American Journal of Computer Architecture 2020, 7(1): 1-3
DOI: 10.5923/j.ajca.20200701.01

Digital Arena and Data Discretion

Chanchal Gupta

Pittsburgh, PA, USA

Abstract Today, its more obvious than ever to protect user information in digital world. All the technologies we are using these days' capture our information in some form or other. Positive side of these information is, Industries/Agencies can use this information and build the newer technologies or tools to help the society. On flip side, these details can be used against individual's wish, it can damage the user's integrity, unauthorized access to details, financial loss, fraudulent charges, etc. Its judicious for general person to read privacy policy of the organization before sharing the personal information. Recently, government has taken major steps to oblige the data privacy laws. Industry/Agency are being held liable to retain the data integrity and take major guide lined steps to avoid data breach. Industry/Agency are also in risk, if they do not protect the data or exploit user's information against their will. It may cause lawsuit and company may go bankrupt to pay the damage it has caused to individual's data breach. There are various data protection laws help citizens to get their data protected and forcing companies to adhere to policies. E.g. Safe Harbor, FCRA, HIPPA, GDPR, PIPEDA, CCPA and more.

Keywords Data Privacy, Digital Arena, Security, Data access, Safe Harbor, FCRA, HIPPA, GDPR, PIPEDA, CCPA, Engineering and Technology

1. Introduction

Internet has boosted the accessibility of information. Almost all the public information we are looking for, are available in our finger touch. We are sharing our personal and confidential information over the internet knowingly or unknowingly. There are various advantages of using internet and sharing data to make our life easier. Internet has made possible to do banking transaction online, send money to remote person in seconds, share your health record with remote doctors, buy car online. All the industries have some kind of digital presence and doing some level of transaction over the Internet. It has made our life easier and made things more accessible. To make the things connected we need data, lots and lots of data. Its required to share details over internet to take advantage of technology. We are relying more and more on internet and sharing our personal details to complete the job, sitting on our couch.

More and more people are getting access to internet and some of the people are accessing confidential data using the technology. We have seen companies who provide some free or paid service use our data to run their business. Some agencies even sell our data to third parties. Some companies do not make proper measure to safeguard our data and being hacked by hackers. In current world people feel vulnerable to lose their confidential details.

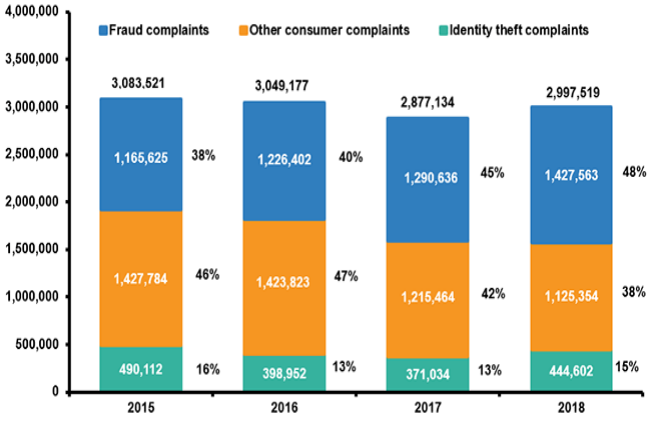

Figure 1. According to insurance information institute there are 3,083,521 cases in year 2015 and 2,997,519 in year 2018. (Figure 1) These analyses escalate to bigger question(s), how to make data safe

2. Method and Techniques

As these fraud incidents are increasing, Governments and Companies are taking steps to make data privacy utmost priority. Recently there are various data protection laws has been introduced by Government(s) to protect user data and privacy. Tech companies are coming up with more and more secure technologies. According to privacyinternational.org, Protecting privacy in the modern era is essential to effective and good democratic governance. However, despite increasing recognition for and awareness of the right to privacy and data protection across the world, there is still a lack of legal and institutional processes and infrastructure to

* Corresponding author:
chanchalpgupta@gmail.com (Chanchal Gupta)
Published online at http://journal.sapub.org/ajca

support the protection of rights. Some parts of the world in particular suffer from a void: a lack of regulatory and legal frameworks in many countries, and the poor implementation and enforcement in others. Technologies used to save privacy data:

1. Firewall: a firewall is network security device that monitors all traffic, it allows and denies access based on the firewall rule. Many companies use firewall to restrict unauthorized access. We could have software or hardware firewall. Software is a program running to monitor traffic where hardware ia a piece of equipment between network and gateway.
2. Data Encryption: Data encryption is a process to transform data into another format using defined algorithms. we use encryption to de-identify data. We can use keys, has tables, and various way which converts data into un-readable format.
3. Data Classification: Data calcification is processed to unify data to make it accessible based on role and security model. It comes handy to be compliance by laws and secure data.
4. Token based access: To access data we can use token-based authentication, so each time user needs to get authorization token key to protect data breach. We can also make two factor authentications in api calls.
5. Relational data management: Use of relational database make data more secure. We can break data into using multiple schemas. This will safeguard direct access to whole information.
6. Cloud data protection: Moving your data to cloud bring another advantage, its secure and can be accessible easily on high traffic needs. Clouds has inbuild data loss and protection to recover data after uninvited situation.
7. Encrypted Transection: While we request data using applications, we should to encrypt transactional data to make it safer.
8. Limit Transection: We should limit transection so bots cannot keep hitting the databse in various ways. It safeguards data from unsolicited transection.
9. Data privacy management platforms: There are various data management platforms available in the market, we can consider these platforms to make data secure. Red-gate has complete solution available to manage the data platform.

Data Protection Law(s):

1. GDPR (General Data Protection Regulation): The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. [1] Superseding the Data Protection Directive 95/46/EC, the regulation contains provisions and requirements related to the processing of personal data of individuals (formally called data subjects in the GDPR) inside the EEA, and applies to any enterprise established in the EEA or—regardless of its location and the data subjects' citizenship or residence—that is processing the personal information of data subjects inside the EEA. It also applies to non-EU companies processing European personal data outside EU.
2. HIPPA (Health Insurance and Portability and Accountability Act): The Health Insurance Portability and Accountability Act of 1996 (HIPAA or the Kennedy–Kassebaum Act) was enacted by the 104th United States Congress and signed by President Bill Clinton in 1996. It was created primarily to modernize the flow of healthcare information, stipulate how Personally Identifiable Information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage.
3. FCRA (Fair Credit Reporting Act): FCRA is U.S. Federal Government legislation enacted to promote the accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies. It was intended to protect consumers from the willful and/or negligent inclusion of inaccurate information in their credit reports. To that end, the FCRA regulates the collection, dissemination, and use of consumer information, including consumer credit information. [1] Together with the Fair Debt Collection Practices Act (FDCPA), the FCRA forms the foundation of consumer rights law in the United States. It was originally passed in 1970, and is enforced by the US Federal Trade Commission, the Consumer Financial Protection Bureau and private litigants.
4. PIPEDA (Personal Information Protection and Electronic Documents Act): The Personal Information Protection and Electronic Documents Act (PIPEDA)is a Canadian law relating to data privacy. It governs how private sector organizations collect, use and disclose personal information in the course of commercial business. In addition, the Act contains various provisions to facilitate the use of electronic documents. PIPEDA became law on 13 April 2000 to promote consumer trust in electronic commerce. The act was also intended to reassure the European Union that the Canadian privacy law was adequate to protect the personal information of European citizens. In accordance with section 29 of PIPEDA, Part I of the Act ("Protection of Personal Information in the Private Sector") must be reviewed by Parliament every five years. The first Parliamentary review occurred in 2007.
5. CCPA (California Consumer Privacy Act): The California Consumer Privacy Act (CCPA) is a state

statute intended to enhance privacy rights and consumer protection for residents of California, United States. The bill was passed by the California State Legislature and signed into law by Jerry Brown, Governor of California, on June 28, 2018, to amend Part 4 of Division 3 of the California Civil Code. Officially called AB-375, the act was introduced by Ed Chau, member of the California State Assembly, and State Senator Robert Hertzberg.

Amendments to the CCPA, in the form of Senate Bill 1121, were passed on September 13, 2018. Additional substantive amendments were signed into law on October 11, 2019. The CCPA became effective on January 1, 2020.

3. Conclusions

Instead of various laws and compliance we still get to know about data breaches. Sometimes due to technology malfunction, sometimes companies' greed to make use of data to run the business in unsolicited way or hackers trying to get access to data. it obvious we need more and more stringent laws to make companies compliance. Also, if technology is getting advanced day by day and we need to keep updating the security rules to make sure we are ahead in the game. Technology and laws both are required to make this place make secure and accessible to make human life easy.

ACKNOWLEDGEMENTS

The heading of the Acknowledgment section and the References section must not be numbered.

SAP Productions wishes to acknowledge all the contributors for developing and maintaining this template.

Disclosure

This section is ONLY for those who requested disclosure. The name of the experts that reviewed your paper, in case they accepted selling disclosure to you, will appear here. Each reviewer is allowed to make their own price for that, since that is a public endorsement of your findings and may be used for varied purposes.

REFERENCES

[1] Insurance information institute, iii.org, facts-statistics-identity-theft-and-cybercrime.

[2] Privacyinternational.org, data-protection.

[3] The Politics Of The Health Insurance Portability And Accountability Act.

[4] en.wikipedia.org/wiki/Health_Insurence_Portability_and_Accountability Act

[5] oag.ca.gov/privacy/ccpa

[6] pric.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief

[7] ftc.gov/system/files/545a_fair-credit-reporting-act-0918.pdf