EXPLORING THE WAY TO PROTECT PRIVACY IN THE ELECTRONIC WORKPLACE PROPOSALS FOR AUSTRALIAN AND CHINESE CONTEXT

Danyang Guo*

Table of Contents

* Dr. Guo Danyang, student in School of Law, Tsinghua University.

EXPLORING THE WAY TO PROTECT PRIVACY IN THE ELECTRONIC WORKPLACE PROPOSALS FOR AUSTRALIAN AND CHINESE CONTEXT

Danyang Guo

Abstract

Surveillance and monitoring have become controversial issues in the modern workplace. The increasing use of electronic surveillance as a management technique, including Email, Internet monitoring, electronic performance measurement, and other workplace surveillance, has changed how employers monitor productivity and job performance, forming a new concept: Electronic Workplace. Especially during the pandemic, these new methods of gathering information in the electronic workplace about workers have become more common and intrusive than traditional forms of physical supervision because employers can conduct monitoring in secret, and it can be continuous and all-encompassing. As a result, employees' privacy interests may be affected even if the employer does not engage in physical monitoring. Thus, it is necessary to protect privacy in the electronic workplace.

Among the countries that have actively drawn on the EU's experience in law-based cyberspace governance and the protection of personal information and data, Australia and China have been particularly prominent in recent years. Since the enactment of the Privacy Act 1988 (Cth), Australia's privacy legislation has been amended and improved over the year. However, it was still hit by a serious data breach in 2021. Thus, Attorney-General's Department released the Privacy Act Review Report 2022 seeking suggestions for improving privacy protection in Australia. Against this background, this article focuses on privacy protection in the Australian electronic workplace and seeks to respond to the Privacy Act Review Report 2022. Similarly, it is not enough protection for employees' privacy in the Chinese electronic workplace. Therefore, based on the suggestions made for Australia and China's current protection status, it also aims to provide suggestions for developing privacy protection in the Chinese electronic workplace.

I. INTRODUCTION

Surveillance and monitoring have become controversial issues in the modern workplace. The increasing use of electronic surveillance as a management technique, including Email, and Internet monitoring, has

changed the way employers monitor productivity and job performance.[1] These new methods of gathering information about workers can be seen as a new problem compared to traditional forms of physical supervision, because employers have the ability to conduct monitoring in secret, and it can be continuous and all-encompassing.[2] Technology has made it easier for employers to pry into employees' private lives and more challenging for employees to detect.[3] Employees' privacy interests may be affected even if the employer does not engage in physical monitoring. In the technological society, it is easy for employers to rely on surveillance and monitoring of employees without considering whether it is necessary.[4] Therefore, Matthew Finkin suggests, "A privacy law is needed, not only because of the occasional wanton invasion of privacy while experiencing frolics but also because of the systematic way in which employers violate legitimate business interests."[5]

In addition to invisibility and continuity, there are unique aspects of employee privacy protection issues compared to general privacy protection.

Firstly, the unequal employer-employee relationship makes the employees difficult to bargain to protect personal information on an equal footing with the employer. The de facto disadvantage of the employer regarding information, financial resources and skills, as well as the subordination of the personality of the labour relationship, makes the employee work on behalf of others, subject to direction and supervision, following the contract, in order to receive remuneration.[6] With the broad scope of the right to privacy, in particular, the complexity of the way personal information is collected and used in the workplace, employees do not have enough time or energy to get well understand what and how their personal information is disclosed or used. Especially in a competitive job market, employees may prefer to forgo protecting personal information to avoid conflict and retain their positions. For example, where face recognition technology is used as an attendance management system, few employees have raised that this appraisal management system involves the infringement of sensitive biometric information. As a result, de facto and de jure vulnerability makes it difficult for employees to freely and voluntarily

[1] Hazek Oliver, Email and Internet Monitoring in the Workplace: Information Privacy and Contracting-Out, 31 Industrial L.J. 321, 372 (2002).

[2] Id.

[3] Frederick Schauer, *Internet Privacy and the Public-Private Distinction*, 38 Jurimetrics 555, 558 (1998).

[4] Hazek Oliver, *supra* note 1, at 330.

[5] Matthew W. Finkin, *Employee Privacy, American Values and the Law*, 72 Chi-Kent L Rev 221, 256 (1996).

[6] Felicia Rosioru, *The changing concelt of subordination*, Recent Developments in a Labour Law 1, 7 (2013).

provide full protection of their personal information in the work environment.

Secondly, the development of the electronic workplace and algorithmic technology have increased the risk of violating employees' privacy. The use of smartphones, laptops, and wearable devices at work has become increasingly popular, and communication systems such as company local area networks (hereinafter LANs) and WeChat groups are frequently used. The daily use of this hardware and software by employees at work is accompanied by the collection, use, processing, and transfer of large amounts of personal information. In the digital work process, the employer can collect a considerable amount of personal information and, with the appropriate algorithms, analyze and predict the employee's information, which can become its employment or assessment indicator.

Finally, the electronic workplace environment makes distinguishing between worker-derived data and company trade secrets difficult. Employees are required to perform their work through the company's equipment, and the derived personal information and data are generated. For example, are web search records, WeChat chat records, and email records derived by the employee at work personal information or trade secrets? Will they be deleted as personal information or stored as trade secrets in the company cloud after the employee departs? Due to these unique characteristics of employee privacy in an electronic workplace, it needs special attention.

Among the countries that have actively drawn on the EU's experience in law-based cyberspace governance and the protection of personal information and data, Australia and China have been particularly prominent in recent years. China has enacted Cybersecurity Law[7], Data Security Law[8], and Personal Information Protection Law[9]. Compared to workplace privacy protection in Europe and the United State, Australia is learning and improving. However, the significant data breaches in 2022[10] are still a wake-up call for privacy protection in Australia. As a result, the Attorney-General's Department (hereinafter "AGD") released the *Privacy Act Review Report 2022* (hereinafter "the Report 2022")[11] in February 2023 after

[7] Wang Luo An Quan Fa （网络安全法）[Cybersecurity Law] (promulgated by the Standing Comm. Nat'l People's Cong Nov. 7, 2016, effective June 1, 2017) (Chinalawinfo).

[8] Shu Ju An Quan Fa （数据安全法）[Data Security Law] (promulgated by the Standing Comm. Nat'l People's Cong June. 10, 2021, effective Sep 1, 2021) (Chinalawinfo).

[9] Ge Ren Xin Xi Bao Hu Fa （个人信息保护法）[Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong Aug. 20, 2021, effective Nov 1, 2021) (Chinalawinfo).

[10] Over a three-week period in 2022, the personal data of over 9.8 million Optus customers and 9.7 million Medibank customers was stolen by cyber criminals.

[11] Australian Government Attorney-General's Department, *Privacy Act Review Report 2022* (Report, 16 February 2023) (Austl.) (hereinafter "Report 2022").

collecting proposals from various industries for reform of the Privacy Act and opening it for public feedback. Thus, this article focuses on privacy protection in the Australian electronic workplace in this context and seeks to respond to the Report 2022. It also hopes to provide suggestions for the Chinese electronic workplace environment facing the same employee privacy protection dilemma.

This article has six parts. Section II defines privacy and the electronic workplace, and then points out that it is difficult to distinguish private and public in the electronic workplace. Section III introduces the current legal framework for protecting the electronic workplace in Australia and, on this basis, states that there is still a lack of employee privacy protection in Australia. Section IV then proposes expanding the definition of "personal information" and removal of exemptions for small business and employee records from the Privacy Act, harmonizing the electronic surveillance Act, and improving company policy to protect privacy in the electronic workplace in Australia. Section V proposes to China, which also does not have a comprehensive law to protect employee privacy, to improve the provisions of the Personal Information Protection Law, to respect the right to reasonable expectations of employees in the employee-employer relationship through the labor contract, and to improve the scenario-based provisions of the Cybersecurity Standard Operating Guide- Telecommuting Security Protection[12] as a guide to distinguish the private and public the electronic workplace.

II. THE CONCEPT, PRIMARY PRIVACY ISSUES IN THE ELECTRONIC WORKPLACE

A. The Definition of Privacy

Due to its inherent subjectivity, it is difficult to define "privacy" in a philosophical sense. However, Professor Gavison argued that privacy should be under the protection of law though it is a shapeless abstraction, because "the functions of privacy in our lives are the promotion of liberty, autonomy, selfhood, and human relations, and furthering the existence of a free society."[13]

While there is no enforceable right to privacy in Australian law, Chief Justice Gleeson argues that "the law should be more astute than in the past to identify and protect interests of a kind which fall within the concept of

[12] Wangluo Anquanbiaozhun Shijianzhinan: Yuanchengbangong Anquanfanghu [网络安全标准实践指南-远程办公安全防护][the Cybersecurity Standard Operating Guide - Telecommuting Security Protection]National Information Security Standarization Technical Committee (NISSTC) (Mar 2020) (hereinafter "Guide of Telecommuting Security Protection") .

[13] Ruth Gavison, *Privacy and the Limits of the Law*, 89 The Yale Law Journal 421,471 (1980).

privacy."[14] Also, *Privacy Act 1988* defines privacy as personal information, which is the "information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether or not true and whether or not in the material form."[15] Moreover, in *Ng v. Department of Education (General)*, personal information is information or an opinion, which is recorded in any form and whether true or not, about identifying an individual or can reasonably be ascertained as individual information or opinion, but it exempts the information which is regulated under the *Health Records Act 2001*.[16]

As regards the definition of privacy in China, there are two opinions. The mainstream view of academia, represented by Wang Liming[17], is that the right to privacy is a defensive right, involving "peace of private life" and "personal secrets not to be disclosed." In contrast, the right to personal information is a positive right, emphasizing the right to self-determination of personal information. But these definitions do not exclude the possibility that the two rights may intersect in some cases. Other scholars[18] believe that the right to privacy includes both privacy and information autonomy and that personal information is still essentially under the traditional concept of privacy. According to China's Civil Code[19] (hereinafter "Civil Code"), it is clear that personal information and personal privacy are not identical, with some distinctions between the two and some overlap. Referring to these definitions, this article defines privacy protection as the protection of personal information, personal data, and its relevant right and interests, and further focuses on preventing the disclosure of personal information and damage to reputation in the electronic workplace.

B. The Scope of Electronic Workplace

[14] Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 185 ALR 1, 13 (Austl.) (hereinafter "ABC v Lenah Game Meats").

[15] *Privacy Act 1988* (Cth), s 16A (Austl.)

[16] Ng v Department of Education (General) [2005] VCAT 1054 1, 38 (Austl.).

[17] Wang Liming (王利明), *Yinsiquan Gainian de Zaijieding*（隐私权概念的再界定）[*Re-Definiion of Right to Privacy*], 1 FAXUEJIA （法学家） [THE JURIST] 108 (2012).

[18] Fang Shaokun (房绍坤), Cao Xiangjian (曹相见), *Lun Gerenxinxi Rengeliyi de Yinsi Benzhi* (论个人信息人格利益的隐私本质)[*On the Privacy Nnature of Personal Information Personality Onterests*],4 FAZHI YU SHEHUIFAZHAN (法制与社会发展) [LAW AND SOCIAL DEVELOPMENT] 99 (2019); Qi Pengfei (齐鹏飞), *Lun Dashuju Shijiaoxia de Yinsiquan Baohumoshi* (论大数据视角下的隐私权保护模式)[*On the Mode of Privacy Protection from the Perspective of Big Data*], 2 HUAZHONGKEJIDAXUE XUEBAO (SHEHUIKEXUEBAN) (华中科技大学学报（社会科学版）) [JOURNAL OF HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY (SOCIAL SCIENCE EDITION) 65 (2019).

[19] Minfa Dian （民法典）[Civil Code] (promulgated by the Nat'l People's Cong May 28, 2020, effective Jan 1, 2021), art 1034 (Chinalawinfo).

According to the Workplace Privacy Options Paper[20], the common forms of workplace surveillance includes video surveillance; audio surveillance, usually in the form of telephone monitoring; tracking surveillance using GPS devices installed in motor vehicles, and E-mail and internet monitoring. With the development of social technologies, the popularity of cell phones with GPS capabilities, and the invention of wearable technology, monitoring by employers has become more accessible, cheaper, and more common. Modern technology is capable of monitoring employee performance and tracking biomarkers. While this tracking may be motivated by concerns for employee health and well-being, it has also allowed monitoring to take a more intrusive form, even putting some workers at risk of 24/7 surveillance by their employers.[21]

Especially since the pandemic outbreak, new heights have been reached for telework and work-from-home arrangements, with digital enhancements in the workplace. According to section 5 of the *Workplace Surveillance Act 2005* (NSW) (hereinafter "*Workplace Surveillance Act 2005*")[22], when an employee works for an employer at the employer's workplace or any other place, s/he is working. Therefore, this article defines the electronic workplace as an environment in which electronic devices, networks, electronic monitoring, GPS, and wearable devices are used for work in a digital environment.

C. The Boundary Between Private and Public is not Clear in the Electronic Workplace

As Gleeson CJ stated in *ABC v Lenah Game Meats* , "There is no bright line which can be drawn between what is private and what is not."[23] Under the electronic workplace, the boundary between private and public is more difficult to distinguish. Compared with past decades, it is obvious that most companies have used electronic devices and web-based technology to monitor employees' behavior in recent years, which could improve working efficiency and reduce corporate resource abuse. However, these technologies broaden the scope of privacy and make it difficult to distinguish between private and public in an electronic workplace. Many factors lead to this situation. Myria Watkins Allen etc. thinks that with the application of electronic monitoring, it is easier for employers to monitor employees' behavior in real-time, which makes the boundary between employees and

[20] Victorian Law Reform Commission, Workplace Privacy: Options Paper, Melbourne, 2004, at [2.3]–[2.15].

[21] Céline Brassart Olsen, To track or not to track? Employees' data privacy in the age of corporate wellness, mobile health, and GDPR 10 International Data Privacy 236, 241-242 (2020).

[22] Workplace Surveillance Act 2005 (NSW), s 5 (Austl.).

[23] ABC v Lenah Game Meats, supra note 14, at 42.

companies turbulent.[24] Besides, Paula McDonald and Paul Thompson argue that social media drive the actions of employers and employees to disrupt traditional relations in organizational life, which re-organize the boundaries between public and private area.[25] Anthony M. Townsend and James T. Bennett state that because of the limitation of current law, employers can monitor employees' communications and workplace activities with little or no notification by using information-gathering technology and web-based technology, which renders privacy boundaries unclear.[26] This section will analyze two primary factors contributing to this phenomenon.

The first factor is the change of working and supervising mode in the current workplace. In the past, most employees finish their work by using paper and manual labor. The only way for employers to monitor employees' performance is to walk around and observe physically, which may not often lead to infringement of privacy. However, with "information and telecommunication technologies becom[ing] the work environment,"[27] the electronic workplace provides essential tools for employees in their work, and also provides a connection between platform and user end. Specifically, electronic products and information-gathering technologies make it possible for employers to observe and record the information created in the workplace, whether private or public, which leads to a higher possibility of privacy invasion. For example, employees' behaviors are recorded and monitored by various electronic technologies in Australian workplaces, such as voice mail, e-mail, phone calls or CCTV camera. According to one survey, the surveillance modes in the workplace include recording phone numbers and monitoring the length of calls (37%), installing CCTV cameras (16%), and storing and reviewing employees' e-mail (15%).[28] GPS systems used in long-haul trucking companies and company cars enable employers to track and record their employees' movements such as car speed, driving route, fuel consumption, locations, etc. Therefore, these electronic devices assist employers to collect and record employees' information with a far broader scope and more detailed scale than in the past, which more or less makes the boundary between private and public equivocal.

[24] Myria Watkins Allen, Stephanie J. Coopman, Joy L. Hart & Kasey L. Walker, *Workplace Surveillance and Managing Privcay Boundaires*, 21 Management Commuication Quarterly 172, 176 (2007).

[25] Paula McDonald & Paul Thompson, *Social Media(tion) and the Reshaping of Public/Private Boundaries in Employment Relations*, 18 International Journal of Management Reviews 69, 69 (2015) (hereinafter "Paula McDonald").

[26] Anthony M. Townsend & James T Bennett, *Privacy, Technology, and Conflict: Emerging Issues and Action in Workplace Privacy*, 2 Journal of labor research 195, 203 (2003) (hereinafter "Anthony & James").

[27] *Id*, at 196.

[28] David C. Yamada, Voices from the Cubicle: Protecting and Encouraging Private Employee Speech in the Post-Industrial Workplace, 19 Berkeley Journal of Employment and Labor Law (1998) 1, 7.

Such a trend is reinforced by the pandemic when online work and Work From Home (hereinafter "WFH") became common. According to the 48th Statistical Report on the Development of China's Internet,[29] from December 2020 to June 2021, the scale of online office users grew by 91.2%, with the average daily usage time of online meetings reaching 36 minutes, and online document editing usage was 23.8%, an increase of 2.6 percentage points compared to December 2020. The online office has transformed into a place of residence, a shift making the distinction between private and public equivocal.

The second factor is the full usage of social media in the workplace. "Social media such as LinkedIn, Instagram, Facebook, YouTube, Snapchat, and Twitter had expanded ubiquitously into all aspects of modern life across work and play, the professional and the personal, public and private life."[30] For instance, when an employee tried to search or connect with someone for business reasons via LinkedIn, at the same time, he or she might also browse some attractive or interesting articles posted on the homepage. Unfortunately, all the mouse clicks, browses, and operation behaviors have been recorded, whether the contents are private or public. This situation also applies to all other social media, which blurs the line between private and work life.

Therefore, with the introduction of electronic devices and social media, it is difficult to make distinctions between private and public information in the electronic workplace. Gleeson CJ also puts forward that "use of the term 'public' is often a convenient method of contrast, but there is a large area in between what is necessarily public and what is necessarily private."[31] Consequently, this unclear boundary makes it difficult for privacy to be effectively protected under current legislation.

III. CURRENT ISSUES ABOUT PROTECTING PRIVACY IN ELECTRONIC WORKPLACE IN AUSTRALIA

A. The Legal Framework for Protecting Privacy in the Australian Electronic Workplace

There are three primary levels in Australia to protect employees' privacy: the common law, commonwealth legislation, and state legislation. Theoretically, employees can negotiate with their employers in the common law system to have surveillance provisions specified in the employment

[29] XLVIII CI ZHONGGUO HULIANWANGLUO FAZHANZHUANGKUANG TONGJIBAOGAO [第 48 次中国互联网发展状况统计报告] [48th Statistical Report on the Development of China's Internet] China Internet Network Information Center (CNNIC), 35-36 (48, Aug 2021) (hereinafter "48th Statistical Report").

[30] Mark Cox, Blurring the boundary between work and play: Disciplining employee conduct in social media and out of hours, 43 Brief 28, 28 (2016) .

[31] ABC v Lenah Game Meats, supra note 14, at 42.

contract, but the unequal employer-employee relationship leaves employees with little bargaining power. In *ABC v Lenah Game Meats*, the High Court presented the possibility of accepting recognition of privacy rights in the future.[32] However, only a few decisions have recognized a tort of invasion of privacy since that decision. [33]

No Commonwealth legislation specifically addresses workplace privacy, but only some relevant provisions in the *Privacy Act 1988* [34], the *Telecommunications (Interception and Access) Act 1979* (Cth) (hereinafter referred "*TIA Act*")[35], and the *Fair Work Act 2009* (Cth) (hereinafter referred "*FW Act*")[36]. The *Privacy Act 1988* (Cth) provides the definition[37], collection, use, and disclosure of "personal information". [38] The Act requires "APP entities" to comply with its Australian Privacy Principles (hereinafter referred "APPs") to process personal information. [39] Therefore, where an employer as an entity processes personal information in the workplace, it should comply with the APPs. Employees who believe that their employer has breached the APP by infringing their privacy can file a complaint to the Office of the Australian Information Commissioner (hereinafter referred "OAIC"). [40] In cases involving serious and repeated interference with personal privacy, the OAIC can also accept enforceable undertakings or apply to the courts to impose civil penalties.[41] However, the Act gives the exemption to the obligations of small businesses and protection of "employee records held by the organisation". [42] In addition, the *TIA Act* provides that no person shall intercept communication without the knowledge of the person making the communication.[43] The Act does not clarify whether email surveillance falls within the scope of this Act. *FW Act* explains Australian privacy principles and employers' obligations when protecting personal information but does not exclude exemptions for small businesses and employees to retain employees' records.

[32] ABC v Lenah Game Meats, supra note 14, at 35.

[33] Cases in support of privacy tort: *Grosse v Purvis* [2003] QDC 151 (Austl.); *Jane Doe v Australian Broadcasting Corporation* [2007] VCC 281 (Austl.). Cases not in support of privacy tort: *Giller v Procopets* [2008] VSCA 236 (Austl.); *Wilson v Ferguson* [2015] WASC 15 (Austl.).

[34] *Privacy Act 1988* (Cth) (Austl.).

[35] Telecommunications (Interception and Access) Act 1979 (Cth) (Austl.).

[36] *Fair Work Act 2009* (Cth) (Austl.).

[37] *Privacy Act 1988* (Cth), s 6 (Austl.).

[38] *Id*, s 16A.

[39] *Id*, s 6: "APP entity" means an agency or organization. *Id*, s15: APP entities must comply with Australian Privacy Principles.

[40] *Id*, s 36.

[41] *Id*, s 13G.

[42] *Id*, s 7B. *Id*, s 6D: A small business is one with an annual turnover of $3 million or less. The annual turnover for the purposes of the Privacy Act includes all income from all sources. It does not include assets held, capital gains or proceeds of capital sales.

[43] *TIA Act*, s6(1), s 7.

At the state legislative level, most states and territories have legislation that applies to the public sector regulating the processing of personal information in Australia.[44] Concerning surveillance management, only New South Wales (hereinafter "NSW") and the Australian Capital Territory (hereinafter "ACT") have specific workplace surveillance laws.[45] As no uniform surveillance law exists, the definition of surveillance,[46] the scope of application, the timing of surveillance, and the form of surveillance[47] vary from state to state, and the degree of protection of privacy in the electronic workplace also varies.

B. Current Issues that Threaten Employees' Privacy in the Australian Electronic Workplace

a. Privacy Act is too general to protect privacy in the electronic workplace

The *Privacy Act 1988* is the primary law to protect individual information among private sector organizations, Australian federal government agencies, and ACT government agencies. Its protective scope covers personal information and sensitive information, such as ethnicity, health information, trade union membership, and sexual preference.

As mentioned before, the *Privacy Act 1988* defines "personal information", which was revised in 2012. Specifically, personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material

[44] Information Privacy Act 2014 (ACT) (Austl.); Privacy and Data Protection Act 2014 (Vic) (Austl.); Information Privacy Act 2009 (Qld) (Austl.); Personal Information Protection Act 2004 (Tas) (Austl.); Information Act 2002 (NT) (Austl.); Privacy and Personal Information Protection Act 1998 (NSW) (Austl.). some legislation releted to human rights protection: Human Rights Act 2019 (Qld) (Austl.); Charter of Human Rights and Responsibilities Act 2006 (Vic) (Austl.); Human Rights Act 2004 (ACT) (Austl.). some states and territories regulated the processing of personal health information from specific legislation: Health Records and Information Privacy Act 2002 (NSW) (Austl.); Health Records Act 2001 (Vic) (Austl.).

[45] Surveillance Devices Act 2007 (NSW) (hereinafter "Surveillance Devices Act") (Austl.); Workplace Privacy Act 2011 (ACT) (hereinafter "WP Act 2011") (Austl.).

[46] *Surveillance Devices Act*: It defines surveillance through a camera that monitors or records visual images or activity, which means that the Act applies to surveillance using cameras from wearable devices such as drones or Google Glass, as well as surveillance using fixed cameras, but excludes mobile phones with GPS. *WP Act 2011*: Under the Act, a tracking device is defined as any electronic device capable of being used to monitor the location of a person or object, and it would therefore cover tracking of an employee using a GPS locator in the employee's smartphone.

[47] NSW: Surveillance that does not meet the notification requirements of the *Surveillance Devices Act* is considered to be covert. Covert surveillance can only be used to determine whether an employee is involved in illegal activities at work, and the employer must obtain authorization for covert surveillance from a magistrate. ACT: *WP Act 2011* requires employers to notify employees of surveillance and consult with them on how it will occur. The notification of surveillance under the *WP Act 2011* must include the matters required by the Act, a statement of which employees will typically be subject to surveillance, the purposes for which the surveillance records may be used or disclosed, and that the employee may consult with the employer about the surveillance conduct to consult with the employer.

form or not.48 This revised definition is easier to recognize a connection between individual and relevant information or opinion to other information. 49 Also, this definition is more closely aligned with the corresponding EU definition of "personal data" and the Asia-Pacific Economic Cooperation Privacy Framework, which makes it easy to attain consistent interpretation in the EU and international organizations.50

Besides, this Act provides thirteen APPs regulating the collection, use, disclosure and other handling of personal information for large private sector organizations and Australian Commonwealth public sector agencies.51 Thus, these entities should collect, process, access and disclose personal information under this guide, and ensure the integrity, quality, and security of personal information.

Furthermore, *Private Act 1988* also protects personal information collected by the non-Australian business.[52] This is because this Act "has a wide extra-territorial scope and is not confined to acts done within Australia or acts done by Australian entities."[53] For instance, if an organization collects personal information of its employees from Australia, whether this organization is set in the domestic area or not, this personal information is under the protection of the *Private Act 1988.*

However, the Australian Law Reform Commission (hereinafter referred "ALRC") indicates that the most significant limitation of the *Private Act 1988* is the exemption of individuals, small businesses, media organizations, and employee records.[54] In the electronic workplace, the most relevant area is the exemption of small businesses and employee records.

Under the Act, small businesses with an annual turnover of less than $3 million are exempt from being regulated under the *Privacy Act 1988*[55] unless these small businesses that trade personal information or process health information write a letter to the Office of the Australian Information Commissioner (hereinafter referred "OAIC") applying for being treated as an organization.[56] This exemption aims at reducing the cost of compliance with the *Privacy Act 1988* and promoting enterprise development to some degree. However, this exemption means that 85% of the Australian private

[48] *Privacy Act 1988* (Cth), s 6 (Austl.).

[49] Anna Von Dietze & Anne Marie Allgrove, Australian privacy reforms—an overhauled data protection regime for Australia, 4 International Data Privacy Law 326, 328 (2014) (hereinafter "Anna Von").

[50] Id.

[51] *Privacy Act 1988* (Cth), s 1 (Austl.).

[52] *Id*, s 5B.

[53] Anna Von, *supra* note 49, at 328.

[54] Australian Law Reform Commission (ALRC), *Serious Invasions of Privacy in the Digital Era Final Report*, Report No 123 (2014) 310 (hereinafter "*Serious Invasions of Privacy Report*") (Austl.).

[55] *Privacy Act 1988* (Cth), s 6C, s 6D (Austl.).

[56] *Id*, s 6D, s 6E, s 6EA (Austl.).

sector can process their employees' personal information without being regulated by the *Privacy Act 1988*[57], which is a potential risk for most employees in Australia.

Another exemption is the records of employees' behavior relevant to their organization or employment relationship. The definition of an employee record is "a record of personal information relating to the individual employee, such as health information, information about performance/conduct, working hours or salary and superannuation." [58] Besides, the exemption applies to the following situations: the employees' behavior is directly related to the employment relationship, or is related to a current or former employment relationship; the behavior is related directly to an individual employee record held by the organization.

The reason why the Act holds this exemption is to coordinate with the workplace relations legislation, which offers protection to these records of employees. However, Anna von Dietze and Anne-Marie Allgrove think that workplace relations legislation does not adequately protect employee records.[59] This is because there are also some State legislations regulating health information, which makes the application of the *Privacy Amendment (Private Sector) Act 2000* (hereinafter called "*Privacy Amendment Act 2000*") complicated. For example, there are some regulations and different rules regarding the collection of personal information by organizations under the *Health Records Act 2001* (Vic) and the *Health Records and Information Privacy Act 2002* (NSW). Thus, if the private sector wants to collect personal information in different areas, it has to follow different rules.

Therefore, these two exemptions are the significant limitations of the *Privacy Act 1988*, which leave a gap for privacy protection in small businesses and employees' records. This is because the proportion of small businesses is large in the Australian industry, and the employees' records are related to personal information, which could disclose employees' acts and practices in the workplace. Thus, as recommended by the Final Report 2005, it is necessary to remove the exemption of small businesses and employee records.[60]

Moreover, ALRC indicates that the contents of the *Privacy Act 1988* cannot adapt to privacy protection in the digital era.[61] Similarly, it also

[57] David Watts & Pompeu Casanovas, 'Privacy and Data Protection in Australia: a Critical overview' (Workshop Paper, W3C Workshop on Privacy and Linked Data, World Wide Web Consortium, 2019) 2 (hereinafter "David Watts").

[58] *Privacy Act 1988* (Cth), s 7B (3) (Austl.).

[59] Anna Von, *supra* note 49, at 328.

[60] Victorian Law Reform Commission (VLRC), *Workplace Privacy Final Report*, Report No 159 (2005) 6 (*hereinafter "*Final Report 2005*"*) (Austl.). Report 2022 also discussed whether it is necessary to remove the employee records exemption.

[61] Serious Invasions of Privacy Report, *supra* note 54, at 36.

cannot give sufficient protection in the electronic workplace. Because with the widespread use of cloud storage technology, human resources personnel prefer to upload and store employees' information on the website, which could store more information and save cost for companies.[62] However, as the information is uploaded to the cloud, which is out of control of employees, it is easy for a hacker or other third parties to obtain this information, which places the employees' personal information in danger.[63] Also, when they are suspended from office, it is necessary for human resources personnel to delete employees' information from the cloud, which is beneficial to protect employees' privacy.[64] However, unlike GDPR, there is no "right to be forgotten", "data portability" rights, or the right to object to the processing of personal information under the *Privacy Act 1988*.[65] Therefore, if personal information is stolen or disclosed by other third parties, there is no effective legislative protection for employees' privacy.

The *Privacy Act 1988* revised the definition of personal information corresponding to the international and EU standard. Also, this Act regulates the collection and disposal of information in the public sector, large businesses, and non-Australian businesses, which protects personal information in the workplace to some degree. However, as this Act is standard legislative protection of privacy in every area, it does not adapt to the development of technology to include specific protection in the electronic workplace. Moreover, its exemption of small businesses and employees' records leaves a gap in protecting privacy in the workplace. Thus, this Act is too general to protect personal information in the electronic workplace.

b. Surveillance device laws and workplace surveillance laws have had some effect but are not enough

Monitoring and surveilling employees in the workplace have been common for centuries.[66] With the advancement of information communication technology, the cost of surveillance devices decreases, and there are more electronic surveillance devices used in the workplace.[67]

In Australia, there are some surveillance device laws and workplace surveillance laws regulating electronic surveillance to some degree. The most significant surveillance device laws are the *Workplace Surveillance Act*

[62] Danyang Guo, The protection of trade secret under the cloud computing environment 8 (2018) (LLM dissertation, Heilongjiang University, 2018).

[63] *Id*, at 21.

[64] *Id*, at 28.

[65] David Watts, *supra* note 57, at 3.

[66] Peter Jeffrey Holland, Brian Cooper & Rob Hecker, Electronic monitoring and surveillance in the workplace: The effects on trust in management, and the moderating role of occupational type, 44 Personnel Review 161, 161 (2015).

[67] *Id*.

2005, the *Surveillance Devices Act 1999* (Vic) (hereinafter "*Surveillance Devices Act 1999*") and the *WP Act 2011*.

According to the *Workplace Surveillance Act 2005*, employers should give notification to their employees about using CCTV cameras at least 14 days earlier,[68] and cameras should be affixed signs to give a hint to others clearly.[69] It also provides the requirements for computer surveillance in the workplace as well as the requirements for tracking surveillance out of the workplace. Besides, *Surveillance Devices Act 1999* prohibits video recording in a private place such as a change room or lactation room,[70] and it also prohibits communicating or publishing the activities or conversations which are observed by the surveillance devices in the workplace.[71] Moreover, the *WP Act 2011* regulates the use of tracking devices and data surveillance devices, except listening devices.[72] This Act requires employers to give notification of using surveillance devices in the workplace to the employees. It also provides employers with "covert surveillance authorities" to observe whether an employee is carrying out an unlawful activity in the workplace.[73] The *WP Act 2011* also prohibits using surveillance in a private place, such as changing room, nursing room, and toilet.[74]

However, one of the limitations of these surveillance laws is that different states and territories have their own legislation to regulate surveillance devices, which leads to the inconsistency of the law application[75] and fails to protect working privacy in a fair way. For instance, the surveillance device laws of the ACT and Tasmania do not give protection to optical surveillance devices.[76] Also, ACT, Tasmania and WA do not regulate the data surveillance devices, and Victorian as well as NT regulate these devices only if law enforcement officers use, install or maintain them.[77] Furthermore, ACT and Tasmania do not regulate tracking devices under the surveillance device laws.[78] Some states and territories, such as Queensland, even do not have a complete surveillance law to regulate surveillance devices and protect personal information. Instead, it prohibits the use of listening devices in private places under the *Invasion of Privacy Act 1971* (Qld).[79] This

[68] Workplace Surveillance Act 2005(NSW), s 10 (Austl.).
[69] *Id*, s 11.
[70] Surveillance Devices Act 1999 (Vic), s 9B (Austl.).
[71] *Id*, s 9C.
[72] *Workplace Privacy Act 2011* (ACT) s 11(1) (Austl.).
[73] *Id*, s 25 (Austl.).
[74] *Id*, s12 (Austl.).
[75] Serious Invasions of Privacy Report, *supra* note 54, at 278.
[76] *Id*.
[77] Id.
[78] Id.
[79] Invasion of Privacy Act 1971 (Qld), s 43 (Austl.).

inconsistent application scope of legislation makes it difficult to protect privacy against the use of surveillance devices.

Another limitation is that current surveillance laws in different states and territories cannot protect privacy adequately. Some scholars argued that although Final Report 2005 gave some suggestions about privacy protection in the workplace, the Victorian State Government only adopted the prohibition of using camera devices in the private areas of the workplace.[80] Other surveillance methods related to personal information such as employee records, email-monitoring, and genetic testing were excluded from the protection under the *Surveillance Devices Act 1999*[81] the *WP Act 2011* and the *Workplace Surveillance Act 2005*. It is evident that privacy protection under current surveillance laws is too narrow to protect personal information in the electronic workplace.

Furthermore, there are no regulations about Internet monitoring and e-mail monitoring in the workplace under the surveillance laws; however, these monitoring methods are most common in the electronic workplace. It is usual for organizations to monitor employees by searching their computer files, voice mail, and e-mail, and the report shows that there is 11.1% of excessive monitoring[82] of employees' work weekly/daily in the workplace.[83] Thus, it is evident that the laws or policies should regulate this electronic monitoring.

c. It is still not adequate to protect privacy under company policy in the electronic workplace

The widespread use of social media has made the relationship between employees and employers tense. This is because most employers believe that excessive use of social media by employees takes up time for them to focus on work, which affects their work efficiency. Employers often claim that "such use constitutes theft, misconduct, or an abuse of resources because that time spent on personal social media is time not spent on paid work-related activities."[84]

[80] Amanda Pyman, Anne O'Rourke & Julian Teictier, *Information Privacy and Employee Records in Australia: Which Way Forward?*, 34 Australian Bulletin of Labour 28, 42 (2008).

[81] Final Report 2005, *supra* note 60.

[82] *Fair Work Act 2009* (Cth) , s 789FD: defines bullying at work as repeated unreasonable behavior towards a worker (or group of workers) which creates a risk to health and safety. One spectrum of workplace bullying is excessive surveillance or micromanagement, which is a repeated unreabsale behaviour by employers occurring inside or outside of working hours to employees (Austl.).

[83] Dr Christopher Magee, Dr Ross Gordon, A/Prof Peter Caputi, A/Prof Lindsay Oades, Dr Samantha Reis, Laura Robinson, '*Workplace Bullying in Australia*' (Report No 6937, Centre for Health Initiatives, University of Wollongong, May 2014) 98.

[84] Paula McDonald, *supra* note 25, at 77.

According to Swaybase's research, 8 in 10 workers say they use social media during working hours.[85] More than 82% of employers said it was appropriate for employees to browse non-work related websites, with 58% saying it was permissible for employees to browse for 15 to 30 minutes a day.[86] As a result, some companies have adopted corporate policies to limit and monitor the use of social media by employees during their work hours to reduce their use of social media. There is also a new social media policy to regulate the use of social media by staff working for the Australian Public Service, whether in an official or unofficial capacity.[87] If an employee breaches this policy, it encourages colleagues to report this behaviour.[88] However, the UK survey also showed that more than half of the respondents thought they were at least as productive as they would have been if they had not used social media.[89] The main reason is that the wide use of email, phone or text messages enables them to finish tasks efficiently. Therefore, excessive restrictions on the use of social media will not necessarily improve employee productivity.

Besides, it is unfair for some companies to monitor and restrict employees' use of company equipment in practice. For example, there are many company policies prohibiting personal emails or phone calls in workplace, and employers have the right to monitor the contents of employees' emails and phone calls. This is because the content is part of a system that the employer owns, thus making it employer property.[90] Therefore, "there is no reasonable expectation of privacy for employees, which is unfair for them."[91] Also, employees often exchange privacy control for a job.[92] As an electronics store employee said in a survey, "We are working under company policy, and once you are under company rules and regulations, you lose all your rights."[93]

[85] Swaybase, *Social Media in the Workplace: Everything You Need to Know*, https://www.swaybase.com/blog/social-media-in-the-workplace (last visited Mar 15 2023).

[86] Charles J. Muhl, Workplace e-mail and Internet use: employees and employers beware, 126 Monthly Labor Review 36, 37 (2003).

[87] My Job Group, *Social media in the workplace* (2010), http://www.myjobgroup.co.uk/socialmediawhitepaper (last visited Jan 3 2019) (hereinafter "My Job Group")

[88] Samantha Maiden, *Colleagues told: Dob in political web posts*, The Daily Telegraph (April 6, 2014 - 12:00AM) https://www.dailytelegraph.com.au/news/nsw/colleagues-told-dob-in-political-web-posts/news-story/703e3b48237cf540819b127bfd116e56 (last visited Mar 15 2023).

[89] My Job Group, *supra* note 87.

[90] Kevin J. Smith & Rachel J, *Tischler, Electronic Monitoring in the Workplace*, 10 Employment Relations Today 73, 75 (2015) (hereinafter "Kevin J. Smith").

[91] Stengart v. Loving Care Agency, Inc., 201 N.J. 300, 323–24 2010.

[92] Sandra Petronio, Boundaries of privacy: Dialectics of disclosure 173 (State University of New York Press, 2002).

[93] My Job Group, *supra* note 87.

IV. A SUGGESTED FRAMEWORK TO IMPROVE PRIVACY PROTECTION IN THE AUSTRALIAN ELECTRONIC WORKPLACE

A. Filling the Gap of the Privacy Act 1988

In the first stage, it is necessary to address the limitations of current legislation, including the *Privacy Act 1988* and existing surveillance device laws.

Although the *Privacy Act 1988* has revised the definition of personal information, which corresponds with the international and EU standard, the scope of the definition is still too narrow to protect privacy in the current workplace adequately. As mentioned in chapter II, the scope of privacy is broadened due to the wide use of electronic devices in the workplace, which makes the boundary between private and public unclear. Thus, it is not sufficient to protect privacy under this Act. Therefore, ASTRA, ABC, and Telstra point out that it is necessary to make the application scope of this Act more precise, clear and specific.[94] It means that the classification of privacy invasion should be more precise to some degree, which could make this Act clearer to apply.

However, it is difficult to enumerate specific circumstances for each kind of privacy invasion in the law. Thus, ALRC suggests that courts could weigh competing interests and apply broader principles, considering all the circumstances of a particular case when deciding whether privacy invasion is involved.[95] Some circumstances could be included: the interference of an individual's living area or family life; unauthorized surveillance subjected to an individual; and the sensitive disclosure issues of an individual.[96] This is because judges are familiar with the decision about what circumstances are related to the privacy issue in a particular case, which makes it easier for them to come up with principles about how to apply the *Private Act 1988* in different cases.

Besides, ALRC suggests that the *Privacy Act 1988* should remove the exemptions of small business and employees records. To decrease the cost of small businesses and improve their competitiveness compared with large businesses, this Act exempts Australian small businesses from protecting employees' personal information. However, since the proportion of small

[94] Subscription Television Australia, Submission No 47 to the Australian Law Reform Commission, *Inquiry into Serious Invasions of Privacy in the Digital Era Issues Paper*, 20 November 2013, 14 (Austl.); Australian Broadcasting Corporation, Submission No 46 to the Australian Law Reform Commission, *Issues Paper on Serious Invasions of Privacy in the Digital Era*, November 2013, 4 (Austl.); Telstra, Submission No 45 to the Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era- Telstra's response to Issues paper 43*, November 2013, 1 (Austl.).

[95] Serious Invasions of Report, squar note 59, at 36.

[96] Australian Law Reform Commission, *Review of Australian Privacy Law: An Overview Review of Australian Privacy Law -- An Overview of Discussion Paper*, Report No 72 (2007) (hereinafter "Review of Australian Privacy Law 2007") (Austl.).

businesses in Australia is 85%,[97] this exemption means that most Australian companies do not have to apply the *Privacy Act 1988* to protect their employees' personal information, which places the employees' personal information under dangerous status. ALRC suggests that removing this exemption of small businesses will provide safer workplace for workers, which will boost their working enthusiasm and may also increase the competitiveness of small businesses to some degree. Also, employees records, especially those related to health, are the dignity of an individual. Removing this exemption from the *Privacy Act 1988* is vital. Moreover, the exemption of employees records also simplifies the application of other Health Information Act in different states.

Furthermore, it is also necessary for the *Privacy Act 1988* to be adaptable to technological change, which makes this Act more applicable in the electronic workplace. A privacy act with specific and certain definitions also should be sufficiently flexible to adapt to rapidly changing technologies and capabilities.[98] Thus, Google suggested that "there should be a flexible, forward-looking and adaptive data policy to ensure that society may benefit from the many beneficial uses of data analytics."[99] Therefore, it is necessary to broaden the applicable subjects to include all organizations, which could prevent disclosing personal information in the electronic environment after employment termination.

B. Unifying Surveillance Device Law

Because the pace of technological development varies from state to state, the legislative process also varies. Therefore, different states and territories have their own legislation about surveillance devices in the workplace. As analyzed in chapter III, the regulations of surveillance devices among the Federal, State and territory laws are inconsistent, and the Media and Communications Committee of the Law Council of Australia believes that the legislation in this area is like an inconsistent patchwork, which needs unified principles to operate.[100] Also, the Australian Privacy Foundation thinks that "uniformity should not be achieved at the expense of watering down Australians' rights to be free from unauthorized surveillance and any

[97] David Watts, *supra* note 57, at 2.

[98] Serious Invasions of Report, *supra* note 54, at 36.

[99] Google, Submission No 54 to the Australian Law Reform Commission, ALRC Issues Paper 43, 25 November 2013, 4 (Austl.).

[100] Media and Communications Committee of the Law Council of Australia, Submission No 124 to the Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era (DP 80)*, 14 May 2014, 4 (Austl.).

standardization should be based on 'best practice' protection of privacy and not on 'lowest common denominator' protection."[101]

Besides, in practice, a uniform surveillance law is beneficial to businesses, especially where a business operates in multiple states or territories. As the submission of the Australian Bankers' Association refers to, it is more efficient for banks and other businesses to conduct their businesses under a nationally uniform or consistent legal framework, which is convincing for their customers to comply with.[102] Also, "national consistency contributes to national productivity and better outcomes for consumers",[103] which could promote the economic development of businesses.

Therefore, ALRC suggests that Commonwealth legislation should introduce a uniform surveillance device law which regulates the use of surveillance devices in Australia.[104] This uniform surveillance device law will take place of existing surveillance device laws in different states and territories.

Some stakeholders like the Australian Privacy Foundation point out that it may take a long time to enact a uniform surveillance device law, which has to weigh the interests of each state, territory, and arrive at an agreement with them.[105] However, since privacy is a primary human right, its protection should be a long-term aim, and it should be under full protection in the electronic era. Also, setting a uniform surveillance device law is essential for an individual to apply the legislation in a certain way that works anywhere in Australia.[106] Therefore, it is necessary to adopt a uniform surveillance device law in Australia.

According to the suggestion of ACRL, it is vital for surveillance legislation to be technology-neutral, which enables the legislation to be applied to any existing or emerging technology that could be used for surveillance.[107] Technology-neutral provisions "refer to technology in general, vague, open-textured terms that specify purposes, effects, functions, and other general characteristics."[108] Although ACRL does not prefer to

[101] Australian Privacy Foundation, Submission No 110 to the Australian Law Reform Commission, *Re: Discussion Paper 80: Serious Invasions of Privacy*, 12 May 2014, 12 (Austl.).

[102] Australian Bankers' Association Inc, Submission No 84 to the Australian Law Reform Commission, The *proposal of Serious Invasions of Privacy in the Digital Era*, 13 Nov 2013, 5 (Austl.).

[103] *Id*.

[104] Serious Invasions of Report, *supra* note 54, at 281.

[105] Australian Privacy Foundation, Submission No 110 to the Australian Law Reform Commission, *Re: Discussion Paper 80: Serious Invasions of Privacy*, 12 May 2014, 15 (Austl.).

[106] Australian Institute of Professional Photography (AIPP), Submission No 95 to the Australian Law Reform Commission, *Submission to the Discussion Paper on Serious Invasions of Privacy in the Digital Era Discussion Paper*, 80 March 2014, 2 (Austl.).

[107] Serious Invasions of Report, *supra* note 54, at 282.

[108] Ohm, Paul, The argument against technology-neutral surveillance laws, 88 Tex. L. Rev 1685, 1687 (2009) (88)

provide a specific definition of technology-neutral, it may narrow its definition and make it less easy to apply in the developing era. Thus, the definition should include existing surveillance devices such as optical surveillance devices, listening devices, data surveillance devices, and tracking devices, as well as a networked system, software, and unmanned aerial vehicle, which do not belong to conventional devices.[109]

However, the UNSW Cyberspace Law & Policy Centre and Policy Community thinks that it is essential to make distinctions between different technologies, as it may be difficult for some technologies such as drones with cameras and data surveillance by software to be used in a neutral way,[110] which may monitor others secretly.

Overall, the benefits of defining technology-neutral outweigh the risks,[111] and it should include existing legislative surveillance devices. Although email and Internet surveillance cannot be treated as technology-neutral, they are widely used in the electronic workplace, which should be regulated by industry codes or policies.

In conclusion, the first stage of reform is to broaden the *Privacy Act 1988* to include small businesses and employees records, and also make this Act specific enough to ascertain what is under its protection, and flexible enough to be used in the electronic era. Meanwhile, the surveillance device law in Australia should be unified, and the definition of technology-neutral should be included.

C. Making Improvements to Company Policy

In the second stage, it is necessary to make some improvements to company policy.

It is impossible for employees to not use the company's system to handle private affairs in practice.[112] Therefore, in the absence of explicit legislation, it is necessary for companies to set policies about monitoring employees' use of the company's devices including email, computers, and networks, which should balance the interests of employees and employers.

Conlon argues that by communicating an electronic monitoring policy, the employer can establish the level of privacy that employees may reasonably expect.[113] In the USA, the employer-friendly decision of the National Labor Relations Board (hereinafter referred "NLRB") recognized that "email is different from the other forms of workplace

[109] Serious Invasions of Report, *supra* note 54, at 283.

[110] UNSW Cyberspace Law and Policy Community, Submission No 98 to the Australian Law Reform Commission, 2010, Proposal 13-1 (Austl.).

[111] Serious Invasions of Report, *supra* note 54, at 284.

[112] George B. Trubow, Constitution v. Cyberspace: Has the First Amendment Met Its Match?, 5 Business Law Today 40, 41-42 (1996).

[113] Kevin J. Conlon, *Privacy in the Workplace*, 72 Chicago-Kent Law Review 285, 290 (1997).

communication."[114] In Purple Communications, Inc., the policy prescribes the reasonably expected use of the company's equipment when special circumstances made the prohibition necessary to maintain the production or discipline. [115] Therefore, according to this policy, employees can use company equipment to communicate with relatives and friends about emergencies or essential issues, which are not monitored by surveillance.

Also, the limitation of the penalty for breaching the policy should be determined. Although the policy provides a reasonable expectation of privacy for employees, it is also necessary to establish a clear standard of what situations are considered as breaching the policy and thus deserving the penalty. Some scholars think that for a company, there is no need to limit the employee's personal use of the company's devices, or to monitor these uses in real time, and punish the behavior which breaks the rules, because doing so may cause the company to lose a valuable employee.[116] Therefore, if Australian companies can develop and apply the policy introduced above, which distinguishes the business information from personal information employees post on social media, they could provide better protection of privacy in the electronic workplace. This policy could motivate employees to work harder in the workplace instead of keeping employees away.

V. PROPOSALS FOR PROECTING EMPLOYEES' PRIVACY IN THE ELECTRONIC WORKPLACE IN CHINA

Most articles about the comparative perspective of privacy protection in the workplace are learned from the UK, US, and EU.**[117]** However, Australia and China, which have been learning from the GDPR on the protection of personal information, there are few comparisons between these two countries.

Although Australia's privacy protection at work is not yet comprehensive, its legislation has been improving. Since the enactment of the *Privacy Act*

[114] Bruce R. Alper, Managing the Electronic Workplace, 25 The Computer & Internet Lawyer 1, 5 (2008).

[115] Purple Communications, Inc. v Communications Workers of America, 361 N.L.R.B. 1050, 1052, 1092 (2014).

[116] Michael A. Verespej, *Inappropriate Internet Surfing*, Industry Week (Dec. 21, 2004) https://www.industryweek.com/talent/article/21958841/inappropriate-internet-surfing (last visited Mar 15 2023).

[117] Yu Shuhong (喻术红), Tang Xiaoying (汤晓莹), Laodongzhe Yinsibaohuwenti Yanjiuxianzhuang jiqi Pingshu (劳动者隐私保护问题研究现状及其评述)[The current study on the protection of workers' privacy and its review] 18(05) Shidai Faxue (时代法学)[Presentday Law Science] (2020); Ban Xiaohui (班小辉)Yuanchenggongzuo Xingtaixia Zhiyeanquan Baohuzhidu de Kunjing yu Yinying (远程工作形态下职业安全保护制度的困境与因应) [Challenges and responses to working safety protection systems in remote working] 5 Gansuzhengfa XueyuanXuebao (甘肃政法学院学报) [Journal of Gansu Political Science and Law Institute] (2019) (hereinafter "Ban Xiaohui"); Tian Silu (田思路), Yuanchenglaodong de Zhidu Fazhan ji Falvshiyong (远程劳动的制度发展及法律适用) [Institutional development and application of the law in relation to remote labour] 5 Faxue (法学) [Law Science] (2020).

1988 (Cth) (hereinafter "*Privacy Act 1988*"), Australia's privacy legislation has been amended and improved over the years. In 2014, the Australian Privacy Principles were introduced to regulate the collection and processing of personal information by public sector agencies and businesses. [118] In 2018, the Notifiable Data Breaches (hereinafter "NDB") scheme was introduced, setting out specific requirements for organizations or agencies in responding to serious harm to personal information.[119] In October 2021, the Attorney-General's Department (hereinafter "AGD") released a consultation Exposure Draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (hereinafter "the Online Privacy Bill Exposure Draft") [120], which introduces an "Online Privacy Code" (hereinafter "OP code") that extends the extraterritorial reach of the Privacy Act and introduces a more specific set of rules for social media and digital agency service platforms. The OP code supplemented the current provisions under the *Privacy Act 1988*. It introduced a more specific set of rules for all large online platforms, social media services and data brokerage services providers. The Australian Council of Trade Unions Executive (hereinafter "ACTU") announced on 12 October 2022 the adoption of a resolution to address significant gaps in the regulation and safeguards for employers regarding the use and protection of employee data.[121] In November 2022, the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (hereinafter "Bill')[122] was introduced and passed. Moreover, New South Wales and the Australian Capital Territory have introduced surveillance acts that protect employees' privacy in the electronic workplace. Also, Australia's state-specific Acts on electronic surveillance and industry standards have effectively protected employee privacy, which are valuable lessons for China. Therefore, this article aims to put forward some suggestions for protecting privacy at work in China based on the above proposal for Australia.

[118] *Privacy Act 1988* (Cth), s 14 (Austl.).

[119] Notifiable data breaches: Under the Notifiable Data Breaches (hereinafter "NDB") scheme, any organisation or agency the Privacy Act 1988 covers must notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.

[120] Exposure Draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Cth) (Austl.).

[121] The resolution outlines key principles for the use of working people's data by their employers: Employers should be required to protect the data of their employees; Workers should have a right to access data collected about them, including the right to rectify, block or erase; Workers and their unions must be consulted and agreement reached before the introduction of new systems which enable surveillance or monitoring of workers; Data collected should be minimised to only what is absolutely necessary; Policies and processes for data collection should be transparent and available to workers and their unions; Biometric and GPS or location data should only be collected where there is no other viable option; These rights should be implemented and enforceable via collective bargaining (hereinafter "ACTU") (Austl.).

[122] Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Cth) (Austl.).

A. Current Issues of Privacy Protection in Electronic Workplaces in China

Chinese scholars define the electronic workplace as "telecommuting," a collaborative work outside the traditional office location with the help of communication devices or tools such as telephone, Internet, and email. [123] Telecommuting is a way of working in the electronic workplace, which is used interchangeably with the electronic workplace in this article below. In recent years, telecommuting has gradually grown in China. Especially, due to the pandemic, telecommuting was even more widely used. According to the data from the Statistical Report on the Development of China's Internet, the scale of online office users in China has reached 381 million since the 2020 epidemic.[124] Instant communication began to develop in the direction of enterprise digital infrastructure and has penetrated all aspects of business operations. This shows that with the support of policies and technologies, telecommuting has a broad development prospect in China. However, in the electronic workplace, China also faces the problem of employee privacy violations.

Firstly, using social media in the workplace has weakened employees' personal and workspace. As WeChat develops features to support work-related functions such as search, file export, group calls and video, more and more people are using WeChat as a work communication tool. Of the over 20,000 web users surveyed, 90% identified WeChat as their first choice for daily work communication. [125] 70% of respondents use WeChat rather than email to check emails or review client or work information.[126] However, as a social networking software, WeChat has features such as Moments, Discover, and Top Stories, making it easier for employers to access, access and utilize information on their employees' social media networks, which becomes key for employers to monitor their employees and use as evidence for performance assessment. Although Tencent developed WeCom in 2016 to separate personal social software from work communication software, 180

[123] Zhang Yinghui (张颖慧), Yuanchenggongzuo Xingtaixia Xingxing Laodongguan de Falvbaohu (远程工作形态下新型劳动关系的法律保护) [Legal Protection of New Labor Relationships in the Form of Telework] 6 Fashang Yanjiu (法商研究) [Studies in Law and Business] 80, 79 (2017) .

124 48th Statistical Report, supra note 29.

[125] Meng jing, *WeChat is top workplace communications app for 90 per cent of Chinese professionals*, South China Morning post, (25 Apr. 2017) https://www.scmp.com/tech/apps-gaming/article/2090472/wechat-top-workplace-communications-app-90-cent-chinese (last visited 20 Mar. 2023).

[126] Wechat Marketing, *WeChat Marketing: Top Strategies Revealed*, GMA (December 26, 2017) https://marketingtochina.com/wechat-marketing-strategy/#:~:text=In%20fact%2C%2070%25%20of%20the,Wechat%20when%20they%20have%20time (last visited 20 Mar 2023).

million users reached only 10% of WeChat's monthly active users. [127] Thus, they did not completely remove WeChat from the workplace. As a result, WeChat's dual attributes as a social media and work communication software make it more difficult for Chinese employees to distinguish between personal privacy and work information in the electronic workplace.

Secondly, existing laws and regulations in China do not provide specific protection for employees' privacy in the electronic workplace. Currently, the laws that relate to employee privacy are the Law on the Protection of Personal Information[128], the Labour Law[129], the Labour Contract Law[130] and the Regulation on the Implementation of the Employment Contract Law[131]. In the electronic workplace, the employer can collect employees' personal information through office equipment and local area network (LAN) to analyse, correlate, predict, judge and provide feedback on employee information via the algorithm. The results of such automated decisions are used as factors in employees' hiring and performance assessment, which may violate their personal information. However, the Personal Information Protection Law only regulates automated decision-making in consumer relationships to prevent problems such as big data discrimination[132], but does not apply to the excessive analysis of employee data in the electronic workplace. In addition, the Labour Contract Law requires that employment contracts contain personal information such as employee's name, domicile, identity card number,[133] which is in line with the requirement of "necessary for the conclusion or performance of a contract" under the Personal Information Protection Law. [134] Under the Labour Law, employers are required to conduct regular health examinations of employees who work

[127] Qiyeweixin Huoyueyonghu Da 1.8 Yi! Weixinkefu Zhengshijieru (企业微信活跃用户达 1.8 亿！微信客服正式接入) [WeCom reaches 180 million active users! WeChat customer service officially accessed] (Jan 11, 2022), https://www.sohu.com/a/515885390_120106203.

[128] Ge Ren Xin Xi Bao Hu Fa （个人信息保护法）[Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong Aug. 20, 2021, effective Nov 1, 2021) art.13(2) (Chinalawinfo).

[129] Lao Dong Fa (劳动法) [Labor Law] (promulgated by the Standing Comm. Nat'l People's Cong Dec. 29, 2018, effective Dec. 29, 2018) art. 54 (Chinalawinfo).

[130] Lao Dong Hetong Fa (劳动合同法) [Labor Contract Law] (promulgated by the Standing Comm. Nat'l People's Cong Dec 28, 2012, effective July 1, 2013) art. 7, art. 8, art. 17(2), art.17 (4), art.17(8), art.17(9) (Chinalawinfo).

[131] Lao Dong He Tong Fa Shi Shi Tiao Li (劳动合同法实施条例) [Regulation on the Implementation of the Employment Contract Law] (promulgated by the Adminstrative Regulations Sep. 18, 2008, effective Sep. 18, 2008) art. 8 (Chinalawinfo).

[132] Ge Ren Xin Xi Bao Hu Fa (个人信息保护法) [Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong Aug. 20, 2021, effective Nov 1, 2021) art.24(2) (Chinalawinfo).

[133] Lao Dong Hetong Fa (劳动合同法) [Labor Contract Law] (promulgated by the Standing Comm. Nat'l People's Cong Dec 28, 2012, effective July 1, 2013) art.17(2) (Chinalawinfo).

[134] Ge Ren Xin Xi Bao Hu Fa (个人信息保护法) [Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong Aug. 20, 2021, effective Nov 1, 2021) art.13(2) (Chinalawinfo).

with occupational hazards,[135] and the collection of personal information for this purpose is necessary for the fulfilment of the employer's legal obligations.[136] However, the law does not specify how the informed-consent rule applies to information that is neither necessary for the conclusion of a labour contract nor for the performance of a legal obligation.

Furthermore, the current labour protection system in China is composed of many sub-categories and multi-level structures of labour safety and health standards.[137] At the second level, the Labour Law stipulates that employees should observe labour discipline[138] and that serious violations may lead to the termination of the employment contract.[139] In the electronic workplace, employees are required to use smartphones, tablets and even wearable devices to perform their work. Is the use of devices that have the ability to track, collect and analyse data considered a labour discipline to be observed by employees? Is it a breach of labour discipline if an employee refuses to use such devices? This is not explained in the Labour Law. The Labour Contract Law stipulates that labour contracts should include the workplace. However, there are no specific instructions on how to define the workplace and thus distinguish the workplace from the living area in labour contracts, such as telecommuting during pandemic times or special labour contracts. Moreover, at the fifth level, the Guide of Telecommuting Security Protection lists application scenarios and also analyses the risks that may face in telecommuting, such as office system security, data security, set up security and personal information protection. However, the Guide of Telecommuting Security Protection only provides a general overview and does not break down specific scenarios, which leaves some space for interpretation and reduces the operability of the Guide of Telecommuting Security Protection. As a result, China does not currently provide sufficient and comprehensive protection for the privacy of remote workers.

[135] Lao Dong Fa (劳动法) [Labor Law] (promulgated by the Standing Comm. Nat'l People's Cong Dec. 29, 2018, effective Dec. 29, 2018) art. 54 (Chinalawinfo).

[136] Ge Ren Xin Xi Bao Hu Fa （个人信息保护法）[Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong Aug. 20, 2021, effective Nov 1, 2021) art.13(2) (Chinalawinfo).

[137] Liang Tiantian (梁甜甜), Liang Yulian(梁玉莲), Laodongfa Xinlun (劳动法新论) [A New Theory of Labour Law] 171 (2016). The first level: the principle provisions on labour protection in the Constitution; the second level: the provisions on labour protection in the Labour Law and the Labour Contract Law; the third level: comprehensive laws on the protection of workers' safety and health, such as the Work Safety Law and the Law on Prevention and Control of Occupational Diseases; the fourth level: special laws or regulations on labour safety technology, labour hygiene technology, management of labour protection, protection of special subjects and supervision of labour protection; and the fifth level: individual departmental regulations or specific labour safety and health standards.

[138] Lao Dong Fa (劳动法) [Labor Law] (promulgated by the Standing Comm. Nat'l People's Cong Dec. 29, 2018, effective Dec. 29, 2018) art. 3(2) (Chinalawinfo).

[139] *Id*, art. 25(2).

It is evident that the current protection of employee privacy in China also faces the problem of a lack of comprehensive laws and clear boundaries between the public and private sectors. Therefore, this article makes the following recommendations for improving employee privacy protection in the Chinese electronic workplace, based on the experience and suggestions presented above for Australia.

B. Proposals for Perfecting Privacy Protection in China's Electronic Workplace

First, the protection of employee data under the Personal Data Protection Law should be strengthened by making organizations and companies the subject of regulation for automated decision-making. Article 51 of the Personal Information Protection Law stipulates that personal information processors need to categorize and manage personal information.[140] Besides, Article 52 stipulates that "[w]here the quantity of personal information processed reaches that specified by the CAC, the personal information processor shall designate a person in charge of personal information protection to be responsible for supervising the activities of processing of personal information and the adopted protection measures."[141] According to these two provisions, the personal information of employees involved in telecommuting can be protected categorically, in which information involving personal privacy should be distinguished from general personal information. Information involving personal privacy should be protected in absolute terms. As the main processor of employee data, the company (or the organization) can establish a management department for processing personal information according to Article 52 of the *Personal Information Protection Law*, making rules, drawing up contracts, and supervising the implementation of rules for the teleworking environment within the company. In addition, companies should be added to the provisions of Article 24(1) of the Personal Data Protection Act as personal data processors. This should be amended as "Where a personal information processor conducts automated decision-making by using personal information, it or he shall ensure the transparency of the decision-making and the fairness and impartiality of the result, and shall not give unreasonable differential treatment to individuals in terms of trading price, other trading conditions, or employment conditions". It is essential to adhere to the informed - consent rule and the principle of "necessity" so that only data that is necessary for collection can be processed by the employer with the consent of the

[140] Ge Ren Xin Xi Bao Hu Fa (个人信息保护法) [Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong Aug. 20, 2021, effective Nov 1, 2021) art. 51 (Chinalawinfo).

[141] *Id*, art. 52.

employee.[142] When the scenario changes, it should get re-authorized by the employee. For example, there are scenarios where a company needs to provide personal information to other information processors, process employees' sensitive personal information (including face recognition), and transfer employees' personal information overseas. When the purpose of processing, the method of processing, the type of personal information to be processed, the subject of processing, or the recipient changes, the employee's consent shall be obtained again before processing.

Second, the workplace and form of work should be specified in the labour contract, and the right to a reasonable expectation of privacy should be respected when setting labour discipline. When entering into a teleworking contract, the employer can enumerate or explain the workplace and the form of work in the contract.[143] On this basis, additional obligations are imposed on the company to reduce the invasion of employees' privacy. On the one hand, it is possible to reduce the scope of surveillance for work from home and monitor only critical situations through spot checks, investigations of specific incidents, or by detecting only high-risk employees, instead of continuous monitoring of all employees.[144] Employees' personal emails can only be checked in exceptional cases, such as those involving harassing letters or trade secret disclosure.[145] On the other hand, for out-of-hours, employers should firmly refrain from monitoring employees. This is because employees have heightened expectations of privacy for non-working hours, which should be protected from the perspective of respecting personal privacy.[146]

Third, it is necessary to clearly distinguish between workplace and residence and clarify the boundary between company information and personal privacy. It may take a process and time to amend legislation and regulations, so it suggests that we can learn from Australia and set industry codes to protect employee privacy first. This article suggests that the Guide of Telecommuting Security Protection can be used for telecommuting operations, which should include a list of situations involving employee privacy violations as a criterion for determining whether an employer has violated privacy. For example, in the case of home working, interference with living areas and family life should be avoided; unauthorised surveillance and data processing by individuals should be prohibited; and the analysis and disclosure of sensitive personal information should be

[142] ACTU, *supra* note 121.

[143] Ban Xiaohui, *supra* note 117, at 154.

[144] Informtiaon Commissioner's Office (ICO), The Employment Practices Code, ICO, Wilmslow 2011, 62.

[145] ICO, The Employment Practices Data Protection Code Supplementary Guidance, ICO, Wilmslow 2005, 50.

[146] ICO, The Employment Practices Code, ICO, Wilmslow 2011, 71.

prohibited. Access control mechanisms can also be established for telecommuting, including regular review of users' permissions and timely removal of expired authorities. This means establishing the departments of the company that enjoy the right to review and setting rules for the retention and deletion of employee data. Concretising this Guide of Telecommuting Security Protection is more conducive to implementation by the company and makes it easier to determine whether the employees' privacy has been violated.

VI. CONCLUSION

In conclusion, current Australian legislation could protect privacy in the electronic workplace to some degree, but it is not completed. As the scope of interpretation of personal privacy in the electronic work environment expands, the *Privacy Act 1988* does not keep up with the era of personal privacy violations by new technologies. Also, there is no consistent surveillance law in Australia, because each state or territory has its own legislation to regulate surveillance, resulting in the inability to apply the surveillance law uniformly in practice and exacerbating the difficulty of protecting personal information. Furthermore, some companies have developed relevant policies to monitor personal information, personal data, and the relevant right and interests of employees, which are not fair enough to meet reasonable privacy expectations from employees. In response to these concerns and the serious data breach in 2022, the AGD has released the Report 2022, seeking public feedback on improving privacy protection in Australia. As a critical area of privacy protection, the protection of employee privacy in the electronic workplace was also discussed in the report.

With this background in mind, this article focuses on responding to Report 2022 and makes three recommendations for improving privacy protection in the Australian electronic workplace:

A. The definition of "personal information" in the Privacy Act 1988 (Cth) should be expanded and revised, which should keep pace with technological development. The court should recognize specific circumstances of privacy invasion in practice. Besides, the exception of employee records and small businesses should be removed from this act.
B. A uniform surveillance law among states and territories in Australia should be established to broaden the definition of the surveillance devices used in the workplace and reflect fair judgment on privacy violations.
C. A fair policy shall be set to meet reasonable privacy expectations from employees, which should clearly indicate what is under surveillance.

Similar to Australia, China lacks comprehensive laws to protect employee privacy and the unclear boundary between public and private in the electronic workplace. Although Australia's privacy protection legislation is imperfect, its efforts and achievements over the years are worthy of reference in China. Therefore, based on the suggestions made for Australia and China's current protection status, this article makes some suggestions for protecting privacy in the electronic workplace in China.

A. From the perspective of the Personal Information Protection Law, it should adhere to the principle of " informed - consent" in the collection and processing of employee information and protect it by classifying it into different categories, making the company the regulated subject of automated decision-making, and establishing a monitoring department to supervise its information processing practices.
B. Employers should be required to respect the right of reasonable expectation of privacy of employees while exercising their rights to disclose personal information under the Employment Contract Law and the Labour Law.

At a stage when legislation has not yet been perfected, the Guide of Telecommuting Security Protection could be used as an action guide for the electronic workplace, enriching the guidelines with scenario-based privacy protections so that they can be used as a practical basis for determining whether a company has violated employee privacy.