Ms. Loveleen Gaur
Asstt. Professor, GL Bajaj Insitute of Management and Research
Greater Noida

Privacy or Security: A Difficult Question and Yet to be Answered

Abstract

In the aftermath of 9/11/2001, The US government undertook many measures to gather intelligence; because it was claimed that intelligence failure was one of the primary reasons behind the inability of US government to thwart that destructive act of terrorism of US soil. Subsequently, the government embarked on a massive program of gathering data from all the possible sources so that they could extract pertinent information, which could help in avoiding the possibility of similar a acts in the future. In this context, the ADVISE (Anlysis, Dissemination, Visualization, Insight and Semantic Enhancement) program was launched in 2003 in order to find unusual patterns in data which could help the government in detecting suspicious activities and prevent the occurrence of a similar terrorist incident in the future. In September 2007, this ambitious multi-million dollar program had to be terminated because of the increasing concern among the people that this program had violated their ***right of privacy.***

INTRODUCTION

Campbell, 2002 quotes a statement from the book "Privacy and Freedom" by Alan Westin which says " The individual's desire for privacy is never absolute, since praticipation in society is an equally powerful desire" This statement is becoming food for thought and a matter of serious concern as the line between public and private persona is fading with the development of new technologies.

To fight terrorism, The US federal government proposed to build a massive computer system which could collect huge amount of data and link information from blogs, emails, government records and intelligent reports. They tried to extract the pattern of terrorist activity using Data Mining technology (Clayton, 2006). The DHS (Department of Homeland Security) tried to develop a research program under Threat and Vulnerability, Testing and Assessment" (TVTA) portfolio named ADVISE (Analysis, Dissemination, Visualization, Insight and Semantic enhancement). The aim with which ADVISE and DHS related Technologies was not merely to identify terrorist or sifts for keywords but to identify critical patterns in data which was supposed to illumine their motives and intentions. The ADVISE program was intended to collect data of corporate and public online information from financial records, emails, blogs, News stories from different channels like CNN and then cross reference it against US intelligence and Law enforcement records. After that these records were intended to be stored as "entities". The ADVISE and analytical tool could be used by all federal, state, local and private sector security entities for database sharing and also to provide full support for analysis and action (US Department of Homeland Security Report, 2007). Critics believe that this kind of technology could be a major challenge for individual's privacy.

Data mining can be used to detect unusual patterns, terrorist activity and fraudulent behavior for saving human lives but the dark side of this technology is Threat to Privacy and Civil Liberties. Data Mining tools

are available on Web and even naive users can easily download them and apply to extract the information stored in various databases and files which can violate the individual privacy (Thuraisingham, 2003).

DEFINING PRIVACY

According to Right to Privacy Act 1974, U.S.C Section 552, the constitutional right to privacy in the cyber context has been applied mostly to workplace privacy issues. Under U.S. law "Private sector employees are afforded virtually no expectation of privacy in the workplace and are not protected by the constitutional right to privacy". A few state laws, including state constitutional provisions which protect privacy in the workplace. Public sector employees however, may have some constitutional rights to privacy.

(a) To restrict discloure of personally identifiable records maintained on them.

(b) To grant individuals increased right of access to agency records maintained on them.

(c) To grant individuals the right to seek amendment of agency records maintained on them upon showing that the records are not accurate, relevant, and timely or complete.

(d) To establish a code of "fair information practices" that requires agencies to comply with statutory norms for collection, maintenance and dissemination of records.

PRIVACY ISSUE

The most Violent Element in Society is Ignorance

–Emma Goldman

The degree to which consumers feel their privacy has been violated depends on:

(a) Their control over their personal information when engaging in market place transactions. ***Do they feel they can decide on the amount and type of information collected by retailer?***

(b) Their knowledge of collection and use of personal information

Do they know what information is being collected and how other party will be using it?
Will they be sharing this information with other parties?

DATA MINING: A BOON OR BANE?

Data Mining is a Multidisciplinary field drawing work from areas including database technology, machine learning, statistics, pattern recognition and data visualization. Data mining, now days, has proved to be a powerful tool and is used to extract different patterns from large databases or massive information repositories. These patterns or knowledge discovered are used in decision making. Data Mining is used in various industries like telecommunication, health, CRM (Customer Relationship Management) etc. and has proved to be very efficient in extracting patterns for decision making. Technology always helps in enhancing the efficiency of business processes. In the era of IT and IT enabled services, development and deployment of new technologies is common. Data Mining is one such technology but, like every coin has two faces, this technology also has a bright side and a dark side. This technology can be used for extracting violate the customer privacy. Technology is a collection of the man made inventions and devices used to sustain, facilitate and enhance the quality of human life. Technology can be a curse or threat once compromised.

WHAT IS MOST IMPORTANT: PRIVACY OR SECURITY?

Civil Liberties are about protecting the right of the individual whether it is privacy rights, human rights or civil rights. Recently, there has been much debate among the counter terrorism experts, civil liberties unions and human rights lawyers about the privacy of individuals, gathering and mining information about people, conducting surveillance activities and examining emails and phone conversations because all these activities are considered to be a threat to privacy and civil liberties. The Mind stretching questions are:

Do we wait until privacy violations occur and then prosecute? or

Do we wait until national security disasters occur and then prosecute" or

Do we wait nutil national security disasters occur and then gather information?

So what is important? Protecting the nation from terrorist attacks or protecting the privacy of individuals?

It is very difficult to analyze where to draw a line. Privacy issues has gone beyond government intrusiveness. There can be times when employer could potentially use a person's DNA to determine if they should be hired based on their future health.

People are still sorting out, how much privacy they need? They are willing to be searched at airports for safe flights, but don't want marketers to know their personal details. They are willing to buy online or order from catalogs but don't want their information sold to solicitors (Campbell, 2002).

The desire of privacy is always situational and the discussion on privacy always became reason of tension between those who control the information and those who don't.

HOW MUCH PRIVACY IS ENOUGH?

The idea behind this debatable issue is how much privacy can be compromised and to what extent this surveillance technology is allowed to dig the patterns which can help them to identify the terrorist activity, if any, without doing any kind of personal damage to consumers. It is wrong to look at ADVISE or related program related to security as good or evil. The emphasis should be "How it will be used?" for *e.g.* if evidence about suspected terrorist is presented to court of law, ADVISE should be allowed to reveal the suspect's message. But if it is installed at every cop on the beat, the privacy is violated. There is a huge difference between one time screenings and storing the information like program which determine the suspect of terrorist activity.

Now days researchers are focusing on the area of Privacy enhanced Data Mining

PRIVACY ENHANCED DATA MINING

The main challenge that Data Mining is facing is "To provide solutions to enhance National Security but at the same time ensure privacy" (Thuraisingham, 2002). There is now research at various laboratories on privacy enhanced sensitive data mining (Aggarwal, 2000), (Clifton 2002).

The idea is to continue with mining but at the same time ensure privacy as much as possible. Dr. Yahuda Lindell of BIU's Department of Computer Science is researching protocols and models which will protect the privacy and data mining simultaneously. For this task Dr. Lindell has assembled a multi disciplinary research team composed of both theoretical and applied data mining researchers, crypotographers and legal scholars. They intend to help the government in obtaining required information and preserve the privacy of individual. The real world applications under review are:

- Privacy and private databases
- Privacy in the workplace,
- Health and Genetic data and privacy.

The various data security enhanced techniques are:

Databases can employ **Multi level security model** to classify and restrict data according to varous security levels, with users permitted access to classify and restrict data to only their authorized level. However, users can still infer some sensitive information and same can occur through data mining too.

Another technique is Encryption technique in which individual items may be encoded. This involves **Blind Encryption** (which builds on public key encryption), **Biometric Encryption** (where image or finger print is used to encode his or her personal information) and **Anonymous Database** (which permits the consolidation of various databases but limits access to personal information to only those who need to know; personal information is encrypted and stored to different locations). Intrusion Detection is a another research area which helps to protect the privacy of personal data.

Privacy – preserving data mining is a new area of data mining research in response to privacy protection during data mining. It deals with mining the data without revealing the underlying data values. The two common approaches:

- Secure Multiparty Computation
- Data Obscuration

In **Secure Multiparty computation,** simulation and cryptographic techniques are used which don't allow any party to learn another data values, this technique is however less beneficial in large databases.

In **Data obscuration,** actual data is distorted by aggregation or by adding random noise. These values are collected using reconstruction algorithm. Mining can be performed using these approximated values. Many advances have been made, and this area will flourish in the near future. (Han and Kamber, 2006)

DATA MINING: A PROMISING TOOL

In spite of many issues and challenges that data mining has put in front of us, it has become a part of our life and shows a promising future in various areas. Now a day, Data Mining is everywhere and affecting everyday things from product stocked at our local supermarket to the advertisement on internet, to crime prevention. Data Mining has innovatively influenced what we buy; the way we shop, and also shaped the on-line shopping experience. Data Mining is used as a competitive advantage over competitors and help in business decision making.

Data Mining solutions cannot be generic as effective data mining requires the smooth integration of business logic with data mining functions, one promising direction towards individual privacy is Privacy – Preserving Data Mining where privacy enhanced algorithms are developed by researchers to secure the privacy.

CONCLUSION

Data Mining has many applications in a no of areas including Marketing and Sales, Medicine, Law, Manufacturing and recently in security also. No doubt data mining is extensively used in pattern extraction and decision making process of organization but

simultaneously the process of generating rule through mining is becoming ethical issure when the results are used in decision making processes that affect people. A lot of progress has been made and there is also a lot of research that needs to be done in the area of privacy preserving data mining. Till then the question will remain intact "Whether one desire will outweight the other"

REFERENCES

1. Campbell kim (2002), *where do we draw the line?* Christian Science Monitor.
2. Clayton Mark (2006), *US plans Massive Data Sweep http:// www.csmonitor. com/2006/0209/p01 s02-uspo. html*
3. Cook Jack (2006), *Ethics on Data Mining*, Encyclopedia of data mining.
4. Thuraisingham Bhavani (2004), *Data mining, National security, Privacy and Civil Liberties*, SIGKDD Explarations Valume 4, Issure 2, 1-5.
5. Thuraisingham Bhavani (2006), *Homeland Security DM and Link Analysis, SIGKDD explorations*, 566-569
6. Lindell Yahuda (2007), **Demise of ADVISE: DHS data mine broaden up,** ARS Technia *http:// research. biu.ac.il/Research Invovations/ current? id = 3*
7. Anderson Nate (2007), *Demise of ADVISE: DHS data mine broaden up, ARS Technia http:// arstechnica.com/news. ars/post/20070906-the-demise-of-advise-dhs-data-mine-boarded-up.html*
8. Privacy Office US DHS Washington DC(2007), *DHS privacy office Review of the ADVISE program, www.cs.ualberta.ca/-oliveira/psdm/psdm index.html*
9. The Privacy act of 1974 (2002), *US department of justice. www.usdoj.gov/04 foia/foia/04-7-1.* html
10. Jiawer Han and Micheline Kamber (Reprint 2006), *Data Mining concepts and Techniques*, Elsevier, US.