Chapter 86
Achieving Balance Between Corporate Dataveillance and Employee Privacy Concerns

Ordor Ngowari Rosette
Concordia University of Edmonton, Canada

Shaun Aghili
Concordia University of Edmonton, Canada

Fatemeh Kazemeyni
Concordia University of Edmonton, Canada

Sergey Butakov
Concordia University of Edmonton, Canada

Ron Ruhl
Concordia University of Edmonton, Canada

ABSTRACT

Big data, like most technological innovations, brings noticeable benefits as well potential risks. Dataveillance using big data is becoming another dimension in the increasing privacy concerns of the workforce. Such concerns emanate from the tension between the correct use of employee personal data and information privacy in big data within and outside the work environment. It has evolved as employees are becoming increasingly cognizant of the ways in which employers can use technologies to monitor social media activities, internet interactions, emails and other online activities outside the work environment. The objective of this research paper is to recommend a set of guidelines which will be mapped to COBIT 5 framework to help medium and large organizations balance the tension between the increasing potential of big data and employee dataveillance privacy concerns in workplaces.

INTRODUCTION

Today's corporations tend to consider less traditional factors when hiring, promoting, or dismissing employees. One example is the increasing use of social networks such as LinkedIn by HR in an attempt to gain an understanding of the professional activities of the potential hire. Employers may go beyond professional activities and study data trails left by employees on social media, forums, user groups, etc. Such examinations allow organizations to monitor employee activities and predict behaviour based on the patterns of these data trails. The collection and analysis of these digital footprints is called Big Data

DOI: 10.4018/978-1-5225-8897-9.ch086

Analytics or often just BD. The concept of Big Data introduced in the last decade deals with the analysis of such trails from different sources. BD refers to datasets which size is beyond the ability of typical database software tools to capture, store, manage and analyze (Dumbill, 2012). Large amounts of data are hidden in the immense volume, variety and velocity of data that is generated today by the workforce. This data consist of new information, facts, relationships, indicators and pointers that either could not be practically discovered in the past or simply did not exist before (PCC, 2012).

BD is a concept closely intertwined with predictive analytics, because the data points are the ingredients that feed the application of predictive algorithms. Predictive analytics is defined as "the branch of data mining concerned with forecasting probabilities" (Matlis, 2006). It is a concept that is more uniquely forward-looking, and when personal information is the raw data, predictive analytics is the process used by organization in attempting to forecast future behaviours or intentions. For example, in financial institutions, BD predictive tools are being used to look for aberrant patterns of customer behaviour within huge claims or billing processing systems log files.

In today's technology-driven society, various individual activities and transactions produce a stream of information entries in massive datasets; some of which may be associated with personal information. From the legislative perspective, the study is mostly concentrated on Canadian context. According to Personal Information Protection Act (PIPA) in Alberta, Canada, personal information includes information, recorded or not, that can identify an individual or is about an individual (e.g. name, address, age, educational history, blood type) (PIPA,2010). There are potential harms within the ubiquitous privacy concerns that are derived from the collection, analysis and use of information that focuses on individual data behavior, known as predictive privacy harms (Crawford, 2013). Predictive privacy harms are becoming increasingly prevalent in the workforce, and need to be re-addressed without hampering the benefits of BD technologies.

As advances in BD predictive analysis continue to evolve, some organizations may use these enhanced capabilities to closely monitor certain key figures in sensitive positions, or even adopt a routine monitoring system of all employees. The term dataveillance was suggested by Clarke as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" (Clarke, 1988). The main objective of this chapter is to suggest guidelines for IT governance that can help corporations to manage dataveillance programs while maintaining balance with employees' privacy concerns.

LITERATURE REVIEW

Privacy of Employees

Today's employers are known to monitor employees in the workplace as a fraud prevention and/or internal security breach violation preventive control. Research by American Management Association indicated that 66% of the surveyed companies monitor internet connections mostly using automated tools (AMA, 2008). Managers also indicated concerns about social network activities and actually act on this concerns – about 50% of the companies blocked social networks (AMA, 2008). But with the technologies advancing at unprecedented speeds, employers may go beyond the company network and monitor user activities that are not occurring within the workplace (Connolly & McParland, 2012;