International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Volume 7 Issue 4, April-2018, Impact Factor: 3.578

Data Privacy: A Leading Issue

Parul Suneja[1], Chirag Anand[2]

Department of Computer Sc. and Applications, Maharshi Dayanand University, Rohtak, Haryana)

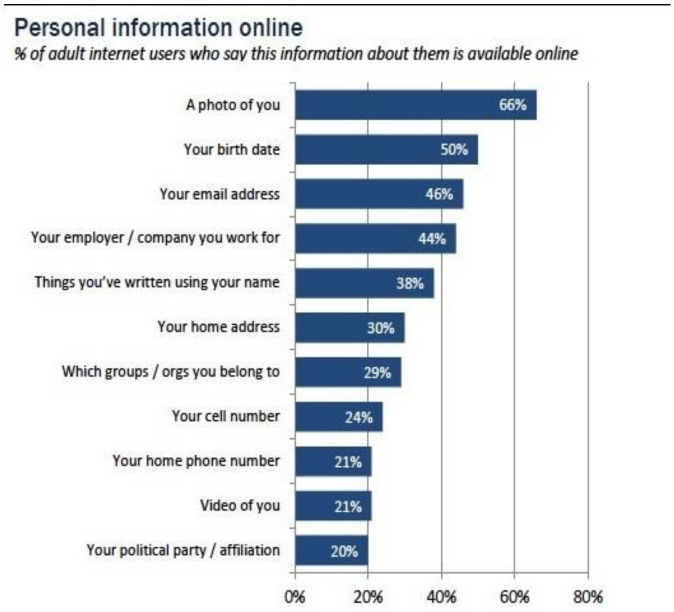
Keywords: Data Privacy, Cybercrime, Ethical behavior, Cyberspace, , Data Security

INTRODUCTION

In the digital economy, data strategic importance with social, economic and governmental activities increasingly carried out online. The flow of personal data is expanding fast, raising issues associated to storage and use. As fast as mankind's methods of communication is evolved, so too have surveillance technology for breaching privacy. Data Privacy breaches happen daily, in too many places at once to keep count. Today they are terrifying and capable of grabbing more information than ever before. Data is all about us; we are the Subject, the Product and the Price. Every phone call, every e-mail, every site we visit, place we go to and text we send can be traced. Current technologies, cloud services, the internet of things and big data as well as future technological innovations and increased connectivity through 4G and 5G networks can deliver enormous benefits but they also make it more urgent to address various concerns over data and its privacy. The aim of this paper is to put light on such concerns and discuss how and to what extent our life had become vulnerable. An attempt has also been made to recommend certain steps to facilitate ethical behavior in an online environment.

WHAT IS DATA PRIVACY

In simple terms, Data Privacy is the practice of keeping data secure from corruption, unauthorized access and wrong hands.



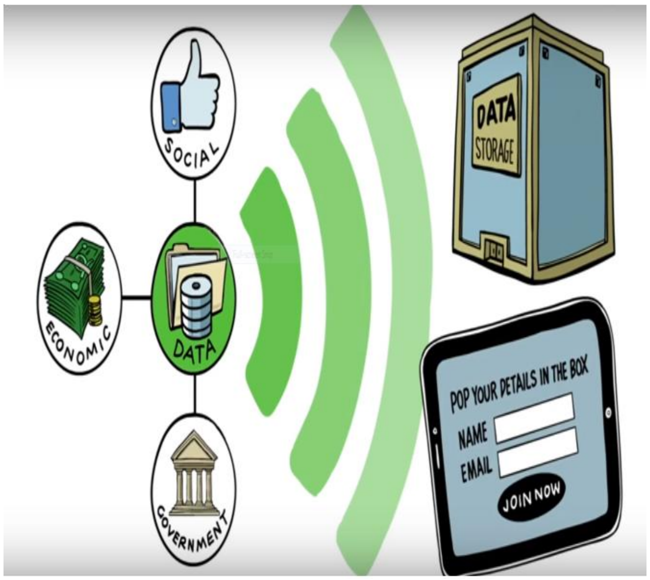
The focus behind data privacy is to ensure security while protecting personal and corporate data. This may be a wide range of information from personal files and intellectual property to market analytics and details intended to top secret. Data could be anything of interest that can be read or otherwise interpreted in human form.

However, some of this information isn't intended to leave the system. The unauthorized access of this data could lead to numerous problems for the larger corporation or even the personal home user. Having your bank account details stolen is just as damaging as the system administrator who was just robbed for the client information in their database.

PERSONAL DATA AND DATA PROCESSING

Take a look at your phone how much information about you is stored on it and how safe do you think that information is? Do you shop online, send messages on social media, Google search and perform general life simplifying tasks?

Of course we all do. It's impossible to participate in this era's social and professional life without doing some of that stuff. And we lock our phone to keep it safe because Hey! We would hate if the information about us is to be in someone else's hand. Google and Facebook and the store we shop at and the location we tuned in yesterday are happy to collect and mine our information. This isn't just our mobile phones or computer, this is our whole life. A pretty comprehension picture about us is built which includes our history and future as well. On the top of that, this isn't the information we give then knowingly, in fact we have very little knowledge or control of what information is being emitted.



What firms do with personal data is known as data processing.

They could do anything with that data from gathering it to ordering it, storing it or making sure its secure to transport and transmit and also it covers how you dispose it when you don't need it anymore.

AREAS OF CONCERN

In section highlights the few areas of concerns where our personal or corporate data is at risk and to what extent.

AADHAAR

Aadhaar card is a unique identity card for the people living in India. It has been made mandatory for an Indian to have an Aadhaar card.

This Aadhaar card has our Demographic and Biometric data like:

- Fingerprints
- Iris scans
- Signature
- Address
- Date of Birth
- Photo, etc.

भारत सरकार
Government Of India
Name
XXX XXXX XXXX
DOB / XX XX XX
Sex / XXX
XXX XXXX XXXX
Aadhaar - Aam Aadmi ka Adhikar
bankbazaar.com
AADHAAR
Unique Identification Authority Of India
Address
XXX XXXX XXXX
XXXX XXXX XXX
XXX XXXX XXXX
XXXX XXXX XXX
XXX XXXX XXXX
XXXX XXXX XXX
XXX XXXX
XXXX XXXX
XXX XXXX XXXX
1947
18003001947
help@uidai.gov.in
WWW
www.uidai.gov.in

We have provided the government with all these sensitive details. Now the question again arises how safe is it with Government?

VULNERAILITIES IN AADHAAR

There is n number of things how a person can misuse your Aadhaar details. These are described in following steps:

- Firstly, host machine takes fingerprint and Aadhaar No. POC: The host machine can store the user Aadhaar No. and Biometrics, which can then be used without individual's consent.
- Secondly, POC: The PID(Personal ID) Block is not encrypted and so it is vulnerable to interception by Hackers or Criminals while data transmission.
- In the Last Process, POC: The host computer is connected to public Internet Servers (ISP) and hence is vulnerable to Viruses and Malware that can also steal the PID BLOCK.

HOW AADHAAR DATA CAN BE USED FOR ILLEGAL ACTIVITIES?

- Once theinformation and biometric are stolen they can be used against you in an Identity Theft.
- Biometrics can be used to make a 3D printed fingerprint clone that can be planted in acrime scene.
- This Information can also be used in a bomb blast to identify a specific person, having this information in wrong hands can save a criminal and ruin your life.

In February 2017, six employees of telecom service provider Reliance Jio were arrested for the fraudulent use of fingerprints to activate and sell SIM cards. There were also reports that month about Axis Bank and other entities storing and using biometric data - without authorization - Aadhaar leaks of pension beneficiaries in Jharkhand. Another report indicates that personal information, including Aadhaar numbers, can befreely obtained through a simple online search.By these cases we can get a gist of how vulnerable our Aadhaar data is.

CREDIT CARDS/DEBIT CARDS

Carding fraud is a form of identity theft in which an individual uses someone else's credit/debit card information to charge purchases, or to withdraw funds from the account. Carding fraud also includes the fraudulent use of a card, and may be accomplished by the theft of the actual card, or by illegally obtaining the cardholder's account and personal information, including the card number, the card's security number, and the cardholder's name and address.

For a country racing towards the adoption of the most sophisticated payments system in the world and the gradual abolition of cash, India seems particularly cavalier about cyber security.

India's banking is substantially done through ATMs, debit cards and credit cards, and now, increasingly by mobiles. As we adopt the Unified Payments Interface, the need for all-round security awareness will be greater.

HOW CARDING FRAUDS ARE CARRIED OUT

Carding is one of the greatest reported cyber-crime and that too in 97% of the cases committed by Youth of the country. There are different ways for a Carding Frauds to be carried out. Some of them are:

- Through Social Engineering
- Use of Skimmers
- Phishing
- Cloning of Card, etc.

Carding Cases

According to a report, Jamtara -a Jharkhand district has in fact turned into the country's hub of phishing calls - a widespread criminal practice of stealing private and financial information from the vulnerable in order to swindle them out of their money, digitally.

Cases of finding skimmers attached in ATM booths have gone considerably high. Credit card fraud is happening at all times of the day and night, which is why it's so important to keep an eye on your accounts. According to a report from Javelin Strategy, there's a new identity theft victim every two seconds, and many of the incidents involve credit cards and debit cards.

According to Mr. Rakshit Tandon-a renowned cyber security expert and director of Council of Information Security(CIS)-he is receiving nearly 30 complaints on daily basis where some sort of carding is involved.

ATM-Debit/Credit Card Fraud Cases
State Bank Cash Deposit Machine
MasterCard
VISA
VISA

This is happening because Skimming data from unprotected smart phones will be infinitely easier, especially when user awareness about safe practices and anti-virus protection for mobiles are practically non-existent.

While the short-term answer to the breaches in banks' security systems is to reissue debit cards, clean up servers and build more firewalls (individuals can change their PINs through internet banking), not handling sensitive details like PIN or card details to just anyone. In the longer term there is no getting away from the fact that India has to invest more in cyber security and anti-hacking capabilities.

FACEBOOK

Facebook is today's biggest social network on the planet. As much as consumers claim to have concerns around Facebook privacy issues, we sure don't mind handing our information over to it left and right.

Every single day, more than a billion active users share their thoughts, photos, news, videos, memes, and more with friends and connections on Facebook. Sure, we know we're sharing that content and the associated meta data that goes with it back to Facebook. Our sign-in and posting locations; where we took a certain photo; what events we attended and which artists we enjoy. We share all of this, much of it indirectly, without a second thought.

And yet some of us are still surprised when it seems like ads are following us around the web.

Have you ever searched for something, only to see that same product pop up in a sponsored post in your Facebook stream the next time you sign in?

Or read an article about a certain topic, then had ads about that topic appear in your Facebook newsfeed?

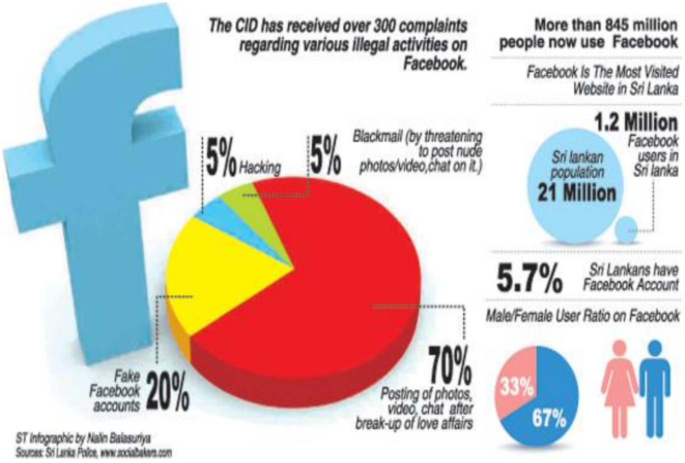
The amount of Facebook data collects about us is staggering, and it's not for no reason. They essentially lease out our online profiles to companies looking to sell us goods and services.

In fact, examining those Facebook ad targeting options sheds a lot of light on just how much personal information they're collecting-everything from relationship status to location, life events, political leanings, interests, digital activities, and personal connections.

Facebook's partnerships with offline data tracking companies means it has a crazy amount of information about your online activities, but also about the money you spend and the things you do in the real world, too.

CASES

Facebook wants to know where you're from, how old you are, who you're friends with, what industry you work in, your likes, your relationship status, where you vacation, etc., etc., in large part because marketers want to know those things.



And just imagine all of your personal data going to someone who can misuse it. The percentage of crimes involving social media platforms like facebook /instagram are increasing at an alarming rate. Crimes like cyber bullying, leaking of private photos by someone getting access to your fb account which often leads to cyber extortion or blackmailing, Impersonation, pornography cases, also crime against community/religion is often spread by Social Media platforms. And the root cause of all these crimes our over sharing and over indulging habits of people.

GOOGLE

The word Google needs no introduction. Google is the World's largest used Search engine of our time. Every search you conduct using Google's ubiquitous search engine allows the company to track your interests and, over time, build a detailed dossier that describes virtually every aspect of your character, food preferences, religious beliefs, medical problems, sexual inclinations, parenting challenges, political leanings and so on.

Even if the company doesn't know your name, it can still track your searches by reading codes, such as your IP address, that are unique to your computer or current location. Through cross-referencing, the company can eventually find your name, address, and telephone number, too. When we use the search engine or any other Google product, Google also installs an identifier cookie on our computer that makes us easier to track. And get this: Google reads and stores every letter we type into its search bar like as you are typing (think: h-a-c-k-i-n-g), so even if your good judgment suddenly kicks in and you don't hit "enter," the company still records what it thinks you were looking for.

Google uses our search history to send us personalized ads. That's how it survives, after all. About 97 percent of the company's revenues are from advertising. Google justifies this business model, which could be viewed as fundamentally deceptive, by insisting that it's providing a unique and valuable service: sending vendors your way who precisely fit your current needs and interests.

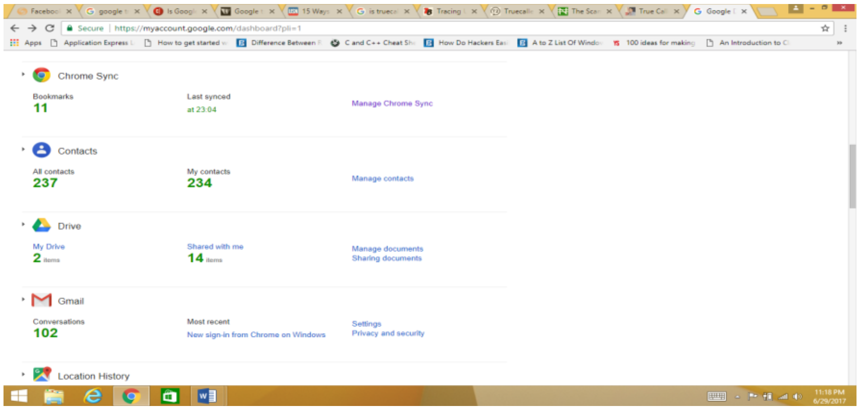
When we use Gmail, Google's email service, the company scans the content of your emails and the email addresses of our correspondents. Google's Gmail system also scans your incoming emails, even the ones coming from Yahoo and Hotmail. If you feel safe because you've deleted emails you regretted sending, think again. Google never erases its own copies, even copies of the drafts you decided not to send – even copies of incomplete messages you didn't save as drafts. And then there are those Google servers, which route the emails of thousands of companies that apparently don't mind running the risk that their emails will be scanned. So whether you use Gmail itself, write to someone who uses Gmail, or, in many cases, simply email, Google's gotcha.

RISKS AND VULNERABILITIES

When it comes to Google, we are at a greater risk than anything else. No amount of repercussion caused by unauthorized access of any other account can bypass that of Google.

This is because our whole life is stored on Google database from our personal pictures and sensitive documents on Google Drive to our work related and personal emails, our searches, our location, our calendar activities, apps stored on our mobiles, photos stored in our phone, mobile phone activities, our contacts, even other apps data that are linked to Google. Phew! The list is even longer which is not feasible for me to cover in a 15 pages report.

If you want to a taste of information Google know about you just write Google Dashboard on your browser and login with your Gmail account. You would be thrilled by the results. Below are some snapshots of the that.



https://myaccount.google.com/dashboard?pli=1

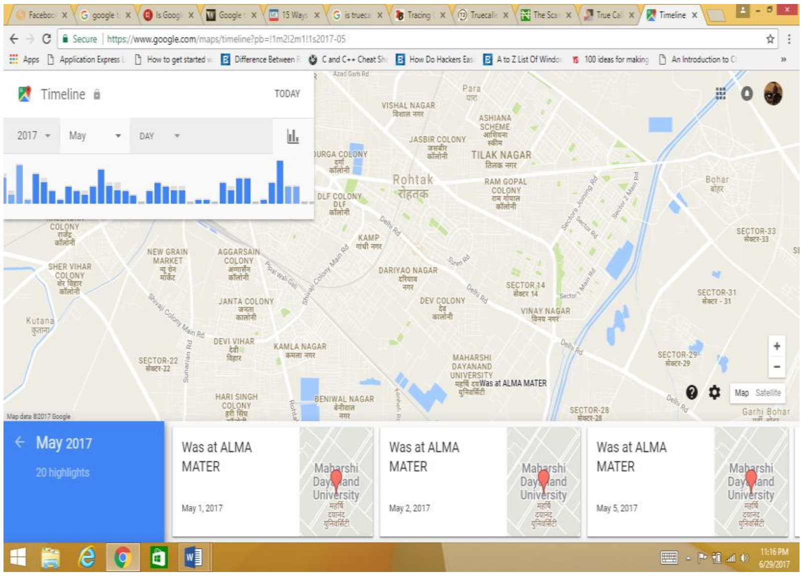
Chrome Sync
Bookmarks 11 | Last synced at 23:04 | Manage Chrome Sync

Contacts
All contacts 237 | My contacts 234 | Manage contacts

Drive
My Drive 2 items | Shared with me 14 items | Manage documents, Sharing documents

Gmail
Conversations 102 | Most recent: New sign-in from Chrome on Windows | Settings, Privacy and security

Location History



https://www.google.com/maps/timeline?pb=!1m2!2m1!1s2017-05

Timeline | TODAY
2017 | May | DAY

May 2017
20 highlights

Was at ALMA MATER
May 1, 2017

Was at ALMA MATER
May 2, 2017

Was at ALMA MATER
May 5, 2017

PREVENTIVE STEPS

- If you want to stop Google tracking your searches for good, head to the activity controls page and toggle tracking off.
- Google's location history, or timeline page, serves up a Google Map and allows you to select specific dates and times and see where you were. Its accuracy depends on whether you were signed into your Google account and carrying a phone or tablet at the time.
- How to delete it: When you visit the timeline page you can hit the settings cog in the bottom right-hand corner of the screen and select delete all from there.
- There's also the option to pause location history by hitting the big button in the bottom left-hand corner of the screen.
- If you've used any of Google's opt-in voice features for yourself, then head to Google's Voice & Audio Activity page to review your voice searches and listen back to them.
- To delete this database of embarrassing searches select one or more of the recordings from the check box beside them and then click "delete" at the top of the screen.
- If you want to stop Google tracking your searches for good, head to the activity controls page and toggle tracking off.
- Using Google's OAuth protocol, which allows third-party users to access your other accounts without finding out your password details, Deseat. me brings up all your online and social media accounts and allows you to delete yourself from them.

How to delete it: Visit Deseat. me and input your Gmail address. It will bring up all the online accounts linked to that email address and allow you to get rid of them.

OLA/UBER

Ola and Uber are ridesharing platforms that connects drivers and partner drivers using a Smartphone application.

For this Ola and Uber application access our location, our phone number, our debit/credit cards details for payments etc. Seems legit enough but give it another thought. Is that it? Well the answer is a big NO!

The applications like that -by just tracking our locations- knows our house address, our office address, our frequent hangout points, the places we visit. In short all of it is stored on their database; tracking us is “halwa” for them.

Which makes it a whole lot of easier for someone to stalk us.

On the top of that a recent news disclosed that these apps are tracking its customers even when they’re not using the app in the interest of being the most precise transportation service around.

The most alarming thing about this is that there are no preventive measures. If you are using these applications, you can not control the data they are able to access.

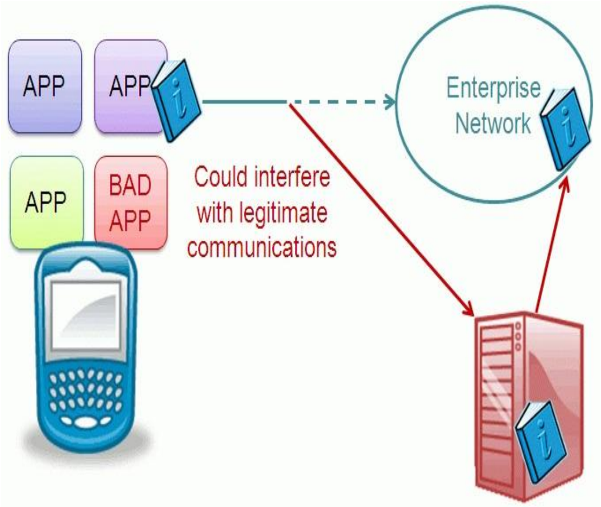
PROTECTING YOUR PRIVACY

•How often do you get asked for information about yourself or fill in a form with your personal details?
•How do you know you are handling it correctly?
•Are you concerned about your own personal data or what people do with yours?

Those are the questions you should ask yourself when talking about our privacy.

There has been a huge emphasis on data security as of late, largely because of the internet. There are a number of options for locking down your data from software solutions to hardware mechanisms. Computer users are certainly more conscious these days.

The first step in protecting your data privacy and security is to identify the types of information we want to protect and where that information is exposed in our organization or day-to-day life. In other words, simply categorizing which type of information or data is okay to share and to whom.

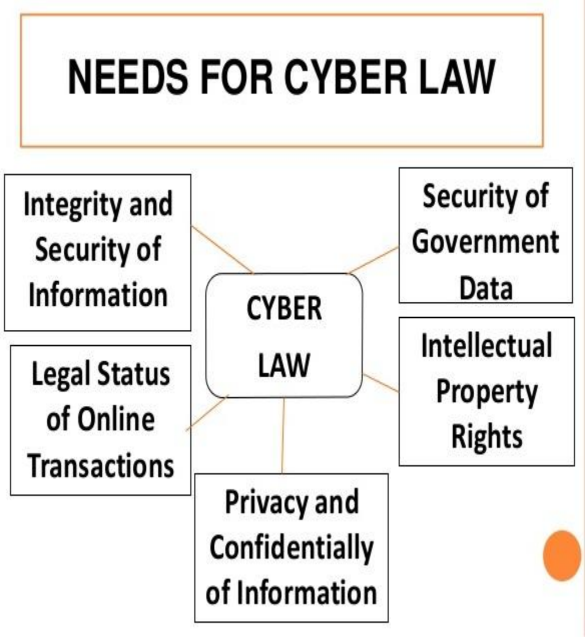


Once completed the audit - identified one's priority information and determine the level of risk of data loss - the next step is to assess your applications and understand what areas of your application portfolio are leaving you vulnerable to external attacks.

According to a recent Gartner report, the market for content-aware data loss prevention solutions continues to grow at more than 20 percent year over year. Yet the report also notes that from an organization point of view, many organizations are struggling to establish appropriate data protection policies and procedures for mobile devices as they interact with sensitive corporate data. These organizations are aware of the data breaches and consequences they might suffer due to it but still facing major problems.

PRIVACY LAWS

The major setback and concern for India in these times when it is working on ambitious projects like Digital India is that there is "No Privacy Law". The Constitution of India doesn't recognize Right to Privacy as a Fundamental Right.


NEEDS FOR CYBER LAW

CYBER LAW

Integrity and Security of Information

Security of Government Data

Legal Status of Online Transactions

Intellectual Property Rights

Privacy and Confidentially of Information

Although Right to Privacy is implicitly covered under Article 213 of the Constitution. Moreover after the amendment in the IT Act 2000, Section 43A and 72A4 were added ensuring reasonable privacy.

But this is not enough as with ever increasing data comes a greater threat of Security and chances of data breaches.

When the entire world is struggling to ensure their Rights to Security and Privacy and Government around the World are passing different laws, amendments, bills; India also needs to tighten the reins of law regarding Rights to Security and Privacy to keep up with the expanding cyber world and ever increasing crimes.

CONCLUSION

From the above discussion we conclude that in India, the most important piece of legislation organizations must worry about is the Data Protection Act and the possibility of fines by the information commissioner (ICO).

It's tempting to believe that important data breaches only happen in the US; it accounts for the overwhelming majority of the really big data breaches that have been made public, some of them absolutely vast. But US laws and regulations force organizations to admit to data breaches involving the customer, something which is not true in all countries. So here arises a greater need for spreading awareness about the current crucial problem of Data Privacy.

The challenge in data protection regimes is in managing the risks and addressing the concerns without restricting or eliminating the potential benefits. The role of government and the industry in protecting online data is of paramount importance. It must be done with a great deal of trust and confidence. This requires collaboration across stake holders and geographies.

Also on a personal level one must put a great effort and thought on cyber ethics that is what kind of data we are putting online. There is no need to over indulge in social and digital platforms and putting our privacy at risks.

REFERENCES

[1] Cybercrime in India up 300% in 3 years: Study by Economic Times http://economictimes.indiatimes.com/ tech/internet/cybercrime-in-india-up-300-in-3-years-study/articleshow/53858236.cms
[2] Special Investigation: How the Jharkhand jungle turned into the central hub of cyber crime in India http://www.dailymail.co.uk/indiahome/indianews/article-4085480/Special-Investigation-Jharkhand-jungle-turned-central-hub-cyber-crime-India.html
[3] In A Shocking Breach, Aadhaar Details Of A Million Pensioners Leaked In Jharkhandhttp://www.huffingtonpost.in/2017/04/22/in-a-shocking-breach-aadhaar-details-of-a-million-pensioners-le_a_22051319/
[4] Google Dashboard maps timeline https://www.google.com/maps/timeline?pb
[5] Role of Cyber Laws and its usefulness in IT industry http://ieeexplore.ieee.org/document/6194495/
[6] News uber wants to track our locations https://www.theverge.com/2016/11/30/13763714/uber-location-data-tracking-app-privacy-ios-android
[7] Data Breaches: What The Underground World Of "Carding" Reveals https://www.pcisecuritystandards.org /pdfs/DataBreachesArticle.pdf
[8] Cyber Laws in India http://www.cyberlawsindia.net/
[9] Vulnerabilities and framework of Aadhaar https://scroll.in/article/833230/explainer-aadhaar-is-vulnerable-to-identity-theft-because-of-its-design-and-the-way-it-is-used