Department of IT, Jagan Institute of Management Studies, Sector-05, Rohini, New Delhi, India

DOI: https://doi.org/10.33545/26648776.2019.v1.i4a.22

Abstract
In today's time, India's digital population is growing rapidly and holds the second place in the world in terms of the largest digital population. The majority of this population is connected to the internet through smartphones. Hence, the large amount of data that is being generated everyday by this population through their smartphones combined with the economy and the demography of the profiles involved makes India the most valuable digital population. The data generated is mainly through the use of various android applications, their iOS versions and websites. But this brings along associated risks, data privacy and protection being the major one. The unavailability of strong data protection law makes India even more vulnerable. The personal data consists of above the surface and below the surface data. Various methodologies and approaches are used to distinguish between the data. Thedata generated is used by many stakeholders and various companies to provide better facilities to the user.

Keywords: data protection, security, data privacy, internet, personal data

1. Introduction

This paper focuses on: What personal data is accessible by the applications/websites? To which third party this data is being shared with? How secure is the data generated? And the policies of the companies regarding the data privacy. The word data eventually seeks its issue on privacy and security. With the rise of new technologies, the need for data storage has increased [1] Data of the user is fundamentally collected by applications through permissions and by websites through trackers/cookies. The permissions taken by the applications is to access the location, contacts, image gallery, list of call details and external storage, camera of a user's mobile. Amusingly, it has been observed that same application that is iOS based were found to be requesting more permissions for access from the user as compared to their android counterpart. This reflects that either some extra features are provided in iOS-based applications or that the iOS-based applications are taking extra permissions than actually needed. Also, it has been recognized that the applications would work just the same even if many of the permissions are not taken. Many of the permissions taken can cause the real threat to the privacy of the user.

On the other hand, in case of websites, the permissions requested are very different as compared to that of applications and therefore cannot be tallied with them. Permissions requested in websites are very less indicating that comparatively less data is accessible by websites as compared to that by applications. Tracking being the preferred mode/option to collect the data of a user.

Through various sources, it has been found that almost every application/website is sharing the data collected by the user to some third party. The third party is some company generally that is using this data to improve advertising, analysis, tools of development-support, improving advertisement being the Common one. This benefits the companies as they use this data to improve the customer experience. Major piece of this data is found to be stored in the USA reflecting the fact that the companies that use these data are majorly USA based.

That privacy policies of the applications/websites and how easily they are understood by the user have always been the topic of debate. Privacy notices are marked "Difficult to read" and "Confusing" in accordance with Fleisch scale which happens to be the standard in industry to measure the readability of the content. Also, it has been observed invariably that the privacy policies are readily available at first touchpoint but not so easily available afterwards. Alarmingly, Indian applications explicitly asked for greater permissions than global counterpart. This difference is even more broad in categories like travelling based, shopping based and mobile wallets. Requesting permission for sms services, microphone and contact details were significantly greater in India based apps.

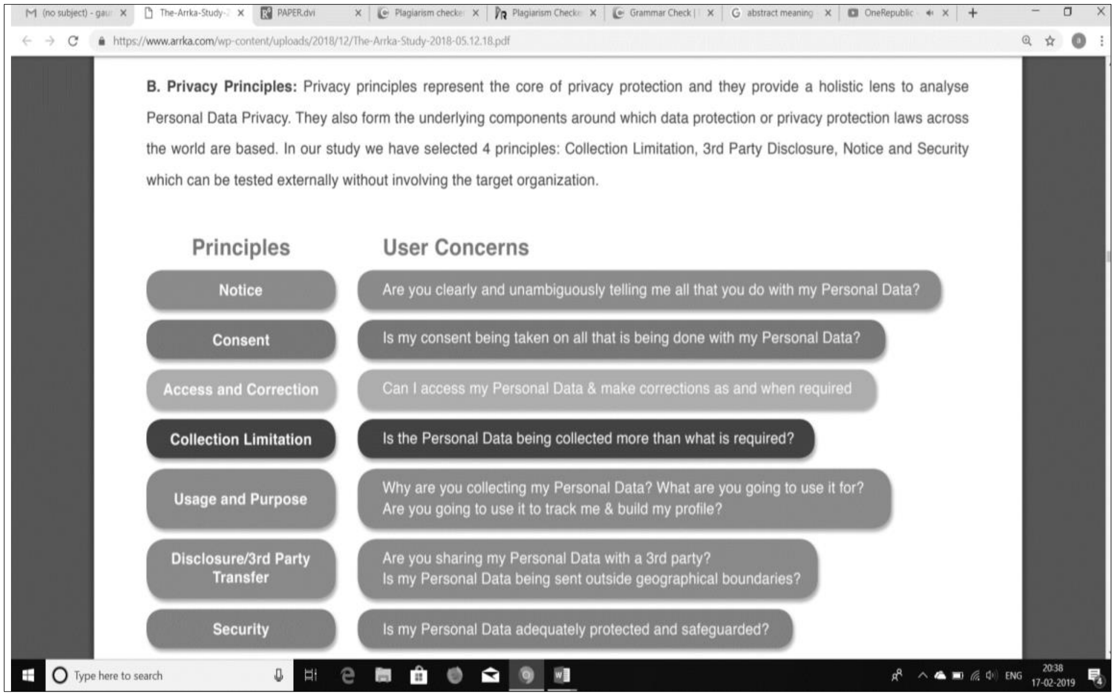
2. Personal Data

Personal data can be divided into two categories namely 'Above-the-surface' data that is visible to the individual and 'below-the-surface' data is a type of data that is normally not notice by a person. The paper mainly focuses on 'below-the-surface' data. This 'below-the-surface' data combined with first hand data provides the company a detailed knowledge of the user, his interests, his preferenecs and also helps in predicting the behaviour. Based on this information, companies used to provide advertisement, recommendations on what should an individual buy, shop, eat and also to impact and shape the behaviour of an individual.

3. Principles of Privacy

Privacy principles sets up the fundamentals of individual's

Privacy protection and provides a key point to analyse the Individual’s personal data policy. These policies are formed keeping in mind user’s privacy concerns.



B. Privacy Principles: Privacy principles represent the core of privacy protection and they provide a holistic lens to analyse Personal Data Privacy. They also form the underlying components around which data protection or privacy protection laws across the world are based. In our study we have selected 4 principles: Collection Limitation, 3rd Party Disclosure, Notice and Security which can be tested externally without involving the target organization.

Principles	User Concerns
Notice	Are you clearly and unambiguously telling me all that you do with my Personal Data?
Consent	Is my consent being taken on all that is being done with my Personal Data?
Access and Correction	Can I access my Personal Data & make corrections as and when required
Collection Limitation	Is the Personal Data being collected more than what is required?
Usage and Purpose	Why are you collecting my Personal Data? What are you going to use it for? Are you going to use it to track me & build my profile?
Disclosure/3rd Party Transfer	Are you sharing my Personal Data with a 3rd party? Is my Personal Data being sent outside geographical boundaries?
Security	Is my Personal Data adequately protected and safeguarded?

Fig 1: Principles & User Concerns of Privacy

3.1 Testing Approach

Collection limitation (what personal data is accessible to an app) are tested using permission and tracker analysis. Disclosure to third parties (what data and to which third party is the data being shared) is tested using network analysis. Security is tested using security storage, transmission, coding and deletion analysis. Notice (is notice easily available and understandable) and transparency tested by content and readability analysis.

3.2 Dangerous Permissions

There are some of the permissions which can be very fatal. These are 1. Can write to the external storage. 2. Have an access to contact details. 3. Have an access to emails. 4. Have an access to the exact location. 5. Have an access to photos. Also, it has been recorded that many applications continue to access them even after they are not been used by the user. But the fact that these permissions help in building greater user experience cannot be downsized too.

The impact of permissions in world of website is not that sturdy yet as the number of permissions are very less in numbers. Hence, websites data collection mechanism is based on tracking mechanism. This is usually in the form of some type of subset of web browsing history. IP address and cookies are also used to track.

3.3 Sharing of Personal Data

Application/Websites share the personal data of an individual to the third party which uses this data to observe the behaviour, interests of an individual and then use this information to influence the user in order to shop or lookout for things according to his interest.

3.4 Security of Personal Data

Security is looked in terms of how data is stored, coded, transmitted, encrypted and deleted. Various statistics has shown that companies take security of the data of an individual with very high priority. Clearing of data post the uninstallation of application (secure disposal), encryption of messages between the user by encryption keys, transferring of data in secure manner, storage of session cookies in websites comes under the section of security of data. Encryption is basically a process of converting confidential data and information in a form of code, which prevent from unauthorized access [2]

4. Future Prospect

In a future to come, some facilities can be provided to the user itself at basic level itself. With higher and advanced technologies, we are putting an effort to make people life at ease [3] When a user download application, some applications ask for permissions to access your data, you can allow or deny those permissions. If you deny the permission then the apps will not be able to access your data, but if you grant them the permission then the apps can access all of your data of that kind. For an example if an app wants to access your photos and you have granted the permission then the app can access all of your photos. Your phone may contain some data that you don't want to share (can be personal or confidential) but once you have granted the permission, the app will access all of that data as it cannot distinguish between the personal and not so personal data. So, for this kind of a problem, a separate section should be introduced in the phones where the data that you want to hide from the apps would get stored. It will reduce the risk to your private data. A focus is made on machines as machines cannot be understood by verbal communication it forms abstractions and concepts [4].

5. Different ways to ensure the data security

1. Data Classification

Classification is type of data security which helps to prioritized the assets of the company which needs to be protected. Many tools are there which supports both user driven and automated classification capabilities. A well-planned data classification system makes essential data easy to find. This can be essential for risk management and compliance.

2. Data Access Policies

Giving access of the data to the individual user sometimes becomes very hard. Authorising only key members of the teams to handle secure data makes sure that the possible data breaches are remaining at a very low state. The tools are helping in sensitive data discovery and cleaning up data access permissions to enforce least privilege.

3. Cloud Data Protection

Encrypting sensitive data and storing it in the cloud makes system backups safer as well, and also it makes accessing data much easier for involved parties. Online document management systems come in handy for every company, as they make accessing files easy, safe and available for all the involved parties. Always use trustworthy cloud-based document management system, make sure the server parks are located inside the EU where strict data policy regulations apply, also, read their contract to see if they have backdoor channels for your files.

4. Two Factor Authentication

It becomes very hard for the attackers to pass the two-factor authentication and access the one's account. Sometimes it happens that attackers pass the 1 step of authentication but this type of security makes sure that the attacker don't pass the 2 step of authentication, it is guaranteed that even if the password is stolen, attackers cannot get into the account.

5. Tokenization

Substituting a randomly generated value, or a token, for sensitive data like credit card numbers, bank account numbers, and social security numbers makes it safer to store sensitive information. Unlike encryption, there is no mathematical relationship between the token and its original data; to reverse the tokenization, a hacker must have access to the mapping database, and this makes it much more difficult to read the data.

6. Conclusion

Data privacy is still at very initial stages in India. While there is lot of dialogues is in progress and development has been made on the policy regulatory front but we still are lagging behind from our counterparts across the globe such as EU, Singapore, Canada, USA being the leading one. Many fundamental steps are needed to be taken to ensure the privacy of user's personal data. In recent times, we have seen how the data is used to influence the citizen of a state to chose the president. However, the other aspect of privacy that is security seems to be in a good position worldwide. This leads us to conclude that as awareness increases and with improved data privacy laws, adoption and maturity of data privacy would go up in India in near future.

7. References

1. Prianga S. "Evolutionary Survey On Data Security In Cloud Computing Using Blockchain," 2018 ieee international conference on system, computation, automation and networking (icscan), Pondicherry, 2018, pp. 1-6
2. Chahal D. Security for Digital Payments: An Update, Int. J. Sc. Res. in Network Security and Communication, 2018; 6(5).
3. Kharb L. Implementing IoT and Data Analytics To Overcome "Vehicles Danger". International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2019; 8(11). ISSN: 2278-3075.
4. Kharb. "Brain Emulation Machine Model for Communication" in International Journal of Scientific & Technology Research (IJSTR), 2019; 8(08).