

A Critical Review On Myths Of Data Security & Privacy

Dr. Ajay Shriram Kushwaha

Associate Professor

School of Computer Application
Lovely Professional University, Punjab

Saptarshi Chatterjee

Student Researcher

School of Computer Application
Lovely Professional University, Punjab

Abstract –Data is & was vital for everyone from humans to organization and every entity which exists. Security of data & privacy is concern for user connected to Internet and transmit & receive data as per his need. Now-a-days we have multiple online portal, web apps which makes personal data collection from users knowingly and unknowingly. Recently selling of personal data in market is in huge demand many big marketing companies collect and sell data, recently Facebook was also blamed for selling data. The importance of data has become so much booming as every business is somehow connected to the Internet, needs promotions via call or email so the user details are like money making idea among companies. In this article authors focus on throwing light how data privacy is myth as Internet users transmit a huge amount of their personal data without knowing and how it could be misused. Further authors also highlighted key important facts about India's Personal Data protection Bill.

Keywords–Data, Privacy, Security, Cyber Security, Social media, E-Commerce, Anonymity, Personal Data Protection Bill, COPPA, GDPR, EU.

I. Introduction

Data privacy is serious issues increasing day-by-day, as social media and other business organizations, firms are in business to collect the personal and private data on their website with various means and thus data is getting more valuable than the real person. Users feels delighted to have their data online their images, videos, social media posts, their online presence, but dark of this trend leads to very serious cybercrimes as data can be easily manipulated with the intent to cause harm to their social image. Hackers with intension to do big crimes enter inside organization to penetrate the physical layer and thus misuse the private data like access data, user actions, behaviour leads to identity theft and data breaches.

People uses Internet for entertainment and for doing their businesses online like online sells, inventory, transactions, stock maintenance, etc. Growth of online business is due to ease of use and anywhere access from any location which also increases risk of user's privacy breaches and thus preventive measures to taken in order to protect user's information online to keep their life running as smoothly as possible. Privacy is nothing but human value which consists their four rights: anonymity, intimacy, research and solitude.

The significant gap between data privacy and the consumer trust as per one of the surveys shows the following conclusions:

- Only 20% of Us customer completely trust organization to keep their data private.
- 77% factor a company's ability to keep their information safe.
- 73% think businesses focus on profits over protecting consumer's privacy Rights.
- 78% of U.S consumers say a company's ability to keep the data private is Extreme importance.

Based on above observation, we can conclude as many countries like us as having trust issues about their privacy, since companies like Google, Facebook, Microsoft are not trustworthy to share and keep your personal data on their server in any form, thus we can't trust on these companies as data safety is biggest issue.

II. How Microsoft collecting personal data–critical review

Everyone using any software or web application asks himself why you should allow to collect your personal data? and why you should give personal to access your personal data from your computer for analysis purpose? Is it mandatory and if yes then why?

Let's talk about Microsoft which is most preferable operating system among many users, it is surprise to know that we our self allows Windows to collect personal information during OS installation and thus users leave everything which is traceable with the fingerprints of the activities they do on their PC and laptops.

Windows OS is very popular among people in India, and due to negligence, people blindly trust and don't even check what is going on in background which OS is running, users don't even check or knows actually windows is Spying without even making a big move, Yes windows also track users every activity what they do, where it's in internet or static condition and some of the settings are so deceptive that if windows want they can also access users family conversations over skype or any other connected tools. With help of in-built camera access windows can spy to know what user is doing in their home and even any encrypted data stored in the PC is also accessible as users tends to login the same account which they use for accessing their online storage and email services. Not only that with help of inbuilt location tracking windows also track your daily movement and places visit even if you are not carrying your Laptop and if it is sync with your mobile phone can share your location information once connected to internet and thus users gets easily traceable.

III. Preventive measures for security against Data Breach:

- Remove unwanted privileges given to the apps which are installed but are over privileged with the permissions.
- Next comes to stop reviling our information on the internet or to the windows.
- Third thing that should be kept in mind could be disabling Cortana.

IV. Precaution to Ensure Data Privacy

- **Use Complex Passwords:** Passwords are the gateways to the data which is present in the internet so choose passwords correctly, basic things to be kept in mind while creating passwords is not to choose anything which relates to personal life and could not be guessable or commonly used passwords like use names, places, dates and other familiar things associated with user. For instance, user can could use his dog's name and the date of graduation together can form super strong password [1].
- **User must be cautious while using Social Networking:** May social networking websites (*like Facebook, Twitter, Pinterest*) that allow user to create public profiles and add personal information like date of birth. Be fully aware of what user wants to display to the World. Identity thieves can take little bits of personal information displayed here to eventually access greater personal information later.
- **Beware of fake emails:** User often receive lucrative offers many emails telling users to have package, gifts, lottery or asks user to check their bank account by providing a phishing link looks like original. Remember never click on any link redirecting from email received. Never do this! It is often best to go directly to the website by typing in the web address, if you are familiar with the website such as your bank and log in there.
- **Bewarewhile Online transaction:** Make sure user is using a secure connection security site of website, "http://" should change to a "https://" The extra "s" stands for secure also comes with a lock or key which must be represented on the lower corner of webpage.

V. Necessity of Personal Data Protection

According to Data Protection, "Over 100 countries around the globe have enacted comprehensive data protection legislation, and around 40 countries are in the process of enacting such laws. Other countries may have privacy laws applying to certain areas, for example for children or financial records, but do not have a comprehensive law on data protection" according to survey published in January 2018.

It's a serious issue for many countries not having any comprehensive data protection framework and data protection is regulated through sectorial laws where it is regulated at all. For instance, though an early leader in the field of data protection, the US Privacy Act 1974 applies only to Federal Government, and subsequent laws apply to specific sectors or groups of individuals (e.g. the Children's Online Privacy Protection Act [COPPA]), but there is no comprehensive data protection law to date this approach is still in place in many countries, including India. A significant development in data protection law occurred with the adoption of the EU General Data Protection Regulation (GDPR), which will take effect on 25 May 2018. The GDPR is comprehensive, covering almost all personal data processing [2].

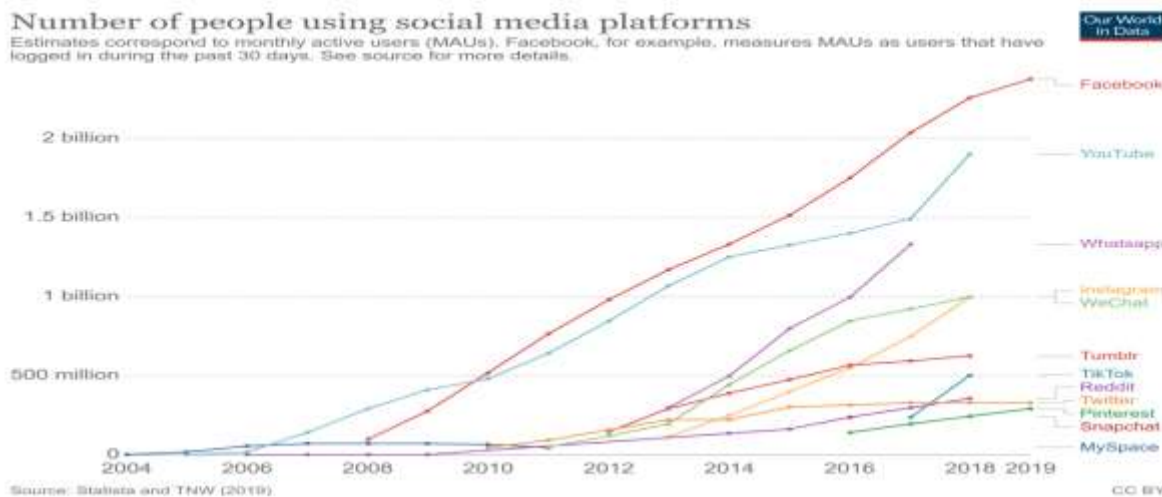


Fig.1 Showing progress in number of people using social media platforms

By analysing above statistics, there is huge population of the earth which are connected to social media and user fond of posting about our life what they are doing, where they are going what are there likings, who are there in their family and where do they live and spend time so it becomes easier for any attacker to attack users who are publicly available on internet via social media to attack or fraud them simply than a person who is isolated from internet.

It's known fact we can't keep people away from social media, but everything in your life is not to be published publicly *sherlock* is tool authors had personally used this and after change the script to track down details of a person which is present on Internet.

VI. How Google collecting personal data—critical review

Google is like water if anyone want to flow in the river of technologies most of the internet users trust Google without knowing which data to be shared with it and sometimes it tracks personal and private information which users don't even like to share. Google uses machine learning technique to gather user data to flash ads to promote their brands and ear a lot from affiliate marketing from where they earn revenue.

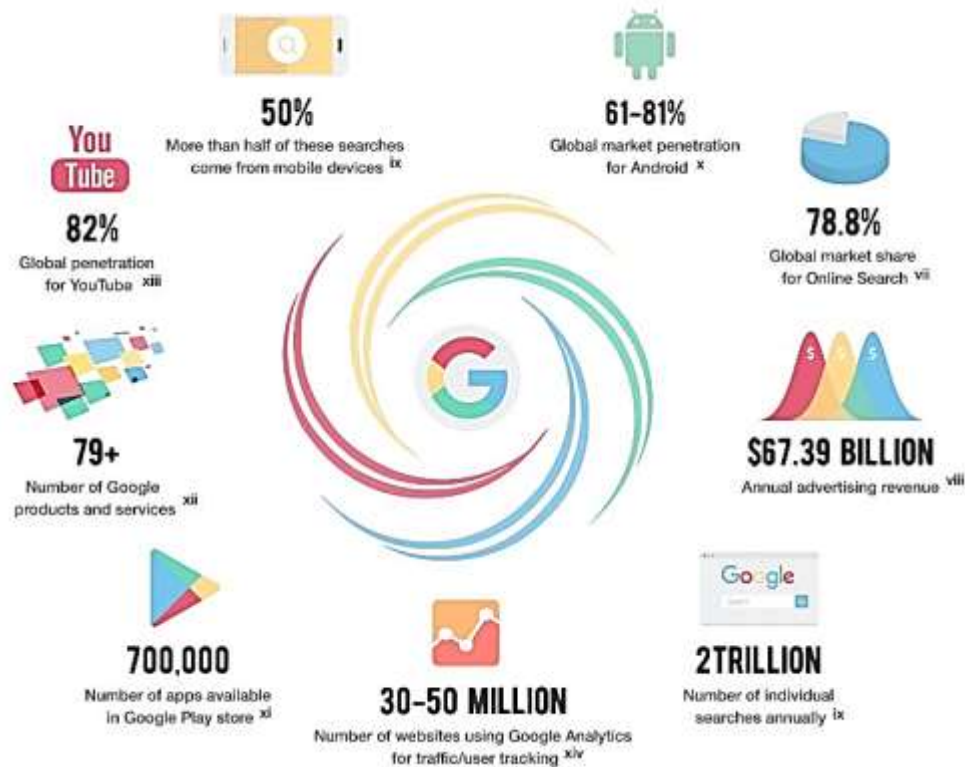


Fig.2. Different kinds of data collected by google

Above figure illustrated how and what kind of data Google collects which is directly or indirectly shared by users using internet. It is very important to know how Google gather data from Internet users for which three simple component gateways are used to dig personal data

- i. Things users do on Internet.
- ii. Things user create using Internet.
- iii. Things which makes to track location and activities performed by users.

Conclusion

Data privacy is not only how the law “*The Personal Data Protection Bill*” presented in 2018 but it is more than a simple privacy word. Being a responsible and educated personal it is forest sole responsibility to understand and stand to protect your own data where, what and how much to be used by big market players companies who had million-dollar marketing businesses based on the personal data gathered from different sources. User itself must ensure to prevent, preserve and protect their personal data without their permission to get sold. Author further explained how social media platforms are mainly responsible for data leaks and information stealing with different strategies. Further author also suggested few preventive steps to avoid private data leaks like keeping their profiles private restricting unknown users to access and changing password frequently, complex choice of password also prevent any hacking, brute force attack. Use of secure online transaction by following various security indicators on webpage or app. Also, authors also explained how to get aware to check whether site is storing any cookies or not, monitor cloud storage what to store or not. Ensure strict compliance of location monitoring by different apps whether you want or not. Last but not the least any rules, policy or law is not going to ensure 100% security of your personal data, thus everyone need to ensure privacy and security of their own by implementing above mentioned techniques.

References-

1. Joe Kissell, “Create stronger passwords”, an article published on dated 6th July 2009 by MacWorld. URL - <https://www.macworld.com/article/1141390/strongerpasswords.html>.
2. An article on Data Protection, “The Keys to DataProtection” published on August 2018 on privacyinternational.org pdf URL - <https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf>
3. The Personal Data Protection Bill - 2018, published by MEITY, Government of India, pdf URL - https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
4. Giannis Stamatellos, “Computer Ethics: A Global Perspective” 1st Edition, published on 5th January 2007, published by Jones and Bartlett Publishers, Inc. ISBN - 978-0763740849.
5. An Article on Crime Prevention, “10 Ways To Protect Yourself From Identity Theft” published by Houstontx Police, URL - https://www.houstontx.gov/police/crime_prevention/id_theft.htm
6. Godbole, Nina, Et.al , “Information system security: Security Management, Metrics, Frameworks and Best Practices”, published by Wiley in Year 2009,, ISBN-978-81-265-1692-6.

