2012

Online privacy policy of the thirty Dow Jones corporations: Compliance with FTC Fair Information Practice Principles and readability assessment

Yuanxiang Li

ONLINE PRIVACY POLICY OF THE THIRTY DOW JONES CORPORATIONS: COMPLIANCE WITH FTC FAIR INFORMATION PRACTICE PRINCIPLES AND READABILITY ASSESSMENT

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Business Administration

in

Information Assurance and Security Management

---

by

Yuanxiang Li

September 2012

ONLINE PRIVACY POLICY OF THE THIRTY DOW JONES CORPORATIONS: COMPLIANCE WITH FTC FAIR INFORMATION PRACTICE PRINCIPLES AND READABILITY ASSESSMENT

A Project

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Yuanxiang Li

September 2012

Approved by:

[redacted]

Dr. C.E. Tapie Rohm Jr., Chair, Information and Decision Sciences

27 Aug 2012
Date

[redacted]

Dr. Anna Ni, Public Administration

[redacted]

Dr. Jack Zhu, Department Chair, Information and Decision Sciences

ABSTRACT

Privacy policy in corporation's business refers to a statement or a legal document that discloses some or all of the ways a party gathers, uses, discloses and manages a customer or client's personal data such as name, age, address, gender, email, etc. In 1998, the United States Federal Trade Commission (FTC) reported a study of online privacy concerns to Congress, which described a widely-accepted Fair Information Practice Principles (FIPs) of Notice, Choice, Access, and Security. This project conducted a statistical study by examining the FIPs compliance for each Dow Jones Corporation's (DJC's) online privacy policy. In addition, a study by George Milne, Mary Culnan, and Henry Greene showed that online privacy had grown in length as well as had declined in readability. Therefore, the project also assessed the readability of DJC's online privacy policy by measuring widely adopted Flesch Reading Ease Score (FRES) and Flesch-Kincaid Grade Level (FKGL). Furthermore, in order to better understand the practical situations regarding privacy concerns and policy readability from a customer's point of view, a customer survey was given to business students at the College of Business and Public Administration at California State University, San Bernardino.

This project focuses on two research questions: 1) How well does DJC's online privacy policy comply with FTC Fair Information Practice Principles; and 2) How is the readability of DJC's online privacy policy; was it easy to understand? From a practical perspective, this project helps DJCs to better comply with FIPs

regulations by providing their policy shortages compared with FIPs principles. In addition, a widely readable online privacy policy would bring more sense for customers' privacy protection. This project also pointed out the discontented performance of DJC's online privacy policy regarding the readability. In the end, recommendations of both improving FIPs compliance and increasing policy readability have given to help DJCs to better satisfy customer's privacy concerns.

ACKNOWLEDGMENTS

I would like to express the utmost gratitude to my committee members: Dr. C.E. Tapie Rohm Jr., Dr. Anna Ni, and Dr. Jake Zhu. Dr. Zhu inspired me to explore the topic of online privacy. Dr. Ni taught me how to do research as well as supported me for methodology learning. Particularly, Dr. Rohm supervised my whole project, sharped my thoughts, and helped me finalize the paper. Once again, I sincerely appreciate all my three advisors; without them, this project would never be completed.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

BACKGROUND

Introduction

On March first, 2012, Google Inc. released its newest online privacy policy combined with more than sixty sub-privacy policies as well as improved the readability. Why would Google like to put so much effort to improve its online privacy policy? Does online privacy policy matter?

Privacy policy in corporation's business refers to a statement or a legal document that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's personal data such as name, age, address, gender, email, etc. (Privacy policy, 2012). While online privacy policy (or online privacy) emphasizes on the right or mandates of personal privacy concerning the storing, repurposing, providing to third-parties, and displaying of information pertaining to oneself via the Internet (Internet privacy, 2012). In the age of the internet, sharing information, communication, and working through the internet, especially the flow of information between companies and customers, has caused a growing concerns regarding online privacy policy. For example, Google, as one of the most popular search engine in the world, has a well-known reputation and vast of cooperation with third parties. However, an announcement from Maryland Attorney General Douglas Gansler and attorneys general from thirty-five other states indicated that Google had tracked people

using computers and mobile devices based on its new privacy components such as searching history without opt-out choice for customers (Acohido, 2012). Furthermore, if Google knew everything about you, your privacy would be in danger. Unfortunately, Google does know everything about its customers.

Therefore, from customer's view a disclosed online privacy would satisfy customer's concerns letting her/him know what information the company collected, what information the company may share with third parties, and how the company may secure her/his information. As mentioned above, the new online privacy of Google revealed the information that Google has been tracking customer's information. Few customers would like to be monitored all the time by Google; however, customers would be like walking on the thin ice without notice if there was no online privacy. In addition, in 1998, the United States Federal Trade Commission (FTC) reported a study of online privacy concerns to Congress. In this report, FTC described a widely-accepted Fair Information Practice Principles (FIPs) of Notice, Choice, Access, and Security[1] (Landesberg, Levin, Curtin, & Lev, 1998). And FTC also defined the Enforcement principle to provide sanctions for noncompliance as a critical component of any governmental or self-regulatory program to protect online privacy. Nonetheless, does every company comply with FIPs? Are their online privacy policies easy to read?

[1] The four principles of FIPs will be discussed in details in Chapter Two.

Statement of the Problems

In July 1997, FTC conducted a survey about consumer privacy on the World Wide Web. The survey includes six sample groups: 1) comprehensive, 2) health, 3) retail, 4) financial, 5) children, and 6) most popular. Only fourteen percent of all sites in the Comprehensive Sample (sample size = 674) posted any disclosure about privacy. Only seventy-one percent of all sites in Most Popular Sample (sample size = 111) have some type of information disclosure about privacy (Landesberg, Levin, Curtin, & Lev, 1998). Furthermore, a study by George Milne, Mary Culnan, and Henry Greene showed that online privacy has grown in length as well as declined in readability (Milne, Culnan, & Greene, 2006). Even though a company discloses its online privacy and complies with FIPs, the unreadable privacy is still impractical for customers. Few people would like to spend half an hour or even a couple of hours to read the online privacy notice, especially when she/he is shopping online. Therefore, FIPs compliance and improving readability seems to be more and more intensive in terms of current online privacy policy.

Purpose of the Project

This project conducted a statistical study of online privacy to examine how well corporations comply with FIPs and assess how easy their privacy was to read. In addition, this project conducted a survey regarding customers' privacy

concerns and policy readability from students in the College of Business and Public Administration at California State University, San Bernardino.

Significance of the Project

On March 30th 2012, Nicole Perlroth from the New York Times reported that approximately one million to three million Visa and MasterCard accounts were exposed at Global Payments. Credit card numbers as well as cardholders' personal information had been hacked when payments were processed. Nicole also mentioned this was the second breach already at Global Payments in the last twelve months. Additionally, Heartland Payment Systems disclosed a breach which caused 130 million credit card to be hacked during two years from 2007 to 2009 (Perlroth, 2012). Credit cards have been the favorite target for hackers since e-business became more and more popular. However, the question can be asked, did the company notice these security issues, especially its e-business? Did the company take any measures to secure customers' personal information; especially their financials? All the related information should be found in a corporation's online privacy policy. Therefore, it is necessary to examine the privacy notice to ensure that it provides a clear statement about what information will be collected from customers, how the company secures the payment transmission when an order is being placed, how the company securely stores customers' information in its database, etc. As already indicated, FIPs is a widely accepted principle to guide a company's

privacy policy from Notice, Choice, Access, and Security. These four principles comprehensively cover the most privacy and security concerns[2]. Thus, a complied, reliable, and security online privacy would safeguard customers' equity.

On the other hand, Nicole mentioned Heartland Payment Systems cost about $140 million in fines, settlements, and legal fees due to the exposure of the data (Perlroth, 2012). As the function of a policy, a complied, reliable, and security online privacy could guide the company to enhance and improve its technology as well as management of privacy concerns. It will effectively manage the risk of privacy exposed by hackers in order to reduce the loss. In addition, as the requirement by FTC, this project would help corporations to self-regulate their online privacy to fulfill with the Law.

Moreover, Matthew Vail's study indicated that the majority of Americans cannot understand the content of most online privacy policy (Vail, Earp, & Anton, 2008). Therefore, a readable privacy could help customers comprehend the content easily and spend less time to do so. Thus, this project assessed the readability of the online privacy policy. Additionally, recommendations about how to improve readability are recommended.

Research Objectives and Questions

In this project, the online privacy policies of thirty Dow Jones Corporations (DJCs[3]) in terms of FIPs compliance and readability were scrutinized. To fully

[2] FIPs don't particularly point out children's privacy. See detailed information about FIPs in Chapter Two.

explore the online privacy policies, Online Privacy Seal[4] such as TRUSTe, BBBOnLine and WebTrust were introduced and checked for each DJC's privacy notice. Secondly, Flesch Reading Ease Score[5] (FRES) was used for assessing readability of each DJC's privacy notice. To summarize the research objectives, two primary research questions were discussed:

I. How well does the DJC's online privacy policy comply with FTC Fair Information Practice Principles?

II. How is the readability of DJC's online privacy policy; was it easy to understand?

Scope and Limitation of the Project

The Dow Jones Industrial Average (DJIA) is the one of the best-known icons of American culture and stock market observers around the world (Dow Jones Industrial Average, 2011). DJIA is composed by thirty modern corporations[6] which cover manufacturers of industrial and consumer goods, financial services, entertainment and information technology, etc. (Dow Jones Industrial Average overview, 2012). Each company plays a significant role with the related industries. Basic Materials is represented by Alcoa, Chevron, and Exxon Mobile. Consumer goods and services are reflected by Coca-Cola, Home Depot, Kraft Foods, McDonald's, Procter & Gamble, Travelers, Wal-Mart, and

[3] DJC will be discussed more in next section: Scope and Limitation of the Project.
[4] Online Privacy Seal will be introduced in details in Chapter Two.
[5] See Chapter Two
[6] See the components in Appendix A.

Walt Disney. Financials are represented by American Express, Bank of America, and JPMorgan Chase. Healthcare is reflected by Johnson & Johnson, Merck & Co, and Pfizer. Industrial Goods are represented by 3M, Boeing, Caterpillar, DuPont, General Electric, and United Technologies. And Technology is reflected by AT&T, Cisco Systems, Hewlett-Packard, Intel, International Business Machines (IBM), Microsoft, and Verizon Communications (Nicholson, 2012). As whole, the Dow Jones Corporations' (DJCs') stocks usually account for 25% to 30% of the total market value of all U.S. stocks (Dow Jones Industrial Average, 2011).

Therefore, since DJCs occupy a large share of the U.S. market and have a broadly representativeness of American corporations, this project focused on the thirty DJCs' online privacy policies to examine their privacy notices as well as assess their readability.

The DJCs have a good reputation in the market as well as good relationships with customers. DJCs might pay more attention on their online privacy rather than the ordinary corporations. Hence, DJCs' performance in terms of compliance with FIPs and easy-to-read might be better than the average found in the FTC's report in 1997. As limitation of this project, the thirty DJCs' online privacy policies may not be sufficient to reflect a random sample of online privacy policies.

Definition of Terms

The following terms are defined as they apply to this project (appeared in alphabetical order).

Flesch Reading Ease Score (FRES) & Flesch–Kincaid Grade Level (FKGL): "The Flesch/Flesch–Kincaid readability tests are designed to indicate comprehension difficulty when reading a passage of contemporary academic English" (Flesch–Kincaid readability test, 2012).

FTC Fair Information Practice Principles (FIPs): "The guidelines that represent widely-accepted concepts regarding fair information practice in an electronic marketplace" (FTC Fair Information Practice, 2011).

Online Privacy Policy (or online privacy): "emphasizes on the right or mandate of personal privacy concerning the storing, repurposing, providing to third-parties, and displaying of information pertaining to oneself via the Internet" (Internet privacy, 2012).

Passive Voice: "A grammatical construction in which the subject of a sentence or clause denotes the recipient of the action (the patient) rather than the performer (the agent)" (English passive voice, 2012).

Privacy Policy (or Privacy Notice): "A statement or a legal document that discloses some or all of the ways a party gathers, uses, discloses and manages a customer or client's personal data such as name, age, address, gender, email, etc." (Privacy policy, 2012).

Privacy Seal: "An online branded trust mark or seal of approval logo which is used by third party site verification entities, (i.e. TRUSTe, BBB, Guardian e-Commerce, etc.) to help protect online consumers by identifying Web sites that have been verified for protecting the online privacy and safety of consumers" (Privacy seal, 2012).

Readability: "The ease in which text can be read and understood" (Readability, 2012).

Organization of the Project

This project has five chapters. Chapter one provides the introduction, statement of the problems, purpose, significance of the project, research objectives and questions, scope and limitation of this project, and definition of terms. Chapter two comprises of a literature review upon the relevant works pertaining to DJC's online privacy policy, FIPs, and readability. Chapter three applies the methodology learned from literature review and documents the steps involved in developing this project including FIPs compliance, readability assessment, and CBPA student survey. Chapter four presents the findings from both overall and sector performance of DJC's online privacy policy responding to chapter three. Chapter five draws the conclusions and proposes some recommendations. The appendices and references follow chapter five. The appendices consist of: Appendix A: The Thirty Dow Jones Corporation Components; Appendix B: U.S. Education Grade Level Structure.

CHAPTER TWO

REVIEW OF THE LITERATURE

Introduction

With the growing e-market, the internet has been treated as both panacea and anathema to marketers interacting with customers (Brown & Muchira, 2004). Modern relationship marketing is largely driven by new technology (Ian, 1998). Internet as one of the greatest inventions in the 20th century and has become a major driver in current markets. In 1997, there were 58 million adults using internet and 10 million of them have actually purchased a product or service online (Landesberg, Levin, Curtin, & Lev, 1998). The high-quality and reliable customer's database which depicts patterns of needs within the customer and prospect population has more contribution to marketers (Khalil & Harcar, 1999). Therefore, company always seeks all the opportunities to identify the needs of customers and collect their personal information in order to better serve customers. For example, sending mail or email advertisements to target customers regularly creates new relationships or maintains old relationships with customers. In order to do so, companies have to collect addresses, emails, gender, names, race, date of birth, interests, etc. from customers. However, most of that information is sensitive for customers and has already caused customers' concerns about threats to privacy in some degree (Petrison & Wang, 1995). Especially, nowadays, personal information has become a tradable

commodity in capitalist societies (Hamelink, 2000). It was reported that customers were anxious about whether the information gathered about them was warranted, whether their information was securely stored in the database, and whether their information was shared with a third party without disclosure and permission. Pew Internet & American Life project reported that seventy percent of internet users felt that they need a new law to protect their online privacy (Lewis & Fox, 2001). Nevertheless, most experts state that a corporation's online privacy policy is currently the best way to balance privacy concerns and online activities (Andrews, 2001). However, Westin conducting a survey found that sixty-five percent customers believed online privacy was too complicated or unclear to understand (Westin, 2004). Hence, the review of the literature was focused on online privacy policy from both FIPs compliance and readability perspectives.

Fair Information Practice Principles

FTC Fair Information Practice Principles (FIPs[7]) are guidelines that represent widely-accepted concepts regarding fair information practice in an electronic marketplace (FTC Fair Information Practice, 2011). It includes five core principles as follows (Landesberg, Levin, Curtin, & Lev, 1998; Pitofsky, Anthony, Thompson, Swindle, & Leary, 2000):

[7] Department of Homeland Security (DHS) has another version of Fair Information Practice Principles (FIPPs) which are a set of eight principles that are rooted in the tenets of the Privacy Act of 1974.

1. Notice/Awareness: Customers should be notified regarding that 1) what information and how the information will be collected from customers, 2) how the information will be used by corporations internally, and 3) whether and how the information will be shared among corporations.
2. Choice/Consent: Customers should have a choice about 1) whether their information collected for a certain purpose will be used for other purposes and 2) whether their information will be shared with third parties unless it is required by law. In other words, whether or not customers are provided opt-in and opt-out options for their information both within and among corporations.
3. Access/Participation: Customers should have right to 1) access to review their information, 2) update any error to keep the information accurately and completely, and 3) delete their information from corporation's database unless it is required by law.
4. Integrity/Security: Customers information, especially personal information, should be protected by corporations from unauthorized access both transmission duration and information storage.
5. Enforcement/Redress: Customers have a right to ensure that corporations comply with those four core privacy principles either through self-regulation (such as privacy seals) or government enforcement (such as audits).

In the report: "A report to Congress" (Pitofsky, Anthony, Thompson, Swindle, & Leary, 2000), it was noted that ninety-two percent of the sites from a comprehensive random sample, collected personal information and only fourteen percent of them disclosed something about the information practices of the corporations. Professor Mary Culnan from Georgetown University conducted another survey which included a hundred most busy sites from the most-heavily trafficked websites. The result showed that there was a significant improvement in the frequency of privacy disclosures in regards to those one hundred websites. However, still only ten percent of those sites disclosed the websites' disclosure online privacy policy.

In addition, Schwaig conducted a survey about FIPs compliance of Fortune 500 (Schwaig, Kane, & Storey, 2006). About eighty percent of those sites had an online privacy disclosure. Sixty-seven percent of the Fortune 500 sites fully complied with the Notice Principle. Less than three percent of the Fortune 500 sites complied with all the required measure aspects of FIPs. Meanwhile, only thirty-five out of 500 sites displayed a seal on its privacy policy. In the report to Congress, FTC indicated that online privacy seal programs would promote company's self-regulation.

Online Privacy Seal Programs

The online privacy seal programs have been developed by industry's primary self-regulatory enforcement (Pitofsky, Anthony, Thompson, Swindle, &

Leary, 2000). The seal programs provide a set of guidelines and a voluntary enforcement mechanism to assure that the site abides by their own privacy policy (Rifon, LaRose, & Choi, 2005). There are three major privacy seals: 1) TRUSTe, 2) BBBOnLine and 3) WebTrust (Pitofsky, Anthony, Thompson, Swindle, & Leary, 2000). These Seals or Trustmark were displayed by websites that adhere to these organizations' established privacy requirements and agree to comply with oversight and consumer dispute resolution processes (Markert, 2002). Therefore, the Trustmark was designed to engender trust between customers and corporations regard to online privacy policy. Customers can review the Trustmark's policy by clicking on the seal logo (see Figure 1). Based on such trust, customers could quickly make informed decisions about whether or not to provide their personally information to the corporations.

Figure 1. Online Privacy Seal Logo

Privacy seal logo. (n.d.). In *Google images*. Retrieved from https://www.google.com/imghp

TRUSTe is the first and the largest privacy seal program in the world certifying more than 3,500 websites (TRUSTe, 2012). TRUSTe complies with the privacy practices and notices guidelines set by the FTC and other trade associations (Rifon, LaRose, & Choi, 2005). BBBOnLine Privacy Seal was launched March, 1999. By 2000, there were already more than 450 websites displaying BBBOnLine Seal. WebTrust is a professional service developed by the American Institute of Certified Accountants (AICPA). WebTrust has licensed its seal to twenty-eight Web sites by the year 2000 (Pitofsky et al., 2000).

As the FTC stated, if those privacy seal programs above were widely adopted, there will be an efficient way to alert customers regarding their privacy concerns. However, only eight percent of the sites from the comprehensive random sample displayed a privacy seal (Pitofsky et al., 2000). Only seven percent of the Fortune 500 firms in Schwaig's study participated in an online seal program (Schwaig, Kane, & Storey, 2006). It seems that FTC needs to further strengthen its efforts for enforcement in order to better protect customers' privacy.

Flesch Reading Ease Score and Flesch-Kincaid Grade Level

Milne's research has shown that online privacy had grown in length but declined in readability over time (Milne, Culnan, & Greene, 2006). Readability refers to the ease in which text can be read and understood (Readability, 2012). Dr. Rudolf Flesch has created a well-known readability test, Flesch Reading

Ease Score (FRES). In his book "The Art of Readable Writing", Flesh (1949) published the widely used FRES formula:

Flesch Reading Ease = 206.835 − (1.015 × ASL) − (84.6 × ASW)

Where:

- ASL = average sentence length (total words divided by total sentences)
- ASW = average word length in syllables (total syllables divided by total words)

In addition, the score is used on a scale from 0 to 100, with 0 equivalents to the 12th grade and 100 equivalents to the 4th grade. The greater the value, the easier the text. Dr. Flesch also conducted a table of FRES verbal description (Table 1) as follows (Flesch, 1949, pp. 149-150):

Table 1. Flesch Reading Ease Score Verbal Description

Description of Style	Reading Ease Score	Estimated Reading Grade	Typical Magazine
Very Easy	90 to 100	5th Grade	Comics
Easy	80 to 90	6th Grade	Pulp Fiction
Fairly Easy	70 to 80	7th Grade	Slick Fiction
Standard	60 to 70	8th and 9th Grade	Digests
Fairly Difficult	50 to 60	10th to 12th Grade (High School)	Quality
Difficult	30 to 50	13th to 16th Grade (College)	Academic
Very Difficult	0 to 30	College Graduate	Scientific

Publishers discovered that the FRES formulas could increase readership up to sixty percent (Readability, 2012). Overtime, FRES has become one of the most tested and reliable measurements for readability. Hence, more and more text editing software has embedded this function to assess the readability of certain context such as Microsoft Office 2010, Readme, OpenOffice, etc.

However, Dr. Flesch did not provide an accurate calculation for a Reading Grade Level even though he provided the estimated reading grade. In 1975, Peter Kincaid and his team developed the widely-adopted Flesch-Kincaid Grade Level (FKGL) based on Dr. Flesch's research. The accurate reading grade level was given and has a better match between FRES and U.S. education grade level structure[8]. FKGL helps teachers, parents, librarians, and others to better judge the readability level of various books and texts (Flesch-Kincaid readability test, 2012). The FKGL formula is a simple mathematical equation as follows (Kincaid, Fishburne, Rogers, & Chissom, 1975):

Flesch-Kincaid Grade Level = 0.39 × ASL + 11.8 × ASW–15.59

Where:

- ASL = average sentence length (total words divided by total sentences)
- ASW = average word length in syllables (total syllables divided by total words)

[8] See Appendix B for the specific structure

Previous research showed that online privacy policy was generally hard to read. Dr. Hochhauser analyzed sixty financial privacy notices and found the average FKGL was 15.6 (Hochhauser, 2001). The grade level means only third to fourth year college educated customers can comprehend the complicated online privacy. According to Table 1, the average readability of those financial privacy policies was defined as "difficult". In addition, Dr. Hochhauser did another study about thirty-one Health Insurance Portability and Accountability Act (HIPAA) privacy notices. The average FKGL was 14.5 which reflected that only second to third year college customers could better understand the online privacy (Hochhauser, 2003). Therefore, the average readability of those HIPAA privacy policies would be marked as "difficult" based on Table 1.

Anton and his coworkers examined forty online privacy statements from nine financial institutions and found the average FKGL was 14.1 (Antón, et al., 2004). In other words, second to third year college educated clients may apprehend the "difficult" online privacy notices. In details, eight of the forty notices needed high school education or less; thirteen of the forty required some college training (12-14 grade); twelve needed senior college education (14-16 grade); and seven even required a post-graduate education. Additionally, Jensen and Potts analyzed another sample of online privacy. They found the average FKGL of the forty-seven high-traffic sites was 14.2; while, the average FKGL for the seventeen health sites was 13.5 (Jensen & Potts, 2004). Moreover,

they did some further exploration and found there was no significant difference between healthcare websites and others.

All the previous research stated above has an approximate 14 Flesch-Kincaid Grade Level. According to Table 1, it seems that only college educated customers could better comprehend the online privacy policy. However, research showed that the majority of people read three-to-five grades lower than their highest level of educational achievement. Furthermore, census data (2011) revealed that about 86.7% of adults had a high school degree and only around 27.8% had one or more college degrees (Educational attainment in the United States: 2011 - detailed tables, 2011). Thus, most online privacy policies of corporations are unreadable for the mass customers. FTC Chairman Jon Leibowitz has already called for simpler, shorter privacy notices in order to answer customers' confusion about the complex online privacy (Leibowitz: privacy notices should be simple, short, 2011).

Passive Voice

Passive voice is defined as a grammatical construction in which the subject of a sentence or clause denotes the recipient of the action (the patient) rather than the performer (the agent) (English passive voice, 2012). For example, "a cat catches a mouse" using passive voice will be "a mouse is caught by a cat." So far, all the reviewed literature above did not mention any former research about how passive voice affects readability. Nonetheless, Susan Rhodes's Ph.D.

thesis concluded that there was no difference regarding comprehensibility between active and passive voice in scientific writing (Rhodes, 1997). Coincidentally, most online privacy policy is written as "scientific" or "academic" text according to Table 1 and to previous review. In addition, few typical current experimental studies have done something to illustrate that passive voice is much harder to understand than active voice based on Dr. Rhodes's literature review. Furthermore, researchers believe that changing passive voice into active voice will affect the meaning of the whole sentence in some degree, it may misplace emphasis or cause ambiguous obligation in terms of legal documents (such as online privacy policy). In addition, in some degree, passive voice could reduce reading speed even though there were still some debates on this topic. Philip Gough indicated that active sentence were faster to read than passive one (Gough, 1965). While, Arthur Siegel and James Burkett found no significant time difference between active voice and passive voice (Siegel & Burkett, 1974). Therefore, the passive voice was not used for assessing the readability of DJC's online privacy, but focused on giving recommendations about it.

Summary

As introduced in the beginning, FTC FIPs is the widely accepted principle to check organization's privacy policy. Readability is used for evaluating customers' understanding of the complicated policies. In details, FRES and FKGL were two of the most popular and reliable measurements for readability.

Additionally, most previous studies focus on either FIPs compliance or policy readability. In this project, the author researched from both those two aspects on corporation's online privacy policy. Due to the scope of this project, only DJC's online privacy policy was explored in this project.

CHAPTER THREE

METHODOLOGY

Introduction

This project mainly applied the methodology from the review of the literature. FIPs is the widely accepted practice principle for privacy regulation. FRES and FKGL are two of the most popular measurements for context readability. Additionally, this project conducted an online survey regarding privacy policy to assist the analysis of DJC's performance in terms of customer's privacy concerns and policy readability.

Data Collection

Thirty DJCs' online privacy policies were sampled. All the thirty corporations have linked privacy notices through their website-homepages. Most of the Privacy Hyperlinks are placed on the bottom of their homepages by using either "Privacy Notice", "Privacy Statement", "Privacy Policy", or "Privacy". Some of them are located on the top area. It is very easy to find out the privacy policies for the thirty Dow Jones Corporations. Since almost all the thirty companies are global business, their privacy policies may vary based on different regions (countries). The scope of this project just focused on their primary privacy policies, which refer to North America. For example, International Business Machines Corporation (IBM) has businesses all over the world. This project just

focused on its American version (http://www.ibm.com/privacy/us/en/) versus other ones, such as British version (http://www.ibm.com/privacy/uk/en/), Hong Kong's version (http://www.ibm.com/privacy/hk/en/), etc.

A survey was taken by undergraduate and graduate students from the College of Business and Public Administration (CBPA) at California State University, San Bernardino.

Design of Fair Information Practice Principle Compliance

This project simulated the practical situation regarding time consumption when customers registered an account or shopped online. Therefore, the author used fifteen to twenty minutes to quickly scan each DJC's privacy policy and compared it with FIPs requirement criteria. As indicated in Chapter Two, the first four principles: Notice/Awareness, Choice/Consent, Access/Participation, and Integrity/Security were the focus since the last principle (Enforcement/Redress) had no business with privacy standards, but only for enforcement or regulation. Additionally, as mentioned in Chapter Two, privacy seals were checked as well. To clarify, Table 2 presented the specific criteria which were used for judgment.

Table 2. Fair Information Practice Principle Requirement Criteria

Main Principle	Sub-principle
I. Notice/Awareness	1) Posted a privacy policy
	2) Stated anything about what specific personal information it collects
	3) Stated anything about how the site may use personal information internally
	4) Stated anything about whether it discloses personal information to third parties
II. Choice/Consent	1) Whether sites provided choice with respect to their internal use of personal information to send communications back to consumers (other than those related to processing an order)
	2) Whether they provided choice with respect to their disclosure of personal identifying information to other entities, defined as third-party choice
III. Access/Participation	1) Whether the site stated that it allows consumers to review at least some personal information about them
	2) Whether the site stated that it allows consumers to have inaccuracies in at least some personal information about themselves corrected
	3) Whether the site stated that it allows consumers to have at least some personal information deleted
IV. Security/Integrity	1) Take any steps to provide security
	2) If (1) so, whether they take any steps to provide security for information during transmission
	3) If (1) so, whether they take any steps to provide security for information after receipt
V. Privacy Seal	1) Whether the site has a privacy seal

Define "Rating" Score

In order to better understand how well DJC's privacy policy complies with FIPs, the concept of national Credit Rating (Credit rating, 2012) was used. Table 3 set up a table for the project to rate the DJC's performance as followed:

Table 3. Fair Information Practice Principle Rating Score

Credit	Rating Grade	Performance
37 ~ 60	AAA	Good
25 ~ 36	AA	Fair
13 ~ 24	A	Poor
0 ~ 12	NC	Noncompliance

Corporations with 37 to 60 points were defines as "AAA" rating with "Good" performance. Corporations with 25 to 36 points were defined as "AA" rating with "Fair" performance. Corporations with13 to 24 points were defined as "A" rating with "Poor" performance. Those corporations with less than 12 points were considered as noncompliance. The following section illustrates how to calculate the score and how it is defined.

Procedure of Dow Jones Corporation's Rating Score

Each DJC's privacy policy was quickly scanned to point out whether or not it had the required criteria. Each principle including privacy seal was worth 12 points, and the sub-principles split the 12 points based on the number of sub-principle. To clarify, Table 4 indicated the specific distribution of points.

Table 4. Fair Information Practice Principle Rating Score Points Distribution

Main Principle	Sub-principle
I. Notice/Awareness (12 points)	1) 3 points
	2) 3 points
	3) 3 points
	4) 3 points
II. Choice/Consent (12 points)	1) 6 points
	2) 6 points
III. Access/Participation (12 points)	1) 4 points
	2) 4 points
	3) 4 points
IV. Security/Integrity (12 points)	1) 4 points
	2) 4 points
	3) 4 points
V. Privacy Seal (12 points)	1) 12 points

According to the Table 4, the maximum score is 60 and the maximum sum of the first four principles is 48. Obviously, a score from 48 to 60 was defined as AAA since privacy seals are only the complementary and regulation for the first four principles. However, not all DJCs' privacy policies are formulated as clear as those four principles; therefore, the author focused on each sub-principles rather than examined the whole principles for the policies. Hence, due to the

mixed examination of sub-principles, the bottom line was reduced to 37 for AAA rating. For example, if one company's privacy policy had principle I and III, but only had 1) for principle II as well as 1) and 2) for principle IV, the FIPs rating score of this company would be 38 (12 + 12 + 6 + 4 + 4) and would still qualify for AAA rating. Similarly, those corporations which earned from 25 to 36 points would be credit as AA rating. Companies with 13 to 24 points would be defined as A rating. Companies which had less than 12 points would be recognized as noncompliance.

Design of Readability Assessment

This project applied the widely adopted two measurements: FRES and FKGL, which were introduced in Chapter Two. Nowadays, more and more text editing software has been integrated those two functions to assess the readability of certain text such as Microsoft Office 2010, Readme, OpenOffice, etc. In this project, the Microsoft Office 2010 was used to measure FRES and FKGL. By default, Microsoft Office 2010 disables those two functions. Thus, the following steps illustrate how to enable the functions:

1. Open a blank Microsoft Office Word[9] 2010.
2. Go to the Menu Bar of Word on the top area of the window and click the menu "File".
3. On the left side of the menu, click "Options" for the further settings.

[9] Word is one of the Microsoft Office 2010's components

4. It will pop out a new window named "Word Options", click "Proofing" on the left side of the new window.
5. Mark the "Show readability statistics" under the "When correcting spelling and grammar in Word" options which are located in the middle of the right part of the new window.
6. Hit "OK" on the bottom of the new window, and the setting is done.

Define "Difficulty" Score

Since FKGL was developed based on FRES, this project chose FRES as the primary measurement; although both FKGL and FRES have been checked. Actually, Dr. Rudolf has already built the table (see Table 1) to define the difficulty of a certain context by measuring FRES. This project adopted his scale; Table 5 shows the FRES difficulty score.

Table 5. Flesch Reading Ease Score Difficulty Score

FRES	Performance
90 ~ 100	Very Easy
80 ~ 90	Easy
70 ~ 80	Fairly Easy
60 ~ 70	Standard
50 ~ 60	Fairly Difficult
30 ~ 50	Difficult
0 ~ 30	Very Difficult

From 0 to 30 points, the context was defined as "very difficult". "Difficult" text had 30 to 50 points of FRES. And the context became easier and easier with the growth of FRES. The following section demonstrated how to use

Microsoft Office 2010 to gain FRES and FKGL scores of each DJC's online privacy policy.

Procedure of Dow Jones Corporation's Difficulty Score

After the readability statistics function of Word has been enabled, Microsoft Office 2010 can be used to measure the FRES and FKGL for each DJC's online privacy policy. Here, IBM was used as an example to illustrate the specific steps:

1. Open a blank Word document, and paste the online privacy policy into it. The following link will shows the detailed privacy policy of IBM, http://www.ibm.com/privacy/details/us/en/
2. Go to the Menu Bar of Word on the top area of the window and click the menu "Review".
3. Click the first button "Spelling & Grammar" on the left side of the menu.
4. Ignore all the spelling and grammar errors by clicking "Ignore All" or "Ignore Rule" button on the right side of the new pop-out window.
5. After all the spelling and grammar checking is skipped, it will pop out another window named "Microsoft Word". And hit "OK".
6. Finally a new window named "Readability Statistics" will be exhibited automatically and it will display the details including FRES, FKGL, Passive Voice Percent, etc.
7. For IBM, FRES is 41.4, and FKGL is 13.4. It may vary since corporations will update their privacy policies occasionally.

Design of College of Business and Public Administration Student Survey

This project applied the approaches learned from literature review, but conducted a survey study also. The study collected a number of information regarding both privacy concerns and policy readability from the CBPA College students. Fortunately, the CBPA College of CSUSB has purchased a license for Qualtrics Online Survey Software, which is a powerful online-based survey software with lots of quantitative statistical analysis. It greatly reduced the time consumption of this project including distributing, collecting, and analyzing for the survey.

Purpose of the Survey

According to the literature review in Chapter Two, privacy concerns have been growing dramatically since personal information has become a tradeable commodity in capitalist societies (Hamelink, 2000). And a number of researches have revealed that most online privacy policies of corporations can only be comprehended by college educated customers, and are unreadable for the mass customers. Meanwhile, this project emphasized on the practical meaning for customers. Therefore, this project conducted a survey from the CBPA College at CSUSB to assistant analyze the practical situation of current online privacy policies from customers' view. The survey helped to better understand how customer think about the current privacy policy, whether or not it is meaningful to launch this project, how is the practical situations in this field at least from the surrounding customer groups, etc.

Procedure of the Survey

In order to improve the respond rate of the survey without incentives, the author requested the survey takers just responded to two simple multiple-choice questions as followed:

1. Do you think Online Privacy Policy is important?
   A. Unimportant
   B. Neither Important nor Unimportant
   C. Somewhat Important
   D. Very Important
   E. Extremely Important
2. How is the READABILITY of Online Privacy Policy according to your experience?
   A. Very Difficult
   B. Difficult
   C. Somewhat Difficult
   D. Neutral
   E. Somewhat Easy
   F. Easy
   G. Very Easy

Around four hundred links were sent out in the CBPA College and only one hundred and seventeen samples were collected. The first question aimed to

collect the general intentions from customers regarding privacy concerns. And the second one roughly gathered the customers' understanding of privacy policy. Although those two questions cannot provide the population intentions of customers and the specific readability of each DJC's privacy policy from customers' view, it is still sufficient to help this project to explore the practical situations from the whole picture as a supplement.

Summary

This chapter introduced the specific approaches learned from the literature viewed to develop the project. And it also gave the detailed procedure for both FIPs compliance and readability assessment approaches. As the project objectives and questions described in Chapter One, this project conducted a survey to assist the two primary questions: 1) How well does DJC's online privacy policy comply with FTC Fair Information Practice Principles, and 2) How is the readability of DJC's online privacy policy; is it easy to understand? The following chapter presented the results for both FIPs compliance and readability assessment for those two questions. And it also reflected the role of the CBPA student survey through the presenting of the results.

CHAPTER FOUR

PRESENTATION OF FINDINGS

Introduction

This chapter presents the findings based on the methodology in Chapter Three. It explored the results from both overall and sector performance of each DJC's online privacy policy. In terms of FIPs compliance, it included privacy seal performance; similarly, passive voice performance is discussed for readability assessment in this chapter as well. As introduced in Chapter One, the thirty DJCs can be classified into six sectors. See Table 6 for the specific classifications for each Dow Jones Corporation:

Table 6. Dow Jones Corporation's Sectors

Basic Materials	Alcoa	AA	Consumer Goods	Coca-Cola	KO
	Chevron	CVX		Home Depot	HD
	Exxon Mobile	XOM		Kraft Foods	KFT
Financials	American Express	AXP		McDonald's	MCD
	Bank of America	BAC		Procter & Gamble	PG
	JPMorgan Chase	JPM		Travelers	TRV
Health-care	Johnson & Johnson	JNJ		Wal-Mart	WMT
	Merck & Co.	MRK		Walt Disney	DIS
	Pfizer	PFE	Technology	AT&T	T
Industrial Goods	3M	MMM		Cisco Systems	CSCO
	Boeing	BA		Hewlett-Packard	HPQ
	Caterpillar	CAT		Intel	INTC
	DuPont	DD		IBM	IBM
	General Electric	GE		Microsoft	MSFT
	United Technologies	UTX		Verizon Communications	VZ

Results of Fair Information Practice Principle Compliance

The following table displays each DJC's FIPs rating score based on the table (FIPs Requirement Criteria) in Chapter Three.

Table 7. Dow Jones Corporation's Fair Information Practice Principle Rating Score

Com.	Notice				Choice		Access			Security			Seal	Total	Rating
	1)	2)	3)	4)	1)	2)	1)	2)	3)	1)	2)	3)	1)		
MMM	3	3	3	3	6	6	4	4	0	4	4	4	0	44	AAA
AA	3	3	3	3	6	6	4	4	4	4	4	4	0	48	AAA
AXP	3	3	3	3	6	6	4	4	0	4	4	4	0	44	AAA
T	3	3	3	3	6	6	4	4	0	4	4	4	12	56	AAA
BAC	3	3	3	3	6	6	4	4	0	4	4	4	0	44	AAA
BA	3	3	0	3	0	0	0	0	0	4	4	4	0	21	A
CAT	3	3	0	3	6	6	4	4	0	4	4	4	0	41	AAA
CVX	3	3	3	3	6	0	0	0	0	4	4	4	0	30	AA
CSCO	3	3	3	3	6	6	4	4	4	4	4	4	12	60	AAA
KO	3	3	3	3	0	0	4	4	0	4	4	4	0	32	AA
DD	3	3	3	3	6	6	4	4	4	4	4	4	0	48	AAA
XOM	3	3	3	3	6	0	4	4	4	0	0	0	0	30	AA
GE	3	3	3	3	0	0	4	4	0	4	4	4	0	32	AA
HPQ	3	3	3	3	6	6	4	4	4	4	4	4	12	60	AAA
HD	3	3	3	3	6	6	0	0	0	4	4	4	0	36	AA
INTC	3	3	3	3	6	0	4	4	0	4	4	4	0	38	AAA
IBM	3	3	3	3	6	6	4	4	4	4	4	4	12	60	AAA
JNJ	3	3	3	3	0	0	4	4	4	4	4	4	0	36	AA
JPM	3	3	3	3	0	0	0	0	0	4	4	4	0	24	A
KFT	3	3	3	3	6	0	4	4	4	0	0	0	0	30	AA
MCD	3	3	3	3	0	0	4	4	4	0	0	0	0	24	A
MRK	3	3	3	3	6	6	4	4	0	4	4	4	12	56	AAA
MSFT	3	3	3	3	6	0	4	4	0	4	4	4	12	50	AAA
PFE	3	3	3	3	6	6	4	4	4	4	4	4	0	48	AAA
PG	3	3	3	3	6	6	4	4	0	4	4	4	12	56	AAA
TRV	3	3	3	3	0	6	4	4	0	4	4	4	0	38	AAA
UTX	3	3	3	3	0	0	4	4	0	0	0	0	0	20	A
VZ	3	3	3	3	6	6	4	4	0	4	4	4	12	56	AAA
WMT	3	3	3	3	6	6	4	4	0	4	4	4	0	44	AAA
DIS	3	3	3	3	6	6	4	4	0	4	4	4	12	56	AAA

Dow Jones Corporation Fair Information Practice Principle Overall Performance

Table 7 illustrates that most[10] DJCs comply with Notice and Security principles. There are a number[11] of companies that do not fully comply with the Choice and Access principles. The average rating score of those thirty companies is equal to 42.07, which still qualified for AAA. The following pie chart presents the weight of each rating grade.

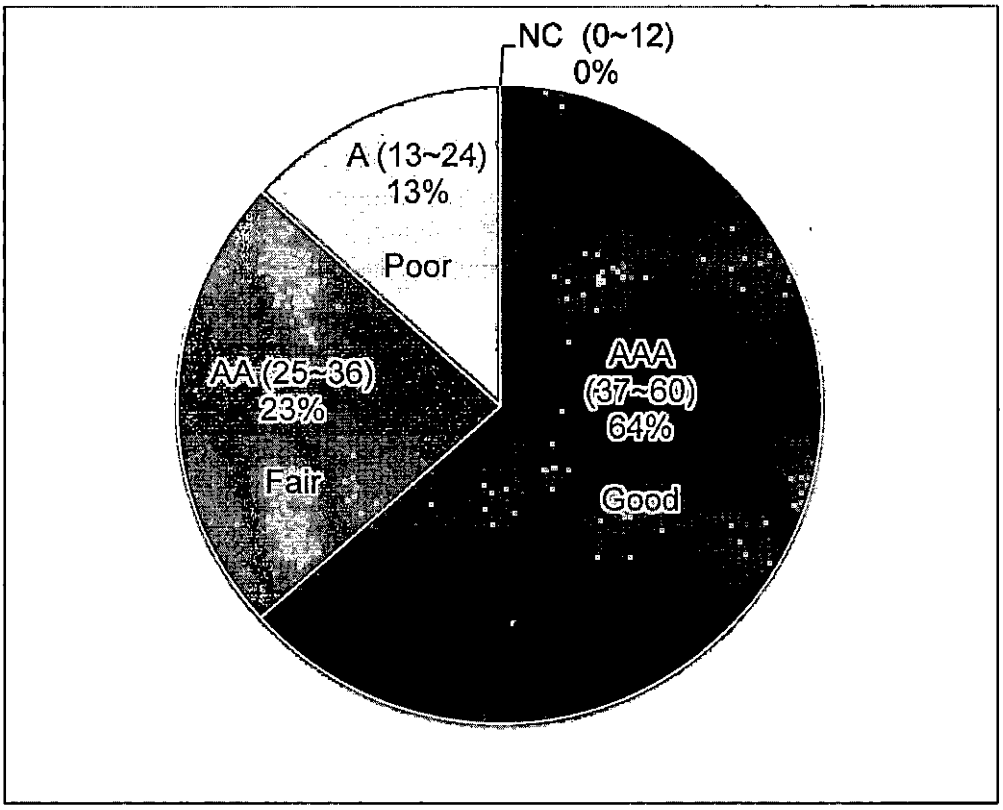

Figure 2. Dow Jones Corporation's Fair Information Practice Principle Overall Performance

[10] Twenty-eight out of thirty (93.33%) corporations comply with the Notice principle in all aspects, and twenty-six out of thirty (86.67%) fully comply with the Security principle.
[11] There are thirteen out of thirty (43.33%) companies do not comply with the Choice principle in all aspects, and twenty out of thirty (66.67%) do not fully comply with the Access principle.

Nineteen companies qualified for AAA rating, seven for AA rating, and four for A rating. Although AAA does not mean one hundred percent comply with FIPs, it still indicated that the overall performance of the thirty DJCs in terms of privacy concerns were relatively better than others according to the review of the literature in Chapter Two. And it also corresponds to the expectation in Chapter One, which indicated DJCs may have better performance in terms of FIPs compliance.

Dow Jones Corporation Fair Information Practice Principle Sector Performance

The standard deviation was 12.3872. Table 8 shows the average rating score for the six sectors of DJCs.

Table 8. Dow Jones Corporation's Fair Information Practice Principle Sector Average Rating Score

DJC's Sector	Average Rating Score	Rating Grade
Basic Materials	36	AA
Consumer Goods	40	AAA
Financials	37	AAA
Health Care	47	AAA
Industrial Goods	34	AA
Technology	54	AAA

Basic Materials and Industrial Goods in Table 8 need to improve their privacy policy to more fully comply with FIPs. Since the FIPs is a widely accepted guideline for privacy concerns, companies still have their own opportunity to formulate the privacy policies. Therefore, those companies that received an AA rating do not mean that they were careless about customers'

privacy, but they need to change their policy layout to better respond to FIPs regulations.

In addition, the following radar map displays the trend of FIPs performance among the six sectors.

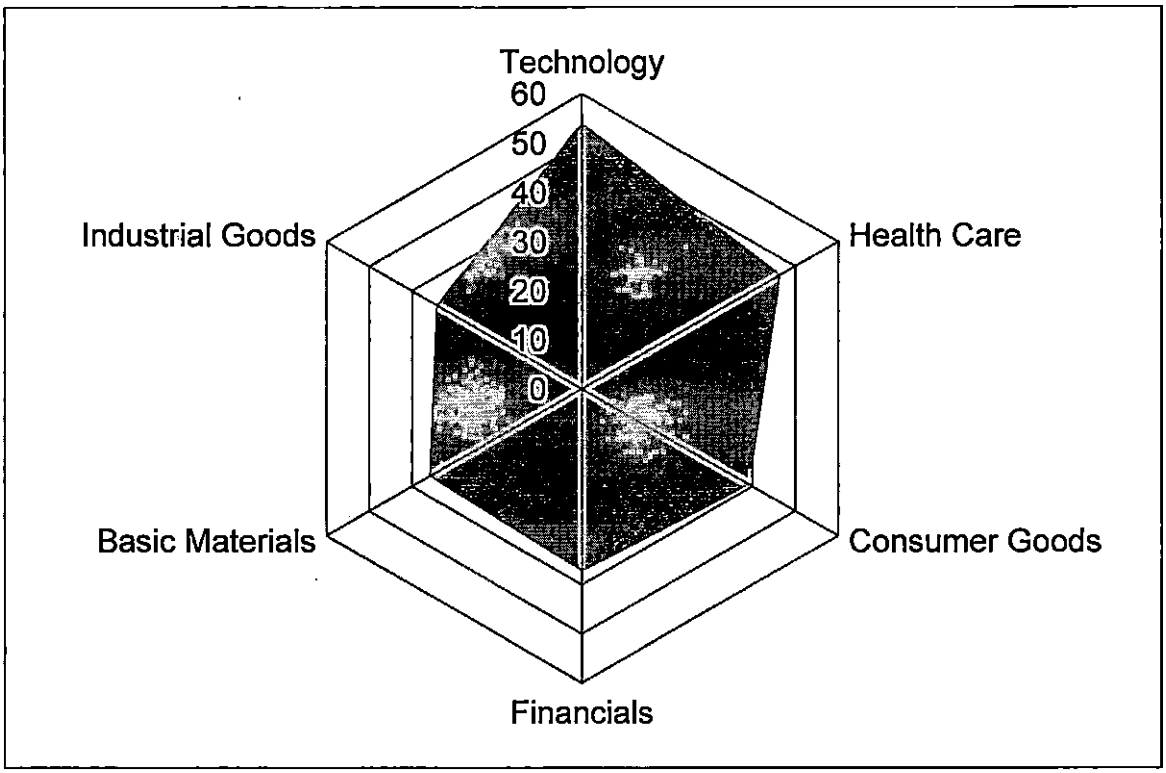

Figure 3. Dow Jones Corporation's Fair Information Practice Principle Sector Performance

Figure 3 shows that Technology, Health Care, and Consumer Goods tend to have better privacy concerns. Those companies have relatively closed activities with customers rather than the rest sectors. Obviously, those companies have to pay more attentions on their privacy policies. In addition, all

the privacy seals are only found in those three sectors, and this will be further discussed in the following section.

Dow Jones Corporation Privacy Seal Performance

Privacy seal aims to give customers a quick and intuitive notification. It helps to self-regulate corporation's privacy policy, and provides a reliable Trustmark for customers. In this project, only nine of thirty (30%) companies display one or more seals in their online privacy policies. Table 9 indicates that specific corporations have privacy seals and their sector classification.

Table 9. Dow Jones Corporation's Privacy Seal Performance

Company	Rating Grade	Sector
Procter & Gamble	AAA	Consumer Goods
Walt Disney	AAA	
Merck	AAA	Health Care
AT&T	AAA	Technology
Cisco Systems	AAA	
Hewlett-Packard	AAA	
IBM	AAA	
Microsoft	AAA	
Verizon Communications	AAA	

It is interesting to note that all the sealed companies were found in Consumer Goods, Health Care, and Technology sectors. Note that all of them have the "Good" performance in terms of FIPs compliance. From this point, it seems that privacy seal does help corporations to better comply with FIPs principles. Additionally, it appears that technology sector pays more attention on

privacy seal rather than other sectors. Actually, only Intel does not have a privacy seal among technology corporations. However, how is the readability of DJC's online privacy policy, especially for technology sector?

Results of Readability Assessment

Table 10 presents each DJC's FRES, FKGL, and Passive Voice Percent score based on the demonstration of IBM's privacy policy readability measurement and the table (FRES Difficulty Score) in Chapter Three.

Table 10. Dow Jones Corporation's Readability Difficulty Score

Com.	FRES	FKGL	Passive %	Df[12]	Com.	FRES	FKGL	Passive %	Df
MMM	33.6	14.4	16%	D[13]	INTC	38.7	12.2	6%	D
AA	40.8	12.8	29%	D	IBM	41.4	13.4	15%	D
AXP	39.9	11.0	4%	D	JNJ	30.0	15.8	36%	V
T	41.5	12.4	9%	D	JPM	44.3	10.1	6%	D
BAC	36.7	13.9	10%	D	KFT	42.4	12.4	16%	D
BA	39.4	12.3	22%	D	MCD	44.5	12.1	11%	D
CAT	27.4	15.2	15%	V[14]	MRK	33.5	14.5	11%	D
CVX	33.1	13.6	24%	D	MSFT	36.5	14.1	22%	D
CSCO	32.1	14.7	20%	D	PFE	37.3	13.6	15%	D
KO	36.0	13.6	15%	D	PG	47.1	10.6	9%	D
DD	31.5	14.8	12%	D	TRV	40.4	12.2	16%	D
XOM	26.5	16.3	9%	V	UTX	48.1	11.3	23%	D
GE	44.4	12.4	11%	D	VZ	27.2	15.5	22%	V
HPQ	34.1	14.0	17%	D	WMT	41.2	11.8	9%	D
HD	35.3	14.3	21%	D	DIS	28.6	14.5	16%	V

[12] Df refers to Difficulty Score.
[13] D refers to "Difficult".
[14] V refers to "Very Difficult".

Dow Jones Corporation Readability Overall Performance

Table 10 indicated all thirty DJCs' privacy policies were either "Difficult" or "Very Difficult" to read. The average FRES of those thirty companies was equal to 37.12, which means "Difficulty" or "Academic[15] text". The average FKGL of them was equal to 13.33, which reveals that only college educated customers can comprehend those difficult privacy policies. The following pie chart displays the weight of each difficulty grade.

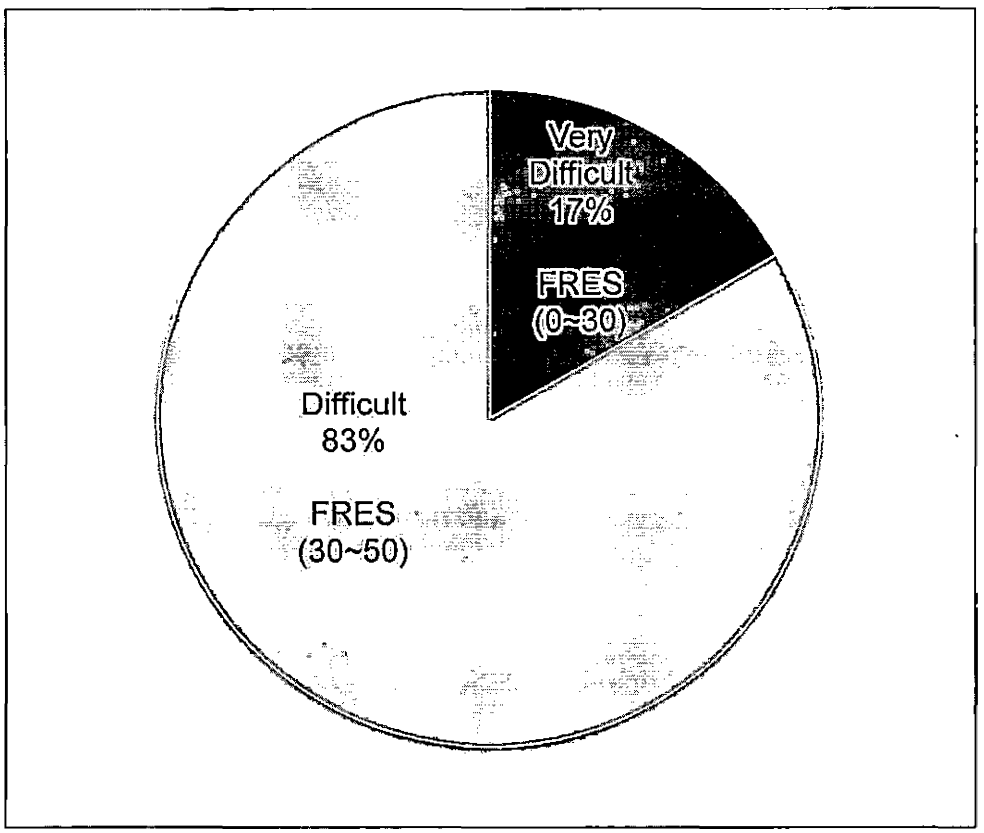

Figure 4. Dow Jones Corporation's Readability Overall Performance

[15] See Chapter Two, Table 1.

There were five companies that were "very difficult" to read, and the rest were "difficult". As indicated in Chapter Three, FRES was treated as the primary measurement for policies readability; therefore, Figurer 4 demonstrated that the overall performance of the thirty DJCs was unsatisfied in terms of readability. It also corresponded to the expectations in Chapter One, which indicated that online privacy policy had grown in length but had declined in readability.

Dow Jones Corporation Readability Sector Performance

Similar with FIPs sector exploration, DJCs' readability sector performance with a 5.9960 standard deviation of FRES is discussed. Table 11 shows the average FRES score for the six sectors of DJCs.

Table 11. Dow Jones Corporation's Readability Sector Average Flesch Reading Ease Score

DJC's Sector	Average of FRES	Difficulty Grade
Basic Materials	33.47	Difficult
Consumer Goods	39.44	Difficult
Financials	40.30	Difficult
Health Care	33.60	Difficult
Industrial Goods	37.40	Difficult
Technology	35.93	Difficult

Table 11 demonstrated that all the privacy policies of those six sectors were difficult to read. To respond to the question, "How is the readability of DJC's online privacy policy, especially for technology sector?", it was obvious that none of the thirty DJCs have an easy-to-read performance, even though the Technology sector with a 35.93 FRES, which was approximately equivalents to

14 FKGL, still needed college education to understand the complicated online privacy policies.

In addition, Figure 5 is a radar map that indicated the trend of readability performance among the six sectors.

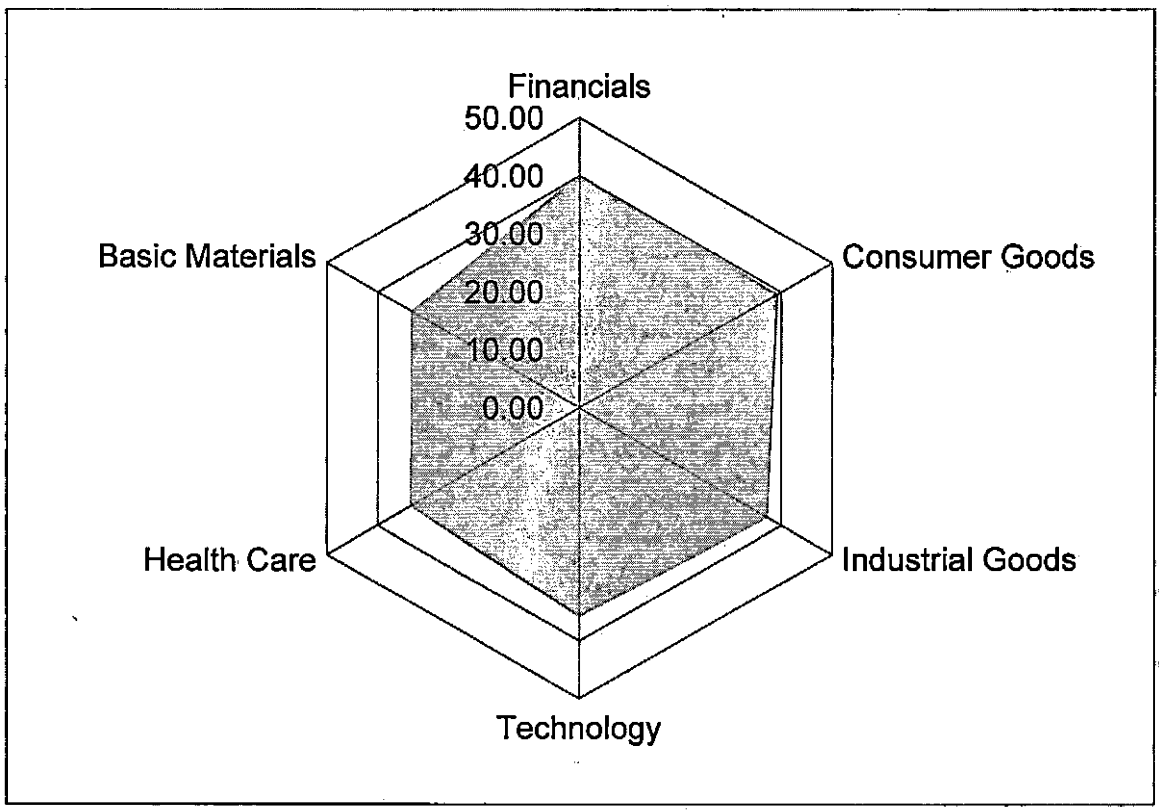

Figure 5. Dow Jones Corporation's Readability Sector Performance

Although those six sectors have very similar performance in terms of readability, it seems that the Financials sector trended to have the best performance among them. Recently, many banks have updated their privacy policies with written letter notice to customers, such as Bank of America,

JPMorgan Chase, etc. As one credit-card holder of Bank of America, the author has had personal experience with several privacy notice received. However, each bank has their own way to draw up their privacy policies, and none of them (limited to DJCs) displayed a privacy seal in their online privacy policies. Meanwhile, banks would like their customers to read the privacy policies, which contain lots of critical personal and financial information, such as Social Security Number, Date of Birth, etc. Therefore, in order to satisfy current and future customers with different educational backgrounds, the Financials sector has to make their privacy policies relatively easy to read and better organized.

Due to the fact that all privacy policies of the thirty DJCs were hard to understand, the analysis of Passive Voice Percent will help to give some direction to the terms of policy readability. Still, there has been continued debates regarding whether or not passive voice will decrease readability or reduce the reading speed, it seems that the passive-voice-percent analysis would help to further explorer the readability performance of DJCs' online privacy policies.

Dow Jones Corporation Passive Voice Performance

According to Table 1 and Table 10, all the DJC's privacy policies were either "scientific" or "academic" text and Dr. Rhodes[16] believed that there no difference regarding comprehensibility between active and passive voice in

[16] See Chapter Two View of the Literature, Passive Voice.

scientific writing, it seems that there will be no relationship between FRES and Passive Voice Percent. However, Figure 6 displays a different finding.

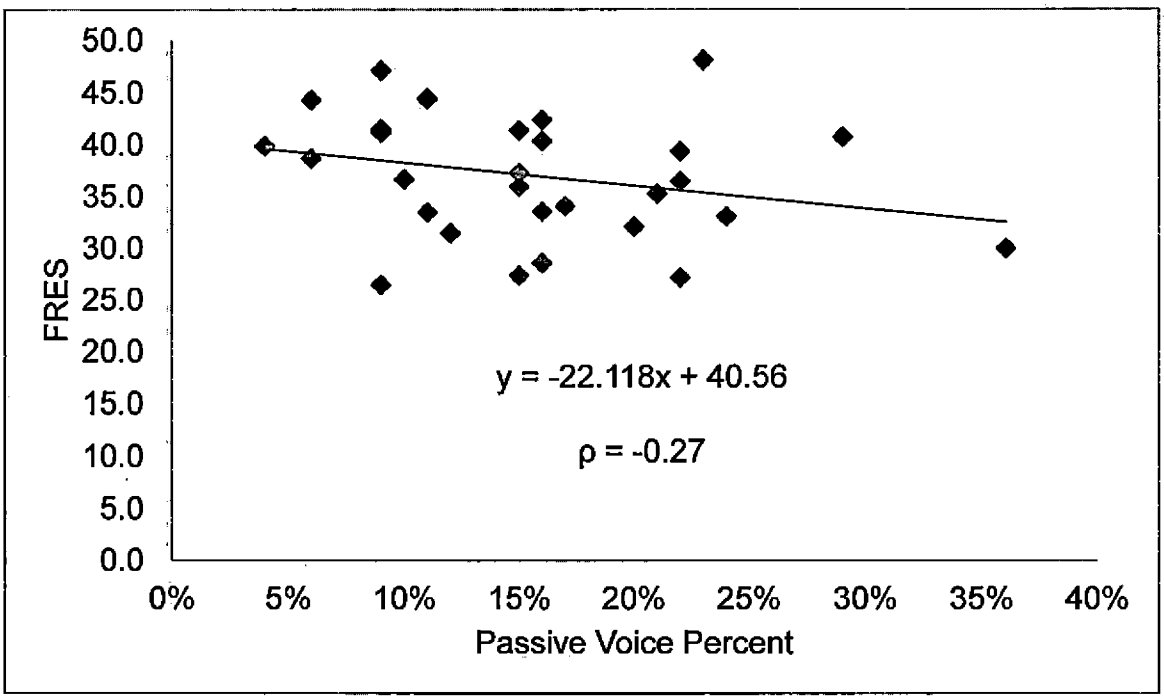

Figure 6. Relationship between Passive Voice and Flesch Reading Ease Score

As indicated in Figure 6, there was a slight negative relationship between Passive Voice Percent and FRES. In other words, passive voice indeed decreases policy readability in a small weight. Furthermore, the Correlation Coefficient (ρ) of those two variables was equal to -0.27, which means the inverse relationship between those two variables is considerable, but not significant.

On the other hand, the regression equation in Figure 6 revealed that as an extreme situation. When passive voice percent was equal to 0, FRES would reach its maximum value of 40.56; however, it was still defined as "Difficulty". Therefore, passive voice essentially cannot change the hard-to-read nature of online privacy policies of DJCs in terms of readability, but may be able to help to improve its performance.

In addition, the average passive voice percent of the thirty DJCs' online privacy policies was equal to 15.57%. What does this amount mean? Using Google Inc. as an example of a well-known and influential corporation towards to U.S. stock market and one that just updated its online privacy policy in March, 2012; However, DJCs do not include Google, either. Thus, Google was used as a reference in this project. The passive voice percent of Google's online privacy policy was just 5%. Although the ten percent difference between the average of DJCs and Google cannot change the hard-to-read nature of DJCs' privacy policies, it still can help customers to better understand the complex privacy policies in some degree. Moreover, the FRES of Google was also a little above the average of DJCs (37.12[17]), which was equal to 38.5. Therefore, 15.57% of passive voice indicates that there was still a little space for DJCs to improve their policy readability by reducing passive voice percent.

[17] See this chapter, DJC Readability Overall Performance

Result of College of Business and Public Administration Student Survey

As mentioned in Chapter Three, a survey was given to undergraduate and graduate students in the College of Business and Public Administration at California State University, San Bernardino. The results were not atypical. The results corresponded to the research conclusions of DJCs' online privacy policies in terms of privacy concerns and policy readability. The following two sections will present the outcomes for the two survey questions: 1) Do you think Online Privacy Policy is important; and 2) How is the READABILITY of Online Privacy Policy according to your experience?

Importance of Online Privacy Policy

Table 12 shows the responds for question one: Do you think Online Privacy Policy is important?

Table 12. Importance of Online Privacy Policy Survey Statistics

#	Answer		Response	%
1	Unimportant		0	0%
2	Neither Important nor Unimportant		2	2%
3	Somewhat Important		12	10%
4	Very Important		51	44%
5	Extremely Important		52	44%
	Total		117	100%

As shown in Table 12, eighty-eight percent of students believed online privacy policy was either very important or extremely important. None of the students considered the privacy policy as unimportant. Thus, the first survey

question provided a solid evidence for intensive privacy concerns and also showed the significance of this project. Table 12 also indicated that most customers indeed care about their privacy nowadays, which was reflected in the review of the literature.

Furthermore, Figure 7, a radar map, shows the trend of customers' privacy concerns at least in the CBPA College.

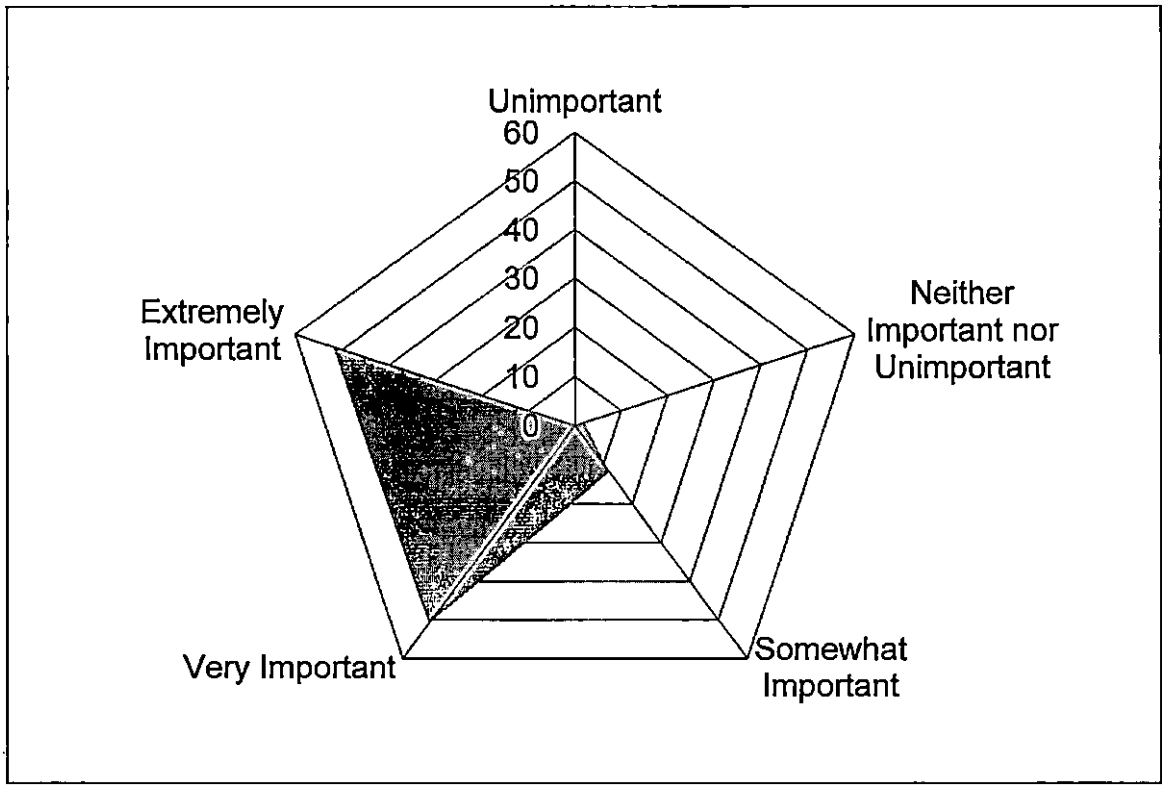

Figure 7. Importance of Online Privacy Policy Distribution Map

Figure 7 clearly demonstrated that most responds were allocated in the "important" area, and indicated the increasing trend for privacy concerns as

demonstrated with increased to the "important" area. While, the privacy policy was critical for customers, the customers did not read or understand it in practice.

Readability of Online Privacy Policy

Table 13 displays the responds for question two: How is the READABILITY of Online Privacy Policy according to your experience?

Table 13. Readability of Online Privacy Policy Survey Statistics

#	Answer		Response	%
1	Very Difficult		15	13%
2	Difficult		18	15%
3	Somewhat Difficult		35	30%
4	Neutral		39	33%
5	Somewhat Easy		7	6%
6	Easy		3	3%
7	Very Easy		0	0%
	Total		117	100%

When developing the second survey question, the phrase, "according to your experience" was added to the end of the sentence since students might not read the privacy policy at all. Coincidentally, the most frequent answer was "Neutral" at 33%. It indicated that there were a quite number of students that did not know the readability of various online privacy policies. In order words, the individual never read the policy or just quickly scanned it to give an answer.

In addition, forty-five percent of the students believed that the online privacy policy was either "somewhat difficult" or "difficult" to read. Thirteen percent of them even felt that the policy was "very difficult" to understand. Less

than ten percent of the people said the policy was "easy" or "somewhat easy" to read. However, none of them stated it was "very easy" to read. Therefore, it can draw a very clear and simple conclusion that most online privacy policies were not easy to read. Actually, in terms of DJCs' online privacy policies, all of them were difficult to read and some of them were even very difficult to understand. Furthermore, the Figure 8, the radar map, gives the distribution of the policy readability and its trend from the customers' point of view.

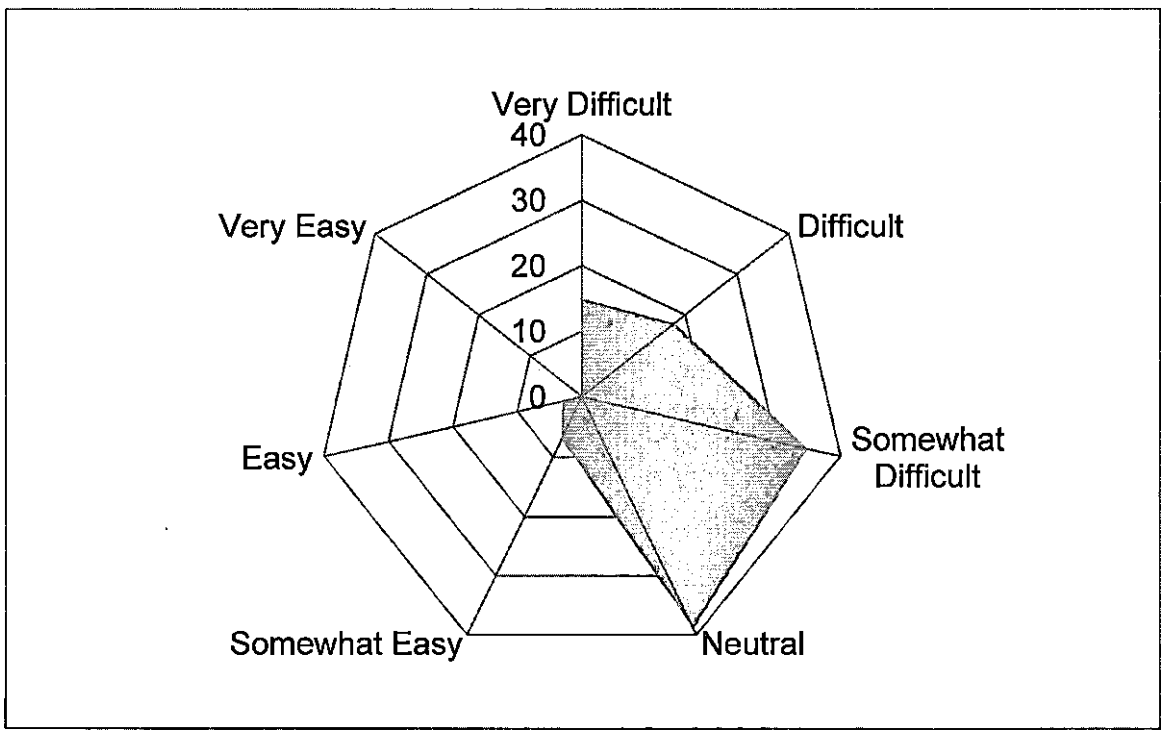

Figure 8. Readability of Online Privacy Policy Distribution Map

Figure 8 indicated the most responds were grouped in the "somewhat difficult" to the "neutral" area. As said above, it could be indicative that the

customers did not read the policy or have any sense about the policy readability. Additionally, people may have a trend of impression for the unreadable online privacy policy although some of them do not think the policy was very difficult to read.

Summary

This chapter presented the research results for DJCs' online privacy policies from both FIPs compliance and readability assessment. Although not all DJCs comply with FIPs principles in every way, there were still sixty-four percent of them have a good performance with AAA rating grade. Unfortunately, the readability performance of DJCs' online privacy policies was quite unsatisfactory. None of them were easy to understand or to read. In addition, the CBPA student survey reveals that most customers believe their privacy was either important or extremely important. However, it seems that a large number of customers did not read the online privacy policy. In next chapter gives some recommendations based on the findings discovered in this chapter.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

This chapter gives a brief overview of the project. It reinforces the intensive concerns of customer's privacy upon DJCs' online privacy policies to better comply with FIPs principles and the needs for the shorter and simpler online privacy policies of DJCs. Furthermore, a clear and conclusive answer based on the findings of chapter four will be presented to respond to the two primary research questions which has been stated in chapter one. Finally, this chapter will be end with recommendations to address the results of those two questions.

Overview of the Project

The internet has been bringing both panacea and anathema to the mass customers (Brown & Muchira, 2004). People take the advantage of convenience and quick services provided by e-market, meanwhile, facing the potential privacy risks caused by the rapidly growing and hard-to-secure e-businesses. Chapter one revealed that customer's credit card information were frequently cracked by hackers through the internet transactions. Moreover, Hamelink stated that personal information has become a tradable commodity in capitalist societies (Hamelink, 2000). It, obviously, has already caught customer's attention regarding their personal privacy in nowadays. Although there is no perfect

protection for customer's privacy, most experts believe that a corporation's online privacy policy is currently the best way to balance privacy concerns and online activities (Andrews, 2001).

FIPs is the widely accept principle introduced by FTC to regulate a company's privacy policy in order to safeguard customer's privacy. While, from a customer's point of view, an easy-to-read and FIPs complied policy means more senses because current online privacy policy had grown in length but declined in readability according to Milne's (2006) research. As mentioned in chapter one, due to the scope of this project, only the thirty DJCs' online privacy policies have been explored.

This project has examined the FIPs compliance of all the thirty DJCs' online privacy policies, and has assessed the policy readability of those corporations from a practice perspective for customers. Additionally, to assist those two primary research questions in chapter one, this project has also conducted a customer (student) survey to better understand the practical situations regarding privacy concerns and policy readability. The following section will focus on the primary questions and draw the overall conclusions for DJC's online privacy policy.

Conclusions

Primary research question one: How well does DJC's online privacy policy comply with FTC Fair Information Practice Principles?

The findings from chapter four revealed that all the thirty DJCs posted an online privacy policy, and sixty-four percent of them, generally speaking, comply with FTC FIPs principles. Nine of those corporations have displayed a privacy seal in their online privacy policies. Among the six sectors of DJCs, Technology sector occupies six seals and has the best performance in terms of FIPs compliance.

Primary research question two: How is the readability of DJC's online privacy policy; is it easy to understand?

Unfortunately, all thirty DJCs' online privacy policies are difficult to read, and require at least college education to comprehend the "academic context". Seventeen of them are even very difficult to read, and need graduate training to understand the "scientific text". Although it cannot change hard-to-read nature of DJC's online privacy policy, the average Passive Voice Percent of those thirty companies are relatively high comparing with Google's. Financials sector and Consumer Goods sector have a slightly better performance than the rest sectors in terms of policy readability.

Overall, the thirty DJCs' online privacy policies have relatively good privacy protection for their customers; however, none of them proposed a widely readable online privacy policy to help customers to better understand it. Overtime, customer's privacy will play a critical role for companies to keep and maintain their business relationships with customers. Therefore, corporations have to consummate their privacy policy, especially complying with FIPs

principles and to reduce the complexity of the policy to help customers to understand. The following section will provide some advice in terms of how to improve DJC's online privacy policy.

Recommendations

The recommendations will be given from both FIPs compliance and policy readability viewpoints. In terms of FIPs compliance, DJCs need to update their online privacy policies more frequently due to the facts of rapidly growing e-businesses and intensive privacy concerns. Although there are some other third parties (e.g. FreePrivacyPolicy.com) provide the service of generating online privacy policy, it is recommended that DJCs to join in the privacy seal program to create the certified online privacy policy by TRUSTe, BBBOnLine or WebTrust. The privacy seal provides a Trustmark for the online privacy policy, and also improves the readability by giving customers a quick and intuitive sense.

In addition, reducing the policy length will shorten the time consumptions spent by customers for reading. Using more ordinary words rather than advanced vocabulary would decrease ASW[18] , thus, to increase FRES score. Similarly, applying more short sentences than complex ones would reduce ASL[19] leading to raise FRES. Eventually, the enlarged FRES will improve the overall readability of DJC's online privacy policy.

---

[18] Average Word Length in Syllables; see Chapter Two literature review, FRES & FKGL.
[19] Average Sentence Length; see Chapter Two literature review, FRES & FKGL, too.

Furthermore, adopting more active voice than passive voice could also mend the policy readability in some degree. However, corporations will face a fact that they have to disclose and clarify the subject of each sentence. It might hurt the companies' equity or offend some certain laws. Therefore, blindly to reduce the passive voice would bring a negative impact on DJC's online privacy policy. To balance, keeping the Passive Voice Percent in a small amount (e.g. 5% like Google's) would be the best way for both corporations and customers.

APPENDIX A

THE THIRTY DOW JONES CORPORATION COMPONENTS

Ticker	Company	URL
MMM	3M Co.	www.3m.com
AA	Alcoa Inc.	www.alcoa.com/global/en/home.asp
AXP	American Express Co.	www.americanexpress.com
T	AT&T	www.att.com
BAC	Bank of America	www.bankofamerica.com
BA	Boeing Co.	www.boeing.com
CAT	Caterpillar Inc.	www.cat.com
CVX	Chevron	www.chevron.com
CSCO	Cisco Systems Inc.	www.ciscosystems.com
KO	Coca-Cola Co.	www.thecoca-colacompany.com
DD	E.I. DuPont de Nemours & Co.	www.dupont.com
XOM	Exxon Mobil	www.exxonmobil.com/corporate
GE	General Electric Co.	www.ge.com
HPQ	Hewlett-Packard	www.hp.com
HD	Home Depot Inc.	www.homedepot.com
INTC	Intel Corp.	www.intel.com/content/www/us/en/homepage.html
IBM	International Business Machines Corp.	www.ibm.com/us/en
JNJ	Johnson & Johnson	www.jnj.com
JPM	JPMorgan Chase	www.jpmorganchase.com/corporate/Home/home.htm
KFT	Kraft Foods Inc. Cl A	www.kraftfoodscompany.com
MCD	McDonald's Corp.	www.mcdonalds.com
MRK	Merck & Co. Inc.	www.merck.com
MSFT	Microsoft Corp.	www.microsoft.com
PFE	Pfizer Inc.	www.pfizer.com
PG	Procter & Gamble Co.	www.pg.com
TRV	Travelers Cos.	www.travelers.com
UTX	United Technologies Corp.	www.utc.com/Home
VZ	Verizon Communications	www.verizon.com
WMT	Wal-Mart Stores Inc.	www.walmart.com
DIS	Walt Disney Co.	www.corporate.disney.go.com/

Components. (2012). In *Dow Jones Indexes, A CME group company*. Retrieved from http://www.djaverages.com/?go=industrial-components

APPENDIX B

U.S. EDUCATION GRADE LEVEL STRUCTURE

Grade Level[20]	Age or Title
Graduate School	
20th Grade	4th Year (ages vary)
19th Grade	3rd Year (ages vary)
18th Grade	2nd Year (ages vary)
17th Grade	1st Year (ages vary)
Undergraduate School	
16th Grade	Senior (ages vary)
15th Grade	Junior (ages vary)
14th Grade	Sophomore (ages vary)
13th Grade	Freshman (ages vary)
High School	
12th Grade	17-18
11th Grade	16-17
10th Grade	15-16
9th Grade	14-15
Middle School	
8th Grade	13-14
7th Grade	12-13
6th Grade	11-12
Elementary School	
5th Grade	10-11
4th Grade	9-10
3rd Grade	8-9
2nd Grade	7-8
1st Grade	6-7
Kindergarten	5-6
Preschool	4-5

Education in the United States. (2012, April 13). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/Education_in_the_United_States#cite_note-13

[20] The author integrated elementary, secondary, and post-secondary educations with continued grade levels.

REFERENCES

Acohido, B. (2012). Obama pushes online privacy rights. *USA Today*, 01b.

Andrews, S. (2001). Protecting your privacy. *Fortune, 142*(12), 27-28.

Antón, A. I., Earp, J. B., Bolchini, D., He, Q., Jensen, C., & Stufflebeam, W. (2004). The lack of clarity in financial privacy policies and the need for standardization. *IEEE Security and Privacy, 2*(2), 36-45.

Brown, M., & Muchira, R. (2004). Investigating the relationship between Internet privacy concerns and online purchase behavior. *Journal of Electronic Commerce Research, 5*(1), 62.

Components. (2012). In *Dow Jones Indexes, A CME group company.* Retrieved from http://www.djaverages.com/?go=industrial-components

Credit rating. (2012, July 27). In *Wikipedia, the free encyclopedia.* Retrieved from http://en.wikipedia.org/wiki/Credit_rating

Dow Jones Industrial Average. (2011, December 31). In *Dow Jones Index, A CME group company.* Retrieved from http://www.djindexes.com/mdsidx/downloads/brochure_info/Dow_Jones_Industrial_Average_Brochure.pdf

Dow Jones Industrial Average overview. (2012). In *Dow Jones Indexes, A CME group company.* Retrieved April 13, 2012, from http://www.djaverages.com/?go=industrial-overview

Education in the United States. (2012, April 13). In *Wikipedia, the free encyclopedia.* Retrieved from http://en.wikipedia.org/wiki/Education_in_the_United_States#cite_note-13

Educational attainment in the United States: 2011 - detailed tables. (2011). In *United States Census Bureau.* Retrieved from http://www.census.gov/hhes/socdemo/education/data/cps/2011/tables.htm l

English passive voice. (2012, April 16). In *Wikipedia, the free encyclopedia.* Retrieved from http://en.wikipedia.org/wiki/English_passive_voice

Flesch, R. (1949). *The art of readable writing.* New York: Harper and Row.

Flesch-Kincaid readability test. (2012, March 31). In *Wikipedia, the free encyclopedia*. Retrieved.from http://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_test#cite_note-McClure1987-2

Flesch–Kincaid readability test. (2012, July 12). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_test

FTC Fair Information Practice. (2011, December 31). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/FTC_Fair_Information_Practice

Gough, P. B. (1965). Grammatical transformations and speed of understanding. *Journal of Verbal Learning and Verbal Behavior, 4*(2), 107-111.

Hamelink, C. J. (2000). *The ethics of cyberspace.* London: Sage Publications Ltd.

Hochhauser, M. (2001, May). *Lost in the fine print: readability of financial privacy notices.* Retrieved April 15, 2012, from Privacy Rights Clearinghouse: http://www.privacyrights.org/ar/GLB-Reading.htm

Hochhauser, M. (2003, April 10). *Why patients won't understand their HIPAA privacy notices.* Retrieved April 15, 2012, from Privacy Rights Clearinghouse: http://www.privacyrights.org/ar/HIPAA-Readability.htm

Ian, G. (1998). *Relationship marketing : new strategies, techniques, and technologies to win the customers you want and keep them forever.* Toronto: John Wiley & Sons Canada.

Internet privacy. (2012, April 3). In *Wikipedia the free encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/Internet_privacy

Jensen, C., & Potts, C. (2004). Privacy policies as decision-making tools: an evaluation of online privacy notices. *CHI, 6*(1), 471–478.

Khalil, O. E., & Harcar, T. D. (1999). Relationship marketing and data quality management. *SAM Advanced Management Journal, 64*(2), 26-33.

Kincaid, J. P., Fishburne, L. P., Rogers, R. L., & Chissom, B. S. (1975). *Derivation of new readability formulas (automated readability index, fog count and Flesch Reading Ease formula) for navy enlisted personnel.* Millington: Naval Technical Training Command.

Landesberg, M. K., Levin, T. M., Curtin, C. G., & Lev, O. (1998). *Privacy online: a report to Congress.* Washington, DC: Federal Trade Commission.

Leibowitz: privacy notices should be simple, short. (2011). *Telecommunications Reports, 77*(21), 25-27.

Lewis, O., & Fox, S. (2001, April 2). *Fear of online crime.* Retrieved April 14, 2012, from PewInternet: http://www.pewinternet.org/Reports/2001/Fear-of-Online-Crime/Report/New-laws-are-needed-to-protect-online-privacy.aspx

Markert, B. K. (2002). *Comparison of three online privacy seal programs.* Retrieved April 14, 2012, from SANS Institute Reading Room: http://www.sans.org/reading_room/whitepapers/privacy/comparison-online-privacy-seal-programs_685

Milne, G. R., Culnan, M. J., & Greene, H. (2006). A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing, 25*(2), 238-249.

Nicholson, J. (2012). *Sectors that make up the Dow Jones.* Retrieved April 13, 2012, from eHow: http://www.ehow.com/list_5941700_sectors-make-up-dow-jones.html

Perlroth, N. (2012, March 30). *MasterCard and Visa investigate data breach.* Retrieved April 11, 2012, from The New York Times: http://www.nytimes.com/2012/03/31/business/mastercard-and-visa-look-into-possible-attack.html?_r=1&ref=mastercardinc

Petrison, L. A., & Wang, P. (1995). Exploring the dimensions of consumer privacy: an analysis of coverage in british and american media. *Journal of Direct Marketing, 9*(4), 19-37.

Pitofsky, R., Anthony, S. F., Thompson, M. W., Swindle, O., & Leary, T. B. (2000). *Privacy online: Fair Information Practices in the electronic marketplace.* Washington, DC: Federal Trade Commission.

Privacy policy. (2012, March 31). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/Privacy_policy#Fair_Information_Practice

Privacy seal. (2012, April 12). In *Wiktionary*. Retrieved from http://en.wiktionary.org/wiki/privacy_seal

Privacy seal logo. (n.d.). In *Google images*. Retrieved from https://www.google.com/imghp

Readability. (2012, March 26). In *Wikipedia, the free encyclopedia.* Retrieved from http://en.wikipedia.org/wiki/Readability#Definition

Rhodes, S. (1997). *The active and passive voice are equally comprehensible in scientific writing.* Ann Arbor: A Bell & Howell Information Company.

Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your privacy is sealed: effects of web privacy seals on trust and personal disclosures. *Journal of Consumer Affairs, 39*(2), 339-362.

Schwaig, K. S., Kane, G. C., & Storey, V. C. (2006). Compliance to the fair information practices: how are the Fortune 500 handling online privacy disclosures? *Information and Management, 43*(7), 805-820.

Siegel, A. I., & Burkett, J. R. (1974). Application of structure-of-intellect and psycholinguistic concepts to reading comprehensibility measurement. *Lowry AFB, CO: Air Force Human Resources Lab.*

TRUSTe. (2012, February 15). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/TRUSTe

Vail, W. M., Earp, B. J., & Anton, I. A. (2008, August). An empirical study of consumer perceptions and comprehension of web site privacy policies. *IEEE Transactions on Engineering Management, 55*(3), 444.

Westin, A. F. (2004). How to craft effective online privacy. *Privacy and American Business, 11*(6), 1-2.