International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

A Study on usage of Online Personal Information By Data Brokers

Divya Dattatray Deulkar[1], Dr. Praveen Gupta[2]

[1]Student, YMT College of Management, kharghar
[2]Associate Professor, YMT College of Management, kharghar
YMT College of Management, Kharghar

Abstract: With increasing use of Internet, many things have changed drastically. From paying bills to booking tickets, nowadays everything is done online. We probably assume Facebook, Instagram, Google knows everything about us through the post we share, things we search and information we post online but there are group of companies who know our name, our email address, mobile number, some of them may also know what our interests are and what are we most likely to buy. Such websites monitor what we search online and follow our trails. Such group of companies are called Data brokers. There are various types of data that they might have about people such as identifying data such as name, address, sensitive identifying data such as driver's license number, birth data, demographic data like age, height, social media and technology data such as social friends, internet provider, online purchases. Such data becomes handy for business or companies who thrive to target us on knowing the respected data. Since such data brokers sell our data of what we search, what we buy and who we are, what we are more likely to get all the unwanted ads and junk mails of which some of it can be from fraudulent sites. One thing we can do is block such ads or report some mails as spam but that won't stop the data brokers from collecting our data and selling them. This paper details the measures to avoid the misuse of data by data brokers.

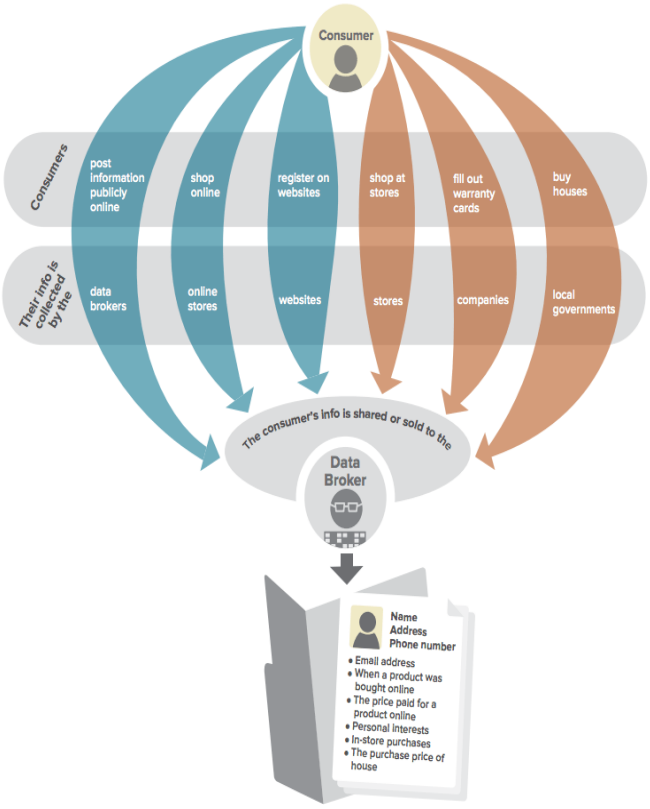
Keywords: *Data brokers, Internet, Information privacy, Social media, Consumer data.*

INTRODUCTION

Internet has become the answer for all our questions as it is a place where information is shared and web is being browsed for data. The screen between openly available information and private data has slowly started to diminish. By agreeing to and accepting the policies, users tend to indirectly permit the use of their information. Sometimes, such policies are difficult to understand. Giving away personal information may also invite stalkers, burglars. Whereabouts of people are easily tracked by these stalkers when pictures along with locations are posted. There are various applications that allow users to check in at their current location. These would also help data brokers to keep on track of places we often visit and they would formulate our data on basis of such information which gives away our interests, places we often visit, things that we often search. Some websites as well as applications offer us with data in exchange of another data. One of example of such application is Truecaller, when we first install truecaller it takes permission from us to track our location and access our contacts and by agreeing to it we provide our as well as others information without even asking them. When some other person searches for any mobile number, Truecaller uses numbers and information uploaded from our phone for that search. It would become of major risk if such applications are hacked or data brokers get hold of this information. Privacy is at stake because of internet and social media.

1.1 About Data Brokers and how the data is collected online?

Browsing something that you want to buy or are interested in would help data brokers to follow your trail wherever you go from one browsing page to another or it may even land in your mail box. This is of no coincidence or it didn't even happen by chance. This is by every means information provided by data brokers to different business companies who know that our interests and browsing searches are related to the products they sell. Data Brokers are those who collect different types of information about people and sell them for monetary gains. [5] Data Brokers collect information from various number of sources which of them includes:



Diagrammatic explanation on how data brokers collect information online and offline.[11]

- Social media sites such as Facebook, LinkedIn, Instagram play a vital role as they are used by data-brokers in obtaining information about people. It cannot be assumed on how and from where the data brokers collect information about people as there is no transparency about from where that data comes from and where it goes. The information that is obtained from such sites includes usernames, age, education, gender, location.
- Purchasing information from other data-brokers. This can be any retailer or data broker company who is selling data without knowledge of people about whom they are selling information.
- Web browsing also gives away majority information about the user. As certain sites use cookies to track user's trails. Data brokers may also attempt to clone a website which get majority hits and can obtain information about user.
- Registering to different websites to obtain certain services such as latest trends, news would lead to leak of user data. This data is mostly demographic data such as name, contact number, email address, age.
- Trading personal information for rewards. Some applications give users cash in place of reward points for downloading, installing and signing up their application and user unknowingly gives away their data like email address, birth date, gender, mobile number. [1][4]

1.2 Types of information Data Brokers collect

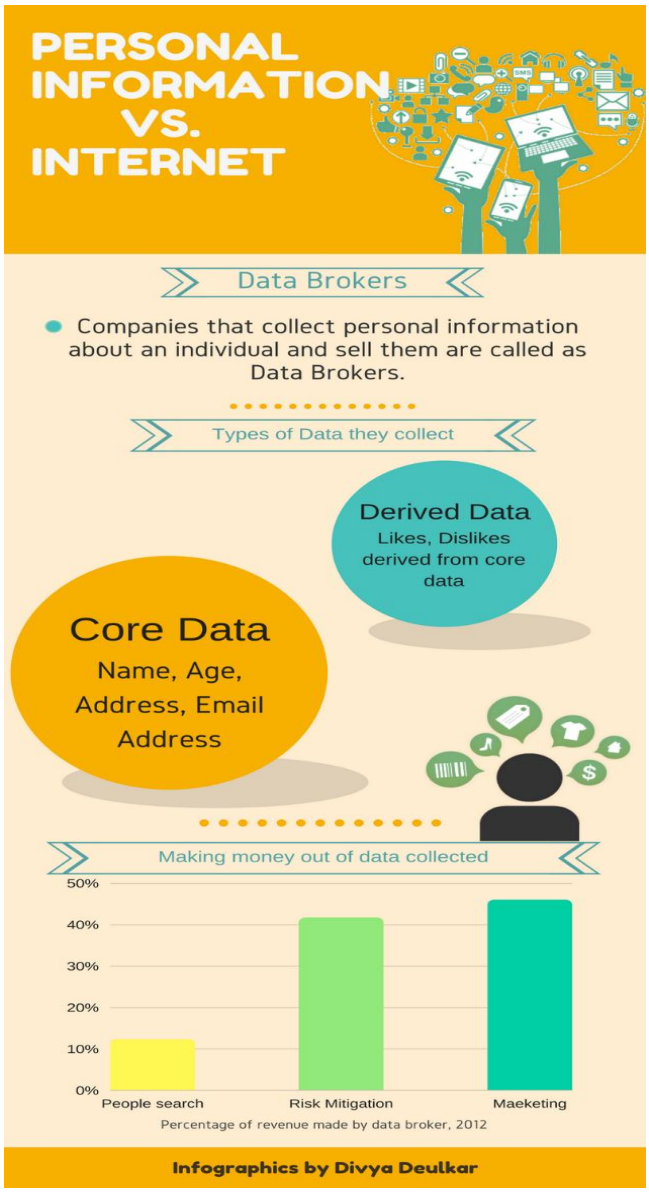
Data brokers usually collect all sorts of data but it is generally categorised as core data and derived data.

- Core data includes data such as address, age, name, phone number, email address and derived data is obtained by analysing the core data. Nowadays collecting data has become easier for data brokers because of heavy use of social media, different online e-commerce websites, internet in general.
- Derived data includes the person's interests, likes, dislikes. [2]

People often reveal details about their personal life without realizing it. Whenever information is posted online, registration is done, data brokers tend to track and collect information, and then sell to businesses and other companies. Data brokers also make guesses about a person and their interests based on other information they have, then sort them into different categories. Therefore, businesses can buy lists of people who might be interested in particular products and services. [6]

There is a fear that fraud companies might misuse personal information to plan fraud against consumers. For example, if certain loan is pending or amount is to come some fraud can be planned and people would be scammed based on this information. Therefore, there is high risk if the information stored by data brokers gets in to wrong hands. [7]

Source: https://aboutthedata.com/



1.3 Different types of data brokers

Data brokers are categorized into different categories based upon the type of data that they provide which are namely 1) marketing products,2) people search products,3) risk mitigation products. This data includes demographic data on the major basis. This data can be used for a good as well as bad purposes.

1) Marketing products that are sold by data brokers which enables their clients to reach to consumers via direct mail, email marketing, online marketing. These includes junk mails that land up in our inbox. This is of no harm as it does not affect user or consumer drastically. It only floods consumer's inbox with different marketing mails.
2) People search products
   It provides personal data of individuals. Users may use people search products to find lost relatives, friends. It can be also used for stalking or for other purposes. People search products may gain information about people from social media sites and other online publicly available sources, such as telephone directories.
   Since users do not have right to prevent data brokers from publishing their personal information, some Data Broker Sites explains how to opt out.
3) Risk mitigation products
   There are two categories namely identification verification and fraud detection. Identification verification is mostly used by banks for confirming identity of an individual whereas fraud detection helps out government agencies in verifying the information submitted by the individual. [4]

1.4 Importance of data collected by Data Brokers to different companies

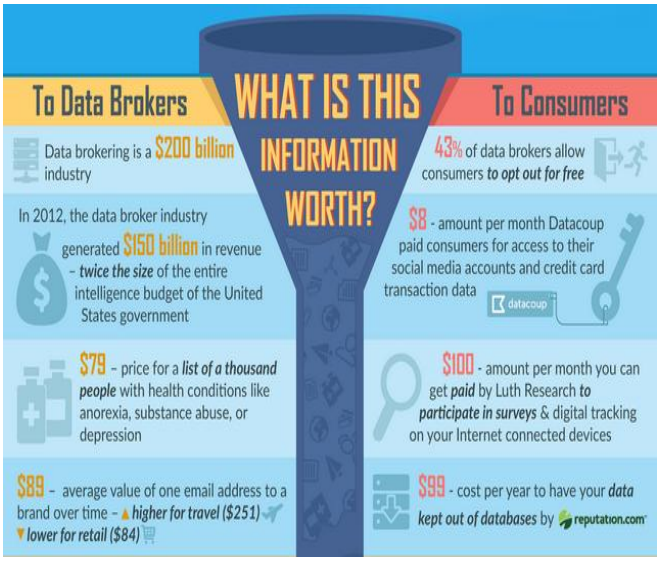
The data collected by the data brokers is very important for the company as it may help to increase the company's business. Companies use different types of data such as core or derived data in order that they may get to know which products users are likely to buy. This would help the company as well as the users and also this would make sure that the content of the mail that lands in the mail box is as per the user's likes and interest. [8]

1.4.1 Importance of data to Data Brokers

Data brokers do make a lot of money by selling an individual's data. Very basic information like email address has minimum value of 89 dollars. Over several years that has passed by passed by data broker industry has generated tremendous revenue of 150 billion dollars in the year 2012. [3]

Source:
https://www.webpagefx.com/blog/general/what-are-

data-brokers-and-what-is-your-data-worth-infographic/



1.4.2 Importance of data to Individuals

Some individuals do sell their personal data in return of another. On the other hand, if the individual wishes to remove the information from data brokers he or she has to pay also some data brokers allow to opt out for free. [5]

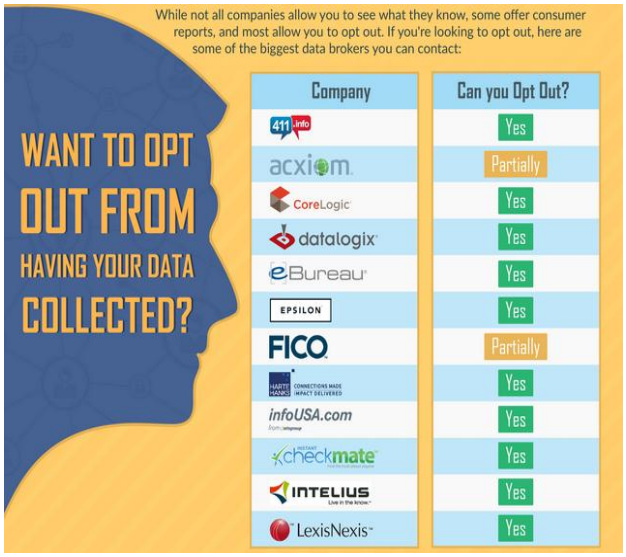
1.5 Accuracy of Data collected by Data Broker

The accuracy of data collected may depend on the data broker and may vary from company to company. There are certain individuals who provide false data which would mislead the business company who may buy that information from data broker. Data broker should always check for reliable resources when it comes to collecting data. [10]

2.1 Individual's rights regarding data correction, data approval by opting out certain data that individual desires not to be disclosed

According to Federal Trade Commission, they are looking into the fact that how and where the data collected by data brokers are being used currently by data brokers to maintain the privacy of individual's data but misuse of the data would invite a big problem. Federal Trade Commission has also issued regarding hoe the data brokers collect the information and use them. The companies that received orders are Acxiom, Corelogic, Dalalogix, eBureau, ID Analytics, Intelius, Peckyou, Rapleaf, Recorded Future. The Federal Trade Commission also wants to know about sources from where the individual's information is obtained, how the information is maintained and used, the extent to which the individuals are allowed to correct and see their information or opt out from being their information to be sold. [5]

Sourcehttps://www.webpagefx.com/blog/general/what-are-data-brokers-and-what-is-your-data-worth-infographic/



2.2 Laws that regulate misuse of data collected by data brokers

Opting out from getting the information being sold or disclosed is not an option for consumer. Some data broker company provide this option once certain amount of money is paid by the individual. Also, other companies allow the individuals to opt out partially. Acxiom is the known company that collects data about the users and also allow the user to correct the data if it is not proper but an individual can do this only when he or she has successfully registered and logged in. There are few steps the user need to follow in order to know what data about the user the company has. The procedure of seeing the data the company acquires in a way delivers the company more and efficient information about the user. As the procedure includes filling up certain form regarding the core information of the user. The individual should be provided with the authority to block the usage and collection of data by the data brokers. These would free the user from the worry of the data getting into wrong hands and being misused. [11]

2.2 Measures that could be taken to stop data brokers from collecting your data.

With increasing use of social media, it becomes almost impossible to keep the personal information out of reach of data brokers. With the constant tagging in pictures and posting pictures reveal important events in our life. These may include someone getting graduated, getting married, getting retired and the list goes on. This helps the data brokers to collect demographic as well as derived data. It can't be stopped completely but certain measures should be taken in order to protect your privacy online.[6]

2.2.1 Do not reveal your identity completely.

True identity is only required while filling up any government forms or if it is required by law. Not every bit of your information on online profiles like Facebook, Instagram, LinkedIn, needs to be completely correct. Also fill in information which is mandatory other boxes can be left blank as they are optional. Revealing your birth date, education, universities you have studied at would help data brokers to collect information about you. Therefore, one should be aware of what and where the information should be shared. [8]

2.2.2 Know that different sites are using cookies to keep track of what you are browsing.

Deleting cookies from time to time is the most important step when it comes to protecting privacy online. Cookies help websites to collect data about what you are surfing online. Privacy settings should be changed in order to block third-party cookies. It won't stop the data brokers from collecting your data but it would help to avoid them tracking your trails. [6]

2.2.3 Sign out of the social media accounts while you browse web.

While we are still logged in to Facebook and browse online we might notice the ads surfacing on Facebook about products we browsed earlier. Therefore, it is a best practice to log out of social media accounts and browse. This would also not attract the fake ads that we get on other websites. [5]

2.2.3 Use updated Virus Protection.

Always keep the virus protection up to date in order to avoid any malware entering into our system. This malware would either corrupt the data or steal the data which could be confidential. [5]

CONCLUSION:

With increasing collection of information by data brokers. There are certain pros and cons which comes along with it. It has impacted consumers as well as businesses drastically in a better way. It provides businesses with data of consumer likings and what consumers are interested in. This has made the work of businesses easier as they target only those individuals who are interested in their products. [1]

Data brokers have also taken few steps in maintaining the privacy of the demographic information of people. Sure, it does give option to opt out but there is lack of transparency as the person won't know if the data broker has completely and permanently deleted his or her information or it is on temporary basis. [2]

This research paper has provided a window on how data brokers collect information, different types of data that is collected, different types of data brokers, use of collected information by the businesses and how an individual can opt out and follow certain measures to avoid leaving digital footprint online. It has also focused on collection of sensitive data and measures to avoid the same. The recommendations and measures provided in this research paper could be used to secure personal data.[11]

REFERENCES

[1]https://www.opensocietyfoundations.org/sites/default/files/data-brokers-in-an-open-society-20161121.pdf

[2]https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

[3]http://crackedlabs.org/en/corporate-surveillance/#3

[4]https://www.privacyrights.org/blog/tutorial-data-brokers-and-people-search-sites

[5]https://www.webpagefx.com/blog/general/what-are-data-brokers-and-what-is-your-data-worth-infographic/

[6]http://time.com/money/2819049/data-brokers-online-privacy-tools/

[7]https://www.le-vpn.com/why-companies-collect-big-data/

[8]https://factordaily.com/online-offline-privacy-identity-theft-cybersecurity/?afu=bmFmfDE5M3wyNi0wNy0yMDE3fDE4OjA5OjQyfDU5NjF8bg==

[9]https://www.researchgate.net/publication/316581149_How_Social_Networks_and_Data_Brokers_trade_with_Private_Data

[10]https://www.csoonline.com/article/2134129/social-networking-security/data-brokers--collection-of-internet-activity-data-raises-privacy-issues.html

[11]https://www.priv.gc.ca/media/1778/db_201409_e.pdf