SYNERGY PUBLISHING PTE. LTD.

Journal of Educational Theory and Management

https://ojs.s-p.sg/index.php/jemt

ARTICLE

Information Privacy, Data Surveillance and Security——How Australian Privacy Law Fully Plays Its Role in the Age of Big Data

Jiexin Zang*

The University of New South Wales, Sydney, NSW 2052, Australia

ARTICLE INFO

Article history
Received: 30 October 2018
Revised: 31 October 2018
Accepted: 3 April 2019
Published Online: 16 April 2019

Keywords:
A big data age
The protection of information privacy
The privacy law in Australia

ABSTRACT

Privacy and the protection of privacy is a common topic studied by many scholars. From the very beginning of human culture, people have personal privacy, which is not willing for them to be unveiled by others. With the development of information technology, especially the internet, knowledge and information are dealt by internet users in conscious or unconscious way, and personal information has been rapidly and quickly distributed and disseminated all over the world. Personal data can be collected by hackers or interlinks from the website, internet not only provides people an era with internet links, but also an age with information collections, a big data age. With the background of big data, this essay tries to put forward the correlative relationship between the protection of information privacy and the privacy law in Australia. It first has an overview of the concepts of information privacy and data surveillance under the background of big data, then highlights the importance of data security in the age of big data; with a literature review on the development of Australian privacy acts, it further claims that privacy acts or regulations by the federal or states provided strong support for the protection of personal data. Then relationship between the protection information privacy and the need of judicial guarantee is further studied for thorough methods or regimes in data protection.

With these points studied, this essay aims to highlight the importance of data protection and information privacy. On the other hand, it aims to provide awareness for readers the vital role privacy laws can play in the protection of people's personal information and emphases the importance of a continuous evolution for privacy law system in the age of big data.

1. Introduction

The development of modern technology, especially the rapidly developed internet age, makes people live under the shadow of privacy violation. With people's information privacy violated, the normal order of human society faced severe test. To maintain the normalization status of people's daily life and the order of the society, judicial safeguard from privacy laws are greatly needed. In Australia, there are series of acts and regulations related with the protection of citizens' privacy rights. These laws are formed and developed with the changing of society; however, it is hard for privacy laws to be synchronous with the fast changing society, especially in the

**Corresponding Author:*
Jiexin Zang,
The University of New South Wales, High St, Kensington, Sydney, NSW 2052, Australia;
E-mail: 228400507@qq.com.

DOI: https://doi.org/10.26549/jetm.v3i1.1168

age of internet and the times of big data. The formation of a systematic privacy law system is inevitably hysteric to keep pace with the judicial safeguard of people's information privacy and data protection. Data collection and different sorts of data surveillance like video surveillance both make it hard for the privacy law to fully play their function in the process of information protection. How to protect information or the flow of data in the age of big data is a tough issue studied and discussed by many scholars, it is important to find a workable way for effective protection of information privacy, and calls for insight study on possible measures from different views. Based on the needs of privacy protection, this essay has a review of the formation of Australasian privacy law system and a study on the critical definition of privacy (mainly focus on information privacy) and data surveillance at the beginning. It aims to combine the difficulties of data protections in the current society with highly developed technology and internet, so that a comparison between traditional data protection and data protection in the age of big date is made, and the protection of information privacy can be studied in "jurisprudential discourse" (Burdon M, Telford P., 2010)[5].

Research methods applied in this thesis include historical research method and comparative research method; with the historical research method, this essay has a review over the establishment of the legal system on privacy protection in Australia, so as to drive a panoramic view of the legal system; with the introduction of comparative research method, the essay has an analysis of the roles played by the privacy protection laws and figures out the importance of them in the protection of information privacy by some cases applied with privacy laws. These introduced methods help the essay trace the development of Australian privacy protection, cases are also used to analyze different sorts of privacy violations and to study the manifestations of them as well as the possible measures or workable approaches for the protection of the information privacy and the security of civil rights as well as the data security. Combining with these research methods, the essay draws the conclusion that in the era of high developed internet technology and big data collection, the security of information privacy of Australians are faced with great challenge, on the other hand, it shows the urgency and the persistence need of judicial safeguard in information privacy protection.

2. Critical Analysis of Concepts of "Privacy"

2.1 Different Definitions on Privacy and Privacy Right

When it comes to the definition of privacy, it is never easy to give a precise interpretation on it. According to the research done by David Lindsay, "the concept of privacy began to receive explicit recognition in the Anglo-American world in the second half of the 19th century" (David Lindsay, 2005)[8]. It is an 'elusive' concept that is difficult to define in any satisfactory manner (ALRC, 1983) [3]. Webster's Dictionary defines confidential information as something that is private or secret, so privacy shall be confidential. These listed researches and studies by scholars and authors give the definition of privacy from different angles. It shows that there are different dimensions of privacy for it applies to different fields, thus, makes it hard demarcate which elements are in the range of privacy. So "privacy can assume different definitions" (P. GUARDA, 2004)[26]. In the age of big data and internet, privacy is not only multi-dimensional, but also flexible and dynamic, the definition of privacy can be changed with the changing of the person's work and the places lived, for different cultural backgrounds, professions, etc. So it becomes more difficult to give a clear definition on privacy, to "define the province of privacy distinctly is impossible" (James Fitzjames Stephen, 1967)[25]. Difficult as it is to give a clear definition of privacy, a general idea on the definition of privacy is accepted, and it is commonly regarded by people that privacy "refers to the peculiar things they do not want to be shared and opened." (Banisar D, Davies S, 1999)[4]

Although discussions and researches are never suspended in the defining of privacy, it takes a long time for privacy to have its definitions and be really regarded as a kind of right for people. The story of privacy right can be traced back into the years of 19th century, with Warren and Brandeis' essay published in the Harvard Law Review, in which, they regard privacy law as a new right of people and defines privacy right to be "the right to be alone" (S. D. WARREN, L. D. BRANDEIS, 1890)[23]. Apart from researching works and studies defining the privacy right of people, privacy laws in some countries also give the definition of privacy right. According to the ACT human rights act (Australian Capital Territory Human Rights Act), 12th clause, in the domain of Part 3, civil and political rights, privacy means that "everyone has the right not to have his or her privacy, family, home or correspondence interfered with unlawfully or arbitrarily."

2.2 Concepts and Characteristics of Information Privacy

The review of the previous researches and studies on the privacy and privacy right shows that it is a widely accepted idea that there is no clear definition of privacy. Difficult to define privacy as it is, it is undisputed that the

 DOI: https://doi.org/10.26549/jetm.v3i1.1168

protection of information is definitely the center function of privacy law.

Agranoff gives the definition of information privacy in his research, he regards information privacy as "the claim of individuals, groups, or institutions to determine when, and to what extent, information about them is communicated to others" (Agranoff, M. H., 1993)[2]. The definition of information privacy given by Agranoff are drawn from the aspects of the content of information privacy, the time and the flowing of information privacy, with the definition given , Clarke further describes that the most dominant aspect of personal privacy is the personal data or issue that is specific to the person, it not only includes the personal behavior of him, but also refers the data produced in the person's daily life; whether the person has the right to freely use his data or control the data by himself. They are now collectively referred to as 'information privacy' that he defines as "the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves" (Clarke 2000, p4)[6]. From the aspects of data controlling and the handling of personal data, Clarke shows the importance of the controlling of information privacy. As one of the main elements of privacy, information privacy includes the management and the use of one's private information, ID number, accountant number, income and financial statues, marital statues and family members, medical files, consumption information and network use, etc.

3. Critical Analysis of "Data Surveillance"

3.1 Definition of Data Surveillance and Importance of Data Security

Data surveillance, defined from the literal meaning, means that data has been monitored, according to the study of Joeseph Donahue, data surveillance "compiles personal information from various sources to investigate or monitor people's daily activities and interactions amongst each other" (Joseph Donahue)[17]. With this definition, Joseph Donahue stresses the personal information been monitored, so that when it comes to data surveillance, the most dominant characteristic is the safeguarding of people's personal information.

In 1785, philosopher Jeremy Bentham puts forward the concept of 'Panopticon' (J. Bentham, 1791)[15], he describes that different from the traditional prisons, a panopticon is a prison with a central tower circles around the prisons. Prison guards standing on the tower can have a panoramic view of the movements in every prison; on the other hand, prisoners cannot see what is happening in the tower. In this way, guards can catch the information of the prisoners without being noticed. Similar to the surveillance method of panopticon, data surveillance happened on internet makes internet users' information privacy collected without being informed.

Data surveillance in the age of big data and internet is an indisputable part in information privacy. Compared with surveillance in traditional forms, it is easier and cheaper to apply, while it bears more useful information. Compared with the traditional meaning of information leak, data leaks happened in the range of internet will have a great influence on the owner. Leaks and misconduct of the users' network using record, like the user's name and password, as well as cellphone numbers all result harassment to the data owners. It is different from the traditional one partly because "Technology used in online marketing has advanced to a state where collection, enhancement and aggregation of information are instantaneous." (Laurence Ashworth, 2001)[13]. It is believed that data surveillance and the urgent need of data security came into the eyes of public first in United States in 2002 when people are aware of the Pentagon's Total Information Awareness (TIA). Some critics argues that data surveillance can provide forecasts for possible dangers and will be a workable way to fight against possible dangers or problems; while other critics holds the idea any kind of surveillance is a type of violation to people's information privacy and bears the potential to be abused for various reasons, no matter it is carried by a person or an organization. Clarke notes that personal surveillance is an important weapon in the fight against social evils, but he points out that it can also deny the subject natural justice, and can be tantamount to coercion or blackmail.

It is a common phenomenon of unauthorized acquisition of information in the age of big data. The most dominant feature of the data in big data times is the vulnerability of it, it is first shown by the flexible way of being collected, stored, used or dealt. The second reason of its vulnerability is the loose controlling of the data base. Faced with temptation of economic interests, data controller might sell the collected data for economic purpose; according to the view of Westin, the concerns of individuals and society are secondary to the need for the efficient operations of business and government, this will frequently happen especially when there existed the absence of legislation. Another common reason resulting in the low security coefficient of personal data is weak defensive technology which can be easily attacked. All of these phenomena together with other reasons lead to the leak of personal data.

Under the security measures provided by privacy laws, data security can be made possible from the level of leg-

DOI: https://doi.org/10.26549/jetm.v3i1.1168

islation, personal data sold by data controllers is protected against those who do not have the authority to see it or use it, so that personal data can be "secured and protected from inappropriate access". (Hewett W G, 2002)[12]

3.2 Ways for the Protection of Data Security

With the improvement of privacy law system and more attention putting on information privacy, data security becomes the spot of discussion, so the security of information privacy and data protection in various ways are in great need.

One way to protect the private information of the net users depends on the development of technology making the net citizens use the internet in an anonymous method. Wikileaks introduced similar technology in the protection of its resource providers, with the help of Onion Tor, the advanced encryption technology successfully makes its providers launch and give interpretation of the related documents without being traced. As a hot topic, wikileaks is usually talked for its ethical value; however the technology used can be a reference in the protection of people's information data in the age of big data.

Another way to protect it is to make sure a thorough privacy law system which is synchronous with the age of big data shall be established and be well implied in the protecting of information privacy and data security. Compared with the flow of data in the age of big data and internet, the traditional way flow of data is easy to be monitored and controlled for the flow is traceable. Before the age of big data, People lost their personal data mainly when they communicate to others or leave their personal information when they go to the school to study, go to hospital to have a health check, or go to a supermarket for some daily used items, etc. For people living in the "reality", it is not hard to protect their information privacy no matter where they leave their data, or who they visit, for their information is recorded in written documents and the documents are kept by special assigned people of the school or hospital. Under this circumstance, not only the data controller, but also the data document can be traced, so that the data security can be easily realized and the data can be perfectly protected.

However, with the sophistication of information technology, the trace and controlling of personal data becomes more and more difficult, firstly due to the increasing of the data collected and disseminated capacity of the modern technology; secondly due to the absence of privacy legislation. Rapidly developed technology makes great progress in different fields like the medical research, the transportation system, the modernized logistics distribution system, the telecommunications, and financial transfers. All these newly born or developed fields have close relationship with people's daily life and can collect their personal data in different ways, citizens using the service offered by the mentioned fields or similar companies can by no means avoid the leaking of their personal data. In this way, there comes the first step of the flow of the data, taking the logistic system for instance, if a client wants to send a parcel to a friend, he has to leave the personal information of both sides. And these information will be collected by the logistic company during the sending of the parcel, after that the data might be collected by data collecting companies, which forms the second step of the flow of the client's data; for data companies, their collecting of data not only happened in the field of logistic system, other sort of personal data happened at the same time in other fields. With data collected from various channels, data companies play the role as an intermediary between the data users and the data owners. Nevertheless, for the powerful surveillance ability of computers, the original owner of the data, the client, has no idea of what happened to his personal information, where it goes to, who uses it or what will happen to it. In a highly developed technological society, it is impossible for citizen to protect his personal information without the judicial safeguarding of the federal government. One way for privacy laws' offering of judicial safeguard is to limit the distribution of third party software products, "such as spy-ware, in cases where consumers' privacy or security is compromised" (SPY ACT, 2005)[24]. Legal systems for "specific rules governing the collection" and "principles of data protection" (Banisar, David, 1999)[4] are needed to help the date owner protect his information and guard his rights to know where the date goes to, how the data is stored, and whether the data is used accurately or not.

4. Retrospective View on Australian's Privacy Law

Privacy right is a big part of human rights, with the development of technology, people's privacy rights currently plays a vital role in the successful implementation of human rights protection laws. Based on other countries' experience on the implementation of human rights acts, and the content of provisional constitutions, Australia passed types of acts or regulations to protect people's privacy from both the federal level and the states level.

The history of Australian privacy law can be traced back to 20th century, In 1980, the Organization for Economic Cooperation and Development (OECD) shows its significant impact on the legislation system of the member countries by issuing the Guidelines on the "Protection of

 DOI: https://doi.org/10.26549/jetm.v3i1.1168

Privacy and Transborder Flows of Personal Data" (OECD, 1980)[18]. As a document developed by experts chaired by Michael Kirby, the guidelines provided foundation for privacy laws in Australian. Michael Kirby was also elected as the chairman of Australian Law Reform Commission and played his influence on the following privacy acts or regulations for the federal and the states.

In 1988, Australian government enacts the Privacy Act; the act gives a clear description on information privacy from three divisions, and stipulates privacy rights known as the Information Privacy Principles (IPPs). This act in the history of Australia, sets up the privacy principles in the form of an act, and applies the clauses to the government as well as the private and the public sectors, so that it can limit the organizations' collecting, using and revealing of people's personal information. At the same time, it restricts government agencies' using of the information data of citizen.

Australia established the Australian Capital Territory Human Rights Act (ACTHA) in 2004. ACT Human Right Act is regarded as the first act from the level of the Federal on the protecting of human rights in Australia, for the act not only shows clear clause on the implementation of the protection of human rights from the level of ordinary people, but also the limitation on the operation of power from the level of the administration party. Being the first human act, ACT has a great impact on the law history in Australia, and symbols the mature of people's rights protection consciousness as well as the triumph of people's movements for human rights. A capital act as it is, ACT evokes the emergence of various regulations and acts on rights protection in other states of Australia, like the Charter of Human Rights and Responsibilities in Victoria States, with these regulations and acts publicized, the Australia' Human Rights Framework legislated by the federal government of Australia. After that act, the Australia Legal Reform Commission published a report on the practice of Australian privacy law in 2008. To fully protect the information data of the nation, Australia passed the Australian Information Commissioner Act in 2010, and established the Office of Australian Information Commissioner (OAIC) based on the act.

In 2014, Australia passed the Federal Privacy Act, this act is regarded as a revolution, for it empowers people more rights on the protection of private information and security information privacy in an uttermost way by putting strict clauses and penalty on the leaking of people's personal information. One feature of the act is the high fines it regulates, according to the act, those companies or organizations violating the clause will receive a ticket as high as 1.7 million Australian dollars; for individual businesses or entities, the number is as high as 0.34 million. By the implementation of strict clauses, the act tries to maximize its function in data protection and make Australians be aware of the flow of their personal data.

5. Privacy Laws' Role in Protecting of People's Privacy

5.1 The Judicial Safeguard on People's Information Privacy and Data

The highly developed technology and internet makes information and data "raw and valuable commodity" (Abdul Raman Saad)[1]. Information and data become more and more important with the development of technology and modern society, data was regarded by some authors as an "overriding public interest" (Times, 2001)[14]. However, in the age of big data and internet, personal information and data are violated for various reasons, so different ways of information and data protection, especially the judicial safeguard, are needed.

Established in 2010, Office of Australian Information Commissioner (OAI) is a government agency independent from the government, with the purpose for better protection of Australians' information privacy and personal data. Since the foundation of the agency, the office received 10576 consultations on the protection of privacy, and 1496 lawsuits from 2012 to 2013. A research carried by the office shown that 96% of Australian held the idea that they should be informed of how their personal information were dealt with and protected, over 60% of the interviewees expressed their worries on the possibility of the misuse of their personal information.

In the judicial safeguarding on its citizens' information privacy and personal data, Australian privacy laws restrict the collecting, spreading and using of people's data. Both acts and regulations from the level of the Federal and the level of States put forward clear restrictions of data use. Taking its restricting of video surveillance for instance, as a type of data surveillance, video surveillance sometimes is used by people in an improper way or illegal measure to trace and collect the sensitive information of private or organization. Cookies used by some websites trace the user's logs and monitor people's behavior by its video monitoring system, which belongs to this type of improper use. However, with spy wares and cookies inserted in websites, no matter what efforts a citizen tries in the protection of his personal data on the internet, it is hardly for him to avoid the violation and leaking of the date. High speed development of the modern technology makes the society and people living in it covered under the surveillance of the electronic monitor.

DOI: https://doi.org/10.26549/jetm.v3i1.1168

Originally used in public place like schools, railway stations, and supermarkets, monitors (also called electronic eyes in some countries), are nowadays introduced in many other fields of people's life. For a person walking on the street, once he looks up, monitors will be found here and there; cafeterias, bookstores, workshops and some other private owned factories or stores are filled with monitors. There is no denying that electronic monitor definitely offers a much better management for the order of the city and the daily running of the business; it also plays a vital role in the preventing and cracking of crimes. On the other hand, with the spreading of video surveillance, the free zone of Australians are narrowed, and the personal activities are monitored.

To better explain the violation of people's personal data caused by video surveillance, the case in New South Wales is an example. In New South Wales, it is very common for a day care centers to have electric monitoring system, school or day care centers introduced the use of video surveillance for a better management of the school or day care centers, apart from this advantage, video surveillance in day care centers can make it possible for the students' parents be aware of the activities of their children. However, with the widely use of monitoring system, protests against the using of video surveillance in day care centers are received by the local government. These protests mainly come from two types of people, both parents of the children and staff in the day care centers want their voices to be heard and their problem to be solved. In this case, Parents hold the view that video surveillance can on one hand makes it convenient for them to check what their children is doing and the surroundings via internet connection, on the other hand, it makes some parents worried that it would be possible for their children been spied by other people who have no kinship with them; apart from this reason, another voice against the use of video surveillance in day care centers comes from the teachers working in the center, as a worker of the spotted place under video surveillance, they felt their life and work have been monitored by parents, and that is a kind of violation to their privacy to some extent. This case happen in New South Wales provides a clear demonstration on the advantages and disadvantages of video surveillance.

With the using of monitors, people's life is always in a state of VCR, there are always ubiquitous electronic monitors monitoring in people's life anytime. Similar to video surveillance, the internet usage in daily life also takes a big portion in collecting the data of citizens' personal information, data collecting and processing are in process without the notice of the internet users when they open websites contain cookies, ad-wares, bugs, or spy wares; the flow of data is collected from one website when the subscriber leaves his user name and personal information to another social network site as the user updates his moments. It is not exaggerated to say that a person's personal data is in the possibility of being violated once he logs the website. There are considerable flow of data on the internet, this calls for specific means not only from the perspective of internet management, but also from the perspective of laws to safeguard the personal information of net citizens, so as to prevent the possible risks of people's personal data violating. When it comes to the judicial safeguard, it calls for the translation and refinement of the privacy laws, for the development of internet "requires even the change of the notion itself, as well as of the contents, of the right to privacy" (G. PASCUZZI, 2006)[11].

To restrict the use of video surveillance, states and the Federal passed types of acts, the state of Victoria and New South Wales passed laws and regulations on surveillance device respectively in 1972 and 1978; in 1999, New South Wales passed the Workplace Video Surveillance Act; based on the Listening Device Act, the Federal further legislated the Surveillance Device Act in 2004.

5.2 The Judicial Safeguard on People's Personal Data under the Background of the Age of Big Data

Briefly speaking, big data refers to the massive or mega scale collection of data, from the very beginning of its appearance, which catches wide attention for its potential values. The Wall Street Journal regards big data as one of the most dominant technological innovation; academic journals like Nature and Science both published monographs specialized in the exploring of big data. Nature issued its "Nature·Big Data" monograph in 2008[20], Science issued its monograph "Science. Special online collection: Dealing with data" in 2012[22]. Reports from prominent magazines and researches done by academic journals makes the wide acceptance of big data as well as the importance of it, people then realized many business fields and organizations can be carried forward with the assistance of big data collection and analysis. Because of the potential values shown by big data, US government invented 0.2 billion dollars to launch the project on Big Date Research and Development Initiative. The world famous consulting company McKinsey also reports that big data has already permeated every field of the society for the "Five V" characteristics of it. It first of all has large volume, and then comes its high velocity, variety, and its high value to companies and industries.

 DOI: https://doi.org/10.26549/jetm.v3i1.1168

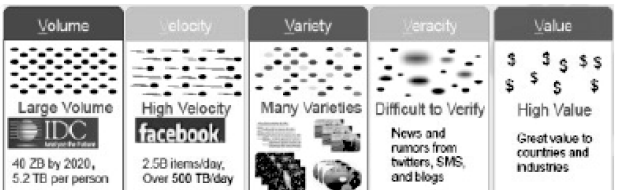

Figure 1. The "Five V" characteristics of big data

Based on the modern technology of data surveillance, data companies further developed data surveillance in large scale, a kind of mass data surveillance, which is also called as Mass dataveillance, it is "concerned with groups of people and involves a generalized suspicion that some (as yet unidentified) members of the group may be of interest." (Clarke, 1991)[7]

There are different sorts of data, with the exponential growth of data after the engorgement of internet, datasets and databases come into being; they are widely used in private or public sectors. "Datasets that may be available to government include but are not limited to open government datasets ("Open Data"), public datasets such as social media data, metadata, and datasets in new fields such as the "Internet of Things," or sensors in Smart Cities." (R. Kitchin, 2013)[19]

According to a research of IBM: within all the data produced in the history of human, 90% is originated in the last several years; to 2020, the total data in human society will increase 44 times from that of 2009, a survey by International Data Corporation shows that the amount of data is growing exponentially, it doubles in every two years, and will reach 35ZB (35 trillion Giga Byte) in 2020. The reason why data can increase in such a rapid speed lies in the huge number of the internet users, for every second, there are about 2 million people logs in search sites like Google; subscribers of Facebook reached 1 billion, and log data originated is above 300 TB.

For the characteristics and advantages carried by big data, it is widely used and sometimes abused in many cases, which calls for the judicial safeguard of it. In the age of internet, big data and cloud computing provides convenient and accurate figure analysis. A most distinguishing difference between the FIFA World Cup Brazil and the previous ones is Brazil's integration of the frontier technology like the "cloud computing" and "big data". Different from the traditional data, in the process of internet use, big data makes the separation of the "data subject" and the "data controller". Faced with economic temptation, some data controllers might sell the data to a third party, the legalistic protection of this kind of data leaking emerges, and the first example of legal instrument on "utilitarian justification" (John Stuart Mill, 1991)[16] is made.

The implementation of privacy laws forms the foundation of the data protection, with this precondition; other methods shall be concluded and used in data security. One of them is the establishment of the management standards of the data, on what kind of personal data can be used by a third party, and what data is personal data, etc. However, with the complexity characteristics and the rapid changing of technology in big data age, acts or regulations are formulated with the references of standards written by technicians or programmers. A poorly made standard cannot have a thorough demonstration of the personal data, which might cause the ineffectiveness of the acts or regulations, for according to Guarda Paolo, "Data protection in the digital environment is dependent on the regulation of the security standards." (Guarda, P., 2009)[9]. So it is vital for acts or regulations to have an effective and scientific standard making team, and the team members shall be highly independent from data collecting companies.

In the process of making standards, some of the technicians are responsible, but for those who do not have high sense of social responsibility, there is a possibility for them to leave "bugs" in the standards. This phenomenon shows the lack of democracy in the establishment of data protecting standards, to fully solve this problem, internet experts independent from the data collecting companies or any third parties are needed, so that objective and effective standards can be made, and the protection of people's personal information will be promoted.

In the implementation of privacy law's protecting of data security, limitations of privacy law is also shown by the unclear categories it had on the elements of privacy, for instance, according to the clause of Privacy Act, "telephone number or address, would not in itself be classed as personal information". However, information like telephone member or address is accreted with other kind of personal information, with the leaking of information like telephone number and address, data collector can easily link them to other databases with more detailed personal information stored, and in this way, personal data can be collected. An unclear expression will result in a discount of the privacy law's legal validity, in the case of Seven Network (Operations) Ltd vs Media Entertainment and Arts Alliance (MEAA), the internal telephone number directory of the staff of Seven Network became the controversial topic for whether the number are provided to MEAA illegally as personal information or not. This case leaves its impact on the establishment of privacy act, for it well demonstrates the

DOI: https://doi.org/10.26549/jetm.v3i1.1168

importance of clear classified categories on the elements of privacy and the scientific description of its clause.

6. Conclusion

With the background of big data time, this essay has a review of the formation of Australian privacy law system chronologically, it can be seen that the country never stops in the seeking of the continually improvement of privacy acts or regulations to fit the development of the society and technology. This essay contends that privacy law is the underpinning for data protection and information privacy and plays an indisputable role in it. With the complex characteristics of data surveillance, and furry definitions of information privacy and the age of big data, data security is hard to be realized.

Although there are privacy laws in Australia, in the protecting of people's information privacy, it shows its shortcomings. The rapid development of modern technology makes it hard for privacy law to keep pace and be synchronized with it, thus, there exists disconnection for a systematic information privacy protection and data security. To build a systematic management of the data, a system centered with privacy laws and combined with self-discipline of the company is in need.

One common measure used is the security defending technological system including firewall, intrusion detection, security audit, and anti-virus system; the other way to promote the security of data controlling company is the improvement of the management of the company, including the network management, system management and the management of computing room, it also calls for the strong responsibility from the data controlling company in the holding of its "moral autonomy" (Robert Post, 2001)[21] in the protecting and using of data. There is value in the present study, but due to the limited evidence, further study should be drawn and made.

References

[1] Abdul Raman Saad & Associates Malaysia, Information Privacy and Data Protection A Proposed Model for the Kingdom Of Saudi Arabia.

[2] Agranoff, M. H., 1993, Controlling the Threat to Personal Privacy, Journal of Information Systems Management.

[3] Australian Law Reform Commission, Privacy, Report No 22, 1983.

[4] Banisar, David, and S. G. Davies., 1999, Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments. John Marshall Journal of Computer & Information Law XVIII.1.

[5] Burdon M, Telford P., 2010, The Conceptual Basis of Personal Information in Australian Privacy Law. Social Science Electronic Publishing, 17(4):1-27.

[6] Clark R., 2000, Current Developments in Internet Privacy.

[7] Clarke, Roger., 1991, Information Technology and Dataveillance. Roger Clarke's IT and Dataveillance. Xamax Consultancy Pty Ltd, Canberra. 25th, May. 2016. <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html>.

[8] David Lindsay, 2005, An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law,Melbourne University Law Review, Melbourne, 131-153.

[9] Dialogues in Human Geography.Guarda, P., 2009. Data Protection, Information Privacy, and Security Measures: an Essay on the European and the Italian Legal Frameworks. Social Science Electronic Publishing.

[10] Geo-Journal; M. Batty, 2013, 'Big Data, Smart Cities and City Planning' ,3(3).

[11] G. PASCUZZI, 2006, Il diritto dell'era digitale, 2nd ed., Bologna.

[12] Hewett W G, Whitaker J., 2002, Data protection and privacy: the Australian legislation and its implications for IT professionals. Logistics Information Management, 15(5-6):369-376.

[13] Laurence Ashworth, 2001, Clinton Free, Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns, Journal of Business Ethics, June 13.

[14] Lord Falconer of Thoroton., 2001, Privacy law and medical research [letter]. Times May 17:21.

[15] J. Bentham, 1791, Panopticon: Postscript, Part II, London: Mews——gate, pp. 29-95.

[16] John Stuart Mill, 1991, 'On Liberty' in John Gray (ed), On Liberty and Other Essays 5, 13-14.

[17] Joseph Donahue, Nicholas Whittemore, Ashley Heerman, Ethical Issues of Data Surveillance.

[18] Organisation for Economic Co-operation and Development, 1980, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Paris: OECD).

[19] R. Kitchin, 2013, 'The Real-Time City? Big Data and Smart Urbanism', 79.

[20] Nature.Big Data[EB/OL]. 26th, May, 2016. <http://www.nature.com/news/ specials/bigdata/index.htm>.

[21] Robert Post, 2001, Three Concepts of Privacy, Georgetown Law Journal 2087, 2095.

[22] Science. Special online collection: Dealing with

 DOI: https://doi.org/10.26549/jetm.v3i1.1168

data[EB/OL]. 26th, May, 2016, <http: //www.sci-encemag.org/site/special/data/>.
[23] S. D. WARREN, L. D. BRANDEIS, 1890, The Right to Privacy, Harv. L. Rev. 193.
[24] Securely Protect Yourself against Cyber Trespass Act (SPY ACT), 2005, H.R. 29, 109th Cong.
[25] Sir James Fitzjames Stephen, 1967, Liberty, Equality, Fraternity (first published 1873, 1967 ed) 160.
[26] P. GUARDA, 2004, Agenti software e sicurezza informatica. Diritto E Tecnologie Evolute Del Commercio Elettronico, 2004.

DOI: https://doi.org/10.26549/jetm.v3i1.1168