THE INFORMATION ERA THREATENS PRIVACY:

A Comparative Study of

Electronic Money’s Privacy Policies and Privacy Laws

By

GUANRU LIU

A thesis submitted to the Graduate Program in the Faculty of Law

in conformity with the requirements for the

Degree of Master of Laws

Queen’s University

Kingston, Ontario, Canada

September, 2011

Copyright © Guanru Liu, 2011
Abstract

This thesis consists of an analysis of electronic money (e-money), e-money’s privacy policies and relevant privacy laws. The value of information and the development of technology enhance the risk of privacy violations in the information era. Consumer privacy interests with respect to e-money are governed in part by the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada and by the European Union’s Data Protection Directive. The analysis is directed at whether the privacy policies of three kinds of e-money – Octopus Card, PayPal and MasterCard – comply with the spirit and letter of these laws. In light of technology change, the laws should be interpreted to apply broadly to protect privacy interests. Enhanced privacy protection may in fact lead to greater adoption of e-money by consumers.
Acknowledgements

I am grateful to many people who provided their help and support to me and this thesis.

My supervisor, Professor Arthur Cockfield, gave me many valuable suggestions about my graduate study, thesis and also my life in Queen’s University. It is difficult to overstate his help and encouragement to me. He is the person who directs me to discover the joy of legal research and makes many efforts to correct and improve my thesis.

I also wish to thank Professor Bita Amani and Professor Nancy McCormack. Professor Amani taught the Information Privacy course in 2010 and as a student in that course, I learnt the basic knowledge and theories about privacy law. Her responsible attitude towards students also moved and encouraged me a lot. In Professor McCormack’s course regarding legal research skills, I learnt how to use and find Canadian legal resource, which greatly helped my research move on smoothly.

Lastly, I want to thank my parents, who support my foreign study and encourage me to pursue my dream all the time. Also, I am grateful to Phyllis Reid, who is the graduate
studies assistant of Faculty of Law, librarians, student colleagues and other friends in Kingston.
Tabel of Contents

Abstract ........................................................................................................................... ii

Acknowledgements ....................................................................................................... iii

Chapter 1: The Information Era vs. Privacy ................................................................. 1

1.1 The Value of Information vs. Privacy ................................................................. 6

1.2 Internet vs. Privacy ............................................................................................... 8

1.3 Privacy .................................................................................................................. 11

Chapter 2: Electronic Money ...................................................................................... 13

2.1 A Brief History of Money ..................................................................................... 13

2.1.1 Bartering ......................................................................................................... 13

2.1.2 Metal Money ................................................................................................... 14

2.1.3 Paper Money .................................................................................................. 15

2.1.4 E-money ........................................................................................................ 16

2.2 The Concept of Money ....................................................................................... 17

2.3 Defining E-money ............................................................................................... 20

2.3.1 Principles of Defining E-money ..................................................................... 21

2.3.2 Definition of E-money .................................................................................... 24

2.3.3 Distinguish E-money from Similar Concepts ............................................. 25
2.3.4 Examples of E-money Selected as Research Targets ...........................................27

Chapter 3 Canadian Privacy Law vs. Electronic Money .................................................30
3.1 PIPEDA ......................................................................................................................34
3.2 Identifying Purposes: Arbitrarily Provided by E-money Organizations ..............37
3.3 Consent: Obtained through Deception and without Withdrawal Regime ..........46
3.4 Limiting Collection, Use, Disclosure and Retention: Intended Vague Instruction ..........................................................................................................................50
3.5 Openness: Not in Accordance with the Accountability Principle ..................55
3.6 Safeguards: Regulated Completely in PIPEDA ......................................................56

Chapter 4 European Privacy Law vs. Electronic Money .................................................60
4.1 The Convention, the Directive and OECD Privacy Guidelines .........................61
4.2 Identifying Purposes Principle: The Central Principle for the Protection of E-
money Users’ Privacy .......................................................................................................65
4.3.1 Identifying Purposes Principle ..............................................................................80
4.3.2 Consent Principle ................................................................................................81
4.3.3 Limiting Collection Principle and Limiting Use, Disclosure and Retention
Principle .........................................................................................................................83
4.3.4 Openness Principle ...............................................................................................83
4.3.5 Safeguards Principle ............................................................................................84
Chapter 5 Conclusion

5.1 The Best Privacy Laws for the Protection of E-money Users’ Privacy

5.1.1 Identifying Purposes: Clearly Listed and Explained by the E-money Providers

5.1.2 Consent: Unambiguously Consent and Withdrawal Regime

5.1.3 Other Four Principles

5.2 Threat from the Internet to Privacy

Selected Bibliography

Books

Journal Articles

Legislation

Canada

European Union

OECD
Chapter 1: The Information Era vs. Privacy

Accompanying the trend of developing technology, the chances for people to use tangible money are becoming less and less.¹ Many people believe that electronic money (e-money)² will ultimately replace tangible money one day, because e-money has been used in trading for half a century and continues its spread. The emergence and boom of e-money rely heavily upon technology.³ Here is a piece of news from Bloomberg stating that: “[e]fforts by Google Inc. and Apple Inc. to embed chips based on so-called near field communications technology into their phones are aimed at locking PayPal out of the nascent mobile-payments market.”⁴ This news is a good example of how technology change promotes the research and application of e-money.

¹ Tangible money means paper money and coins.


³ Discussions about the background, definition and categorization of e-money are in the next chapter.

From plastic cards to mobile payment, the carrier of e-money becomes more convenient.\(^5\) Although mobile payment is not presently widespread, it is inevitable that the carrier of e-money will become more convenient.\(^6\) Eventually, there may be no carrier at all – for example, your fingerprint will play the role as the carrier. Let us imagine a scenario without actual money. People get paid every month after working hard and their wages go into their bank accounts directly. If they go shopping at supermarkets and convenience stores, they only need to swipe their bank cards to finish the payment. Similarly, other service providers use bank cards through point-of-sale machines to avoid the process of paying and receiving cash. After mobile payments technology becomes more mature, the use of e-money will expand even further.

Nevertheless, it is becoming increasingly important to protect the privacy of individuals with respect to their financial details. In the public sector, pressure on privacy

\(^5\) Here, carrier means the item, for example, paper or plastic card, to which the value of money is attached. In 1950, the Diners Club credit card was invented by Diners' Club founder Frank McNamara. The credit card was intended to pay restaurant bills. Frank went out to eat with his friend and he embarrassingly, at the end of the meal, found that he had forgotten his wallet. He had to ask his wife to bring some money to him. The idea of a credit card came into Frank’s mind after this incident. See Jennifer Rosenberg, “The First Credit Card”, online: About.com <http://history1900s.about.com/od/1950s/a/firstcreditcard.htm>.

\(^6\) Plastic cards are types of e-money in which the monetary value is stored in cards made of plastic, such as a smart card and Visa Card. Mobile payment is a newly invented method of payment by using mobile phones. For example, a consumer may use his or her mobile phone to finish payment by sending a short message to a short code, and the merchant will be informed of this payment.
protection has increased as a result of government surveillance after 9/11. Many nations have enhanced and expanded their surveillance measures to avoid attacks of terrorism.\textsuperscript{7} Furthermore, cases occurring in the private sector, which form the research focus of this thesis, also need our attention.\textsuperscript{8}

In 2005, a large data security breach occurred in the United States (US). Information from more than 40 million credit cards was stolen by an intruder who used security vulnerability to infiltrate the network of a third-party processor of payment data. Both Visa and Master Card, the two biggest credit card operators in the world, were affected by this event.\textsuperscript{9} It is a typical privacy violation case in the private sector.

Similar cases about releasing customer data have occurred in recent years. For example, Facebook and Myspace regularly sent users’ data to advertising companies, Sony’s


\textsuperscript{8} See Roger LeRoy Miller & Gaylord A. Jentz, Fundamentals of Business Law: Summarized Cases (US: Cengage Learning, 2010) at 387. In the E-money and Online Banking section of this book, the author reviews some cases about e-money. For example, \textit{Gerber & Gerber P.C. v Regions Bank} and \textit{Union v Branch Banking & Trust Co.} demonstrate that people may use the innate unreliability of e-money to steal other people’s asset, and thus relevant tort lawsuits came out.

PlayStation Network was hacked and users’ data was lost, and bank’s employees may release customers’ information. In general, there are two ways of releasing its users’ personal data through a network – one is hacking and the other is sale.

Another example is an Octopus Card scandal which was disclosed in 2010. Octopus Holdings Limited sold two million personal data records to six insurance companies without obtaining the users’ direct consent and earned HK$44 million in revenue. This is also a case which represents privacy violations in the private sector, as the leak of information was intentionally done by Octopus Holdings Limited – the seller and operator of the Octopus Card. We could blame the third-party processor in the above case for not providing enough technological protection for customer information, but in

---


11 Octopus Card is issued by Octopus Holdings Limited (Hong Kong) and can be used for public transit, in convenience stores, supermarkets, parking lots and fast-food restaurants. Recharging methods for Octopus Cards are various – through the staff of information desks or recharging machines that can easily be found at each subway station, transferring online from bank accounts and recharging in convenient stores.

12 Liang Lusi & Sonya Bryskine, “Hong Kong’s Privacy Laws Slammed after Octopus Fiasco” The Epoch Times (4 August 2010), online: The Epoch Times <http://www.theepochtimes.com/n2/content/view/40410>. 
this case the behaviour of Octopus Holdings Limited must be criticized because the company mishandled personal information through intention rather than ignorance.

Report from the Hong Kong Monetary Authority also proved the severe situation about privacy intrusion in the private sector. In August 12, 2010, the Hong Kong Monetary Authority announced that six of the twenty-five retail banks in Hong Kong transferred the personal data of more than six billion customers to a third entity in the past five years. Five of the six banks even got revenue from the transfer of their customers’ personal data.¹³

Why have there been these scandals in the private sector? We may give many superficial answers to this question, such as the deficiencies of current technology, a lack of goodwill on the part of enterprises or even the nonfeasance of governments. Fundamentally, however, this problem comes from the nature of human beings in pursuing benefits and the development of technology. The value of information is what some individuals and entities pursue. It is the internal reason for the theft of information and the violations of information privacy. The emergence of plastic cards, point-of-sale machines and, in particular, the Internet constitutes the external reason – the development of technology.

1.1 The Value of Information vs. Privacy

Our personal information is valuable not only to ourselves, but also to other persons and entities. Just like journalists who need to react quickly on news to avoid losing the value of information, commercial entities must compete intensely with each other – the party who successfully obtains the accurate and prompt information can take advantage of information by acting in advance and by having a clear target.

Nowadays, enterprises are paying a lot of attention to information and feedback from consumers. On one hand, personal information can be used as fundamental analytical materials for market studies and marketing strategies. On the other hand, a database of users’ personal information could benefit the creation of new products and the development of enterprises. Although the value of personal information cannot be accurately calculated, it is impossible for entrepreneurs to ignore personal information as market competition is becoming increasingly brisker. Therefore, commercial entities are always eager to get a consumer’s personal information through every possible means.

Personal information is valuable and also vulnerable. While commercial profits are the priority for companies, personal information is paramount to an individual’s dignity
It is debatable about what the conceptual basis for privacy is. Most scholars consider either dignity or liberty as the conceptual basis, and some of them discuss this issue in a certain context. For example, Avner Levin and Mary Jo Nicholson conclude that privacy protection is essentially liberty protection in the US, while privacy respectively protects dignity in the EU and individual autonomy in Canada.

With the conflict of interest between an enterprise’s urgent need for personal information and an individual’s defence of his or her privacy rights, people are faced with three choices. First, consumers tolerate potential disturbance and oversight by service providers and, thus, give up on protesting the violation of personal information. Second, consumers fight against commercial profits and for privacy rights by maintaining personal dignity as the paramount value. Third, consumers try to find a balance between the commercial need of personal information and the personal need of dignity.

These choices relate to a debate about the extent to which privacy should be protected. At the very least, legal scholars must make sure that the necessity to protect privacy

---

rights originates from individuals rather than merely from a theoretical discussion. Although the invasion of privacy by commercial entities is fiercely criticized now, some special situations should not be neglected. For example, some people would like to hide their personal information on Facebook while others would like to share personal information with their friends and even strangers.

There is a standard for determining the extent of privacy protection with respect to government searches – reasonable expectation. In other words, the law protects the right to privacy to the extent that a reasonable person expects, but does not protect people who are overly sensitive about privacy rights. It is not clear, however, that this standard should apply to information collection practices in the private sector.

1.2 Internet vs. Privacy

The great invention of the Internet is showing both its positive and negative sides. The Internet is a platform in which a large amount of information is produced, collected and

---

15 See Helen Nissenbaum, “Privacy as Contextual Integrity” (2004) 79 Wash L Rev 119 (“[p]ublic surveillance violates a right to privacy because it violates contextual integrity; as such, it constitutes injustice and even tyranny”).

16 See, for example, R v Edwards (1996) 1 SCR 128. This case is one of the leading Canadian cases regarding reasonable expectation of privacy.
disseminated every day. Needless to say, the convenience supplied by the Internet was not imaginable 20 years ago. Since an increasing amount of business can be completed online, the Internet has become a huge database for storing information. Meanwhile, external sources of information are constantly channelled into the Internet. The combination of internal and external information further consolidates the status of the Internet as the biggest information source in the world.

However, potential risks of information invasion underlie the prosperity of the Internet. The Internet is not only a platform for the production and collection of information, but also for the dissemination of information. A lesson from the scandal of Octopus Holdings Limited is that the collection and storage of customers’ personal information can be a threat to the protection of privacy. Furthermore, how to save, use and delete the collected personal information also needs clear legal rules.

For example, in China, one of Google’s functions is called “human flesh search” through which the identity of a particular person can be exposed to the public.\(^\text{17}\) Since

\(^{17}\) Google China quit the market of Mainland China on March 23, 2010. The users of Google.cn will be redirected to Google.com.hk if they type www.google.cn into the address column of an Internet browser in Mainland China. See “Google China’s Latest Statement” (23 March 2010), online: Google <http://www.google.com/press/new-approach-to-china/update.html>. Although “human flesh search” is not a major service provided by Google to Chinese users through Google.com.hk, the concept of “human flesh search” has widely spread throughout China and surrounding areas. Some Internet service operators supply a bulletin board for those who would like to find someone or the truth about something. Some people may
2006, through various human flesh search tools, Internet users in China can find details about people whom they have a great curiosity, such as a kitten killer in Hangzhou City and a drunk driver in Hebei Province.

Under certain circumstances, one of the functions of the human flesh search appears to be surveillance of public actors. Indeed, an arbitrary conclusion that this function is only for the fulfillment of public curiosity is unfair to some of the Internet users who engage in human flesh searching. For example, many corruption cases have been exposed via human flesh searches in recent years, which is a positive signal for people to strengthen and unite their individual power and to promote ongoing Chinese government reform.

Although the target of a human flesh search may be a person who has committed an immoral or illegal act, it is still debatable whether this searching behaviour constitutes a violation of that person’s privacy rights. When is it a necessity to find personal information, is it still a violation of privacy rights? To what extent is the necessity allowed to overwhelm privacy rights? Is it necessary for common individuals to start leave messages including useful information for the one who started a particular topic. The whole process of such a search completely depends on the information provided by strangers through the Internet. Although these people do not know each other, they feel close by doing such a search together. Therefore, the search done through the Internet and the information collected from unknown people is called “human flesh search”. See “Ren-rou”, online: Wikipedia <http://en.wikipedia.org/wiki/Ren-rou>.
such searches in order to fight against a corrupt government? These questions seem to go beyond the field of law, but they can reflect conflicts between Internet use and privacy. Another issue is, seen from a purely legal view, that the evidence obtained through such a survey may constitute the fruit of the poisonous tree, which is a legal metaphor used to describe illegally obtained evidence.

1.3 Privacy

The history of the concept of privacy can be dated back to 120 years ago. Since 1890, the year in which Warren and Brandeis wrote *The Right to Privacy*, “privacy rights” have become a hot topic in legal research. In that article, the authors raised the concept of legal “privacy rights” for the first time, and analyzed the limitations and remedies to this right.\(^\text{18}\) Since then, many scholars have contributed to the research of privacy rights by discussing the definition of privacy, the value of privacy and the categorization of privacy. For example, Ethan Katsh defines privacy as the power to control what others can come to know about you.\(^\text{19}\) Jerry Kang categorizes privacy into three clusters – space, decision and information – as some scholars support.\(^\text{20}\)

---


\(^\text{20}\) Space privacy concerns an individual’s territorial solitude. For example, nobody can invade another person’s house without permission. Decision privacy focuses on people’s autonomy to make their own
As a branch of privacy, information privacy is quite vulnerable in the information era. Jerry Kang took the definition of information privacy from the *Principles for Providing and Using Personal Information* as “an individual’s claim to control the terms under which personal information—information identifiable to the individual—is acquired, disclosed, and used.”\(^{21}\) By connecting it to e-money, personal information provided by customers may be identifiable. If there are no safeguards and privacy policies provided by the e-money issuers, the privacy of a customer’s private information may be subjected to intrusion.

In summary, the value of information and the development of technology enhance the risk of privacy violations in the information era. Several examples of e-money – Octopus Card, PayPal and MasterCard – which have identifiable personal information will be discussed in the following chapters. I will compare the privacy policies of these selected examples of e-money with the relevant privacy laws of Canada and the European Union (EU). At the conclusion of this thesis, I will endeavour to identify the best privacy laws required to govern the use of e-money.

\(^{21}\) *Ibid* at 1205. The *Principles for Providing and Using Personal Information* is made by the Clinton Administration’s Information Infrastructure Task Force.
Chapter 2: Electronic Money

This chapter introduces the history, definitions and functions of money and discusses the definition of e-money. Throughout history, various definitions and fundamental functions of money – and the clues underlying them – are the basis of understanding e-money. Because e-money, which emerged in the mid-20th century, is a relatively new electronic product, it provides many questions for discussion including those related to privacy issues.

2.1 A Brief History of Money

This simple graph illustrates the emergence and development of money:

| Bartering | Livestock and foodstuffs as universal equivalents | Shells and stones as universal equivalents | Metal currency | Paper money | E-money |

2.1.1 Bartering
Bartering is the most ancient method by which people interacted with each other as buyers and sellers. At the very beginning of bartering, no uniform item served as a medium of exchange. The logic behind bartering is human nature – when a person needs something, he or she will get it from another person by giving him or her something of equivalent value. Although bartering is a symbol of ancient people’s wisdom, it still exists today – history has not pushed bartering out of trading completely, but has left narrow space for its continued existence.

The common use of bartering was eventually replaced by media of exchange – such as livestock, foodstuffs, shells and stones – which were used universally within a territory or society. For instance, in American history, tobacco was once recognized as legal tender in the 17th century. However, after discovering that tobacco was difficult to store and spoiled easily, people began to use shells and stones as substitutes, as they were able to overcome the drawbacks of tobacco.

### 2.1.2 Metal Money


24 *Supra* note22 at 3.
Eventually, metal currency appeared as a tool which had the same function as shells and stones but was much firmer, more durable and more official. As a specially-valued commodity, if metal currency was issued by a government, people would often passively admit its social status and abide by the rules of its usage. For instance, the Qin Dynasty implemented the use of a unified currency for the first time in Chinese history after winning wars against six other enemies. Copper coins, with a square in the middle, were used as a standard form of currency from the Qin Dynasty (221-207 BC) until the Qing Dynasty (1636-1912 AD).\(^\text{25}\)

### 2.1.3 Paper Money

Paper money was the next great invention in the history of currency. Its origin can be dated back to the Song Dynasty (960-1279 AD) in China with the name Jiaozi. Initially, Jiaozi emerged as a convenient tool for businessmen. In the Song Dynasty, the commodity economy flourished and, as a result, copper coins were lacking in the market. In addition, businessmen had to take a mountain of copper coins with them when they wanted to complete large business transactions. This was very troublesome when two

businessmen lived far apart. As a result, private Jiaozi emerged. Businessmen set up special stores for the safekeeping of copper coins and issued a certificate to illustrate how much money the store kept for a particular businessman. With this certificate, businessmen could exchange private Jiaozi instead of heavy copper coins as a payment method. Eventually, the Song authority issued public Jiaozi, which was the earliest official paper money in world history.

2.1.4 E-money

Whether e-money will replace paper money has been a hot topic ever since the emergence of electronic payment. The electronic payment industry came into being in the mid-20th century and has rapidly developed since then. The Diners Club launched the first payment card in 1950 for use in restaurants in New York City. Eight years later, the American Express Company and the Bank of America issued payment cards accepted by various

---


27 Supra note 25.

28 E-money is defined in the third part of this chapter. Here, “electronic payment” means a kind of payment method through electronic devices, e.g., point-of-sale machines and computers.
kinds of vendors.\footnote{Supra note 22 at 6.} Since then – corresponding to the development of technology and the Internet – increasing varieties of payment cards and online payment options have emerged: Visa, Master Card, PayPal, mobile wallet, etc.

2.2 The Concept of Money

Although no uniform definition of money is given by economists, money is usually defined in functional terms.\footnote{Supra note 22 at 7.} The following are some typical definitions and descriptions of money. Aristotle was the first to determine two of money’s most important functions: medium of exchange and standard of value.\footnote{Ibid. See also Richard McKeon, ed, \textit{The Basic Works of Aristotle} (New York: Random House, 1941), Book 5, Ch 8 (“Aristotle in the \textit{Ethics} describes money as: ‘[i]t is therefore indispensable that all things which can be exchanged should be capable of comparison, and for this purpose money has come in, and comes to be a kind of medium, for it measures all things and so likewise the excess and defect…; the need as was stated above of some one measure of all things’”).} Charles L. Prather explicitly figured out the functions of money that are imperative under economic and social tendency – medium of exchange, store of value and standard of deferred payments.\footnote{See Charles L. Prather, \textit{Money and Banking} (Homewood I11: Richard D Irwin, 1965) at 6.} Fredric Mishkin defined money as “any object that is generally accepted as payment for goods and services and
repayment of debts in a given country or socio-economic context.”\(^{33}\) Karl Marx gave a concrete definition of money: “[t]he commodity that functions as a measure of value and, either in its own person or through a representative, as the medium of circulation is money.”\(^{34}\)

A non-economic researcher may confuse money, cash and currency. It is common for an item to be defined differently in different fields, so let us divert our attention from economics to law to make clear the concept of money in the legal field. Take Canadian legal rules, for instance. Under federal law in Canada, “cash” is defined as coins and bank notes which are intended for circulation in Canada, and coins and bank notes of countries other than Canada.\(^{35}\) In most provincial and territorial statutes, “money” means a medium of exchange authorized by the Parliament of Canada, or authorized or adopted by a foreign government as part of its currency.\(^{36}\) Meanwhile, explanations of


\(^{35}\) *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*, SOR/2002-184, s 1(2).

\(^{36}\) *Personal Property Security Act*, RSA 2000, c P-7, s 1(1); *Personal Property Security Act*, RSBC 1996, c 359, s 1(1); *Personal Property Security Act*, CCSM, c P35, s 1; *Personal Property Security Act*, SNB 1993, c P-7.1, s 1; *Personal Property Security Act*, SNL 1998, c P-7.1, s 2(1); *Judgment Enforcement Act*, SNL 1996, c J-1.1, s 37; *Personal Property Security Act*, SNWT 1994, c 8, s 1(1); *Personal Property Security Act*, SNS 1995-96, c 13, s 2; *Legal Profession Act*, RSNWT 1988, c L-2, s 42; *Personal Property Security
the categories of money are provided by some provincial and territorial legislation. In British Columbia, "money" includes cash, a negotiable instrument and a payment by means of a credit card.\textsuperscript{37} In the Northwest Territories, Nunavut and Yukon, "money" includes currency; government or bank notes, cheques; drafts and post office, express or bank money orders. \textsuperscript{38}

Legal definitions and explanations can help to explain the relationship between cash, money and currency. First, cash is a kind of money. Second, legislation does not make a distinction between money and currency. Third, no uniform definition of money exists. Concerning the last point, although most regional legislation contains similar definitions of money, only four of them have specified categories of money. Comparatively, both federal law and other provincial and territorial laws provide definitions of money that are less clear than those of the four aforementioned Canadian jurisdictions.

\textit{Act, RSO 1990, c P.10, s 1(1); Personal Property Security Act, RSPEI 1988, c P-3.1, s 1; Personal Property Security Act, SS 1993, c P-6.2, s 2(1); Personal Property Security Act, RSY 2002, c 169, s 1(1).}

\textsuperscript{37} \textit{Election Act, RSBC 1996, c 106, s 1.}

\textsuperscript{38} \textit{Legal Profession Act, RSNWT 1988, c L-2, s 42; Legal Profession Act, RSNWT 1988, c L-2, s 42, as enacted for Nunavut, pursuant to the Nunavut Act, SC 1993, c 28; Legal Profession Act, RSY 2002, c 134, s 60.}
Clarifying what money does is more important than trying to find a comprehensive definition for it. Money should have three main functions: medium of exchange, unit of account and store of value. Money’s fundamental purpose is to facilitate the exchange of goods and services – to lessen the time and effort required to engage in trade. Although the words used to describe money in economics and law are different, the core concept is the same. Money is a multifunctional tool widely used in trading. From an economic standpoint, social reproduction has four steps – production, distribution, trading and consumption. Money is used in each of them. The form of money has changed throughout human history, but regardless of the form it takes, its function has never been altered. Where there has been a motivation to change forms of money, it has primarily related to convenience and functionality, just as there has been a transition from bartering to livestock, and from metal money to paper money.

2.3 Defining E-money


40 *Supra* note 22.

2.3.1 Principles of Defining E-money

Three principles should be followed to define e-money.

First, e-money is a kind of money. As described previously, no standard definition of money exists, but the basic function of money is well-known and widely accepted. Therefore, if e-money could perform the same functions as traditional money, it should be admitted as money – a new type of money.\(^{42}\)

Superficially, the major distinction between traditional money and e-money lies in that traditional money is made from metal or paper while e-money is stored in a card. However, we cannot ignore the fact that traditional money is used anonymously while e-money may connect to personal information. According to the definitions of money, anonymity is not a requirement for an item to be identified as a kind of money. Furthermore, different kinds of e-money may be categorized according to their anonymity. For example, a prepaid phone card is only a substitute for cash, so it should be completely anonymous, whereas credit card companies need to collect some personal information to determine the credit limit for a particular customer.

\(^{42}\) Traditional money means the types of money introduced in the first part of this chapter – a brief history of money – excluding e-money.
The second is to obey money’s evolutionary rule. Here, the chicken-and-egg problem presents itself based on the relationship of buyers and sellers. If a new type of payment is increasingly accepted by buyers and takes up a large proportion of the entire payment system, sellers will adapt to this change, and accept and develop the new payment method. On the other hand, sellers are unlikely to actively invest in a new payment method until it has been widely accepted by buyers. So, which comes first? Just as the chicken-and-egg dilemma is debatable in biology, the exact origin of e-money’s acceptance is hard to determine.

We can find some clues as to the origin of e-money from the history of money. From bartering to paper money, the evolutionary trend of money is towards types that are easier to store and easier to carry than the former. This is also one of the characteristics of 21st century’s technological revolution – dematerialization. For example, today Facebook is a very popular social network, but in the beginning it was only used at Harvard University. Commercial interests are always waiting for profitable business opportunities. The origin of e-money was potentially derived from a coincidence, and its supply and demand have been simultaneously increasing. This is the answer to the chicken-and-egg problem.

43 Here, “dematerialization” has the same meaning as “digitization”. See Robert Guttmann, *Cybercash: The Coming Era of Electronic Money* (New York: Palgrave Macmillan, 2003) at 56 (“[t]he history of money is one of its progressive dematerialization, a trend illustrated foremost when metal money gave way to paper money”).
For the purpose of this thesis I have adopted a forward view rather than a backward view to define and analyze e-money, because privacy problems resemble potential commercial interests and are difficult to determine at the initial developing stage of e-money. For example, living in Hong Kong, as discussed in Chapter 1, an Octopus Card can help you handle most of your daily expenses – taking buses and subways, shopping in convenience stores and supermarkets, and eating delicious food in restaurants. However, an Octopus Card scandal occurred recently when it was disclosed that Octopus Holdings Limited sold two million personal data records to six insurance companies without obtaining the users’ direct consent. The selling of personal data earned Octopus Holdings Limited HK$44 million in revenue.44

The third is to find a balance between the economic and legal definitions of money. As discussed in the concept of money, the most remarkable difference between these two categories of definition lies in the fact that legal money requires governmental authorization but in economics no such requirement exists. Because of the different standpoints of these two disciplines, legal definitions tend to specify the types of money which are admitted by government, whereas economic definitions focus on the function of money in the market. Moreover, almost all existing types of legal money

are tangible – they can be seen and felt, so simply adopting an existing definition of e-money may cause it not to be legally admitted.\textsuperscript{45}

\textbf{2.3.2 Definition of E-money}

Unofficial and official definitions of e-money now exist. Traditionally, e-money refers to money or information from a magnetic strip or chip which can only be exchanged electronically.\textsuperscript{46} More recently, in 2000, the group at the vanguard of e-money – the European Union – defined e-money in its \textit{E-money Directive}, as “a claim on the issuer stored on an electronic device, issued on receipt of funds of an amount not less in value than the monetary value issued and accepted as means of payment by undertakings other than the issuer.”\textsuperscript{47}

\textsuperscript{45} For example, British Columbia is the only province in Canada in which credit card is a kind of specified money. Other provinces and territories’ legislation represents that only traditional money, which is with physical and visible appearance, is legal tender.


In this thesis, *e-money is defined as the type of money in which monetary value is stored electronically*. Specifically, e-money must play as complete a role as traditional money and it must be issued by either private or public entities, including government. In other words, an individual or individuals cannot issue e-money. However, e-money is intangible. You cannot see the exact amount of money in the face of an e-money carrier or perhaps there is no carrier at all. Based on carriers, three types of e-money exist today – card-based, mobile-based and virtual e-money.

### 2.3.3 Distinguish E-money from Similar Concepts

Many concepts which have, or do not have, the same meaning as e-money, confuse people about the real meaning of e-money. In fact, different concepts of e-money have developed, such as electronic currency/cash and digital money/currency/cash. Meanwhile, some concepts resembling e-money are also widely used, such as virtual money and electronic fund transfer.

Whether virtual money belongs to the category of e-money, or the other way around, is controversial. Some people believe that virtual money is like a virtual product or a kind of virtual service.\(^48\) According to their opinion, virtual money is adopted by many

\(^{48}\) But see Elinor Harris Solomon, *Virtual Money: Understanding the Power and Risks of Money’s High-Speed Journey into Electronic Space* (New York, Oxford: Oxford University Press, 1997). The author of
companies operating online games or online movies. If one wants to get some virtual money, he or she should use e-money first. For example, if a player needs to buy some virtual weapons in an online game and these weapons worth 500 game coins, in order to obtain the coins, he or she should pay $5.00 through an e-money transfer. After the individual deposits $5.00 into his or her bank account, the real money becomes e-money. After finishing the online transfer of the $5.00, the e-money becomes virtual money. The process of transferring $5.00 worth of e-money from an account to the company’s account is called electronic fund transfer (or EFT, for short).  

According to this explanation of virtual money, virtual money has an inner limitation concerning the scope of use. In the real world, many shopping malls, stores and supermarkets provide gift cards, which can only be used to purchase items at specific retailers. From this standpoint, virtual money shares the same characteristic with the gift cards provided by the above sellers. Currently, virtual money can only circulate between one company and its customers. In comparison, other kinds of e-money can be used between many companies and their respective customers. Because in this thesis e-money is defined broadly, virtual money is also included in the definition of e-money.

---

this book defines virtual money as “money never to be touched, held, or seen”, so virtual money includes “plastic money, credit and debit cards, and the newly hatched e-money that plies the Internet trade.”


26
2.3.4 Examples of E-money Selected as Research Targets

One further question is to what extent different types of e-money should be involved in this thesis discussion. Just as the British pound circulates solely in Great Britain and the euro is used throughout the EU, various types of e-money have their own circulating scope. Prepaid phone cards and transportation cards are widely used in many countries: Visa Card’s global network covers 170 countries and territories;50 China’s UnionPay covers 98 countries and territories; 51 Octopus Card is limited to Hong Kong; mobile payment is commonly used in Japan; and so-called virtual money is available through many websites. From these examples, we can see that each kind of e-money has its own circulation domain.

Hence, two factors should be considered for selecting the research targets for discussion. One factor is the circulation domain, because e-money which is circulating in a relatively large domain provides more value for further research and applies to more jurisdictions. Furthermore, the selection is based on an assumption – widely-used e-money should provide the strongest protection to a consumer’s privacy. Otherwise, it


should not take a large market quote according to the theory of self-regulation of market economy.\textsuperscript{52} Simply speaking, in a market economy, the supply and demand relationship is decided by the market itself. Only if a product or service supplier increases its production efficiency, regulates its operation and outputs products or services making its consumers satisfied, this supplier can survive after competition. Regarding e-money suppliers, if a supplier cannot provide enough protection to consumers’ privacy, a rational person will not continue using its products and services unless this supplier stands on a monopoly status.

The other factor is the relationship between a particular type of e-money and personal information. As discussed previously, some kinds of e-money do not need the consumer to provide personal information while some other kinds of e-money may require consumers to give this information.\textsuperscript{53} Because this thesis focuses on privacy law, it is obvious that e-money relevant to personal information is the target of discussion. Moreover, although the categorization of e-money indicates that e-money has different carriers, and there may be a few differences in privacy issues based on the different carriers, the purpose for the collection of personal information should not vary greatly.

\textsuperscript{52} This theory is also called invisible hand hypothesis. This metaphor was first used by Adam Smith. See “Privacy Guide for Small Businesses: The Basic”, online: Office of Privacy Commissioner of Canada <http://www.priv.gc.ca/information/pub/guide_sb_e.pdf>. (“[p]rivacy is the best policy handling privacy concerns correctly can help improve your organization’s reputation”).

\textsuperscript{53} See Part 2.3.1 Principles of Defining E-money, above, the first principle for defining e-money.
Based on these two factors, three examples of e-money are used as the target for discussion – MasterCard, Octopus Card and PayPal. MasterCard operates its electronic payment in retail stores, restaurants and other locations through point-of-sale (POS) terminals. Octopus Card is a rechargeable stored-value smart card used to transfer electronic payments in online and offline systems in Hong Kong. Although both MasterCard and Octopus Card are under the categorization of card-based e-money, their original functions are different. Ever since its emergence, MasterCard has focused on money clearance as a substitute for cash. Octopus Card was only a transportation card at the beginning, but additional functions were developed with its widespread use. In other words, MasterCard Company is a financial institution, whereas Octopus Holdings Limited is a company operating payment system. Due to this distinction, different standards for personal information protection may be applied to these two cards.

PayPal has a role as a trusted middleman between consumers and online merchants. Consumers and merchants can register on PayPal, create a PayPal account and link the account to their bank accounts. When a registered consumer buys something from a registered merchant, the specific amount of money will be deducted from the

54 The account information of the swiping or inserting card will be read automatically by the issuing bank. After the information stored in the bank’s system is approved, the trade at point of sale is accomplished.

55 Supra note 11.
consumer’s bank account and then be paid to the merchant after the consumer confirms the trade.

Obviously, prepaid phone cards and transportation cards do not require customers to provide personal information. Hence, they are not the target for discussion in this thesis. However, if these cards were to raise the requirement for personal information they would be categorized as another kind of e-money similar to an Octopus Card, for example.

As a conclusion, e-money is defined as a particular kind of money in which monetary value is stored in this chapter. The introduction about the history and concept of money is to provide an overview of the development of e-money. For instance, the history and concept of money is used to determine the principles for defining e-money. The brief overview and introduction of e-money together act as a framework which specifies the common characteristics and traits of e-money. On the basis of this framework, three examples of e-money are selected as research targets. The privacy policies of these targets will be compared and discussed in the context of privacy laws of Canada and the EU.

Chapter 3 Canadian Privacy Law vs. Electronic Money
In this chapter, the focal point will be a comparative analysis between the privacy policies of three kinds of e-money – MasterCard, PayPal and Octopus Card – and the principles of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Two issues should be explained in advance. First, since personal information in PIPEDA is defined as “information about an identifiable individual” and a user of e-money could be either anonymous or use a real name, the following discussion of the Octopus Card is only related to the “Personalised Octopus Card,” namely the Octopus Card connected to a particular user’s real information rather than that which could be easily bought without providing any personal information.56

Second, the discussion of this entire thesis follows the methodology of comparative law. Therefore, the privacy policies of the three e-money organizations are assumed to be under different jurisdictions. While PIPEDA only applies to business operation in Canada, its principles will nevertheless be directed at the Octopus Card to see whether such a card follows fair information practice principle, as set out in PIPEDA. For instance, Octopus Card is a commercial item that originated in and is used only in Hong Kong, so actually the privacy policy of Octopus Card is under the jurisdiction of

---

56 *Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 2(1) [PIPEDA].*
Hong Kong. Yet, a comparative analysis based on the assumption that Octopus Card fell under the regulation of PIPEDA is still meaningful in that legal transplantation is an efficient means to improve legislation. In other words, the possibility of transplanting privacy laws about e-money between different jurisdictions constitutes the basis for the following discussion.

Regarding the issue of legal transplantation let us take Canada and Hong Kong, for example. On one hand, both Canada and Hong Kong possess a similar system of common law, so there is room for the two legislatures to adopt or learn useful stipulations from one another. On the other hand, Hong Kong is the financial centre of Asia and one of the most developed areas for the application of e-money. Nevertheless, a new kind of e-money, such as the Octopus Card, may emerge in Canada one day. If

---

57 There are three jurisdictions in China, namely Mainland China, Hong Kong and Macau. According to The Basic Law of the Hong Kong Special Administrative Region of the People’s Republic of China, the law in force in Hong Kong before July 1, 1997, when the sovereignty of Hong Kong was transferred from United Kingdom to China, shall be maintained, except for any that contravene the Basic Law. Therefore, the Personal Data (Privacy) Ordinance of Hong Kong applies to the legal privacy issues relevant to e-money in the private sector. Macau performs the same rule as Hong Kong. See The Basic Law of the Hong Kong Special Administrative Region of the People’s Republic of China, art 8. See also Personal Data (Privacy) Ordinance of Hong Kong (Cap 486, 2007 Rev Ed HK).

58 Legal transplantation is the moving of a legal rule or a system of law from one country to another and is the most fertile source of legal development. Alan Watson, Legal Transplants: An Approach to Comparative Law, 2d ed, (Athens: University of Georgia Press, 1993).
Canada does a better job than Hong Kong in the protection of privacy in the private sector, the legislature of Hong Kong may obtain some valuable ideas from Canadian privacy law and apply them into Hong Kong privacy law.59

If we examine only the text of the privacy policies, they may appear to be legal; however, the reasonableness of some rules in the policies, and whether such rules are in accordance with legal interpretation, are questionable. Take the personalized Octopus, for instance – according to the text of the privacy policy, Octopus seems to be permitted to sell customer information. Under the personal data provision of the application form, applicants agree that all personal information and data provided in the application form, and all the information relating to the use of personalized Octopus Card, may be used for the marketing of goods and/or services by the Octopus Holdings Limited, its subsidiaries or affiliates and selected business partners.60

Accompanying this provision, superficially, the applicants do not have the right to request that their personal data not be used for direct marketing purposes because it is

59 Kevin E. Davis, “Law-making in Small Jurisdictions” (2006) 56 UTLJ 15. In this article, the author argues that legal transplantation is more attractive to small jurisdictions – the law of which governs a low volume of activities. The jurisdiction should be assessed by a particular activity regarding its size. For example, Hong Kong is a large jurisdiction in business law but a small jurisdiction in privacy law.

an opt-out provision. If an applicant submits an application form without requesting his or her personal information not be delivered to a business partner of Octopus, it would be hard to argue that Octopus has violated the contract. From the standpoint of PIPEDA, some points are controversial – different interpretations of the rules of PIPEDA influences how they are put into practice. Furthermore, more protection of personal information should be provided by PIPEDA according to the following analysis.

3.1 PIPEDA

There are several reasons for choosing PIPEDA as an example of Canadian privacy law. First, PIPEDA is a nationwide privacy law in Canada despite the fact that some provinces are exempt from it. British Columbia, Alberta and Quebec have passed substantially similar legislation to PIPEDA. In British Columbia and Alberta, retail outlets and other private enterprises are respectively subject to the act with the same name – *Personal Information Protection Act*; In Quebec, the commercial entities are subject to *An Act Respecting the Protection of Personal Information in the Private*

---

61 *PIPEDA, SC 2000, c 5.*
Sector. But even in these three provinces, PIPEDA still applies to federally-regulated, interprovincial and international transactions and privacy cases in the private sector.\(^6^2\)

Second, sector-specific legislation concerning privacy also contributes to privacy protection in Canada, but such legislation is irrelevant to privacy issues involving e-money. For example, legislation dealing with personal health information has been passed in several provinces. However, this thesis only focuses on privacy issues involving e-money, so legislation regarding personal health information is irrelevant to the theme. Although, theoretically, an analysis of legislation concerning personal health information may offer approaches to better understand privacy issues related to e-money, such an analysis is not approachable in legal practice – healthcare and e-money are entirely different subject matters. Hence, when a violation of privacy occurs, a judge needs to decide which privacy law or laws should be applied. If it is a case relevant to healthcare, both PIPEDA and legislation dealing with personal health information will be referred to. But if it is a case only relevant to e-money, the judge will only approach PIPEDA – there is not a specific law regulating privacy issues involving e-money in Canada.

Another example is the privacy provisions in some statutes and regulations, such as the Bank Act. In this act, there are provisions about the electronic access of data, and

---

requirements to maintain copies and process information in Canada. But there is no privacy-specific provision. Besides this, the Bank Act merely applies to banks, but the organizations which can issue e-money are not limited to banks or even financial institutions. Thus, the statutes and regulations similar to the Bank Act are not directly relevant to, or not mainly engaged in, solving privacy protection of e-money users, so these statutes and regulations will not be discussed in this thesis.

Third, the Privacy Act, as a federal statute, focuses on the public sector rather than the private sector, so it is irrelevant to the privacy issues of e-money, which mainly belong to the private sector. Under the background of the following discussion, the enterprises issuing the MasterCard, PayPal and Octopus Card are not controlled by the government. Thus, potential violations of privacy in the public sector will not be discussed.

Lastly, PIPEDA contains rules and principles regarding the collection, use and disclosure of personal information in commercial activities in Canada. Schedule One of PIPEDA sets out fair information practice principles (FIPs) that generally follow earlier

---

63 Bank Act, SC 1991, c 46, ss 239, 245.

64 Privacy Act, RSC 1985, c P-21, s 2.
OECD initiatives.\textsuperscript{65} Whether in theory or in practice, PIPEDA is the law that should be applied to cases when violations of privacy involve e-money.

3.2 Identifying Purposes: Arbitrarily Provided by E-money Organizations

The requirements for the organization collecting personal information under the identifying purposes principle of PIPEDA include:

(a) documenting the purposes for which personal information is collected;

(b) identifying the purposes at or before the time of collection;

(c) purposes specified to the individual from whom the personal information is collected; and

(d) a new purpose being identified prior to use.\textsuperscript{66}

The provision specifying the purposes for the collection of personal data in the Octopus Card’s privacy policy violates the requirements (a) and (b). First, the expression “other


\textsuperscript{66} \textit{PIPEDA}, Schedule 1, cl 4.2.
related purposes” violates the original intention of lawmakers. After stating some common purposes in the front of the whole provision in Octopus Card’s privacy policy, an indefinite statement – “other related purposes” – follows.\textsuperscript{67} It is not possible to recognize what the real meaning of “related purposes” is. This statement could be clearly explained by Octopus\textsuperscript{68}.

Octopus, at the beginning, did not want to admit that it sold customer information to other companies. Later, Octopus announced that the information was provided to two companies for the benefits of customers – to help customers receive special promotions from these two companies. Eventually, after the scandal was fully disclosed, Octopus admitted that the information was sold for its own commercial profits rather than for the benefit of customers.\textsuperscript{69}


\textsuperscript{68} See “Report of Findings: Google Inc. Wifi Data Collection”, online: Office of Privacy Commissioner of Canada <http://www.priv.gc.ca/cf-de/2011/2011_001_0520_e.cfm#purposes>. (“[i]f Google never intended to collect payload data – or to use that data in any of its products – it follows that it was not in a position to properly identify the purposes for the collection of that information, or to seek the consent of individuals”). Hereafter, Octopus means the Octopus Holdings Limited.

\textsuperscript{69} “Octopus Admitted the Disclosure of Customers’ Data” (21 July 2010), online: People <http://hm.people.com.cn/GB/42273/12205609.html>.
By and large, the circumstances under which such broad wording is used should comply with an individual’s reasonable expectation. In other words, the organization is not allowed to circumvent potential challenges relating to the use of personal information by implementing such an approach.

From another standpoint, the requirement (a) implies that definite and explicit purposes for collecting personal information should be specified by Octopus. If such statement – “other related purposes” – is allowed by PIPEDA, many other entities may imitate Octopus by providing vague and broad purposes in their information privacy policies. However, the intention of lawmakers in setting this requirement is to impose the duty of providing explicit purposes in the privacy policies of organizations.

Article 4.3.2 and 4.3.3 of Schedule 1 represent lawmakers’ real intention. Article 4.3.2 dictates that “[t]o make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed”. Article 4.3.2 dictates that “[a]n organization shall not...require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes.”

Second, the sale of personal information as a purpose for collection is not identified prior to use. Under the personal data provision, the purpose for sale is not mentioned at
all and whether the purpose for marketing includes actual sale is debatable. Marketing is a broad concept that could include advertisements, telemarketing and data collection. As PIPEDA requires, the purposes for which the information will be used must be stated in a manner that the individual can reasonably understand.\textsuperscript{70} Hence, the question is whether marketing includes the sale of personal information. That is one of the tricks that Octopus utilizes. To understand this trick, a consumer not only needs to distinguish the concepts of marketing and sale, but also needs to prove that he cannot reasonably understand this distinction. If the consumer succeeds in doing so, the requirement (d), as mentioned at the beginning of this section, would also be violated by Octopus because the purpose of sale is a purpose which was not previously identified.

Comparatively, PayPal and MasterCard do a better job than Octopus in identifying the purposes for collecting personal information. PayPal explicitly states that it will not sell or rent any of a user’s personal information to third parties for marketing purposes without a user’s explicit consent. In addition, PayPal illustrates seven ways in which it may use personal information and emphasizes that its primary purpose in collecting personal information is to assist users.\textsuperscript{71} Yet, a marketing purpose is still one of the seven specified purposes and users must log into their accounts to stop receiving

\textsuperscript{70} \textit{PIPEDA}, Schedule 1, cl 4.3.2.

marketing communications. MasterCard also includes “to operate, evaluate and improve our business” as a potential way of using collected personal information.\(^7^2\)

From the above discussion, one can see a deficiency concerning the identifying purposes principle of PIPEDA – no concrete limitation has been set for the purposes required. The Article 4.2.6 under Schedule 1 of PIPEDA states that “[t]his principle (identifying purposes principle) is linked closely to the Limiting Collection principle and the Limiting Use, Disclosure, and Retention principle.” Literally, the lawmakers’ logic has three steps concerning how to limit the approaches of collecting and using personal information. The first step is to request that organizations identify their purpose for collection, the second step is to limit the collected information within what is necessary for the identified purposes, and the third step is to restrict the use, disclosure and retention of the information.

There should be more regulations for the identifying purposes principle, which is the logical starting point of the aforementioned three steps. In other words, although PIPEDA requests that the purposes should be appropriate to a reasonable person, explicitly specified and legitimate; more protection for an individual’s privacy is still needed. Neither “explicitly specified” nor “legitimate” is sufficient to protect individual

\(^7^2\) “Global Privacy Policy”, online: MasterCard Worldwide < http://www.mastercard.us/privacy/#Use>.
privacy. 73 The purposes for collecting personal information are given by the organizations, so expectations for these entities to protect their customers and provide fair purposes for these customers is not realistic. In particular, for example, the marketing purpose of Octopus is explicitly specified and legitimate. Although lawmakers hoped that the appropriate purposes requirement could restrict this organization, it is still not clear enough to put this provision into practice. Because the vague wording used in this provision cannot actually impose explicit obligations on the organization. Consequently, the real problem that may cause an organization to circumvent their obligation of protecting the personal information of consumers is the desire to earn extra benefits from this personal information. Presently, there is a lack of limitations on the use of personal information.

Furthermore, is it reasonable that customers should bear the burden of helping an organization realize its listed purposes? Take the specified purposes of the Octopus Card, for example. The first two purposes – processing application for Octopus Card and normal management, and the operation and maintenance of the Octopus system, including audits – are in accordance with the purposes of the contract between a particular applicant and Octopus. The last two purposes – designing new services or improving existing services and marketing – are imposed by Octopus without reasonable explanation. Octopus exists not only as a monopoly transportation enterprise in Hong Kong, but also as a monopoly source of personal information.

73 PIPEDA, Schedule 1, cl 4.3.3.
Because of its various functions and wide usage, 95% of people in Hong Kong aged 16 to 65 use Octopus to travel, shop and dine.\textsuperscript{74}

Octopus created a commercial miracle, and a great danger for individual privacy, at the same time. Octopus has obtained a huge amount of users’ personal information and continues to obtain more and more personal information due to its monopoly position. Consumers do not have an obligation to help Octopus maintain and expand the commercial territory of this company, but Octopus can use its monopoly status to impose obligations which should not be borne by the consumers. The reasonableness and legality for consumers to provide their personal information for service improvement and marketing of the Octopus Card is doubtful. Furthermore, from a legal perspective, the law encourages fair and complete competition, so even if such purposes are explicitly specified and legitimate they still should be prohibited by PIPEDA.

The real problem between customer interests and the listed purposes, or even the whole privacy policy, lies in that these provisions and purposes are standard clauses.\textsuperscript{75} It is

\begin{itemize}
  
  \item \textsuperscript{75} Standard clauses have three main characteristics: (1) they are made by the products or services providers; (2) they are steady in form and could be repeated using with different customers; and (3) they are not negotiable.
\end{itemize}
easy to notice that each of MasterCard, PayPal and Octopus takes a large percentage of market shares. These enterprises do not have to be overly concerned if they lose a small percentage of customers due to their bad privacy policies. However, customers do not have substitutes for these products or services. Even if the purposes of these three companies are against a customer’s will, the customer will still accept these unfair provisions because he or she would not like to be encumbered by the inconvenience of being unable to use these products or services. These enterprises may use “tricks” in their privacy policies, such as using characters of a small font and vague expressions.

Hence, rules of explaining standard clauses should be introduced into PIPEDA. In general, two principles should be adopted. First, e-money providers should make their standard clauses reasonable and easy to understand. Here, “reasonable” means that the organizations cannot arbitrarily set any purposes against consumer interests. Both directly and indirectly taking advantage of consumer interests correlates to the legal meaning “against consumers’ interests.”

The meaning of directly and indirectly taking advantage of consumer interests is as follows: if an organization states in its privacy policy that it may sell the personal

---


information of a consumer to a third party, this is a direct advantage taken by it. Also, if an organization states that it may transfer personal information to a third party for the benefit of consumers, such as getting promotion, this is an indirect advantage. It is impossible to expect any entity to transfer personal information without obtaining any benefit. Thus, no matter the superficial expressions, the core concept is to obtain free benefits from consumer information.

“Easy to understand” means that the organizations have the obligation to make the privacy policies clear and brief. Some organizations, such as Octopus, use extremely small font in their privacy policies, while some other organizations use numerous pages and obscure words in their privacy policies. All of these behaviours can be understood as the intention of an organization to mislead customers or prevent customers from completely understanding privacy policies. Therefore, the organizations should obey the bona fide principle and make the rules of their privacy policies well understood by customers.

Second, the interpretation of the standard clauses should be in favour of customers. Sometimes, customers and companies may have different interpretations of some clauses of privacy policies. The reason for this may be the inborn limitation of language or the intended obscurity of the language used by the organizations. No matter the real reason, these clauses should be interpreted against the interests of the organizations. Since the standard clauses are provided by the organizations they are in a
favourable position, because they are in control of the process and outcome of making such clauses. This means that customers are placed in an unfavourable position, because they can only accept these clauses passively. In order to make a balance, if a conflict about the understanding of such standard clauses occurs, customers should be treated more favourably via this interpretation.

3.3 Consent: Obtained through Deception and without Withdrawal Regime

Under the consent principle of PIPEDA, three requirements must be fulfilled by the organization collecting personal information:

(a) purposes for the collection of personal information are reasonably stated before requesting consent;

(b) consent shall not be obtained through deception and shall be in accord with individuals’ reasonable expectations; and

(c) the organization shall inform individuals of the implications of withdrawing consent.\(^78\)

Octopus violates requirement (b) because it does not set out the purposes in good faith. Similar to the example provided by PIPEDA, an individual would not reasonably

\(^{78}\) *PIPEDA*, Schedule 1, cl 4.3.
expect that the personal information given to Octopus would be sold to insurance companies. 79 Superficially, Octopus has notified its users about the possibility of using their personal information for marketing, but many barriers are set out to prevent users from protecting their privacy rights. Users could hardly be expected to read the terms of the application form due to its extremely small font. Even if they have sufficiently good eyesight to recognize those characters they will, unfortunately, discover that they have to contact Octopus directly to cancel this potential usage.

While PayPal and MasterCard elaborately explain the purpose for collecting personal information, Octopus, PayPal and MasterCard do not act properly concerning the withdrawal of consent. In the terms of their privacy policies, there are no words related to the withdrawal of consent for collecting personal information. However, even if the last clause – contact information – on the privacy policies of PayPal and MasterCard could be regarded as an approach to apply for withdrawal, it is still an indirect and inefficient description. 80

79 PIPEDA, Schedule 1, cl 4.3.5 (“an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained”).

80 Supra note 72 (“Any request for access to data or correction of data or for information regarding our policies and practices and kinds of data held by us should be made in writing addressed to…”); Supra note 71 (“If you have questions or concerns regarding this policy, you should contact us by using this form or writing to us at…”).
Analyzing terms under the principle of consent of Octopus, PayPal and MasterCard, all of them are in conflict with PIPEDA. First, the second example of how individuals can give consent under the principle of consent is an opt-out method with a check-off box, which may be unfair to users under certain circumstances. This is exactly what Octopus has used and is criticized for. Obviously, an opt-in method is friendly for users because they need not worry about missing any provision or content about their personal information, especially under a circumstance in which an organization, like Octopus, intends to mislead its users. Hence, compared with other examples of ways in which individuals can give consent, the check-off box method gives the least protection to consumers. The deficiency of the check-off box method does not completely prevent it from being used in any situations, such as when the purposes for collecting personal information are many and necessary. Under such circumstances, the organization should bear the burden of notifying and explaining the purposes to users in a proper way. In other words, the organization should obey the principle of good faith and determine customer consent according to the sensitivity of information.

Second, PIPEDA should supplement the content about how to withdraw the consent for the collection of personal information. The existing stipulation about a user’s

---

81 PIPEDA, Schedule 1, cl 4.3.7.

withdrawal of consent has two meanings which are interrelated. On one hand, PIPEDA entitles individuals to withdraw at any time subject to legal or contractual restrictions and reasonable notice. On the other hand, PIPEDA imposes the obligation on the organization to inform individuals of the implications of such a withdrawal.\(^{83}\) This framework is a good, but not practical, direction for individuals to withdraw consent. As to the measures taken by Octopus and PayPal, uncertainty and troublesome procedures could prevent users from acting. The lack of a definite withdrawal regime is actually in favour of the organization. Plus, some organizations have monopoly status which could allow them to impose unfair terms in requesting a user’s personal information. The balance of interests is unjust to users.

Third, most people do not read the entire privacy policy when they decide to receive the service of a particular type of e-money. One of the reasons for this phenomenon is that the privacy policies are usually quite long. Moreover, people are not willing to read such a long privacy policy especially when they have already decided to use that form of e-money. Consequently, a bad situation develops – the organizations provide lengthy privacy policies which enhance a customer’s unwillingness to read them, which results in customers tending to ignore privacy policies before signing an e-money contract. Often not until a customer’s privacy is violated, does he or she comprehend the details of a privacy policy.

\(^{83}\) PIPEDA, Schedule 1, cl 4.3.8.
One solution for this problem is to enhance the obligation for an organization to explain the terms in its privacy policy. Before obtaining content, an organization should perform this obligation in order to make customers clear about their privacy rights. This obligation is relevant to the previously described purpose principle and is also related to the methods of perfecting the purpose principle.\(^{84}\)

Together with the discussion under the identifying purposes principle, the organizations should notify and explain the following items to their customers: (1) the purposes for collecting the customers’ personal information; (b) the measures that will be taken to protect and process the personal information; and (c) when and how the personal information will be deleted from the organizations’ records.

3.4 Limiting Collection, Use, Disclosure and Retention: Intended Vague Instruction

Based on Principles 4 and 5 of Schedule 1 under PIPEDA, the collection, use, disclosure and retention of personal information should be accompanied by certain limitations:

(a) necessary for the identified purposes;

(b) through fair and lawful means;

(c) extra disclosure needed when personal information is used for a new purpose;

and

(d) guidelines and implement procedures with respect to the retention and destruction of personal information should be developed.\textsuperscript{85}

Let us compare the information requested by the application form and the identified purposes of Octopus. The requested information includes name, gender, date of birth, photo, identity card number, contact phone number, mobile phone number, home address, office address, fax and email address. As mentioned, the identified purposes are very broad, including processing the application, normal management and operation of the Octopus system, designing new services, improving existing services and marketing. Since the target of the analysis is the Personalised Octopus Card, the relevant requested information for the first two purposes could embrace the name, date of birth (some measures may be taken towards children and elders), photo (printed on Octopus) and identity card number. Octopus is not like a credit card which is issued by a bank, so it need not collect information such as contact phone number and home address to reduce its commercial risk and facilitate potential debt collection. Consequently, as the last two purposes have been verified to be irrelevant to direct interests of a user and purely for the commercial interests of Octopus, the relevant

\textsuperscript{85} PIPEDA, Schedule 1, cls 4.4, 4.5.
personal information collected is correspondingly beyond the necessary scope for collection.

PayPal’s problem is even more severe than that of Octopus. A couple of flexible statements exist in PayPal’s privacy policy. Aside from the necessary contact and financial information, PayPal leaves space for the further collection of personal information by using subtle expressions, such as “we may require you to provide additional information” and “we may collect additional information from or about you in other ways”. Since a marketing purpose also exists in PayPal’s privacy policy, it is risky for individuals to allow PayPal to collect their information from other entities. This can be seen in what has happened to Octopus users, in which their personal information was sold to insurance companies as a common commodity.

MasterCard’s problem is similar to that of the Octopus Card and PayPal. As stated in MasterCard’s global privacy policy, the types of personal information that MasterCard may obtain are contact information, business contact information, username, password, payment card information, financial information, access code, contact information for friends or other people a customer would like MasterCard to contact, content the customer provides (such as photographs, articles and comments), employment information and other information (such as shopping behaviour and preferences, age, gender and family status).
There are potential benefits for MasterCard to collect these stated types of personal information. Superficially, MasterCard uses uncertain wording to describe the types of personal information that may be collected, and even the expression “the types of personal information we may obtain” appears to be flexible and indefinite. However, it is with the intent of gathering information that MasterCard uses such unclear wording. MasterCard states, “[y]ou (a customer) may do so...when you participate in an offer or promotion, or in connection with an actual or potential business or employment relationship with us.”

It is relevant to their marketing purpose, as well. MasterCard’s logic is: the more personal information is collected from its customers, the closer the relationship is between MasterCard and its customers. Moreover, MasterCard has a lot of sources and ways to obtain the aforementioned information. Because of the widespread use of MasterCard, it is well-connected with various financial institutions and commercial entities, and these institutions and entities can collect information through each interaction with a MasterCard. Hence, the information shared by these entities constitutes a common source and this source is actually controlled by MasterCard. Thus, it is not hard to imagine the great value of this information.

For instance, a bill could show what a customer has purchased at a commercial entity. As the number of bills increases, the commercial entity can analyze which product or service is more favourable to customers – the most commonly purchased products or
services indicate that they are popular among their customers. The commercial entity, in question, is not able to know the sale situation of its competitors because this type of information is undoubtedly treated as trade secret. MasterCard, however, stands as a middleman between a customer and a particular entity as a product seller or service provider, and has access to all of the sales information of every entity. That means MasterCard has the capacity to do an analysis on which product or service is the most popular within the market.

Another issue of importance is whether the collection and buying of personal information is legal. In the information era, the organization that can control information in advance, and to a large extent, will always be the winner. Under current legislation, the only possible way for individuals to sue a party buying their information for violating privacy rights is through tort law. In other words, there is no direct expression in PIPEDA clarifying whether trading personal information is lawful or not.

Finally, Octopus, PayPal and MasterCard have not made it clear how they deal with the retention and destruction of the collected information. PIPEDA sets obligations regarding the retention and destruction of the collected personal data. What is lacking in PIPEDA is how to make the retention and destruction known to the individuals from
whom the information is collected.\textsuperscript{86} Otherwise, from both a legislative and practical point of view, not until their privacy rights are violated can consumers investigate why an organization did not destroy, erase or make anonymous their personal information, as required by PIPEDA.

3.5 Openness: Not in Accordance with the Accountability Principle

PIPEDA declares two requirements under the principle of openness:

(a) individuals shall be able to acquire the privacy policies and practices without unreasonable effort, and the information shall be generally understandable; and

(b) certain types of information shall be included in the privacy policies.\textsuperscript{87}

In general, Octopus, PayPal and MasterCard effectively obey the principle of openness. Only one deficiency is apparent – PayPal does not provide the name or title of the person who is accountable for PayPal’s privacy policy. In other words, PayPal violates requirement (b) of the openness principle. In comparison, Octopus and MasterCard

\textsuperscript{86} See Jeremy Warner, “The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps” (2005) 2:1 UTLJ 75. This article argues that PIPEDA fails to provide necessary stipulations about the data-retention periods for the organizations to process personal information.

\textsuperscript{87} PIPEDA, Schedule 1, cl 4.8.2.
clearly, and separately, appoint “the data protection officer” and “global privacy and data usage officer” as the accountable person. From a practical point of view, there is no clear reason for these organizations to specify the “officer” or not, because they have their own inside operating system and management rules. Furthermore, only for their own profit, these organizations would make efforts to clarify the responsibility of each employee. However, as for customers, there may be no specific person who may be accountable when they claim a violation of privacy, due to the internal chaos of the management of the organization.

In fact, the openness principle is closely relevant to the accountability principle. The accountability principle requires that organizations designate a particular individual, or individuals, who are responsible for personal information issues.\textsuperscript{88} Under the requirement of the openness principle, PIPEDA goes one step further – requiring organizations to announce the individual, or individuals, to their customers. This requirement is obviously in favour of customers.

3.6 Safeguards: Regulated Completely in PIPEDA

The underlying meanings of the principle of safeguards include:

\textsuperscript{88} PIPEDA, Schedule 1, cl 4.1.
(a) the organizations shall prevent the personal information from loss, theft, unauthorized access, disclosure, copying, use and modification;

(b) the sensitivity of the information decides the nature of the safeguards; and

(c) the organizations shall make their employees understand the importance of maintaining the confidentiality of personal information.

Requirement (a) imposes the obligation of safeguards on the organizations, and the following two requirements declare two specific aspects during the process of practising the general obligation.\textsuperscript{89}

Octopus stipulates two provisions with a subtitle “security of personal data” about the safeguards issue. The first provision states that physical records of personal information are securely stored in locked areas and/or containers, when not in use. Currently, users can only apply for a personalized Octopus Card by filling in a physical application form and submitting it to an Octopus customer service centre (usually at the entrance or exit of a subway station).\textsuperscript{90} The second provision states that, under certain circumstances, users may submit their personal information to Octopus via the Internet, but Octopus is not responsible for information that is being intercepted or tampered with.

\textsuperscript{89} \textit{PIPEDA}, Schedule 1, cl 4.7.

PayPal and MasterCard make a similar stipulation concerning the safeguards issue. Both of them mention that they provide appropriate measures to achieve the aim of safeguards, and even include specific technology, such as firewalls and data encryption.

Two issues could be found after comparing the stipulations of the three organizations and the principle of safeguards in PIPEDA. The first is that the manner of collecting personal information often determines the method of storage. Octopus uses a physical application form to collect personal information, which does not transfer the information into an electronic version. Therefore, the only way for Octopus to store application forms is to store them at a particular location. Regarding the safeguards adopted by PayPal, relevant information is encrypted since it is collected through the Internet. Thus, although PIPEDA determines methods of safeguarding information, such as physical measures, organizational measures and technological measures, it does not mean every organization must adopt all three measures.\footnote{\textit{PIPEDA}, Schedule 1, cl 4.7.3.} In fact, adopting all three measures is impossible.

For a reasonable person, it is hard to understand the real meaning of the technology which is used for data protection. This is the second issue. For example, it requires a professional in the field of computer science to understand the standards of encryption. For a common person, he or she is not expected to comprehend and recognize various levels of security. Hence, although organizations write one or more paragraphs to declare
their duty and methods of protecting personal information, such declarations do not actually mean a lot to most users. What users really want is a guarantee of reasonable remedies, if information is stolen or lost.

Based on the above concerns, when organizations violate their obligation of protecting the personal information of consumers, users expect guaranteed remedies. In reference to these remedies, PIPEDA has a very detailed stipulation in Division 2. This division declares the procedures for the filing of complaints, investigations of complaints, preparing a commissioner’s report and the hearing by a court.

By comparing the privacy policies of three kinds of e-money with the stipulations of PIPEDA, it is evident that there are problems related to privacy policies and the enactment of PIPEDA. There are two ways to solve these problems. Concerning the problems within the privacy policies, government administrators, e-money providers and e-money users could use existing legal rules in PIPEDA to improve privacy policies, because it is an issue regarding the practice of law rather than how to make new laws. The other way is to implement new legal rules in PIPEDA, because there are some apparent deficiencies within PIPEDA. A further comparison will be made in the next chapter in order to achieve the primary goal of this thesis – ascertaining the best privacy laws to protect the privacy of e-money users.
Chapter 4 European Privacy Law vs. Electronic Money

Europe is a leading region in establishing privacy legal rules in the world. The EU has published several directives to regulate privacy issues in electronic communications and the free movement of data. Compared with other countries, no such complete and detailed privacy legal rules exist. Some countries are trying to learn from and adopt the advanced stipulations found in EU privacy laws. For example, the United States (US) prefers to depend on the market itself to adjust to a proper standard for the protection of information privacy rather than depending on government control through certain legal rules. 92 However, there are some voices within the US supporting the adoption of, or at least reference to, EU privacy laws. 93

In this chapter, two European privacy laws and three privacy policies of commercial entities will be discussed. 94 The two European privacy laws are the Convention for the

92 See Avner Levin & Mary Jo Nicholson, “Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground” (2005) 2:2 University of Ottawa Law and Technology Journal 361.

93 Ibid at 374.

94 There are also other privacy laws in the EU. For example, The Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 is concerning the processing of personal data and the protection of privacy in the electronic communications sector. It is also known as the Directive on privacy and electronic communications. However, the purpose of this Directive is to protect the fundamental rights and freedoms, in particular the right to privacy with respect to the processing of personal data in the
Protection of Individuals with Regard to Automatic Processing of Personal Data\textsuperscript{95}, and the Directive 95/46/EC of The European Parliament and of the Council of 24 October 1995 (on the protection of individuals with regard to the processing of personal data and on the free movement of such data)\textsuperscript{96}. The privacy policies include the privacy policies of Personalised Octopus, PayPal and MasterCard.

\section*{4.1 The Convention, the Directive and OECD Privacy Guidelines}

The Convention was published on 28 January 1981 and set out basic principles for data protection. The principles are summarized as follows:

\begin{itemize}
  \item The Convention was published on 28 January 1981 and set out basic principles for data protection. The principles are summarized as follows:
\end{itemize}

\begin{itemize}
  \item Electronic communication sector. Telephone calls and e-mails are typical examples involved in the electronic communication sector. What this thesis focuses on is the privacy issues in the collection, process, retention and erasure of personal information through e-money rather than electronic communication.
  \item Although these two sectors are closely related to each other (for example, the personal information may also be collected through electronic communication at or after the time a customer decides to use e-money), the purpose of this thesis is not to exhaust every detail or situation relevant to privacy during e-money circulation. Hence, this Directive differs from the Directive 95/46/EC and is not quite relevant to privacy issues on e-money. Fundamentally, the goal of this thesis is to find a balance of interests between the commercial entities and their users regarding privacy protection. According to this goal, general principles of privacy protection constitute the research target.
\end{itemize}

\textsuperscript{95} Hereafter referred to as simply the Convention.

\textsuperscript{96} Hereafter referred to as simply the Directive.
(1) Personal data should be obtained and processed fairly and lawfully;\(^97\)

(2) Personal data should be stored for specified and legitimate purposes; The data should be adequate, relevant and not excessive in relation to the purposes for which they are stored;\(^98\)

(3) Personal data should be accurate and, where necessary, kept up-to-date;

(4) Personal data should be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored;

(5) Special categories of data may not be processed automatically unless domestic law provides appropriate safeguards;\(^99\)

(6) Appropriate security measures shall be taken by the organization;

(7) The data subject shall be enabled to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him

---

\(^97\) In the Convention, "personal data" means any information relating to an identified or identifiable individual. Such an identified or identifiable individual is called “data subject”. See Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, art 2, online: Council of Europe <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>.

\(^98\) Personal data further processed for statistical or for scientific purposes may not be considered as incompatible with those purposes. See ibid, art 9.3.

\(^99\) Special categories of data include personal data revealing racial origin, political opinions or religious or other beliefs, health or sexual life, criminal convictions, etc. See ibid, art 6.
are stored in the automated data file, as well as communication to him of such data in an intelligible form;

(8) The data subject shall be enabled to obtain rectification or erasure of such data if these have been processed contrary to the provision of domestic law giving effect to the basic principles; and

(9) The data subject shall be enabled to have a remedy if a request for confirmation, communication, rectification or erasure is not complied with.

The Directive retains the principles in the Convention and expands them to a considerable extent. Besides this, the Directive was published in 1995, which is 14 years later than the Convention. According to the principle that new laws trump old laws, the Directive shall take priority over the Convention if there are any conflicts. However, there are no obvious conflicts between these two laws – merely a few differences. Thus, the

100 “New laws trump old laws” is a fundamental principle in legal theories in the civil law system. In detail, if two legal rules are published by the same legislature or the legal effect of two legal rules are the same, the relatively new rule will trump the old one where conflicts exist between the two different versions of law. Because the EU performs the civil law system, this principle can be used in solving conflicts, if any, between the Convention and the Directive.

101 For example, statistical and scientific purposes could be a reasonable basis for the collection of personal data without confirmation or consent from an individual or individuals. This is an exemption of the principle that personal data should be obtained and processed fairly and lawfully or that the individual’s consent of collecting their personal information should be obtained at, or before, the collection. In the Convention, lawmakers use the expression that this exemption “may be provided by law;” in the Directive,
Directive is adopted as an appropriate privacy law associated with e-money issues and will be discussed in this chapter.

Similarly to the selection of privacy laws between the Convention and the Directive, the OECD (Organization for Economic Co-operation and Development) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines), which were adopted by the OECD Council on September 23, 1980, also provide valuable stipulations associated with the discussion of this thesis. Originally, the OECD was created in 1960 by 18 EU countries, the US and Canada. The member countries agreed that the European Commission should take part in the operation of the OECD. Therefore, the OECD Guidelines on privacy also affect the EU greatly. However, since the principles provided by the OECD Guidelines are almost the same as in the Convention and the Directive, and the OECD Guidelines are used to develop Canada’s privacy standard and subsequent privacy legislations, there is no need to discuss OECD Guidelines separately.102

the expression is “[f]urther processing of data for historical, statistical or scientific purposes shall not be considered as incompatible (with the purposes for which the data is collected) provided that Member States provide appropriate safeguards.” Obviously, the legal effect of the words “may” and “shall” are distinguished in both legal theory and practice.

4.2 Identifying Purposes Principle: The Central Principle for the Protection of E-money Users’ Privacy

Lisa M. Austin argues that the identifying purposes principle under PIPEDA is not complete for the protection of personal information. As to the relationship between the principle of identifying purposes and consent the author believes that consent principle should not be considered as the central principle of PIPEDA, because it is easy for the organizations to use so-called reasonable purposes for getting extra business benefits with consumers’ consent which actually violates their privacy rights. On one hand, she has figured out two important issues within PIPEDA – the consent principle is not the central principle and the purposes principle is insufficient for the protection of privacy. On the other hand, she does not try to find an approach to handle the issues that she has found. Therefore, I will try to find a proper way of solving the issues by comparing the relevant articles in PIPEDA and the Directive.

Looking through the privacy policies of Octopus, PayPal and MasterCard, it is clear that there are similarities and distinctions between them regarding how to use personal information. The similarities encompass:

103 Supra note 84.
(a) Normal operation, management and maintenance of their service;\textsuperscript{104}

(b) Evaluating and improving their service;\textsuperscript{105} and

(c) Marketing.\textsuperscript{106}

The distinctions lie in the fact that each kind of e-money may have its own unique purpose according to its specific issuer. In detail, the distinctions include:

(a) MasterCard dictates that the information could be used to monitor the use of and to improve the interactive assets of both the organization and the customer who provides the information; moreover, the information could also be used to evaluate a particular customer’s interest in employment and contact the customer regarding possible employment;\textsuperscript{107}

\begin{footnotesize}
\textsuperscript{104} This purpose includes enforcing the terms of use, processing transactions, application and authorization for service, clearing, settlement, chargebacks, dispute resolution, fees collection, communication with customers and protection from illegal activities etc. See supra note 67,71,72.

\textsuperscript{105} This purpose includes data analysis and further commercial activities based on the analysis, and developing new products or services etc.

\textsuperscript{106} The marketing purpose may have two situations. One is the marketing of goods or services by an e-money organization itself, its subsidiaries or affiliates. The other is the marketing activities by the e-money organization’s partners, namely a third party. The marketing activities may be providing information, advertisements or promotions about these organizations’ products or services.

\textsuperscript{107} Supra note 72.
\end{footnotesize}
(b) PayPal stipulates that the information could be used to compare information for accuracy and to verify it with third parties;¹⁰⁸ and

(c) Octopus adds “other related purposes” as the last term under the article about the purposes for which the personal data of the customers may be used.¹⁰⁹

If we combine the similarities and distinctions outlined previously, it is evident that there are two layers related to the purposes for the collection of personal information. The first layer is to maintain the normal operation of the e-money system. This purpose benefits both the organizations and their customers, but it is difficult to judge if it is friendlier to organizations or customers.¹¹⁰ MasterCard’s second distinguished purpose and PayPal’s distinguished purpose belong to this layer, as well.

¹⁰⁸ Supra note 71.

¹⁰⁹ Supra note 67.

¹¹⁰ This purpose constitutes the basis of the agreement on using e-money between an e-money organization and a customer. In a common trade, the e-money organization uses the collected information to establish its marketing network, for example, to contact relevant partners and determine the profit rate or administration fees if the customer uses e-money after purchasing the partners’ products or services. On the other hand, the customer could facilitate its purchase by using e-money instead of cash. Furthermore, there may be some unpredictable problems after signing the agreement on using e-money. From the perspective of the customer, he or she may raise a claim about his or her case and the first step for solving the case is to identify who he or she is and his or her relevant information. This personal information is collected at the time of signing the agreement so that both the organization and the customer could decrease the complicated procedures of identifying each other.
The second layer is to deepen the co-operative relationship between organizations and customers. The purposes of “evaluating and improving their service” and “marketing” belong to this layer. The normal operation of e-money, the first layer of the purposes for the collection of personal information, can only guarantee that the existing trade relationship is effective. If the organizations would like to enhance customer loyalty, they may take measures to deepen their close connection with their customers. From this point of view, holding personal information in hand is a good start and basis for organizations to recognize the importance of customer loyalty.\textsuperscript{111}

Therefore, organizations usually add the second layer of purposes to their privacy policies with a statement that it is in favour of their customers. However, this layer of purpose is actually more favourable to the organizations themselves rather than to their customers. Essentially, only profits motivate organizations to evaluate, improve and market their products or services. The relationship between the organizations and their customers will be strengthened, if such a strategy of improving customer loyalty is performed successfully. A closer and more stable connection between the organizations and their customers could help the organizations greatly by excluding external competition. Thus, customers will not only show loyalty to products and services that they already possess,

\textsuperscript{111} Customers’ loyalty means the preference of customers to repeat their purchase behaviour with a particular seller.
but they will also trust future products or services from a particular organization or other entities recommended by the organization with whom they are loyal.

From a legal point of view the intention of such a commercial strategy may not be criticized, as “evaluating and improving their service” and “marketing” purposes may be illegally imposed upon customers.\textsuperscript{112} We can analyze this issue from two perspectives – the text of law and legal theory.

The purposes principle for the collection of personal information is represented in Article 6 of the Directive. The requirements for the purposes principle can be summarized into three aspects:

(a) the purposes should be specified, explicit and legitimate;

(b) the personal information should not be processed in a way incompatible with these purposes, except for historical, statistical or scientific purposes; and

\textsuperscript{112} In the legal theory of the civil law system, especially in criminal law theory, intention is not a decisive element to judge whether behaviour is legal or constitutes a crime. There are three elements to judge such behaviour: (a) whether an actor violates the rules of criminal law; (b) whether there are any legitimate reasons for the actor to do that behaviour, and (c) shall a common person be expected to solve that situation in a way without the violation of criminal law. Beyond these three elements, intention is only used to decide the penalty on the actor. If the actor behaves without a bona fide intention, his or her penalty shall be much more severe than the one with a bona fide intention.
(c) the personal information should be adequate, relevant and not excessive in relation to the purposes.\textsuperscript{113}

Superficially, the purposes specified by the e-money organizations do not conflict with the legal text because all three privacy policies provide specific, explicit and legitimate purposes as required by law.

However, the legal standard for the organizations to stipulate their purposes for collecting personal information is void. Obviously, the requirements that such purposes should be explicit and legitimate only constitute a minimum limitation to the organizations. This limitation can only exclude purposes which are apparently in violation of law, such as gambling and money laundering. But as to purposes like marketing, it is a grey area of law – without legal stipulations.

In fact, the use of personal information for marketing purposes may be unfair to customers in certain circumstances. First, the organizations tend to use customer ignorance of their potential interests. Octopus is blamed for its sale of personal data, because it obtained a huge amount of money in direct exchange. The natural interaction of an affected consumer, as a rational person, may be anger accompanied by the question:

“How can Octopus use my information to earn money and put money into its own pocket?” The sale of information is a simple and apparent trade, so the consumer would readily view such behaviour as unreasonable and could even view it as illegal.

However, as to using personal information for the purpose of marketing the consumer is likely to have difficulty determining the real intention behind this purpose. Often an organization’s real purpose is hidden through illusive wording, such as “to make consumers get the information of promotion”, “to update their new products or services” and so on. For a common enterprise, its marketing strategy usually takes a large percentage of its total expense, via advertisements on TV and websites, posters and special promotional activities. In response, smart marketers have thought out a direct and efficient marketing method – using existing customers’ personal information and keeping in close contact with them.\(^{114}\)

\(^{114}\) For example, after leaving your personal information at Shoppers Drug Mart and acquiring a loyalty card, you will receive promotional advertising every week. A customer is aware that he or she has left an email address in order to obtain this card, but the customer does not know that he or she will receive the promotion message via email in such a high frequency. Superficially, Shoppers notifies its customers that this card can be used to earn credits and that customers can get gifts or discounts as soon as the credit level has reached a certain limit. However, Shoppers’ underlying purpose is to encourage customers to purchase more and more items at their stores. Even if the aforementioned intention is discovered by customers, customers will typically accept the card together with the regulations on the application form. Customer may be surprised the first time they see advertisements from Shoppers in their email box, because they were never informed that their email address in the application for a loyalty card would be used to contact them about promotions. Although there are rules governing this behaviour on the back of the application form,
Fairness is an important value found within privacy laws and FIPs and, as a result, such a marketing practice may be unfair to customers, especially if it violates a customer’s privacy rights. To begin with, it is necessary to clarify what fairness is. Take Octopus, as an example. A customer intends to obtain relevant services provided by Octopus through a personalized Octopus Card, while Octopus intends to obtain commercial profits from the supply of Octopus Cards.

With the customer’s and Octopus’ respective intentions, fairness may have different meanings according to different points of view. From a customer’s point of view, fairness means that he or she can obtain the intended services completely, fully and punctually. Fairness means that he or she should not have obligations imposed beyond those that are necessary. According to legal theory, a right of a customer means that an obligation is accorded upon Octopus. For example, the customer has the right to require Octopus to

the cashier who instructs the customer to fill out the form does not explain them. In addition, the customer does not know how to terminate the subscription for the email promotions. The customer could call the Shoppers hotline or reply to email listed in the email promotion, but most people are not willing to make the effort required to terminate the card.

Generally speaking, a person having a particular legal right means that another person has a relevant obligation, and meanwhile, the person with the particular legal right often has a particular obligation as well. However, some exceptions exist under this rule. For example, parents have the obligation to take care of their children, and the children have the right to require that their parents should fulfill the obligation as a guardian. In this legal relationship, while the parents purely have the obligation without having a right, the
protect his or her personal information through specific safeguards. Therefore, Octopus has the obligation to provide these safeguards. In other words, if the customer’s right is reasonable and valid, Octopus obliges to guarantee the realization of the customer’s right (see the chart below).

<table>
<thead>
<tr>
<th>Customer</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right</td>
<td>→ Obligation</td>
</tr>
<tr>
<td>Obligation</td>
<td>→ Right</td>
</tr>
</tbody>
</table>

Similarly, from the point of view of Octopus, having obligations also means that they have rights. W.N. Hohfold stated that all legal relations could be fundamentally summarized into the relationship between rights and obligations, with even the most complicated legal problems regarding profits being solved following this logic.\textsuperscript{116} In the

\begin{flushright}
children have such a right without bearing any obligation. This is the core idea of the reciprocity and non-reciprocity of rights and obligations theory in the civil law system. See Wang Wendong, “On the Reciprocity and Non-reciprocity of Rights and Obligations” (2007) 5 Journal of Capital Normal University (Social Science Edition) 49.
\end{flushright}

theory of civil law, legal scholars often discuss and contemplate the validity of rights.\textsuperscript{117} Most scholars believe that the validity of rights is the originality of rights. In other words, if a so-called right is merely stipulated by law without validity, this right is not a real or legitimate right. Rather, it is only a meaningless privilege set by the rule-maker or a privilege owned by some powerful people in a non-democratic country.

There are some standards to clarify whether a right is valid or not. The lowest standard is the accumulated requirement of justice in long-term social development. We may understand this standard from two perspectives. The first are the basic and simplest principles and values in everyday life, such as the bona fide principle\textsuperscript{118}. This perspective is from the standpoint of an individual. The second is that one’s rights should be in accordance with the interests of society. For example, every member of society should abide by civic laws. This perspective is from the standpoint of the entire society. Just as we have seen that principles of bona fide and public order have become basic legal rules, these common values have both moral and legal meanings. Morality and laws may conflict under rare situations, but in general, the acknowledgement of morality constitutes the basis of acknowledgement by law.


As supported by Karl Marx’s political economy, *productivity determines the relations of production*. Productivity means the capacity of a whole society to produce and reproduce products. Added value could be used to as an index to measure productivity. Without considering other variables, if a society can obtain high added value with little input, this society has high productivity. The relation of production is the relationship formed in the process of production and reproduction. It includes three aspects: (1) the ownership of capital goods; (2) the relationship of exchange between different people and/or entities; and (3) the relationship of consumption, which is determined by the first two relationships. In general, the concepts of productivity and the relations of production are broad, and they are basic concepts in Marx’s economy.  

Meanwhile, the relations of production can also react on productivity. This rule includes two aspects. On one hand, if the relations of production perform well with productivity, the relations of production will promote the development of productivity. On the other hand, if the relations of production cannot coordinate with productivity, the relations of production will impede the development of productivity. In the context of privacy issues about e-money, whether the e-money providers can properly safeguard their customers’ privacy will influence the relations of production.

---

Accompanying the development in productivity in current society, the newly emerged requirement of justice requires a higher standard to determine the validity of a particular right. In the information era, technology has become the target that most enterprises focus on and compete with, because it is the major tool utilized for improving productivity. Meanwhile, technology injects significant energy into the enhancement of productivity. However, updated technology also causes problems with relations of production.

For example, one of the biggest Chinese web portals declares that one website is publicly selling private information of 60,000 patients and the information of each patient costs 1 RMB.120 Until now, China has not passed a comprehensive privacy statute and does not have a statute regulating the protection of healthcare information. Comparatively, although the US also does not have a comprehensive privacy statute regarding information collection practices in the private sector it has the Health Insurance Portability and Accountability Act, which establishes minimum standards for the protection of a patient’s personal information by related entities.121 Apparently, the US is more advanced than China in productivity, and conflicts between a patient and a hospital

120 Wei Boxing, “60,000 patients’ information is on sale” Sohu News (22 April 2011), online: Sohu <http://news.sohu.com/20110422/n306248419.shtml>; RMB is short for Ren Min Bi, which is the name of Chinese currency.

or a doctor regarding privacy issues reflects a subtle change within the relations of production. Therefore, this comparison shows that once there is some improvement in productivity, associated relations of production will be affected. Hence, lawmakers need to publish new legal rules correspondingly.

The two-layer theory on the standards to clarify whether a right is valid can be used to analyze issues about customer and organizational rights in the context of e-money. First of all, the tricky expression “marketing purpose” conceals the real intentions of an e-money provider. For example, Octopus Holdings Limited expresses its marketing purpose as follows:

marketing of goods and/or services by us, our subsidiaries, our affiliates or any of our selected business partners. We, our subsidiaries, our affiliates or any of our selected business partners may need to carry out matching procedure (as defined in the Ordinance) to enable us to better understand your characteristics and to provide other services better tailored to your needs (such as offering special birthday promotions to you), to assist us in selecting goods and services that are likely to be of interest to you and to establish whether you already have a relationship with our selected business partners.

It is hard to argue that this expression is a violation of the lowest standard – the accumulated requirement for justice in long-term social development, because Octopus has clearly explained the benefits of marketing purpose for both customers and itself. As
to third party Octopus partners, they could be seen as a whole together with Octopus, because their interests are closely connected.

Nonetheless, this expression violates the standard of the second layer – the newly emerged requirement of justice in current society. The emergence of e-money provides a platform for the potential sale, and other uses, of personal information. According to the theory that productivity determines relations of production and that relations of production will react to productivity, if newly emerged e-money causes some potential risks or violates people’s existing rights, the law should react quickly on this issue.

Just as Lawrence Lessig states in the book Code and Other Laws of Cyberspace, you are always in real space and in cyberspace at the same time. Once your personal information is collected by e-money providers, you lose control of your own information because it has been coded and stored in an intangible way. Thus, the privacy policies of e-money organizations are the last defence for customers to make them aware of the process of dealing with the information and relevant safeguards.

Many examples have shown that information has great value in the current era, so any actions which are for the purpose of taking advantage of customer information by e-money organizations shall be considered as unjustified actions by law. Privacy, as Ethan

122 Supra note 19 at 21.
Katsh defines it, is the power to control what others can come to know about you.\textsuperscript{123} Hence, information that could be collected by e-money organizations should be limited to a minimum standard which satisfies the purpose of a single trade. As to another single trade which may be a result of successful marketing through follow-up connections with customers, at least customers should have a right to decide whether they would like to be the subject of such a marketing strategy. In other words, the organizations have the obligation to guarantee customers the freedom of choice. The organizations should not directly request that customers accept their marketing purpose without negotiations or notifications. To the contrary, they should explain this purpose to customers clearly and get the permission of customers to accept additional information such as promotional advertisements.

All in all, certain marketing purposes may not have validity because it treats customers unfairly against the background that information has becoming more and more valuable. Because law enforcement has two major conceptions – reactive and preventive, privacy law should react in time and prevent the potential risk of privacy violations.\textsuperscript{124} Thus, marketing purposes existing in privacy policies should be regulated more strictly via statutes. The Directive practises this idea by stating that a data subject has the right to object to direct marketing.

\textsuperscript{123} Ibid at 143.

\textsuperscript{124} Ibid at 158.
4.3 A Comparison of the Directive with PIPEDA

4.3.1 Identifying Purposes Principle

In comparing the terms stated in the identifying purposes principle in the Directive, one notable difference lies in how to deal with new purposes required by the organizations. In PIPEDA, it requires that new purposes shall be identified prior to use. In the Directive, there is no regulation about such new purposes. This is an issue as to what extent it is reasonable and legal to use and benefit from the personal information of users. This issue resembles another issue that to what extent the purposes provided by the organizations are valid.

Consequently, an analysis using the validity of right theory is also available. Within a particular transaction, the customer’s rights correspond to the organization’s obligations, and vice versa. Furthermore, their rights and obligations are rooted in this particular

---

125 The following comparison is based on the categorization of principles in PIPEDA. In the Directive, there is no such categorization.

126 In the Directive, the articles 6, 10, 11, 19 and 21 include the content of the identifying purposes principle. In summary, they require that the purposes shall be specified, explicit, legitimate and publicized. These requirements are also included in PIPEDA.
transaction, so any extra rights and obligations irrelevant to this transaction are not under the protection of contract or agreement.

An argument may arise that the new purposes are not about marketing, but about processing the information for the benefits of both parties. Following the validity of right theory, it is easy to interpret – because it shall be an organization’s obligation to guarantee the normal process of their users’ information. If it still asks for purposes relevant to such matters the organizations violate their duty of making such purposes specified and explicit in advance, according to the identifying purposes principle.

Therefore, the Directive does not mention anything relevant to new purposes provided by the organizations and the relevant stipulations could be learned from PIPEDA.

4.3.2 Consent Principle

Also, a notable difference about the consent principle exists between PIPEDA and the Directive.\(^\text{127}\) The Directive asks for “unambiguously consent” from the data subject, while PIPEDA permits both express consent and implied consent according to the sensitivity of information. Moreover, the reasonable expectations of the individual are

\(^{127}\) See Supra note 113, Arts 2, 7, 8, 26.
also relevant under PIPEDA. An example provided by PIPEDA is that if an individual subscribes to a magazine, the organization can assume that the individual has consented to this contact as a purpose for collecting personal information about the renewal of the subscription.

It is hard to judge whether a particular person would like to be contacted about the renewal of the subscription. It is understandable that some people do not like to be bothered, because if they like the magazine they can, and will, contact the publisher directly. In the current information era, many magazine publishers provide electronic magazines and electronic ways to subscribe, which makes the magazine convenient to read and easy to subscribe to. Nevertheless, some people may prefer having the publisher contact them about the renewal of a subscription, because they are familiar with the magazine and would like to simplify future subscriptions.

However, if we strictly follow the definition of privacy, this issue gets much easier to explain. Since the right to privacy means the right to be left alone, an individual shall not be bothered without his or her consent. There is no common understanding of “being bothered”. Since there is no common understanding of this term, the attitude of privacy law is extremely significant.
Comparatively, the Directive’s makers are more deep-sighted than that of the lawmakers that produced PIPEDA. There is a seeming paradox in law – law is constantly protecting and restricting freedom, at the same time. Also, freedom is one of the core values of law together with fairness and justice. Thus, “unambiguously consent” provides consumers with more space to make their own decisions, because implied consent is actually a risk for them to argue whether they have consent or not when a violation of privacy occurs. In other words, following the “unambiguously consent” principle more freedom is provided to customers. Meanwhile, the freedom of organizations is not greatly restricted.

4.3.3 Limiting Collection Principle and Limiting Use, Disclosure and Retention Principle

Under the limiting collection principle and the limiting use disclosure and retention principle, the core requirements of PIPEDA and the Directive are almost the same, except that PIPEDA requests organizations to develop guidelines and implement procedures regarding the destruction of personal information. These two principles of PIPEDA are more practical than that of the Directive, as they elaborate on more details about how to realize the limiting purpose.128

4.3.4 Openness Principle

128 See Supra note 113, Arts 6, 11; PIPEDA, SC 2000, Schedule 1, cls 4.4, 4.5.
PIPEDA and the Directive have similarities and differences under the openness principle. Both of them focus on what information shall be open to customers, but PIPEDA also focuses on the procedures for customers to actually realize this principle. Thus, PIPEDA requests that individuals shall be able to acquire information, as stipulated, without unreasonable effort. This requirement has significant meaning for customers to argue for the right of knowing an organization’s policies and practices before giving consent. Hence, PIPEDA does a better job than the Directive on the openness principle.129

4.3.5 Safeguards Principle

The core idea under the safeguards principle, which is shared by PIPEDA and the Directive, is that the organizations shall protect personal information against accidental or unlawful loss, theft, access, disclosure and alteration. The level of safeguards is determined by the nature and sensitivity of information.130

Regarding the above idea, PIPEDA and the Directive show their own focal points. PIPEDA focuses on the training of employees by organizations to guarantee the

129 See supra note 113, arts 10, 11; PIPEDA, SC 2000, Schedule 1, cl 4.8.

130 See supra note 113, art 17; PIPEDA, SC 2000, Schedule 1, cl 4.7.
confidentiality of processing, which is also mentioned by the Directive. Comparatively, the Directive goes one step further than PIPEDA on the relationship with third party processors. In detail, the Directive requires that organizations choose appropriate information processors and that a governing contract exists between a particular organization and its selected information processor. Therefore, the Directive stipulates more details than PIPEDA on the safeguard principle.

Based on the discussion in the third chapter, this chapter pays more attention to the identifying purposes principle and confirms that this principle is the core of all principles. A comparison between the four principles of PIPEDA and relevant rules in the Directive indicates that lawmakers in Canada and the EU may learn from one another’s privacy laws in order to supplement and improve their respective privacy laws.

Chapter 5 Conclusion

5.1 The Best Privacy Laws for the Protection of E-money Users’ Privacy

5.1.1 Identifying Purposes: Clearly Listed and Explained by the E-money Providers
According to the comparison and analysis of PIPEDA and the Directive, the identifying purposes principle is the most significant principle to protect the privacy of e-money users. Although PIPEDA has better rules on this principle, two improvements could still be made. The first is to restrict the scope of new purposes asked by the e-money providers. For example, the marketing purpose may be without reasonableness and legality, so the providers should not ask their users to submit personal information for this purpose. The second is to introduce the rules of standard clauses into PIPEDA. This improvement would incur that e-money providers make their privacy policies explicit and easy to understand, because otherwise the terms in the privacy policies will be interpreted in favour of the users.

5.1.2 Consent: Unambiguously Consent and Withdrawal Regime

Regarding the consent principle, adopting the unambiguous consent principle of the Directive is the better choice than adopting that in PIPEDA – express or implied consent principle. Moreover, there are three deficiencies, which are also within the Directive, in the consent principle of PIPEDA: (1) PIPEDA allows e-money providers to use the opt-out method to obtain a user’s consent, (2) PIPEDA does not stipulate how the users can withdraw their consent, and (3) PIPEDA does not require the e-money providers to make their terms of privacy policies simple to understand. In summary, the consent principle in PIPEDA cannot give users complete protection.
Thus, following the unambiguous consent principle can guarantee that users are aware of their rights and obligations under a particular privacy policy. If lawmakers can solve these three deficiencies by making deeper and clearer rules, the protection for users will become more complete.

5.1.3 Other Four Principles

As discussed in the third and fourth chapters, PIPEDA and the Directive do well in the limiting collection principle, the retention principle, the openness principle, the safeguards principle, and at limiting use and disclosure, although a few improvements could still be made. For example, both PIPEDA and the Directive could explicitly declare that trading personal information is a violation of privacy law, and stipulate relevant penalties and procedures for e-money users to claim for damages.

In a word, PIPEDA and the Directive can cover most potential privacy issues against the background of the rapid development of e-money, but the value of information may be undervalued. It is easy for e-money providers to use the grey areas of privacy laws and to benefit from users’ personal information. Consequently, as pointed out earlier, some improvements to the privacy laws could be made to guarantee the complete protection of users’ privacy.
5.2 Threats from the Internet to Privacy

In fact, potential risks under e-money’s privacy policies are the same as the risks to people’s information privacy with the development of Cloud computing (see the following diagram). One branch of Cloud computing is that some network service providers connect with each other and constitute a “cloud” so that customers can access all of them conveniently. The original model of cloud computing – a search engine – has been popular with people for years, but has only become commercial utility in recent years. The datacentre, including both hardware and software, is the key part of a cloud. Based on this centre, many network service providers join together and share

\[\text{Cloud computing is a computer technique which goes even further than the trend of digitization. Digitization makes humans use less paper than before. Similarly, the cloud computing technology makes humans use less software at least on their personal computers than before and reduces the personal computers’ disposition request. Simply speaking, if the speed and coverage areas of network permits one day and you have a computer terminal which allows you to connect to network, you will not need to download any software or purchase a computer with quite high disposition, because all of that you need could be found online. For example, the online document provided by Google and the Windows Live have emerged just as substitutes of Microsoft Word and MSN. See Michael Armbrust et al, “Above the Cloud: A Berkeley View of Cloud Computing” EECS Department, University of California, Berkeley (10 February 2009), online: EECS, UC Berkeley <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html>. Also see “Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing”, online: Office of Privacy Commissioner of Canada <http://www.priv.gc.ca/resource/consultations/report_201105_e.cfm#toc6e>. (“most participants agreed on the challenges to privacy and data protection posed by the cloud model”).}]}
their users’ personal information. Thus, if there is a network service provider which just supplies an online platform for the other providers, it could hold a great amount of personal information. This type of platform has emerged during the transforming period from Web 2.0 to Web 3.0.

(From CyberVally: http://www.cybervally.com/2010/11/cloud-computing)
The transformation of the Internet from Web 2.0 to Web 3.0 increases the difficulty of protecting privacy.\textsuperscript{132} For example, an Israeli boy named Daniel Gross gained an angel investment in 2010 through his work – “Greplin.” Greplin is a website that searches all of one’s online data, while the famous technology blog, Tech Crunch, recognizes this site as a personal search engine for one’s online life. Greplin can make an index of the personal data stored by Gmail, Google Docs, Facebook, Twitter, Dropbox, LinkedIn, Evernote, etc., and helps users quickly search for information they have published. However, once the password of a user is stolen by a hacker, then the privacy information of the user will be completely disclosed. Consequently, Greplin makes it possible for hackers to access all of an Internet user’s personal data by merely stealing one password, which makes the use of Greplin extremely risky.\textsuperscript{133}

The purpose of writing this thesis is to confront the newly emerging risks of privacy violation against the background of technology development. Through the two-layer theory, which has been used to prove the validity of rights in the context of e-money, other privacy issues relevant to the development of technology can also be interpreted following the same logic. From a micro perspective, the best privacy laws for the protection of e-money users’ privacy were determined by defining e-money, selecting three kinds of e-money as a research target and comparing current privacy laws. From a


\textsuperscript{133} See “About Greplin”, online: Greplin <https://www.greplin.com/about>.
macro perspective, e-money is a good example of technical development which may threaten people’s privacy.

Therefore, clarifying the legal methods for protecting e-money users’ privacy can also direct the research of privacy on other technical developments through which a person’s privacy may be released. On one hand, privacy laws and privacy policies should be strictly complied with. On the other hand, because of technology change – digitization combined with the rise of the Internet – strict compliance with the existing privacy laws and policies is insufficient. Rather, privacy laws and policies should be interpreted broadly to better protect privacy rights and interests.
Selected Bibliography

Books


**Journal Articles**


Legislation

Canada

Bank Act, SC 1991, c 46.

Election Act, RSBC 1996, c 106.


Legal Profession Act, RSNWT 1988, c L-2.

Legal Profession Act, RSNWT 1988, c L-2, as enacted for Nunavut, pursuant to the Nunavut Act, SC 1993, c 28.

Legal Profession Act, RSY 2002, c 134.

Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

Personal Property Security Act, CCSM, c P35.

Personal Property Security Act, RSA 2000, c P-7.

Personal Property Security Act, RSBC 1996, c 359.


Personal Property Security Act, RSPEI 1988, c P-3.1.

Personal Property Security Act, SNB 1993, c P-7.1.


Personal Property Security Act, SS 1993, c P-6.2.

Privacy Act, RSC 1985, c P-21.

Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, SOR/2002-184.

European Union


Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.


OECD